UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

PROGRAMA ACADÉMICO DE MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN

Aplicación de Hacking ético para gestionar la prevención de ataques a la red de comunicación de Inversiones Mayito – Agente BCP

TESIS PARA OBTENER EL GRADO ACADÉMICO DE:

Maestro en Ingeniería de Sistemas con Mención en Tecnologías de la Información

AUTOR:

Beltrán Canessa, Pedro Oswaldo (ORCID: 0000-0002-8883-8494)

ASESOR:

Dr. Pacheco Torres, Juan Francisco (ORCID: 0000-0002-8674-3782)

LÍNEA DE INVESTIGACIÓN:

Auditoría de Sistemas y Seguridad de la Información

TRUJILLO – PERÚ

2021

Dedicatoria

Dedico la presente investigación a mi esposa e hijos, quienes en todo momento han sido fuentes inagotables de inspiración.

Pedro Oswaldo Beltrán Canessa

Agradecimiento

Agradezco a Dios por darme la firmeza, fuerza y voluntad para culminar tan noble objetivo, como es el de lograr la elaboración de la presente investigación y a todos mis docentes quienes siempre estuvieron alentándome con sus sabios consejos y muy en especial al **Ing. Juan Francisco Pacheco Torres**, quien fuera mi asesor durante la etapa de pregrado y posgrado.

Pedro Oswaldo Beltrán Canessa

Índice de contenidos

Índice de tablas

Índice de figuras

Resumen

En la presente investigación se utilizó la investigación aplicada y el diseño experimental, se han empleado las técnicas como la observación y encuestas para los trabajadores, asimismo se aplicó los instrumentos como cuestionarios y fichas de información. Se mitigó el nivel de vulnerabilidad de la red de telecomunicaciones de 9.33 a 1.5 ataques, alcanzando una reducción de 7.83 representados en 83.93%. El segundo indicador el nivel de vulnerabilidad de los discos HDD y SSD era de 3.67 de infecciones y mediante la implementación de la aplicación de hacking ético ahora es de 0.5, reduciéndose en 3.17 infecciones, representados en 86.38%. El tercer indicador de vulnerabilidad de los puertos de la CPU principal era de 4 intrusiones y mediante la implementación de hacking ético se bajó a de 0.67 de intrusión, consiguiendo una reducción de 3.33 de intrusión representados en 83.25%. Finalmente, con la escala de Likert de 1 a 5 puntos, para lograr medir el nivel de capacidad y destreza sobre el manejo del hacking ético del personal que interactúa directamente con la red de telecomunicaciones, antes de la implementación era de 9.5 puntos y mediante la implementación ahora es de 23.33 puntos, obteniendo un incremento de 13.83 puntos.

Palabras claves: Hacking Ético, vulnerabilidad, red de comunicación.

Abstract

In this research, applied research and experimental design were used, techniques such as observation and surveys for workers were used, and instruments such as questionnaires and information sheets were also applied. The vulnerability level of the telecommunications network was mitigated from 9.33 to 1.5 attacks, reaching a reduction of 7.83 represented in 83.93%. The second indicator, the level of vulnerability of HDD and SSD disks was 3.67 infections and through the implementation of the ethical hacking application it is now 0.5, reducing by 3.17 infections, represented by 86.38%. The third vulnerability indicator of the main CPU ports was 4 intrusions and through the implementation of ethical hacking it was lowered to 0.67 intrusion, achieving a reduction of 3.33 intrusion represented in 83.25%. Finally, with the Likert scale of 1 to 5 points, in order to measure the level of capacity and dexterity on the management of ethical hacking of the personnel who interact directly with the telecommunications network, before the implementation it was 9.5 points and through the implementation is now 23.33 points, obtaining an increase of 13.83 points.

Keywords: Ethical Hacking, vulnerability, communication network.

I. INTRODUCCIÓN

La difusión y desarrollo de las aplicaciones de las Tics en los diversos ámbitos productivos y educativos, tanto privados como públicos, convierten a éstas en una plataforma habitual para realizar nuestras actividades. Durante muchas generaciones ha venido evolucionando el empleo de las TIC como un soporte en la existencia de los seres humanos y es por ello que se mantienen cada vez más vigentes.

Por ende, estas deben ser protegidas con el objetivo de no ser utilizadas de manera incorrecta y aplicando metodologías de seguridad. Se entiende por seguridad informática, a las técnicas encargadas de resguardar la privacidad e intangibilidad de la información existente en un medio informático. Aun así, no se conoce práctica alguna que permita garantizar totalmente la protección de un sistema digitalizado. Pero, así como hemos sido testigos del abrumador desarrollo de estas tecnologías de seguridad informática diseñadas e implementadas por profesionales dedicados al hacking ético, también lo hemos sido de aquellas prácticas que se han enfocado de manera específica, en penetrar o vulnerar las diferentes vallas de seguridad proveídas.

Se tratan en su mayoría, de personas no necesariamente profesionales, pero con muchos conocimientos de informática y redes de comunicación, que se dedican a hallar los agujeros de penetración o vulnerabilidades en las redes, a efectos de llevar a cabo acciones delictivas, las mismas que pueden devenir en los peores casos, en pérdidas millonarias tanto para las personas naturales como jurídicas. En este sentido, debemos resaltar que últimamente ha aumentado de una manera considerable y muy preocupante, el índice de los delitos informáticos, obligando a las empresas e instituciones a contar con personal especializado en hacking ético para mantener una supervisión constante y actualizada de los sistemas de seguridad de información digital.

Revisando los grandes ataques cibernéticos a nivel mundial, podemos citar como ejemplos emblemáticos al gigante tecnológico de China: Alibaba, que es la empresa matriz, entre otras, de ***AliExpress***, quien ha expresado a todos los medios en octubre del 2019, a través de su fundador y ex presidente ejecutivo

de la compañía, Jack Ma, ***que diariamente son víctimas de unos 300 millones de ataques cibernéticos***, Bobillo (2019).

Así también, tenemos al otro gigante de la tecnología digital: ***Huawei***, manifestó a través de su jefe de seguridad, de ser también ser blanco de un promedio de un millón de ataques cibernéticos por día. Existen otras grandes compañías tecnológicas que prefieren mantener perfil bajo y no revelar sus vulnerabilidades frete a los ataques cibernéticos. En el plano nacional, el diario ***Gestión***, que es un gran referente del empresariado peruano, en su edición de agosto de 2020 publicó que el ***Perú sufrió más de 613 millones de intentos de ataques informáticos hasta junio del 2020***.

En este sentido, la empresa de seguridad Fortinet, declaró que la Pandemia del COVID-19 y los ataques de *"fuerza bruta", fueron grandes catalizadores para el incremento de las actividades cibercriminales durante la primera mitad del año*. En el plano local, el Banco de Crédito del Perú, declaró a **Gestión** en enero del presente año, haber sido víctima de un ataque en el 2018 que expuso los datos confidenciales de sus clientes, incluyendo las cuentas bancarias y numeración de tarjetas de un buen número de clientes.

El espíritu del presente trabajo de investigación, es demostrar la aplicabilidad de las buenas prácticas del hacking ético que se puedan subsumir en los procedimientos rutinarios de la seguridad informática para la protección de invaluable información.

Contar con profesionales en hacking ético, implica resolver aquellos conflictos encontrados como vulnerabilidades de penetración y prevenir o mitigar aquellos ataques o amenazas que se puedan presentar en un futuro inmediato y en el caso que nos ocupa, se aplicarán las técnicas de hacking ético a la empresa Inversiones Mayito – Agente BCP, ubicada en la calle Julio Chiriboga N° 1259 de la Urbanización Las Quintanas y registrada con **RUC N° 10269605958**, la misma que se dedica a la distribución de productos farmacológicos, así como de **Agente Bancario del Banco de Crédito del Perú (BCP)** y funcionando para los servicios de depósito y retiro de dinero y de pago de recibos de servicios múltiples. Esta empresa ha sufrido en ciertas oportunidades, de ataques

cibernéticos que han derivado en la sustracción de información confidencial de los clientes, pérdida de dinero, buena reputación y deterioro de su imagen, motivo por los cuales ha tenido que indemnizar directamente a los clientes afectados y evitar la propalación de haber sido víctima de estas malas prácticas.

Es por ello se investigó previamente al respecto, tomando las manifestaciones de los propietarios del negocio, los mismos que manifestaron su gran incomodidad al ver mermada su buena imagen en contra de los clientes a los cuales se deben. El sistema informático de Inversiones Mayito – Agente BCP se diseñó y estructuró sin considerar la seguridad de la información y es por ello que se encuentra expuesta a intrusiones y ataques, los mismos que exponen al riesgo a la data con la cual se trabaja. Los trabajadores de esta distribuidora, no se rigen por ningún protocolo de seguridad o programas les procuren detectar problemas en el sistema informático y es por ello que, frente a ataques a los servicios informáticos, perderán tiempo y dinero durante el restablecimiento o recuperación de la data. Los ingresos de la distribuidora no solo dependen de los servicios financieros brindados a su clientela, sino también del voluminoso número de transacciones que se puedan realizar, las mismas que a su vez son dependientes del sistema informático instalado y de su seguridad.

Después de Analizar la problemática de Inversiones Mayito – Agente BCP, hemos planteado esta problemática en el siguiente cuestionamiento:

¿De qué manera la aplicación de Hacking Ético influirá en la seguridad de la red de telecomunicaciones de Inversiones Mayito – Agente BCP?

Como objetivo general, podemos plantear lo siguiente:

Aplicar las técnicas empleadas en ***hacking ético para mejorar la seguridad de la red de telecomunicaciones*** de Inversiones Mayito – Agente BCP; y respecto de los objetivos específicos, tenemos que:

Al ***identificar y neutralizar las amenazas y riesgos de su red de telecomunicación***, Inversiones Mayito – Agente BCP aminorará significativamente los costos durante la gestión de la información al ejecutarla con mayor protección y evitando así la sustracción de información sensible, así

como también obtendrá una mayor seguridad respecto de su data almacenada al investigarse y conocer lo que ocurrió en su computador principal luego de haber transcurrido cierto tiempo (meses o años), después de ***practicar una auditoría forense a su unidad de almacenamiento interna*** (disco duro o disco sólido), Solvetic (2020). Asimismo, y luego de auditar las unidades de almacenamiento de la CPU principal de la empresa, se ***identificarán los puertos vulnerables de la misma, a fin de bloquearlos***. Finalmente, y para garantizar la sostenibilidad y mantenimiento de las aplicaciones empleadas, ***se otorgarán charlas virtuales de capacitación al personal involucrado directamente con el manejo de la red de telecomunicación de la empresa***, puesto que es posible entrenar a los trabajadores para mejorar la rutina de operaciones, ya que ello genera una ventaja competitiva. Dentro de la empresa se encuentra personal con conocimientos elementales de informática, los mismos que podrán proporcionar un buen servicio de soporte técnico a la aplicación de hacking ético, beneficiando así a la seguridad de la información. La métodos y técnicas necesarios para llevar a cabo la aplicación de hacking ético se encuentran libres en el mercado y se pueden aplicar para lograr una mayor protección.

Lo anteriormente expuesto, nos conlleva a plantear la siguiente hipótesis: La aplicación de Hacking Ético mejora significativamente la prevención de ataques cibernéticos a la red de comunicación de la empresa Inversiones Mayito – Agente BCP.

Figura N° 1: Árbol de Problemas.

Fuente: Elaboración propia

II. MARCO TEÓRICO

En el presente trabajo de investigación, se ha tenido a bien considerar como aporte y soporte cognitivo a los siguientes antecedentes científicos. Así tenemos, en el plano internacional:

Según Grant (2019), aquellos profesionales o personas con suficiente conocimiento tecnológico informático que se dedican a la seguridad digital, son generalmente mal vistos por los clientes, puesto que estos dudan muchas veces de sus buenas intenciones y temen poder ser en algún momento víctimas de algún ataque informático. En la presente obra demostraremos que se puede contar con profesionales suficientemente capacitados (previamente identificados), con los cuales se puede contar para proveer protección a sus redes de teletransmisión.

De manera similar, Walker (2020), afirma en su obra que existen tres tipos de los llamados “Hackers”: los de “sombreros blanco, negro y gris”, refiriéndose a los primeros como profesionales que prestan sus servicios exhibiendo siempre una actitud muy recta y responsable, a los segundos, como a aquellos que solo persiguen hacer daño moral y/o económico a terceras personas y como “grises” a aquellos que mantienen una conducta “intermedia”, es decir que resultan ser una mixtura de los dos primeros anteriormente citados. En esta investigación, señalaremos con estos adjetivos a los personajes que puedan estar involucrados de manera directa o indirecta en algún procedimiento sospechoso e irregular.

Al respeto, Himanen (2015), realiza una descripción muy acuciosa del perfil ético adecuado que debe presentar todo especialista en seguridad digital y es la misma que tendremos que asumir durante el desarrollo de todo el proceso de investigación.

Asimismo, Wolf y Soria Guzmán (2016), resaltan en su investigación la gran importancia y ventajas tanto técnicas como económicas que se obtienen al utilizar software libre en la aplicación de las prácticas de Hacking Ético. De esta manera, quedan sustentadas las bases por cuales, utilizaremos este tipo de software en nuestro trabajo de investigación.

En cuanto a la seguridad, Wolf (2017), efectúa un objetivo análisis respecto del uso de los protocolos de seguridad: HTTP y HTTPS, señalando las ventajas y desventajas de los mismos. Estos aspectos serán tomados en cuenta, en su momento, en la presente investigación.

En este orden de ideas, Wolf (2014), se refiere a la seguridad con mecanismos criptográficos, así como también el gran arraigo que en los últimos años estos han venido obteniendo en los diferentes planos tanto públicos como privados. Estos mecanismos serán adoptados en esta investigación por ser implementaciones que garantizan mayor seguridad a los sistemas. En su obra sobre Hacking Ético, Astudillo (2017), realiza un exhaustivo análisis de los diferentes métodos de ataque que utilizan los “hackers de sombrero negro” para vulnerar y penetrar la seguridad de las redes de información. Estas descripciones serán tomadas en cuenta en la presente obra a efectos de poder elaborar estrategias que permitan rechazar este tipo de penetraciones.

Referente a la construcción y reconstrucción de los sistemas informáticos, Schütte (2019), nos cita en su obra diferentes pautas que se deben considerar para estos fines y que formarán parte del presente proyecto.

Nuevamente y a nivel muy especializado, Barrera (2019), nos presenta nuevas estrategias para el análisis y debida protección que deben tener las redes de comunicación frente a los ataques digitales y que serán considerados por los autores en la presente obra.

Son muy interesantes los métodos de testeo de software utilizados y descritos por Giannone (2019) en su obra, ya que ello servirá como insumo para enriquecer la hermenéutica que se utilizará en el presente proyecto y desde ya se le reconoce una gran contribución al mismo.

Según Ordoñez (2016), los diez sistemas operativos más utilizados por los hackers, son: Kali Linux, Back Box, OS Security Parrot, Live Hacking OS, DEFT Linux, Samurai Web Testing Framework, Net Work Security Toolkit, Bugtraq, NodeZero y Pentoo, los cuales serán tomados en cuenta en el presente proyecto de investigación a efectos de determinar el nivel de efectividad y peligrosidad de los mismos puesto que también son materia de análisis.

En cuanto a la parte estadística, Graus (2017), nos orienta muy acertadamente en cuanto al método estadístico a emplear en el análisis de las variables, tanto la dependiente como la independiente y en lo concerniente a la recolección de datos, Díaz del Castillo (2020), nos brinda unas pautas efectivas para ejecutar estos pasos de manera correcta.

En lo concerniente a las aplicaciones de las técnicas estadísticas y probabilísticas, Boaglio et al. (2020), de manera muy simple pero a la vez eficiente, nos muestra algunas metodologías para determinar el tamaño de la población, así como de la muestra y las técnicas de muestreo, no sin antes presentar previamente algunos ejemplos muy didácticos.

Existen también algunas aplicaciones de software estadístico. En este sentido, Urquizo, López y Sandoval (2020), nos ilustran al respecto y también nos otorgan la hermenéutica necesaria para su desarrollo e implementación.

En lo referente a los lineamientos estadísticos a seguir en el presente proyecto de investigación, Arias (2012), nos ilustra al respecto del tamaño de la población y la muestra, así como en qué casos y dependiendo del tamaño de la población, se puede obviar el tamaño de la muestra. Cabe resaltar que su obra sobre procedimientos estadísticos fue premiada en su momento como “El Mejor Libro Técnico del Año”.

Durante el desarrollo del Congreso de Seguridad de la Información del Instituto Politécnico Nacional, Wolf (2014), nos señala al respecto, la gran importancia que tiene la criptografía para la implementación de la seguridad informática. Y a la vez, nos hace reflexionar sobre los avances que han logrado procurar los ciberdelincuentes a efectos de vulnerar este tipo de defensa de la integridad digital, por lo que debemos de estar siempre a la vanguardia de este tipo de tecnología para contrarrestar dichos ataques.

Cuando hablamos de las metodologías de las buenas prácticas de penetración, y desde la Universidad Nacional Abierta y a Distancia (UNAD), Barrera y Rocío (2019), nos plantean ciertas buenas prácticas de pruebas de pentesting (prueba de penetración), con la finalidad de realizarlas dentro del marco ético que deben ser inherentes a la aplicación del Hacking Ético.

Engebretson (2013), en su obra: “The basics of hacking and penetration testing: ethical hacking and penetration testing made easy”, presenta una interesante metodología diseñada para las personas interesadas en aprender sobre piratería y pruebas de penetración, sobre todo para aquellos “iniciados” en este tipo de investigaciones, por lo que en su lectura se puede apreciar el avance desde su modo más básico y coloquial hasta la parte más completa y científica en este ámbito. Asimismo, el autor asegura que, al culminar la lectura del libro, el lector tendrá una comprensión sólida de los procesos de pruebas de penetración y podrá adaptarse cómodamente a las herramientas necesarias para implementar estas aplicaciones.

Similarmente, la obra de Baloch (2017): “Ethical Hacking and Penetration Testing Guide”, nos brinda de manera fácil y detallada, los pasos a seguir para aquellos investigadores que desean iniciarse en los métodos del pentesting utilizando una guía bastante comprensible e intuitiva al respecto.

Najera-Gutierrez y Ansari (2018), nos brindan en su texto: “Web Penetration Testing with Kali Linux: Explore the methods and tools of ethical hacking with Kali Linux”, explicada de una manera muy práctica, la forma de realizar testeos y penetraciones web, utilizando la conocida herramienta para estos fines, el Kali Linux, mostrándonos paso a paso, cómo es que se tienen que emplear los comandos y sentencias de este sistema operativo para realizar un testeo desde su parte inicial y más fundamental hasta un nivel casi profesional en la penetración web. Así también, explican de manera detallada las funciones específicas de estos comandos y los riesgos que se podrían correr en caso de no utilizar correctamente los mismos.

En cuanto al IoT (Internet de las cosas), tenemos la obra de Visoottiviseth et al. (2017), en la cual nos detalla acerca de la tecnología IoT y como ha crecido rápidamente con muchas implementaciones. Sin embargo, debido a su capacidad para realizar tareas y manejar la información confidencial y también a la escasez de conciencia de seguridad del usuario, los dispositivos de IoT contienen muchos riesgos potenciales y son el nuevo objetivo de los ataques. En este documento, se desarrolla un sistema de prueba de penetración para dispositivos IoT llamado PENTOS con el fin de aumentar la conciencia de

seguridad del usuario. El sistema viene con la GUI que se ejecuta en Kali Linux, que está diseñada específicamente para la piratería ética. PENTOS recopila automáticamente la información del dispositivo IoT de destino a través de la comunicación inalámbrica, que son Wifi y Bluetooth. El sistema permite a los usuarios realizar varios tipos de pruebas de penetración en sus dispositivos de IoT, como el ataque de contraseña, el ataque web y el ataque inalámbrico para obtener el acceso privilegiado mediante múltiples algoritmos. Algo sumamente interesante.

En lo referente al uso de tarjetas con microprocesador, tenemos la obra de Yevdokymenko, Mohamed y Onwuakpa (2017). Este documento está dedicado al campo de la defensa de las redes y la infocomunicación a lo largo de la plataforma de ciberseguridad para profundizar en lo que ahora se conoce como “HACKING ÉTICO”, con el fin de definir, analizar, discutir y resolver algunos de los problemas más comunes. y las amenazas ampliamente difundidas y sus funcionalidades, según las cuales las vulnerabilidades están actualmente disponibles en la mayoría de los incidentes de amenazas y tratar de encontrar nuevas técnicas para resolver estos problemas de manera más efectiva, utilizando para ello, en calidad de herramientas de simulación, las tarjetas Raspberry PI.

También cabe citar, respecto a las intrusiones en la web, al artículo de Jiménez (2016). Este artículo se centra en el conocimiento de la técnica de pentesting en aplicaciones web, analiza las diferentes fases en donde los más comunes en estos ataques pudieran ser víctimas, así como también actualiza herramientas de software para realizar una prueba de penetración.

En el texto de Nicholson (2019), nos explica cómo es que a medida que las tecnologías digitales se integran en todos los aspectos de la vida, los ciberataques pueden provenir de muchas direcciones. Una proporción significativa de estos ataques presenta serios riesgos para los datos, la infraestructura y los procesos críticos dentro de todo tipo de organizaciones, tanto grandes como pequeñas.

Asimismo, en el texto de Sabih (2018), nos explica otra metodología de penetración, aprendiendo a piratear sistemas como hackers de sombrero negro y protegerlos como expertos en seguridad. Reconocer las características y comprender cómo funcionan los sistemas informáticos y sus vulnerabilidades. A cómo explotar sus debilidades y piratear máquinas para probar su seguridad para poder proteger a sus sistemas de información.

También tenemos la publicación de Devi y Kumar (2020), en la cual narra cómo es que en el mundo digital, todo se conecta a través de la red, y cuando las aplicaciones web brindan varios servicios, las personas son susceptibles de ser pirateadas. Según el informe de Symantec sobre amenazas a la seguridad en Internet de 2019, un promedio de 4.800 sitios web son vulnerables al ataque de robo de información digital (robo de formularios). El objetivo principal de este documento es reconocer la apertura y las fallas en las redes y aplicaciones web utilizando pruebas de penetración para proteger a las instituciones de las amenazas cibernéticas. Hay muchos métodos de exploración sugeridos por muchos autores para identificar la debilidad.

Según Radholm y Abefelt (2020), los dispositivos de Internet de las cosas (IoT) son cada vez más frecuentes. Debido al rápido crecimiento del mercado de estos dispositivos, las medidas de seguridad inadecuadas conducen a una gama cada vez mayor de ataques. Existe una gran cantidad de pruebas y protección de estos dispositivos para contribuir a una sociedad más sostenible. Esta tesis ha evaluado la seguridad de un refrigerador IoT mediante el uso de piratería ética, donde se elaboró un modelo de amenazas para identificar vulnerabilidades. Se realizaron pruebas de penetración basadas en el modelo de amenazas. Los resultados de las pruebas de penetración no encontraron vulnerabilidades explotables. La conclusión de evaluar la seguridad de este refrigerador Samsung puede decir que el producto es seguro y contribuye a una sociedad conectada, segura y sostenible.

Según Patil et al. (2017), la piratería es básicamente experiencia en cualquier campo. Los piratas informáticos se clasifican según el trabajo y el conocimiento. Los piratas informáticos éticos se clasifican como piratas informáticos de sombrero blanco. Los piratas informáticos éticos utilizan técnicas de piratería

para brindar seguridad. Son piratas informáticos autorizados legalmente. Se utilizan varias herramientas para realizar piratería. La técnica de piratería más utilizada es el phishing. Dado que hay un rápido crecimiento en el número de ataques, es necesario que las personas aprendan conceptos de piratería ética para protegerse.

El análisis de la tesis de Metso (2019), las pruebas de penetración (pentesting), también conocidas como Ethical o White Hat Hacking, son un tema que intriga a muchas personas, especialmente a las que trabajan en el área de tecnología de la información empresarial. El autor de esta tesis ha querido aprender pentesting desde hace un tiempo y el fino arte del pentesting es un gran activo para un administrador de sistemas. Obtener conocimientos sobre pentesting proporciona buenas herramientas para controlar y documentar la seguridad del sistema del que uno es responsable.

Conde Ortiz (2020), nos explica en su artículo, que casi ningún software está exento de vulnerabilidades. Se pueden utilizar pruebas de penetración o piratería ética para identificarlos. Esta tesis realiza una serie de pruebas siguiendo el método de prueba de penetración en un sistema de control industrial a gran escala. El objetivo es descubrir qué tipo de vulnerabilidades existen en estos sistemas, centrándose en los ataques desde el interior de su red. Se tomaron varios enfoques en relación a cómo atacar los servidores y servicios que forman la red, tanto desde el exterior como desde el interior de las máquinas. Se encontraron vulnerabilidades críticas en relación con el uso de servicios no autenticados y la interrupción de la comunicación entre servidores, que deben mitigarse correctamente para evitar futuros ataques potenciales.

Según Khan (2019), con el cambio tecnológico y de infraestructura actual, las pruebas de penetración ya no son una actividad orientada a procesos. Las pruebas de penetración modernas exigen mucha automatización e innovación; el único lenguaje que domina a todos sus pares es Python. Dada la gran cantidad de herramientas escritas en Python y su popularidad en el espacio de pruebas de penetración, este lenguaje siempre ha sido la primera opción para los probadores de penetración. Las pruebas prácticas de penetración con

Python lo guían a través de construcciones avanzadas de programación de Python. Una vez que esté familiarizado con los conceptos básicos, explorará los usos avanzados de Python en el dominio de las pruebas de penetración y la optimización. Luego pasará a comprender cómo Python, la ciencia de datos y el ecosistema de ciberseguridad se comunican entre sí. En los capítulos finales, estudiará casos de uso de desarrollo de exploits, ingeniería inversa y ciberseguridad que se pueden automatizar con Python.

Asimismo, Rakshitha (2020), nos señala que, en el mundo de vanguardia, con los avances más recientes en tecnologías y plataformas, una gran cantidad de clientes interactúan entre sí de manera constante. Todos y cada sesenta segundos pueden ser vulnerables y exorbitantes para las redes privadas y personales debido a la proximidad de diferentes tipos de ataques antiguos y nuevos en todo el mundo. La red pública es la opción más conocida y rápida para difundir ataques en todo el mundo. Códigos y secuencias de comandos maliciosos, virus, spam y software malicioso están continuamente a su disposición. La seguridad de la información debe proporcionar técnicas y procedimientos para proteger los datos y los marcos de datos de acceso no aprobado, revelación de datos, utilización o modificación. El aumento de las activaciones maliciosas, los delitos cibernéticos y la aparición de diferentes formas de ataques avanzados requieren la necesidad de un tester de penetración que penetre en la seguridad del sistema y las redes para determinar, preparar y tomar medidas de prevención contra estos ataques agresivos. La piratería ética y las pruebas de penetración son términos comunes, populares en el entorno de seguridad de la información. El aumento de los delitos cibernéticos y la piratería son una prueba notable para los profesionales de la seguridad, los especialistas y las reglas durante la última década. Las técnicas y procedimientos para proteger los datos y los marcos de datos del acceso no autorizado llegan a la revelación o modificación de datos. La política de seguridad de la información garantiza la Confidencialidad, Integridad y Accesibilidad. Una organización sin estos enfoques de seguridad y reglas de seguridad adecuadas corre un peligro extraordinario y la información confidencial identificada con esa asociación no está segura sin estas políticas de seguridad.

Shebli y Beheshti (2018), enfatizan respecto a la seguridad de la información, que ésta es más vulnerable que nunca; y cada avance tecnológico plantea una nueva amenaza a la seguridad que requiere nuevas soluciones de seguridad. Las pruebas de penetración se realizan para evaluar la seguridad de una infraestructura de TI al exponer de manera segura sus vulnerabilidades.

También ayuda a evaluar la eficacia de las herramientas y la política de los mecanismos de defensa existentes. Las pruebas de penetración se realizan con regularidad para identificar riesgos y gestionarlos para lograr estándares de seguridad más altos. En este artículo se discute la importancia de las pruebas de penetración, los factores y componentes considerados al realizar una prueba de penetración, presentamos una encuesta de herramientas y procedimientos seguidos, el rol de la prueba de penetración al implementar en el gobierno de TI en una organización y finalmente la ética profesional debe ser poseído por el equipo involucrado en la prueba de penetración.

Según Saha et al. (2020), al definir el estado severo de la seguridad de la información en el mundo actual, nos encontramos con un término técnico muy reconocido conocido como "piratería ética". La piratería ética se refiere al arte de desenmascarar las vulnerabilidades y la debilidad en una computadora o un sistema de información. El proceso implica la duplicación de intenciones y acciones de otros piratas informáticos malévolos. La piratería ética también se puede denominar "prueba de penetración", "prueba de intrusión" o "formación de equipos rojos". Hablando del término "piratería", es básicamente un procedimiento desafiante y estimulante para robar información de un sistema informático desconocido o puede ser un dispositivo sin el conocimiento previo del propietario de ese sistema. Ahora, con el término "ético", entendemos que el proceso de piratería se realiza con un propósito ético que resultará en una bendición para la sociedad. Un pirata informático ético intenta recuperar o destruir la información o los datos robados por los piratas informáticos no éticos. El proceso de piratería puede convertirse en una bendición y una maldición para la sociedad, y depende de la intención de un pirata informático. Este es sin duda un procedimiento muy fuerte y severamente basado en la forma en que se usa. Este artículo analiza las diversas metodologías y conceptos relacionados con la piratería ética, así como las herramientas y el software

utilizados en el proceso, junto con los aspectos futuros y las tecnologías emergentes en este campo.

Respecto de los hipervisores, Sinha (2018), nos indica que cuando se van a realizar pruebas de penetración o pruebas relacionadas con la piratería, es necesario crear un laboratorio porque no se puede experimentar en un sistema en vivo. Por lo tanto, necesita un entorno virtual, también conocido como hipervisor. Para los usuarios de Linux, VirtualBox es una gran solución; KVM también es bueno. Para Windows, VMware Player es una buena solución; Windows Virtual PC también es bueno, pero no puede ejecutar distribuciones de Linux en él. Para macOS X, tanto QEMU como Parallels son buenas opciones.

Georg, Oliver y Gregory (2018), refieren en cuanto al documento de su autoría, que este analiza los problemas de la confianza implícita en la piratería ética. A diferencia de muchas otras profesiones establecidas desde hace mucho tiempo, como abogados, médicos y contables. La piratería ética es una profesión relativamente nueva. Como resultado, esta profesión no tiene actualmente un código uniformado u obligatorio, ni requiere ningún tipo de licencia. Debido a que los piratas informáticos éticos podrían obtener acceso a información altamente sensible y confidencial y existe la posibilidad de un uso indebido de dicha información, la necesidad de garantizar que se mantenga el profesionalismo asegurando la competencia y el comportamiento ético es fundamental.

Wang y Yang (2017), sostienen que la piratería ética práctica y la defensa de la red se han convertido en un componente esencial en la enseñanza de la ciberseguridad. Sin embargo, sin comprender las vulnerabilidades de un sistema informático, sería difícil llevar a cabo una defensa de red con éxito para evitar intrusos en el mundo real. Por lo tanto, enseñar piratería ética y escaneo de vulnerabilidades es un elemento clave para el éxito del plan de estudios de ciberseguridad. En este documento, se revisa el estado del arte de las herramientas actuales de escaneo de vulnerabilidades de código abierto. Se introduce un entorno de laboratorio virtual como parte del diseño de laboratorio. Presentan laboratorios prácticos diseñados en detalle utilizando la herramienta

de escaneo de vulnerabilidades OpenVAS. Se revisan los resultados después de realizar los laboratorios prácticos en los cursos de ciberseguridad y se identifica el trabajo futuro para áreas de investigación abiertas.

De manera análoga, Shree (2019), señala en su artículo que el Ethical Hacking, a veces llamado prueba de penetración, es una demostración de irrumpir o infiltrarse en un marco o sistemas para descubrir peligros, vulnerabilidades en esos marcos que un agresor maligno puede descubrir y aventurar causando pérdida de información, desgracias relacionadas con el dinero u otros daños reales. El motivo de la piratería moral es mejorar la seguridad del sistema o los marcos al corregir las vulnerabilidades descubiertas durante las pruebas. Los programadores morales pueden utilizar técnicas e instrumentos similares utilizados por los programadores malignos, pero con el consentimiento de la persona aprobada para mejorar la seguridad y proteger los marcos de los ataques de clientes perniciosos. Este artículo trata sobre los usos y técnicas de la piratería ética y además estudia los diferentes tipos de piratas informáticos y la piratería con sus fases.

Cruz y Simoes (2019), narran en su artículo, sobre la tasa y la diversidad de los delitos cibernéticos que están creciendo rápidamente.

Se ha vuelto más común, más sofisticado y más dañino, y le cuesta a la economía mundial miles de millones de euros en pérdidas cada año. Para contrarrestar esta creciente amenaza, las organizaciones aumentan continuamente su inversión en seguridad de la información y ciberseguridad, incluidos los servicios de pruebas de penetración o piratería ética.

Tradicionalmente, los piratas informáticos éticos siempre han utilizado hardware costoso y potente desde el punto de vista informático para ejecutar distribuciones especiales de Linux orientadas a la seguridad. Sin embargo, la llegada de las computadoras de placa única en la última década ha ofrecido nuevas posibilidades para la piratería ética. Esta investigación tiene como objetivo explorar, de manera práctica, la viabilidad real de realizar tareas de piratería ética de una manera no tradicional, es decir, siguiendo un enfoque novedoso que aún utiliza las mismas distribuciones de seguridad de Linux.

Respecto de las métricas de seguridad, Al-Shiha y Alghowinem (2019), indican que, con la creciente preocupación por la seguridad en Internet, surgió un campo para superar esas preocupaciones, que se llama Cyber Security.

La seguridad cibernética se compone de muchas secciones, donde la piratería ética es una parte importante de ella.

La piratería ética, también conocida como prueba de penetración, consiste en garantizar la seguridad de un sistema pirateándolo sin causar ningún daño al sistema o sus datos.

A los piratas informáticos éticos se les asigna la responsabilidad de probar las vulnerabilidades en el sistema obteniendo acceso a la seguridad, la información confidencial y los datos del cliente.

Es importante que esos sistemas no se vean comprometidos ni se aprovechen de los proveedores de servicios. Con la tecnología que evoluciona rápidamente, es difícil para el consumidor medio mantenerse actualizado con la última tecnología y podría fácilmente ser víctima de las empresas de seguridad. Sin embargo, hay una falta de estudio de la métrica que los piratas informáticos éticos deben seguir para lograr la confianza y la integridad de ambas partes, es decir, el proveedor de seguridad y el consumidor.

El propósito de esta investigación es identificar la métrica ética que deben seguir los piratas informáticos para no confundir a sus clientes. Para reconocer estas métricas, se evaluaron las métricas de seguridad del sistema y ciberseguridad para obtener las métricas de piratería ética más adecuadas.

Según Ochang e Irving (2017), el Protocolo de Voz sobre Internet (VoIP) se está convirtiendo gradualmente en el estándar de facto en la tecnología de las comunicaciones y ahora se lo considera una alternativa económica a las redes telefónicas públicas conmutadas (PSTN) debido a su bajo costo y flexibilidad. Sin embargo, la flexibilidad y la capacidad de VoIP para proporcionar una red de voz y datos convergentes conlleva vulnerabilidades y amenazas de seguridad, algunas de las cuales son el resultado de la arquitectura IP existente. Sin embargo, el uso de pruebas de penetración puede proporcionar

un marco para analizar e identificar vulnerabilidades y fallas en una red VoIP que, a su vez, puede ayudar a mejorar la seguridad.

Esta investigación presenta cómo se puede lograr un nivel integral de seguridad de la red VoIP mediante la realización de pruebas de penetración a través de Ethical Hacking.

En esta investigación se utilizó la taxonomía de VoIP Security Alliance (VoIPSA) para clasificar las amenazas de VoIP que condujeron al diseño de una prueba de penetración que se llevó a cabo contra una red de VoIP en otra para identificar vulnerabilidades y exploits relacionados con la clasificación de amenazas de VoIPSA.

Esto resultó en el desarrollo de una metodología de prueba de penetración de VoIP adecuada para redes VoIP. La metodología de prueba de penetración desarrollada identificó con éxito vulnerabilidades en la implementación de VoIP que ayudaron a proporcionar recomendaciones de seguridad.

En la conocida obra “Penetration Testing and Network Defense: Penetration Testing”, Whitaker y Newman (2005), nos relatan las técnicas, tácticas y estrategias para rechazar y proteger a las redes de comunicación de los ataques a los que pueden estar expuestas las mismas. A diferencia de otros libros sobre piratería, este libro está específicamente orientado a las pruebas de penetración. Incluye información importante sobre cuestiones de responsabilidad y ética, así como procedimientos y documentación. Utilizando aplicaciones comerciales y de código abierto populares, el libro muestra cómo realizar una prueba de penetración en la red de una organización, desde la creación de un plan de prueba hasta la realización de ingeniería social y reconocimiento de host y la realización de ataques simulados en redes cableadas e inalámbricas.

Según (Matero (2020), los constantes avances en todas las áreas tecnológicas han comenzado a preocupar cada vez más tanto a los propietarios de empresas como a los particulares. La seguridad es una de las áreas donde se requiere educación y mejora constante para mantener un sistema inaccesible para el personal no autorizado. La piratería ética es una forma de prueba de

penetración en la que el evaluador asume el papel de un atacante legítimo e intenta acceder al sistema por medios no autorizados. Este ataque muestra las vulnerabilidades en el sistema y la red y señala los componentes que deben reforzarse en caso de un verdadero ataque.

Asimismo, Sabih (2018) nos indica a través de su obra, que se comenzará por comprender cada etapa de pentesting e implementación de máquinas virtuales de destino, incluidos Linux y Windows. A continuación, el libro nos guiará a través de la realización de pruebas de penetración intermedia en un entorno controlado. Con la ayuda de casos de uso prácticos, también podrá implementar el aprendizaje en escenarios del mundo real. Al estudiar todo, desde la configuración de su laboratorio, la recopilación de información y los ataques de contraseñas, hasta la ingeniería social y la explotación posterior, podrá superar con éxito las amenazas de seguridad. El libro incluso ayuda a aprovechar las mejores herramientas, como Kali Linux, Metasploit, Burp Suite y otras herramientas de pentesting de código abierto para realizar estas técnicas.

En los capítulos posteriores, se centra en las mejores prácticas para resolver rápidamente las amenazas de seguridad.

Análogamente, (Robberts y Toft 2019), indican que los dispositivos de Internet de las cosas (IoT) se están volviendo más omnipresentes que nunca y, si bien la seguridad no es tan importante para todos los tipos de dispositivos, es crucial para algunos. En esta tesis, se examina una cerradura inteligente Bluetooth ampliamente disponible a través de la lente de la seguridad.

Adicionalmente, (Tayag y De Vigal Capuno 2019), señalan que en el mundo cibernético se cometen cada vez más ciberataques. Los piratas informáticos se han convertido ahora en los guerreros de Internet. Atacan y hacen cosas dañinas al sistema comprometido. Este artículo muestra la metodología que utilizan los piratas informáticos para obtener acceso al sistema y las diferentes herramientas que utilizan y cómo se agrupan en función de sus habilidades.

En el artículo de Martin Cooper, (Cooper 2016), informa sobre sus hazañas de ingeniería social y sus puntos de vista sobre la seguridad cibernética y cómo mantenerse seguro en línea.

Según (Moldovan y Ghergulescu 2020), Con la creciente necesidad de profesionales calificados en ciberseguridad y la conciencia cibernética, muchas universidades están creando programas de ciberseguridad y muchas empresas están invirtiendo en la capacitación de sus empleados en ciberseguridad. Al mismo tiempo, existe un número creciente de plataformas de ciberseguridad para educación y capacitación, que varían ampliamente en su oferta y costo de soluciones

(Mansfield-Devine 2017) nos indica que constantemente se nos dice que el Reino Unido y otros países padecen una grave falta de habilidades en seguridad de la información. Es casi seguro que eso sea cierto cuando se trata de satisfacer las habilidades de seguridad operativa del día a día de las organizaciones. Pero en un área específica, la piratería ética o las pruebas de penetración, no se trata tanto de una cuestión de cantidad como de calidad. Como explica Lawrence Munro, director senior para EMEA del equipo SpiderLabs en Trustwave, lo más importante es conseguir personas con las habilidades y actitudes adecuadas.

Según Thomas, Burmeister y Low (2019), en todo el mundo, ha habido un aumento notable en la adopción de leyes de divulgación de infracciones diseñadas para proteger la privacidad de las personas. Para validar los controles de seguridad implementados por una organización para proteger los datos confidenciales, los probadores de penetración a menudo se involucran para probar la seguridad de los sistemas de información e informar cualquier vulnerabilidad. Utilizando un enfoque constructivista e interpretivista, este artículo informa sobre un estudio piloto que compara los enfoques de EE. UU. y Australia sobre la piratería ética. La necesidad de regular el pirateo ético para ayudar a proteger a las organizaciones de conductas poco éticas fue un tema recurrente. Con los cambios en las regulaciones de privacidad en todo el mundo, la divulgación no autorizada de información personal y privilegiada podría tener consecuencias importantes. Este artículo explora la importancia

de la conducta ética por parte de los probadores de penetración basada en la investigación empírica y el potencial de uso indebido de la información.

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

Tipo de investigación: Aplicada.

Diseño de investigación: Experimental del tipo pre – experimental.

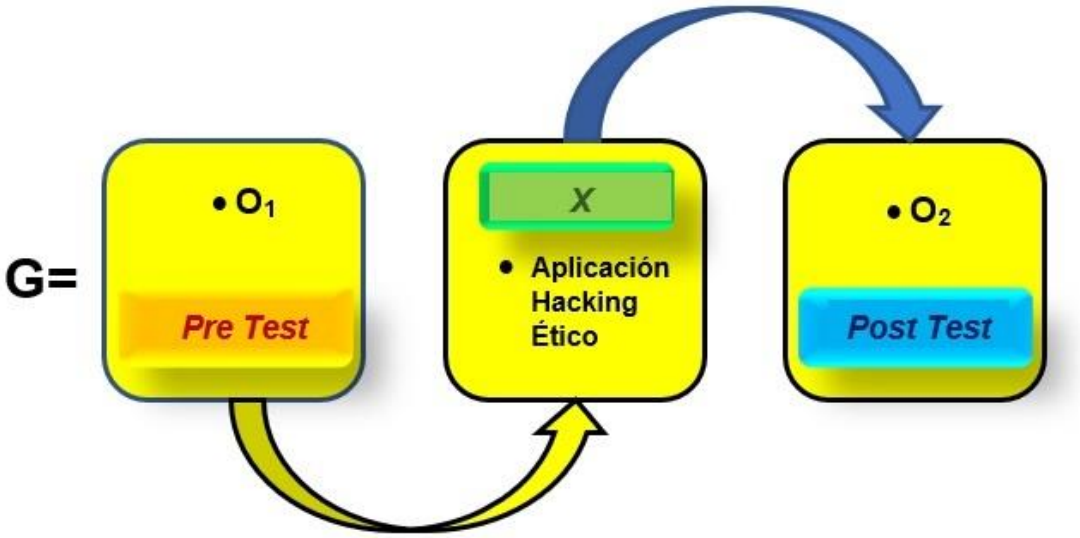


Figura N° 2: Diseño de Investigación.

Fuente: Elaboración propia

Dónde:

- G: Grupo experimental
- O_0: Gestionar la prevención de ataques a la red de comunicación antes de la aplicación de hacking ético.
- X: Aplicación de hacking ético.
- O_1: Gestionar la prevención de ataques a la red de comunicación después de la aplicación de hacking ético.

3.2. Variables y operacionalización

Según Graus y Enrique (2017, p. 5), pueden existir en un trabajo de investigación, variables independientes y variables dependientes.

Las variables independientes, son aquellas que pueden causar algo dentro del entorno de un sistema, mientras que las variables

dependientes son aquellas que muestran un cambio o resultado diferente luego de la intervención o aplicación de la variable dependiente (Ver Anexo 1: Matriz de operacionalización de variables, definición conceptual, definición operacional, indicadores y escala de medición).

3.2.1. Identificación de las variables

- ✓ Variable Independiente: Aplicación de Hacking Ético
- ✓ Variable Dependiente: Gestionar la prevención de ataques a la red de comunicación.

3.3. Población, muestra, muestreo y unidad de análisis

Según Arias (2012), en su obra galardonada con el “Premio Nacional al Mejor Libro Técnico”, nos explica que si la población en función del número de sus elementos integrantes, resultan ser asequibles en su integridad, no es necesario determinar una muestra, por lo tanto, se podrá llevar a cabo la investigación a efectos de recolectar todos los datos que sean pertinentes de la población objetivo involucrada. Paralelamente, señala que este contexto debe de explicitarse dentro del marco metodológico, en el cual se obviará todo lo relativo a la determinación de una muestra.

3.3.1. Población

Red de telecomunicación inalámbrica, puertos y la unidad de almacenamiento interno del CPU de la empresa Inversiones Mayito – Agente BCP.

3.3.2. Muestra

Dado que la población sujeta de investigación es pequeña, la muestra está constituida por estos tres elementos: la conexión inalámbrica de la red, los puertos y la unidad de almacenamiento interno del CPU.

3.3.3. Muestreo

El muestreo ya no aplica en este caso por las consideraciones anteriormente expuestas.

3.3.4. Unidad de análisis

La unidad de análisis, será el equipo de cómputo principal de la empresa en estudio.

3.4. Técnicas e instrumentos de recolección de datos

Técnicas

- ✓ **Observación:** Es la técnica que se ejecutara por medio de la observación de campo.
- ✓ **Encuesta:** Es la técnica que permitirá encuestar a los 6 trabajadores de Inversiones Mayito – Agente BCP.

Instrumentos

- ✓ **Cuestionario**: Es el instrumento que se empleara para encuestar a los trabajadores de Inversiones Mayito – Agente BCP, para conocer las ventajas y bondades que tiene la aplicación de hacking ético.
- ✓ **Ficha de información del aplicativo:** Es el instrumento que se manejara para brindar información sobre la aplicación de hacking ético.

3.5. Procedimientos

En primera instancia, tuvimos conocimiento por conocidos, que la Empresa Inversiones Mayito – Agente BCP sufría de constantes pérdidas de dinero, tanto de sus ingresos por la distribución de sus artículos farmacológicos, así como también, por el cobro de los pagos de recibos por diferentes conceptos, tales como agua, luz, teléfono, arbitrios y otros valores y siendo que los encargados de manipular el dinero a través de transferencias conocían las claves de acceso para realizar operaciones importantes de dinero, los propietarios optaron por trasladar determinada cantidad de efectivo cada vez que éste se acumulara en caja, hasta la agencia bancaria más cercana, cantidad que por razones de confidencialidad no se pueden revelar.

En segundo lugar y por tener cierto grado de amistad con los propietarios, nos manifestaron tanto a mi persona como a algunos conocidos, que se encontraban muy preocupados por la constante pérdida de dinero.

Por los motivos anteriormente expuestos, en tercer lugar, solicitaron mis servicios como profesional relacionado con esta disciplina, para lo cual se firmó un acuerdo de confidencialidad, tal como se estipula en todo contrato de informática forense.

En cuarto lugar, se habilitó un equipo básico de pentesting (prueba de penetración), el mismo que tuvo que contar como mínimo con los siguientes elementos:

- ✓ Un módulo hacker con sistema operativo Kali Linux
- ✓ Tres o más módulos víctimas con diferentes sistemas operativos
- ✓ Un Router Wireless para poder atacar al sistema inalámbrico

Para poder implementar esta topología básica sin incurrir en sumas muy onerosas durante la adquisición de hardware, así como también de licencias, se virtualizaron los módulos empleando software de código abierto.

Respecto de las especificaciones tecnológicas, tanto del hardware como del software, se tuvieron en cuenta las siguientes consideraciones:

Del hardware: Una PC o Laptop con un microprocesador Core i7 como mínimo y con una memoria RAM no menor a los 16 Gb.

La tarjeta gráfica tenía que disponer de 4 a 6 Gb; una tarjeta Wifi y un Router que soporte los protocolos WEP, WPA, WPA2, WPA3.

Del software: El sistema operativo de la PC o Laptop puede ser Windows, Linux o MacOS, dependiendo de las habilidades del investigador; un hipervisor o virtualizador, el cual puede ser indistintamente el VirtualBox o el VMWare Workstation Player el cual tiene versiones gratuitas disponibles tanto para Windows como para Linux y para el caso del MacOS se encuentra disponible el VMWare Fusion también en su versión gratuita.

Una vez implementados el hardware y software referidos, se instalaron los módulos virtuales. Ahora, si bien es cierto que Kali Linux es el software preferido por los expertos en esta materia para efectuar los ataques, también es cierto que existen otras distribuciones de muy buena performance respecto de la seguridad de la información.

Una vez instalados los módulos virtuales, se instaló el Kali Linux, descargado de: http://www.kali.org/downloads. En los módulos víctimas, se instalaron las distribuciones de Debian, Centos y Raspbian por ser los más utilizado en la aplicación de diversos tipos de ataque.

Además, debemos advertir que, dentro de este software especializado, existe el conocido ***Metasploitable2***, que es una virtualización del Linux para ser utilizado específicamente como un módulo vulnerable dentro del Laboratorio de Hacking Ético, el mismo que puede ser descargado de https://sourceforge.net/projects/metasploitable/.

Bajo estas circunstancias, nos preguntamos sobre el costo de las licencias de Windows a adquirir, sin embargo, la solución para ello es acudir a proyectos tales como ***Metasploitable3*** y de la misma Microsoft (https://github.com/rapid7/metasploitable3). los cuales nos permitieron y sin costo alguno, obtener módulos o máquinas virtuales de software privado ya activadas con su respectiva licencia, descargadas de: https://developer.microsoft.com/en-us/microsoft

edge/tools/vms/#downloads, y cuya finalidad es la de proveer módulos virtuales a los desarrolladores a efectos de que puedan poner a prueba sus aplicaciones con diversos sistemas operativos y toda la gama de navegadores producidos por Microsoft, asimismo, no existe ningún impedimento legal para trabajarlos con pruebas de penetración.

Por tales motivos, la licencia legalmente otorgada es de carácter temporal (tres meses), sin embargo, si el caso apremia más tiempo, se pueden realizar nuevas exportaciones, tanto de VirtualBox o de VMWare siguiendo siempre las cláusulas descritas en dicho sitio web.

En quinto lugar y luego de haber firmado el contrato de auditoría y confidencialidad, se pasó a la fase 01 de hacking ético o también denominada Fase de Reconocimiento, en esta primera fase, se ilustró al cliente respecto de las pruebas necesarias a realizarse (Anexo), tales como la captura de la Información, en donde se trató de recopilar la máxima cantidad de información sobre el objetivo de la auditoría, toda vez que mientas más abundante haya sido esta, existirá una mayor probabilidad de éxito durante los ataques.

Durante esta fase se tuvieron que efectuar dos tipos de reconocimiento: el ***reconocimiento activo*** y el ***reconocimiento pasivo***.

Respecto del reconocimiento pasivo se procuró conseguir la información pertinente sin interactuar directamente con el objetivo a través del uso de técnicas tales como el escaneo de red, investigación por internet, instalaciones de vigilancia, ingeniería social, etc., para obtener toda la información posible sobre los empleados y las personas con las cuales interactúan, las personas con acceso al objetivo y la disposición de la infraestructura (layout).

El uso de un escáner de red, también denominado ***sniffer***, o analizador de red, de paquetes o protocolos, es un software informático que tiene como función analizar y controlar el tráfico de paquetes en la red de punto a punto en toda la red. El uso de estos escáneres, resultó vital para la obtención de información y son relativamente fáciles de emplear.

En cuanto al reconocimiento activo, este abarcó el análisis de la red para determinar los equipos de manera individual, cuáles son las direcciones IP involucradas, así como el tipo de servicio que prestan. Este procedimiento implicó más riesgo en la detección que el reconocimiento pasivo.

Tanto el reconocimiento activo como el pasivo, nos condujeron a la obtención de información sensible y útil para poder determinar las debilidades o vulnerabilidades que se pudieron encontrar en las redes que se utilizan o gestionan y la efectividad de la protección de su información.

En sexto lugar, se llevó acabo la Fase 02 o Fase de Escaneo

3.6. Método de análisis de datos

Se autorizaron los instrumentos a través del juicio del experto para verificar la confiabilidad de los instrumentos.

Se utilizó el enfoque cuantitativo, en el cual se aplicaron instrumentos antes y después en la variable dependiente. Asimismo, se empleó la hipótesis específica de cada indicador.

Tabla N° 1: Hipótesis del nivel de vulnerabilidad de la red de telecomunicaciones

Indicador	Nivel de vulnerabilidad de la red de telecomunicaciones
H_1: La aplicación de hacking ético mitigará la vulnerabilidad de la red de telecomunicaciones H_0: La aplicación de hacking ético no mitigará la vulnerabilidad de la red de telecomunicaciones.	
Donde: **NVRTa**: Nivel de vulnerabilidad de la red de telecomunicaciones antes de aplicar hacking ético **NVRTd**: Nivel de vulnerabilidad de la red de telecomunicaciones después de aplicar hacking ético	
Hipótesis Nula H_0: Nivel de vulnerabilidad de la red de telecomunicaciones actual es menor o igual que el nivel de vulnerabilidad de la red de telecomunicaciones con el sistema propuesto. $Ho = \mathrm{NVRT}_a - \mathrm{NVRT}_d \leq 0$	
Hipótesis Nula H_1: Nivel de vulnerabilidad de la red de telecomunicaciones actual es diferente o igual que el nivel de vulnerabilidad de la red de telecomunicaciones con el sistema propuesto. $Ho = \mathrm{NVRT}_a - \mathrm{NVRT}_d \neq 0$	

Fuente: Elaboración propia

Tabla N° 2: Hipótesis del nivel de vulnerabilidad de los discos HDD y SSD de la red de telecomunicaciones

Indicador	Nivel de vulnerabilidad de los discos HDD y SSD de la red de telecomunicaciones
H_1: La aplicación de hacking ético mitigará la vulnerabilidad de los discos HDD y SSD de la red de telecomunicaciones H_0: La aplicación de hacking ético no mitigará la vulnerabilidad de los discos HDD y SSD de la red de telecomunicaciones	
Donde: **NVDRTa**: Nivel de vulnerabilidad de los discos HDD y SSD de la red de telecomunicaciones antes de aplicar hacking ético **NVDRTd**: Nivel de vulnerabilidad de los discos HDD y SSD de la red de telecomunicaciones después de aplicar hacking ético	
Hipótesis Nula H_0: Nivel de vulnerabilidad de los discos HDD y SSD de la red de telecomunicaciones actual es menor o igual que el nivel de vulnerabilidad de los discos HDD y SSD de la red de telecomunicaciones con el sistema propuesto. $Ho = \mathrm{NVDRT}_a - \mathrm{NVDRT}_d \leq 0$	
Hipótesis Nula H_1: Nivel de vulnerabilidad de los discos HDD y SSD de la red de telecomunicaciones actual es diferente o igual que el nivel de vulnerabilidad de los discos HDD y SSD de la red de telecomunicaciones con el sistema propuesto. $Ho = \mathrm{NVDRT}_a - \mathrm{NVDRT}_d \neq 0$	

Fuente: Elaboración propia

Tabla N° 3: Hipótesis del nivel de vulnerabilidad de los puertos de la CPU principal de la red de telecomunicaciones

Indicador	Nivel de vulnerabilidad de los puertos de la CPU principal de la red de telecomunicaciones.
H_1: La aplicación de hacking ético mitigará la de vulnerabilidad de los puertos de la CPU principal de la red de telecomunicaciones. H_0: La aplicación de hacking ético no mitigará la de vulnerabilidad de los puertos de la CPU principal de la red de telecomunicaciones.	
Donde: **NVPPRTa**: Nivel de vulnerabilidad de los puertos de la CPU principal de la red de telecomunicaciones **NVPPRTd**: Nivel de vulnerabilidad de los puertos de la CPU principal de la red de telecomunicaciones después de aplicar hacking ético	
Hipótesis Nula H_0: Nivel de vulnerabilidad de los puertos de la CPU principal de la red de telecomunicaciones actual es menor o igual que el nivel de vulnerabilidad de los puertos de la CPU principal de la red de telecomunicaciones $Ho = \text{NVPPRT}_a - \text{NVPPRT}_d \leq 0$	
Hipótesis Nula H_1: Nivel de vulnerabilidad de los puertos de la CPU principal de la red de telecomunicaciones actual es diferente o igual que el nivel de vulnerabilidad de los puertos de la CPU principal de la red de telecomunicaciones con el sistema propuesto. $Ho = \text{NVPPRT}_a - \text{NVPPRT}_d \neq 0$	

Fuente: Elaboración propia

Tabla N° 4: Hipótesis del nivel de capacidad y destreza sobre el manejo del hacking ético del personal que interactúa directamente con la red de telecomunicaciones.

Indicador	Nivel de capacidad y destreza sobre el manejo del hacking ético del personal que interactúa directamente con la red de telecomunicaciones.
H_1: La aplicación de hacking ético incrementará la capacidad y destreza sobre el manejo del hacking ético del personal que interactúa directamente con la red de telecomunicaciones. H_0: La aplicación de hacking ético no incrementará la capacidad y destreza sobre el manejo del hacking ético del personal que interactúa directamente con la red de telecomunicaciones	
Donde: **NCDSMHEa**: Nivel de capacidad y destreza sobre el manejo del hacking ético del personal que interactúa directamente con la red de telecomunicaciones. **NCDSMHEd**: Nivel de capacidad y destreza sobre el manejo del hacking ético del personal que interactúa directamente con la red de telecomunicaciones después de aplicar hacking ético	
Hipótesis Nula H_0: Nivel de capacidad y destreza sobre el manejo del hacking ético del personal que interactúa directamente con la red de telecomunicaciones actual es menor o igual que el de capacidad y destreza sobre el manejo del hacking ético del personal que interactúa directamente con la red de telecomunicaciones. $Ho = \text{NCDSMHE}_a - \text{NCDSMHE}_d \leq 0$	
Hipótesis Nula H_1: Nivel de capacidad y destreza sobre el manejo del hacking ético del personal que interactúa directamente con la red de telecomunicaciones actual es diferente o igual que el nivel e capacidad y	

destreza sobre el manejo del hacking ético del personal que interactúa directamente con la red de telecomunicaciones con el sistema propuesto. $Ho = \text{NCDSMHE}_a - \text{NCDSMHE}_d \neq 0$

Fuente: Elaboración propia

Se mencionan la prueba de normalidad de KOLMOGOROV SMIRNOV, en el cual se utiliza para poblaciones superiores a 35, asimismo es una prueba no paramétrica de wilconxon. Además, se tiene la prueba de SHAPIRO WILK, que se utiliza para poblaciones inferiores de 35 y las cuales son pruebas paramétricas. Toda prueba de normalidad se desarrolló con el software SPSS IBM versión 25.

3.7. Aspectos éticos

Para la ejecución de la presente investigación, se consideraron 04 (cuatro) fuentes para los aspectos éticos, a saber:

- ✓ El código de ética para la investigación, propio de la UCV
- ✓ El código de ética establecido internacional y específicamente para el Hacking Ético
- ✓ Las buenas prácticas ético profesionales establecidas en las normas ISO 27000, 27001 y 27002, respectivamente, y,
- ✓ El código de ética para las Ingenierías (IEEE)

Según Kerberos (2015), el proyecto de investigación forense que nos ocupa, se rige por un diseño muy riguroso respecto de su metodología, ya que el Hacking Ético se ciñe a los códigos de ética y estándares mundiales de investigación informática forense, lo que implica proteger al extremo la confidencialidad con el cliente a auditar, debido más que todo, al alto grado de vulnerabilidad al que puede estar expuesto. Asimismo, y para tener una mejor noción de los parámetros a los que está sometida esta disciplina informática, debemos mencionar a instituciones tales como el American College of Forensic Examiners Institute y el High Technology Crime Investigation Assosiation (HTCIA), las cuales son dos entidades de las más

reconocidas a nivel mundial y en donde el experto en informática forense encuentra todos los códigos y estatutos de ética pertinentes establecidos para los aspectos técnicos, así como toda la normatividad legal vigente para poder ejecutar sus funciones como un especialista certificado en esta área.

De manera paralela establece, por ejemplo, que el auditor no debe tener ningún parentesco o interés personal específico con el auditado respecto de los resultados de la pericia practicada, ya sean éstos de índole económico o por alguna otra relación preexistente con el (los) investigados. Asimismo, el profesional en esta área, debe mantener siempre una posición imparcial en relación al caso a resolver y ser muy formal y veraz en cuanto al informe a elevar. Esta posición debe llevar siempre al informático forense a hablar solo con la verdad, aunque esta no sea del agrado de las partes y puedan contribuir a que, de ser el caso llevado en una corte, contribuya a que los magistrados tengan una referencia objetiva, lo cual conllevará a una buena toma de decisiones durante la audiencia y siempre apegados al debido proceso y mejor aplicación de la ley.

Conforme al progreso de la actual investigación se respetaron todas las observaciones establecidas por la Universidad, tomando los aspectos éticos con fundamentos teóricos y las pertinentes referencias bibliográficas bajo la norma ISO 690, respetando las citas respectivas con contenidos obtenidos totalmente veraces, puntuales e inteligibles.

La investigación presenta una importante implicancia en la sociedad por tener una ponderación de carácter benéfico, con rigor científico, que aumenta la seguridad y calidad de vida de los usuarios en general y beneficia particularmente en las circunstancias actuales a la empresa en estudio.

IV. RESULTADOS

- ✓ **Análisis descriptivo: Indicador nivel de vulnerabilidad de la red de telecomunicaciones.**

Se realizó una aplicación de hacking ético para conocer la vulnerabilidad de la red de telecomunicaciones en la empresa Inversiones Mayito – Agente BCP, en el cual se tiene el método de pretest para conocer la situación actual del negocio sobre el nivel de vulnerabilidad de la red de telecomunicaciones, luego se aplicó la aplicación de hacking ético el método del postest, en donde se evalúa el nivel de vulnerabilidad obteniendo información favorable para el negocio.

Tabla N° 5: Análisis descriptivo del nivel de vulnerabilidad de la red de telecomunicaciones

Estadísticos descriptivos					
	N	Mínimo	Máximo	Suma	Media
NVRTa	6	8	12	56	9,33
NVRTd	6	1	2	9	1,50
N válido (por lista)	6				

Fuente: Elaboración propia

En la tabla 5, se tiene N, los días de la semana, además se tiene la cantidad del pretest que es un mínimo de 8 ataques y el máximo de 12 ataques por semana, además se tiene la sumatoria y el promedio de 9.33. En el método del postest se tiene un mínimo de 1 y un máximo de 2 ataques, en el cual se ve representado en una media de 1.50 ataques a la semana.

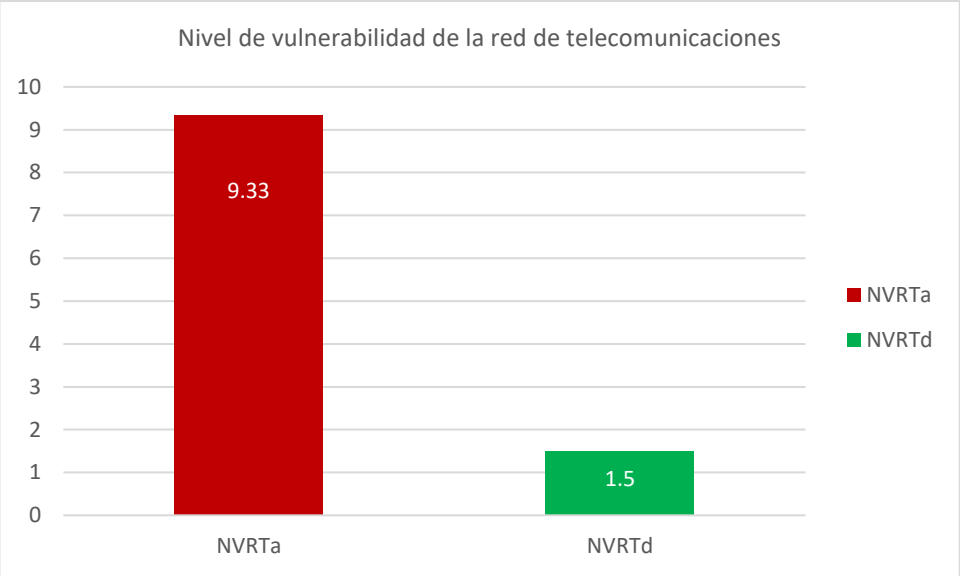


Gráfico N° 1: Comparativa del Indicador 01

Fuente: Elaboración propia

Como se observa en el grafico 1, se tiene el pretest de 9.33 ataques antes de la aplicación de hacking ético, y mediante la implementación se logró un postest de 1.50 ataques. Entonces se revela que existe una diferencia antes y después de la aplicación de hacking ético.

- ✓ **Análisis Inferencial del nivel de vulnerabilidad de la red de telecomunicaciones.**

  Se realizó la prueba de normalidad para el nivel de vulnerabilidad de la red de telecomunicaciones, en el cual su población es menor a 35, de esta manera se trabajó con Shapiro – Wilk. además, es una prueba paramétrica, se realizó en el software SPSS IBM y se tiene un nivel de confianza del 95%.

Tabla N° 6: Prueba de normalidad del indicador I

Pruebas de normalidad						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
NVRTa	,254	6	,200*	,866	6	,212
NVRTd	,319	6	,056	,683	6	,004

Fuente: Elaboración propia

Como se observa en la tabla 6, una población de 6 (gl), se aplicó la prueba de Shapiro Wilk, en el cual se tiene una diferencia (Sig) = 0.212 que es superior a 0.05, lo cual significa que los datos tienen una distribución normal. Asimismo, se trabajó la prueba paramétrica de T-Student para la validación de la hipótesis.

- ✓ **Prueba de hipótesis del nivel de vulnerabilidad de la red de telecomunicaciones**

Tabla N° 7: Prueba de hipótesis del indicador I

Indicador	Nivel de vulnerabilidad de la red de telecomunicaciones
H_1: La aplicación de hacking ético mitigará la vulnerabilidad de la red de telecomunicaciones H_0: La aplicación de hacking ético no mitigará la vulnerabilidad de la red de telecomunicaciones.	
Donde: **NVRTa**: Nivel de vulnerabilidad de la red de telecomunicaciones antes de aplicar hacking ético	

NVRTd: Nivel de vulnerabilidad de la red de telecomunicaciones después de aplicar hacking ético
Hipótesis Nula H_0: Nivel de vulnerabilidad de la red de telecomunicaciones actual es menor o igual que el nivel de vulnerabilidad de la red de telecomunicaciones con el sistema propuesto. $$Ho = \mathrm{NVRT}_a - \mathrm{NVRT}_d \leq 0$$
Hipótesis Nula H_1: Nivel de vulnerabilidad de la red de telecomunicaciones actual es diferente o igual que el nivel de vulnerabilidad de la red de telecomunicaciones con el sistema propuesto. $$Ho = \mathrm{NVRT}_a - \mathrm{NVRT}_d \neq 0$$

Fuente: Elaboración propia

Se manejaron los siguientes valores:

- ✓ Nivel de confianza = 95%.
- ✓ Nivel de error = 5%.
- ✓ Se utilizo la prueba T-Student.

Tabla N° 8: Correlaciones de muestras emparejadas del indicador I

Correlaciones de muestras emparejadas				
		N	Correlación	Sig.
Par 1	NVRTa & NVRTd	6	,000	1,000

Fuente: Elaboración propia

Tabla N° 9: Prueba de muestras emparejadas del indicador I

Prueba de muestras emparejadas									
		Diferencias emparejadas					t	gl	Sig. (bilateral)
		Media	Desviación estándar	Media de error estándar	95% de intervalo de confianza de la diferencia				
					Inferior	Superior			
Par 1	NVRTa - NVRTd	7,833	1,602	,654	6,152	9,515	11,977	5	,000

Fuente: Elaboración propia

La Sig (bilateral) es 0.00, debido a que es menor a 0.05, entonces se concluye que la hipótesis alterna con 95% de nivel de confianza $\boldsymbol{Ha = NVRT_a - NVRT_d \neq 0;}$ existe una diferencia; de tal manera se rechaza la Hipótesis Nula y se acepta la Hipótesis Alterna.

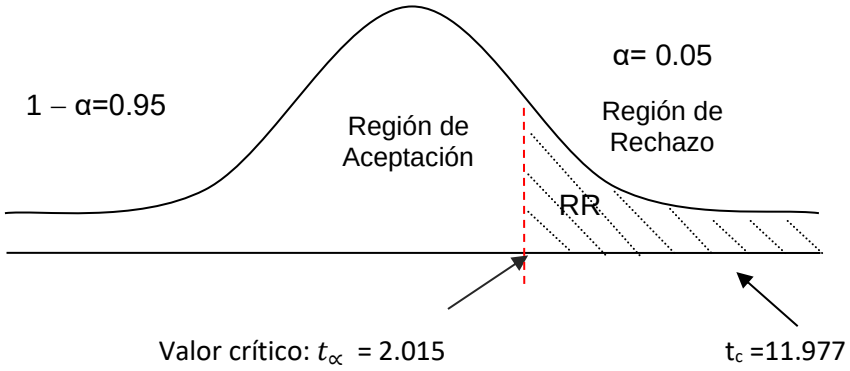


Figura N° 3: Aceptación de la hipótesis del indicador I

Fuente: Elaboración propia

- ✓ **Análisis descriptivo: Indicador nivel de vulnerabilidad de los discos HDD y SSD de la red de telecomunicaciones.**

Se realizó una aplicación de hacking ético para conocer la vulnerabilidad de los discos HDD y SSD de la red de telecomunicaciones en la empresa Inversiones Mayito – Agente BCP, en el cual se tiene el método de pretest para conocer la situación actual del negocio sobre el nivel de de vulnerabilidad de los discos HDD y SSD de la red de telecomunicaciones, luego se ejecutó la aplicación de hacking ético con el método del postest, en donde se evalúa el nivel de de vulnerabilidad de los discos HDD y SSD de la red de telecomunicaciones obteniendo información favorable para el negocio.

Tabla N° 10: Análisis descriptivo del nivel de vulnerabilidad de los discos HDD y SSD de la red de telecomunicaciones

Estadísticos descriptivos					
	N	Mínimo	Máximo	Suma	Media
NVDRTa	6	3	5	22	3,67
NVDRTd	6	0	1	3	,50
N válido (por lista)	6				

Fuente: Elaboración propia

En la tabla 10, se tiene N, los días de la semana, además se tiene la cantidad del pretest que es un mínimo de 3 y el máximo de 5 caídas de discos por semana, además se tiene la sumatoria y el promedio de 3.67 caídas de los discos En el método del postest se tiene un mínimo de 0 y un máximo de 1 caídas de los discos HDD, en el cual se ve representado en una media de 0.50 fallas del disco a la semana.

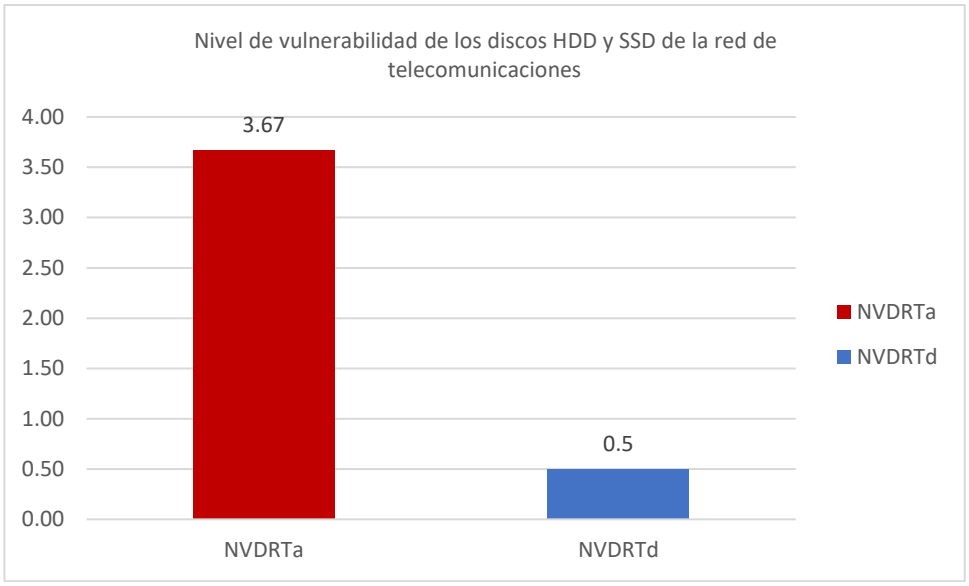


Gráfico N° 2: Comparativa del Indicador II

Fuente: Elaboración propia

Como se observa en el grafico 2, se tiene el pretest de 3.67 infecciones de disco duro antes de la aplicación de hacking ético, y mediante la implementación se logró un postest de 0.50 infecciones. Entonces se aprecia que existe una diferencia entre el antes y después de la aplicación de hacking ético.

- ✓ **Análisis Inferencial del nivel de vulnerabilidad de los discos HDD y SSD de la red de telecomunicaciones.**

  Se realizó la prueba de normalidad para el nivel de vulnerabilidad de los discos HDD y SSD de la red de telecomunicaciones, en el cual su población es menor a 35, de esta manera se trabajó con Shapiro – Wilk. además, es una prueba paramétrica, se realizó en el software SPSS IBM y se tiene un nivel de confianza del 95%.

Tabla N° 11: Prueba de normalidad del indicador II

Pruebas de normalidad						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
NVDRTa	,293	6	,117	,822	6	,091
NVDRTd	,319	6	,056	,683	6	,004

Fuente: Elaboración propia

Como se observa en la tabla 11, una población de 6 (gl), se aplicó la prueba de Shapiro Wilk, en el cual se tiene una diferencia (Sig) = 0.091 que es superior a 0.05, lo cual significa que los datos tienen una distribución normal. Asimismo, se trabajó la prueba paramétrica de T-Student para la validación de la hipótesis.

- ✓ **Prueba de Hipótesis del nivel de vulnerabilidad de los discos HDD y SSD de la red de telecomunicaciones.**

Tabla N° 12: Prueba de hipótesis del indicador II

Indicador	Nivel de vulnerabilidad de los discos HDD y SSD de la red de telecomunicaciones
H_1: La aplicación de hacking ético mitigará la vulnerabilidad de los discos HDD y SSD de la red de telecomunicaciones H_0: La aplicación de hacking ético no mitigará la vulnerabilidad de los discos HDD y SSD de la red de telecomunicaciones	
Donde: **NVDRTa**: Nivel de vulnerabilidad de los discos HDD y SSD de la red de telecomunicaciones antes de aplicar hacking ético **NVDRTd**: Nivel de vulnerabilidad de los discos HDD y SSD de la red de telecomunicaciones después de aplicar hacking ético	
Hipótesis Nula H_0: Nivel de vulnerabilidad de los discos HDD y SSD de la red de telecomunicaciones actual es menor o igual que el nivel de vulnerabilidad de los discos HDD y SSD de la red de telecomunicaciones con el sistema propuesto. $Ho = \mathrm{NVDRT}_a - \mathrm{NVDRT}_d \leq 0$	
Hipótesis Nula H_1: Nivel de vulnerabilidad de los discos HDD y SSD de la red de telecomunicaciones actual es diferente o igual que el nivel de vulnerabilidad de los discos HDD y SSD de la red de telecomunicaciones con el sistema propuesto. $Ho = \mathrm{NVDRT}_a - \mathrm{NVDRT}_d \neq 0$	

Fuente: Elaboración propia

Se manejaron los siguientes valores:

- ✓ Nivel de confianza = 95%.
- ✓ Nivel de error = 5%.
- ✓ Se utilizo la prueba T-Student.

Tabla N° 13: Correlaciones de muestras emparejadas del indicador II

Correlaciones de muestras emparejadas				
		N	Correlación	Sig.
Par 1	NVDRTa & NVDRTd	6	-,447	,374

Fuente: Elaboración propia

Tabla N° 14: prueba de muestras emparejadas del indicador II

Prueba de muestras emparejadas									
		Diferencias emparejadas					t	gl	Sig. (bilateral)
		Media	Desviación estándar	Media de error estándar	95% de intervalo de confianza de la diferencia				
					Inferior	Superior			
Par 1	NVDRTa - NVDRTd	3,167	1,169	,477	1,940	4,394	6,635	5	,000

Fuente: Elaboración propia

La Sig (bilateral) es 0.00, debido a que es menor a 0.05, entonces se concluye que la hipótesis alterna con 95% de nivel de confianza $\boldsymbol{Ha = NVDRT_a - NVDRT_d \neq 0}$**;** existe una diferencia; de tal manera se rechaza la Hipótesis Nula y se acepta la Hipótesis Alterna.

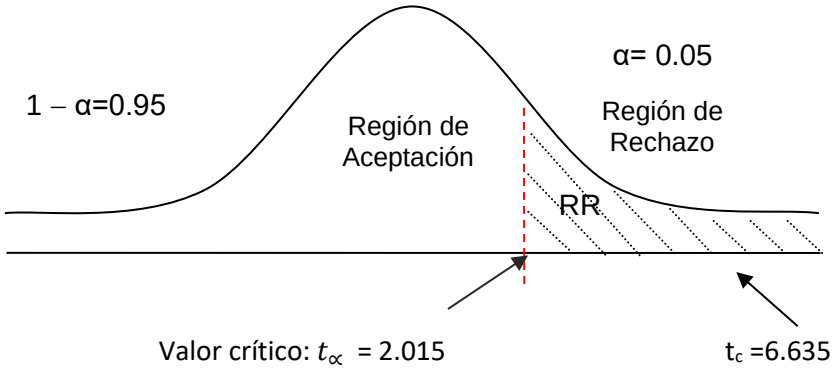


Figura N° 4: Aceptación de la hipótesis del indicador II

Fuente: Elaboración propia

- ✓ **Análisis descriptivo: Indicador nivel de vulnerabilidad de los puertos de la CPU principal de la red de telecomunicaciones.**

Se realizó una aplicación de hacking ético para conocer la vulnerabilidad de los puertos de la CPU principal de la red de telecomunicaciones en la empresa Inversiones Mayito – Agente BCP, en el cual se tiene el método de pretest para conocer la situación actual del negocio sobre el nivel de de vulnerabilidad de los puertos de la CPU principal de la red de telecomunicaciones, luego se aplicó la aplicación de hacking ético el método del postest, en donde se avalúa el nivel de de vulnerabilidad de los puertos de la CPU principal de la red de telecomunicaciones obteniendo información favorable para el negocio.

Tabla N° 15: Análisis descriptivo del nivel de vulnerabilidad de los puertos de la CPU principal de la red de telecomunicaciones

Estadísticos descriptivos					
	N	Mínimo	Máximo	Suma	Media
NVPPRTa	6	3	5	24	4,00
NVPPTd	6	0	1	4	,67
N válido (por lista)	6				

Fuente: Elaboración propia

En la tabla 15, se tiene N, los días de la semana, además se tiene la cantidad del pretest que es un mínimo de 3 y el máximo de 5 fallas de los puertos a la semana, además se tiene la sumatoria y el promedio de 4.00 fallas. En el método del postest se tiene un mínimo de 0 y un máximo de 1 fallas de los puertos, en el cual se ve representado en una media de 0.67 fallas de los puertos a la semana.

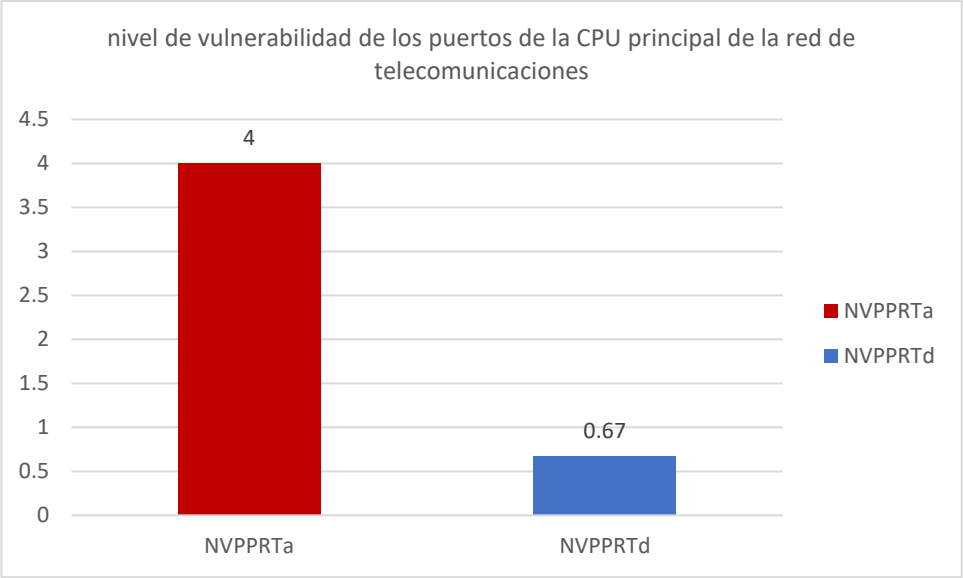


Gráfico N° 3: Comparativa del Indicador III

Fuente: Elaboración propia

Como se observa en el grafico 3, se tiene el pretest de 4 fallas de los puertos de red antes de la aplicación de hacking ético, y mediante la implementación se logró un postest de 0.67 fallas. Entonces se revela que existe una diferencia antes y después de la aplicación de hacking ético.

- ✓ **Análisis Inferencial del nivel de vulnerabilidad de los puertos de la CPU principal de la red de telecomunicaciones.**

  Se realizó la prueba de normalidad para el nivel de vulnerabilidad de los puertos de la CPU principal de la red de telecomunicaciones, en el cual su población es menor a 35, de esta manera se trabajó con Shapiro – Wilk. además, es una prueba paramétrica, se realizó en el software SPSS IBM y se tiene un nivel de confianza del 95%.

Tabla N° 16: Prueba de normalidad del indicador III

Pruebas de normalidad						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
NVPPRTa	,202	6	,200*	,853	6	,167
NVPPTd	,407	6	,002	,640	6	,001
*. Esto es un límite inferior de la significación verdadera.						
a. Corrección de significación de Lilliefors						

Fuente: Elaboración propia

Como se observa en la tabla 16, una población de 6 (gl), se aplicó la prueba de Shapiro Wilk, en el cual se tiene una diferencia (Sig) = 0.167 que es superior a 0.05, lo cual significa que los datos tienen una distribución normal. Asimismo, se trabajó la prueba paramétrica de T-Student para la validación de la hipótesis.

- ✓ **Prueba de hipótesis del nivel de vulnerabilidad de los puertos de la CPU principal de la red de telecomunicaciones.**

Tabla N° 17: Prueba de hipótesis del indicador III

Indicador	Nivel de vulnerabilidad de los puertos de la CPU principal de la red de telecomunicaciones.
H_1: La aplicación de hacking ético mitigará la de vulnerabilidad de los puertos de la CPU principal de la red de telecomunicaciones. H_0: La aplicación de hacking ético no mitigará la de vulnerabilidad de los puertos de la CPU principal de la red de telecomunicaciones.	
Donde: **NVPPRTa**: Nivel de vulnerabilidad de los puertos de la CPU principal de la red de telecomunicaciones **NVPPRTd**: Nivel de vulnerabilidad de los puertos de la CPU principal de la red de telecomunicaciones después de aplicar hacking ético	
Hipótesis Nula H_0: Nivel de vulnerabilidad de los puertos de la CPU principal de la red de telecomunicaciones actual es menor o igual que el nivel de vulnerabilidad de los puertos de la CPU principal de la red de telecomunicaciones $Ho = \mathrm{NVPPRT}_a - \mathrm{NVPPRT}_d \leq 0$	
Hipótesis Nula H_1: Nivel de vulnerabilidad de los puertos de la CPU principal de la red de telecomunicaciones actual es diferente o igual que el nivel de vulnerabilidad de los puertos de la CPU principal de la red de telecomunicaciones con el sistema propuesto. $Ho = \mathrm{NVPPRT}_a - \mathrm{NVPPRT}_d \neq 0$	

Fuente: Elaboración propia

Se manejaron los siguientes valores:

- ✓ Nivel de confianza = 95%.
- ✓ Nivel de error = 5%.
- ✓ Se utilizo la prueba T-Student.

Tabla N° 18: Correlaciones de muestras emparejadas del indicador III

Correlaciones de muestras emparejadas				
		N	Correlación	Sig.
Par 1	NVPPRTa & NVPPTd	6	,866	,026

Fuente: Elaboración propia

Tabla N° 19: prueba de muestras emparejadas del indicador III

Prueba de muestras emparejadas									
		Diferencias emparejadas					t	gl	Sig. (bilateral)
		Media	Desviación estándar	Media de error estándar	95% de intervalo de confianza de la diferencia				
					Inferior	Superior			
Par 1	NVPPRTa - NVPPTd	3,333	,516	,211	2,791	3,875	15,811	5	,000

Fuente: Elaboración propia

La Sig (bilateral) es 0.00, debido a que es menor a 0.05, entonces se concluye que la hipótesis alterna con 95% de nivel de confianza $\boldsymbol{Ha = NVPPRT_a - NVPPRT_d \neq 0}$**;** existe una diferencia; de tal manera se rechaza la Hipótesis Nula y se acepta la Hipótesis Alterna.

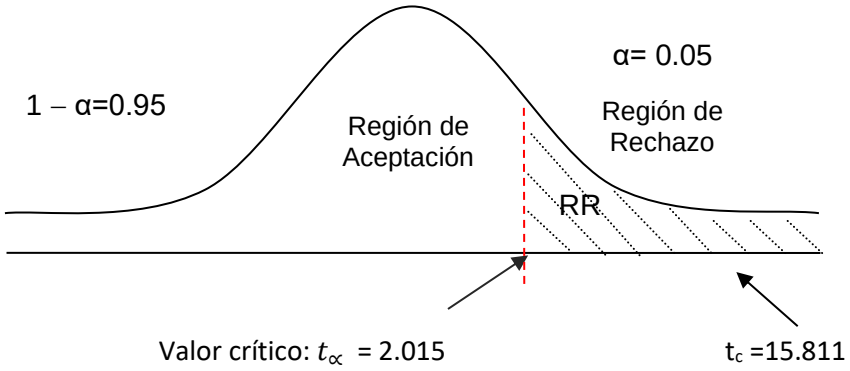


Figura N° 5: Aceptación de la hipótesis del indicador III

Fuente: Elaboración propia

- ✓ **Análisis descriptivo: Indicador nivel de capacidad y destreza sobre el manejo del hacking ético del personal que interactúa directamente con la red de telecomunicaciones.**

  Se realizó una aplicación de hacking ético para conocer el nivel de capacidad y destreza sobre el manejo del hacking ético del personal que interactúa directamente con la red de telecomunicaciones en la empresa Inversiones Mayito – Agente BCP, en el cual se tiene el método de pretest para conocer la situación actual del negocio sobre el nivel de capacidad y destreza sobre el manejo del hacking ético del personal que interactúa directamente con la red de telecomunicaciones, luego se aplicó la aplicación de hacking ético el método del postest, en donde se avalúa el nivel de capacidad y destreza sobre el manejo del hacking ético del personal que interactúa directamente con la red de telecomunicaciones.

Tabla N° 20: Análisis descriptivo del nivel de capacidad y destreza sobre el manejo del hacking ético del personal que interactúa directamente con la red de telecomunicaciones

Estadísticos descriptivos					
	N	Mínimo	Máximo	Suma	Media
NCDMHEa	5	1,83	2,00	9,49	1,8980
NCDMHEd	5	4,17	5,00	23,33	4,6660
N válido (por lista)	5				

Fuente: Elaboración propia

En la tabla 20, se tiene N, la cantidad de preguntas, además se tiene el puntaje mínimo de 1.83 y el puntaje máximo de 2, además se tiene la sumatoria y el promedio de 1.89 puntos. En el método del postest se tiene un puntaje mínimo de 0 y un máximo de 5 puntos, en el cual se ve representado en una media de 4.6660 puntos.

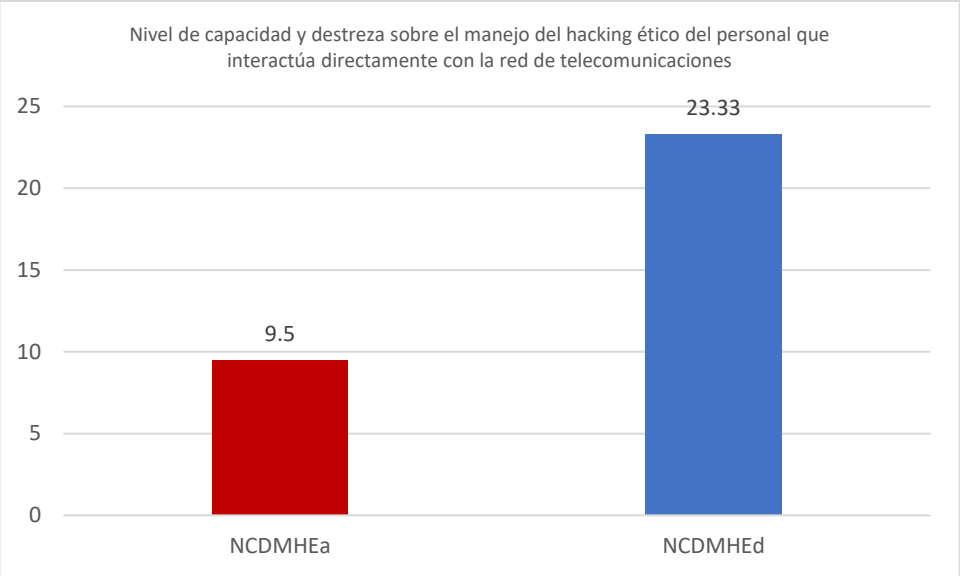


Gráfico N° 4: Comparativa del Indicador IV

Fuente: Elaboración propia

Como se observa en el grafico 4, se tiene el pretest de 9.5 puntos y mediante la implementación se logró un postest de 23.33 puntos. Entonces se revela que existe una diferencia antes y después de la aplicación de hacking ético.

- ✓ **Análisis Inferencial del nivel de capacidad y destreza sobre el manejo del hacking ético del personal que interactúa directamente con la red de telecomunicaciones.**

  Se realizó la prueba de normalidad para el nivel de capacidad y destreza sobre el manejo del hacking ético del personal que interactúa directamente con la red de telecomunicaciones, en el cual su población es menor a 35, de esta manera se trabajó con Shapiro – Wilk. además, es una prueba paramétrica, se realizó en el software SPSS IBM y se tiene un nivel de confianza del 95%.

Tabla N° 21: Prueba de normalidad del indicador IV

Pruebas de normalidad						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
NCDMHEa	,367	5	,026	,684	5	,006
NCDMHEd	,263	5	,200*	,836	5	,153
*. Esto es un límite inferior de la significación verdadera.						
a. Corrección de significación de Lilliefors						

Fuente: Elaboración propia

Como se observa en la tabla 21, una población de 5 (gl), se aplicó la prueba de Shapiro Wilk, en el cual se tiene una diferencia (Sig) = 0.153 que es superior a 0.05, lo cual significa que los datos tienen una distribución normal. Asimismo, se trabajó la prueba paramétrica de T-Student para la validación de la hipótesis.

- ✓ **Prueba de hipótesis del nivel de capacidad y destreza sobre el manejo del hacking ético del personal que interactúa directamente con la red de telecomunicaciones.**

Tabla N° 22: Prueba de hipótesis del indicador IV

Indicador	Nivel de capacidad y destreza sobre el manejo del hacking ético del personal que interactúa directamente con la red de telecomunicaciones.
H_1: La aplicación de hacking ético mitigará la capacidad y destreza sobre el manejo del hacking ético del personal que interactúa directamente con la red de telecomunicaciones. H_0: La aplicación de hacking ético no mitigará la capacidad y destreza sobre el manejo del hacking ético del personal que interactúa directamente con la red de telecomunicaciones	
Donde: **NCDSMHEa**: Nivel de capacidad y destreza sobre el manejo del hacking ético del personal que interactúa directamente con la red de telecomunicaciones. **NCDSMHEd**: Nivel de capacidad y destreza sobre el manejo del hacking ético del personal que interactúa directamente con la red de telecomunicaciones después de aplicar hacking ético	
Hipótesis Nula H_0: Nivel de capacidad y destreza sobre el manejo del hacking ético del personal que interactúa directamente con la red de telecomunicaciones actual es menor o igual que el de capacidad y destreza sobre el manejo del hacking ético del personal que interactúa directamente con la red de telecomunicaciones. $Ho = \text{NCDSMHE}_a - \text{NCDSMHE}_d \leq 0$	

Hipótesis Nula H_1: Nivel de capacidad y destreza sobre el manejo del hacking ético del personal que interactúa directamente con la red de telecomunicaciones actual es diferente o igual que el nivel e capacidad y destreza sobre el manejo del hacking ético del personal que interactúa directamente con la red de telecomunicaciones con el sistema propuesto.

$$Ho = \text{NCDSMHE}_a - \text{NCDSMHE}_d \neq 0$$

Fuente: Elaboración propia del Autor

Se manejaron los siguientes valores:

- ✓ Nivel de confianza = 95%.
- ✓ Nivel de error = 5%.
- ✓ Se utilizo la prueba T-Student.

Tabla N° 23: Correlaciones de muestras emparejadas del indicador IV

Correlaciones de muestras emparejadas				
		N	Correlación	Sig.
Par 1	NCDMHEa & NCDMHEd	5	-,190	,760

Fuente: Elaboración propia

Tabla N° 24: prueba de muestras emparejadas del indicador IV

Prueba de muestras emparejadas									
		Diferencias emparejadas					t	gl	Sig. (bilateral)
		Media	Desviación estándar	Media de error estándar	95% de intervalo de confianza de la diferencia				
					Inferior	Superior			
Par 1	NCDMHEa - NCDMHEd	-2,76800	,41794	,18691	-3,28694	-2,24906	-14,810	4	,000

Fuente: Elaboración propia

La Sig (bilateral) es 0.00, debido a que es menor a 0.05, entonces se concluye que la hipótesis alterna con 95% de nivel de confianza $\boldsymbol{Ha = NCDMHE_a - NCDMHE_d \neq 0}$**;** existe una diferencia; de tal manera se rechaza la Hipótesis Nula y se acepta la Hipótesis Alterna.

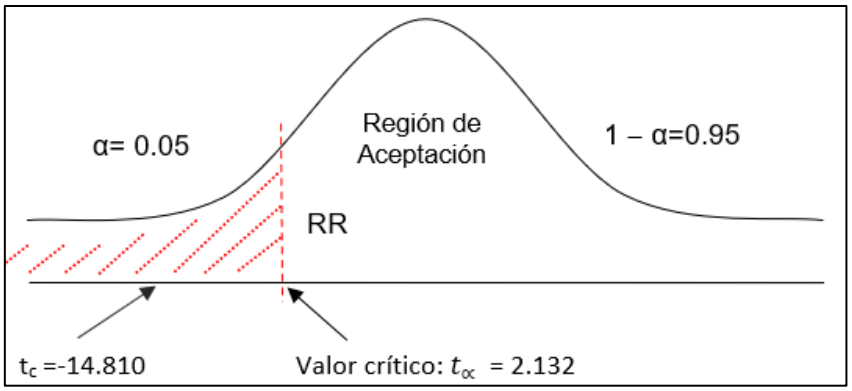


Figura N° 6: Aceptación de la hipótesis del indicador IV

Fuente: Elaboración propia

ASESOR ESPECIALISTA:

Mg. Ing. Humberto Pedro Jiménez Jara
CIP. 171931 - Ing. Sistemas
Docente Asesor

V. DISCUSIÓN

Tal y como se citó en la parte introductoria del presente trabajo de investigación, a medida que avanza la tecnología, también lo hace la ciberdelincuencia.

Ya se han detallado previamente los casos muy sonados de grandes empresas como el Banco de Crédito del Perú y el Banco de Chile en Sudamérica y otros gigantes corporativos de renombre mundial, tales como PlayStation de Sony, Alibabá.com y recientemente el Cineplanet durante este año 2020, solo por citar algunos, los mismos que han reportado millonarias pérdidas, muchas veces en cuestiones de horas o minutos, debido a “un agujero” encontrado por algún ciberdelincuente en sus sistemas financieros o mercantiles.

En estos casos, los activos” preferidos” por los atacantes son las bases de datos de los clientes, la sustracción de sus identidades digitales, sus números de cuentas bancarias y obviamente sus contraseñas personales.

Es imperativo resaltar que toda esta andanada de ataques a estas grandes empresas ha tenido un crecimiento exponencial debido a la Pandemia del Covid-19, toda vez que el consabido confinamiento, ha obligado a muchos usuarios a utilizar mucho más a menudo sus cuentas bancarias por internet para las compras delivery.

Es por ello que las modalidades más empleadas en estos tiempos, han sido el ***pishing*** y el ***ransomware***. El nombre del primero deriva del vocablo “pescar” en inglés, mientras que el segundo significa literalmente “secuestro de datos”.

Con el ***pishing*** se intenta sorprender a los usuarios con páginas web falsificadas, con la finalidad de que estos introduzcan sus datos personales y financieros, especialmente sus códigos de usuario, contraseñas y números de tarjetas de crédito o débito, las mismas que son capturadas por los malhechores con la evidente finalidad de hacerse del dinero ajeno de manera rápida y fácil.

Por otro lado, y esto es mucho más peligroso, el ataque con ***ransomware***, el cual persigue: ***capturar y secuestrar los datos***, ya sean estos personales o de bases de datos de corporaciones que manejan ingentes cantidades de dinero por tener muchos clientes o afiliados.

De esta manera, la víctima o víctimas, quedan totalmente inhabilitadas para realizar sus operaciones o transacciones financieras o comerciales. La mecánica que usa este tipo de delito es la de “capturar los datos con un cifrado de tipo militar” (se le llama así por su alto grado de seguridad y complejidad), para de esta manera, lograr que las víctimas paguen un “rescate” por la liberación de su información.

Antes de proseguir en el desarrollo de esta discusión, debemos aclarar que, y hasta la fecha, no se puede decir que exista un sistema informático “ciento por ciento seguro”, eso no se da, no existe y es por ello que la actualización de la seguridad informática es muy imprescindible en estos tiempos de vertiginoso desarrollo tecnológico.

Asimismo, muchos de los casos sobre fraudes informáticos o ataque a las vulnerabilidades de corporaciones de renombre, nunca son denunciados, por temor al escándalo, desprestigio o alguna fuga masiva de clientes o accionistas, por lo que las estadísticas que nos muestran los medios a nivel mundial, son ***solo referenciales***, hay que tener en cuenta ese aspecto.

Cabe resaltar la gran utilidad que representan las contraseñas cifradas o hash, ya que son contraseñas muy difíciles de romper y es bastante difícil que los softwares que se emplean con esta finalidad puedan vulnerar su seguridad. Claro que siempre existirá la posibilidad de que se pueda quebrantar esta protección, sin embargo, el tiempo que demorará en descifrar la contraseña, el cual puede tardar semanas o hasta uno o dos meses, ahuyentarán a los atacantes de proseguir con este propósito.

Los hash o funciones de resumen son algoritmos que consiguen crear a partir de una entrada (ya sea un texto, una contraseña o un archivo, por ejemplo), una salida alfanumérica de longitud normalmente fija que representa un resumen de toda la información que se le ha dado (es decir,

a partir de los datos de la entrada crea una cadena que solo puede volverse a crear con esos mismos datos).

Estas funciones no tienen el mismo propósito que la criptografía simétrica y asimétrica, tiene varios cometidos, entre ellos está asegurar que no se ha modificado un archivo en una transmisión, hacer ilegible una contraseña o firmar digitalmente un documento.

En definitiva, las funciones hash se encargan de representar de forma compacta un archivo o conjunto de datos que normalmente es de mayor tamaño que el hash independientemente del propósito de su uso.

Este sistema de criptografía usa algoritmos que aseguran que con la respuesta (o hash), nunca se podrá saber cuáles han sido los datos insertados, lo que indica que es una función unidireccional. Sabiendo que se puede generar cualquier resumen a partir de cualquier dato nos podemos preguntar si se podrían repetir estos resúmenes (hash) y la respuesta es que teóricamente si, podría haber colisiones, ya que no es fácil tener una función hash perfecta (que consiga que no se repita la respuesta), pero esto no supone un problema, ya que si se consiguieran (con un buen algoritmo), dos hashes iguales los contenidos serían totalmente distintos.

Las funciones hash son muy usadas, una de las utilidades que tiene es proteger la confidencialidad de una contraseña, ya que podría estar en texto plano y ser accesible por cualquiera y aun así no poder ser capaces de deducirla. En este caso, para saber si una contraseña que está guardada, por ejemplo, en una base de datos es igual a la que hemos introducido no se descifra el hash (ya que debería de ser imposible hacerlo), sino que se aplicará la misma función de resumen a la contraseña que especificamos y se comparará el resultado con el que tenemos guardado (como se hace con las contraseñas de los sistemas Linux).

Otro uso que tiene esta función es la de garantizar la integridad de los datos y es algo que se ha visto muchas veces en algunas webs que proporcionan descargas de archivos grandes, por ejemplo de softwares, dando junto a su vez el resumen del archivo y la función usada.

Por citar un ejemplo, en la página de descarga de Virtual Box podemos encontrar esta página con todos los resúmenes de las descargas disponibles con los que podemos comprobar que el archivo se ha descargado correctamente y que nadie ha modificado su contenido durante la transmisión.
Para poner en práctica este uso, se coge esta imagen en HTML5 y se le aplica una función de resumen con el algoritmo MD5.

Respecto del trabajo de investigación que nos ocupa, el mismo que está referido a la seguridad de la red de telecomunicaciones de la sucursal de una agencia bancaria, la misma que ha sufrido pérdidas considerables de dinero, al parecer por cuestiones de vulnerabilidades en su sistema informático, se ha tenido a bien investigar las presuntas debilidades en sus sistemas informáticos a nivel de: red inalámbrica (Wifi), discos duros y sólidos (HDD y SSD), puertos de conexión y capacidades y destrezas de los trabajadores involucrados en el manejo de los sistemas informáticos.

En el primer indicador, nivel de vulnerabilidad de la red de telecomunicaciones actual es de 9.33 ataques por semana (detectados con pruebas de penetración o pentesting utilizando las herramientas de Wifislax, Linset y OpenVAS con una frecuencia de tres veces diarias durante seis días), mientras que luego de la ejecución de la aplicación del hacking ético, ésta arroja como resultado 1.5 ataques a la semana, lo que significa una reducción del 83.93 % de vulnerabilidad a la red de telecomunicaciones. Al respecto, Shebli y Beheshti reportan lo siguiente sobre la vulnerabilidad a las redes y las pruebas de penetración: “La información es más vulnerable que nunca; y cada avance tecnológico plantea una nueva amenaza a la seguridad que requiere nuevas soluciones de seguridad. Las pruebas de penetración se realizan para evaluar la seguridad de una infraestructura de TI al exponer de manera segura sus vulnerabilidades. También ayuda a evaluar la eficacia de las herramientas y la política de los mecanismos de defensa existentes. Las pruebas de penetración se realizan con regularidad para identificar riesgos y gestionarlos para lograr estándares de seguridad más altos. En

este artículo discutimos la importancia de las pruebas de penetración, los factores y componentes considerados al realizar una prueba de penetración, presentamos una encuesta de herramientas y procedimientos seguidos, el rol de la prueba de penetración durante la implementación en el gobierno de TI en una organización y finalmente la ética profesional para ser poseído por el equipo involucrado en la prueba de penetración". De esta manera, enfatizan la suma importancia que tienen las pruebas de penetración a efectos de determinar la vulnerabilidad en las redes de telecomunicación.

En el segundo caso, se tiene como indicador el nivel de vulnerabilidad de los discos HDD y SSD de la red de telecomunicaciones, los mismos que inicialmente eran de un nivel de 3.67% infecciones de los discos (representados en número de bytes), y aplicando las herramientas de OpenVas, Nmap y SubNetCalc para el hacking ético, se llegaron a mitigar las infecciones a un nivel de 0.5 de los discos duros y sólidos durante seis días, lo que significa una reducción del 86.38% sobre la vulnerabilidad de los discos HDD y SSD de la red de telecomunicaciones. Estos resultados son similares a los que tiene el autor Metso (2019), cuando menciona las buenas herramientas como Ethical o White Hat Hacking, para que se pueda controlar y documentar la seguridad de la información de los discos duros HDD y SSD. El tema de esta tesis son las pruebas de penetración (pentesting), también conocidas como Ethical o White Hat (Hackear). Es un tema que intriga a muchas personas, especialmente a las que trabajan en empresas en el área de tecnología de la información. El autor de esta tesis ha querido aprender pentesting durante un buen tiempo, así como el fino arte del pentesting, lo cual es un gran activo para un administrador de sistemas. Adquirir conocimiento acerca del pentesting brinda buenas herramientas para controlar y documentar la seguridad del sistema responsable. Al mismo tiempo que aprender pentesting abre la puerta a un mundo completamente nuevo,

Hay que saludar al autor de esta tesis al proporcionar una buena base de conocimientos para el mundo de las pruebas de penetración. Esta tesis solo trata sobre la teoría del pentesting en general y la introducción de

herramientas de pentesting y no cubre ningún otro aspecto de seguridad y pruebas de red.

En el tercer indicador, se mesura el nivel de vulnerabilidad de los puertos de la CPU principal de la red de telecomunicaciones, siendo la encontrada de 4 vulnerabilidades y con la ejecución de aplicaciones de hacking ético se llegaron a las 0.67 vulnerabilidades, logrando reducir el 83.25% de vulnerabilidades de los puertos del CPU. Comparando con la tesis del autor Conde Ortiz (2020), se basa en descubrir qué tipo de vulnerabilidades existen en estos sistemas, centrándose en los ataques desde el interior de su red. Se tomaron varios enfoques en relación a cómo atacar los servidores y servicios que forman la red, tanto desde el exterior como desde el interior de las máquinas. Se encontraron vulnerabilidades críticas en relación con el uso de servicios no autenticados y la interrupción de la comunicación entre servidores, que deben mitigarse correctamente para evitar futuros ataques potenciales

Y por último se tiene el indicador del nivel de capacidad y destreza sobre el manejo del hacking ético del personal que interactúa directamente con la red de telecomunicaciones que era de 9.5 puntos y mediante la implementación de la aplicación hacking ético se tiene 23.33 puntos, lo que significa una gran mejora.

En lo referente al marco conceptual, si bien es cierto que actualmente existe mucha bibliografía al respecto y luego de conocer la problemática de la empresa en cuestión, se optó desde un primer momento por tener como guías o manuales, las obras de la Hacker Ético y profesional de mucho renombre a nivel latinoamericano: Karina Astudillo (https://karinaastudillo.com), en primer lugar, por tener una vasta experiencia como informática forense en el Ministerio Público y Fiscalía del Ecuador (cargo que tuvo que dejar por las constantes amenazas recibidas por los ciberdelincuentes y que ella misma narra en sus propias obras), y en segundo lugar, por ser la autora de una respetable cantidad de obras sobre esta disciplina, siendo algunas de las más resaltantes: “Hacking Ético” y “Hacking Wireless 101”, convirtiéndose estos textos en

una guía de formidable ayuda, en especial para todos aquellos que quieran iniciarse en esta disciplina.

De esta manera y por ser de una necesidad relevante el hecho de implementar un LABORATORIO DE HACKING ÉTICO, hizo necesario que se adquirieran todos los implementos descritos en su manual, a efectos de recolectar la información requerida, así como llevar a cabo la selección del software disponible que fuera más eficiente para implementarlo en nuestras aplicaciones prácticas de hacking.

VI. CONCLUSIONES

Luego de haber aplicado las herramientas y protocolos de Hacking Ético en la empresa de Inversiones Mayito – Agente BCP, se pudo arribar a las siguientes conclusiones:

1. Se logró mitigar el nivel de vulnerabilidad de la red de telecomunicaciones con un pretest de 9.33 ataques cibernéticos y mediante la implementación de la aplicación de hacking ético actualmente es de 1.5 ataques, alcanzando una reducción de 7.83 ataques cibernéticos, representados en 83.93%.

2. Se logró mitigar el nivel de vulnerabilidad de los discos HDD y SSD de la red de telecomunicaciones con un pretest de 3.67 de infecciones o intrusión de virus y mediante la implementación de la aplicación de hacking ético actualmente es de 0.5 de infecciones, alcanzando una reducción de 3.17 infecciones o intrusión de virus representados en 86.38%.

3. Se logró mitigar el nivel de vulnerabilidad de los puertos de la CPU principal de la red de telecomunicaciones actual es de 4 intrusión o ataque y mediante la implementación de la aplicación hacking ético es de 0.67 intrusión en los puertos, consiguiendo una reducción de 3.33 intrusión o ataques a los puertos representados en 83.25%.

4. Se tiene en cuenta la escala de Likert de 1 a 5 puntos, para lograr medir el nivel de capacidad y destreza sobre el manejo del hacking ético del personal que interactúa directamente con la red de telecomunicaciones antes de la implementación era de 9.5 puntos y mediante la capacitación al personal sobre las fases de hacking ético, ahora es de 23.33 puntos, obteniendo un incremento de 13.83 puntos.

VII. RECOMENDACIONES

Posteriormente, y luego de haber arribado a las conclusiones anteriormente descritas, nos encontramos facultados para alcanzar a los propietarios de la Empresa Inversiones Mayito – Agente BCP y al personal involucrado en el manejo de su red de telecomunicaciones, las siguientes recomendaciones:

- ✓ Se recomienda realizar el cambio semanal de la clave del Router que brinda el Wifi para evitar posibles vulnerabilidades a la red de telecomunicaciones de Inversiones Mayito – Agente BCP, cifrando esta clave a través del software Online MD5 (Message Digest Algorithm - Algoritmo de resumen de mensajes): https://md5online.es/ . El MD5 es un algoritmo de codificación de 128 bits que genera un hash hexadecimal de 32 caracteres, independientemente de la longitud de la palabra de entrada. Este algoritmo no es reversible, siendo normalmente imposible encontrar la palabra original a partir de un MD5. Esta herramienta emplea una amplia base de datos con el fin de aumentar al máximo las posibilidades de encontrar la palabra inicial.

- ✓ Si bien es cierto que el Windows Defender, está considerado como uno de los mejores cortafuegos en el mundo, se recomienda la instalación de un mejor firewall para bloquear el acceso no autorizado de personas o programas extraños a través del internet. Entre los firewalls gratuitos más recomendados para Windows, tenemos a: ZoneAlarm, Comodo, PeerBlock, Tinywall, GlassWire, Netdefender, Firewall AVS, Open DNS, Norton Free Firewall y el SolarWinds Network Firewall Security Management.

- ✓ Se recomienda la adquisición de software y antivirus licenciados para proteger los equipos de los virus o intrusión ataques. Según https://www.pcworld.es/mejores-productos/seguridad/antivirus-windows-3675796/, los mejores antivirus reconocidos durante el año 2020 son (en ese orden): Norton 360 Deluxe, Bitdefender Total Security (2020), ESET Internet Security, Kaspersky Security Cloud, BullGuard Premium Protection, McAfee Total Protection (2020), 7 AVG Ultimate y 8 Sophos Home Premium.

- ✓ Se recomienda implementar cursos de capacitación obligatorios sobre seguridad informática y ciberseguridad a todo el personal involucrado en las áreas de TI. Para nuestro caso en particular, hemos utilizado las siguientes plataformas educativas y de capacitación:

  http://campus.pedrobeltrancanessa.org/, y

  http://www.pedrobeltrancanessa.com/moodle

REFERENCIAS

AL-SHIHA, R. y ALGHOWINEM, S., 2019. Security Metrics for Ethical Hacking. En: K. ARAI, S. KAPOOR y R. BHATIA (eds.), *Intelligent Computing*. Cham: Springer International Publishing, pp. 1154-1165. ISBN 978-3-030-01177-2. DOI 10.1007/978-3-030-01177-2_83.

ARIAS, F.G., 2012. El proyecto de investigación, 6ta Edición Fidias G. Arias FREELIBROS.ORG. [en línea], [Consulta: 30 septiembre 2020]. Disponible en: https://www.academia.edu/23573985/El_proyecto_de_investigaci%C3%B3n_6ta_Edici%C3%B3n_Fidias_G_Arias_FREELIBROS_ORG.

ASTUDILLO, K., 2017. *Hacking Etico 101*. S.l.: Babelcube Inc. ISBN 978-1-5475-0183-0.

BALOCH, R., 2017. *Ethical Hacking and Penetration Testing Guide*. S.l.: CRC Press. ISBN 978-1-4822-3162-5.

BARRERA, D. y ROCÍO, E., 2019. Análisis de metodologías para pruebas de penetración mediante Ethical Hacking. En: Accepted: 2019-09-10T01:13:41Z [en línea], [Consulta: 13 septiembre 2020]. Disponible en: http://repository.unad.edu.co/handle/10596/27647.

BOAGLIO, L., DIMITROFF, M., GONZÁLEZ, A., INGARAMO, R., LUCZYWO, N., NEPOTE, V., PIEROTTI, S., ZANAZZI, J.F. y ZANAZZI, J.L., 2020. *Probabilidad y estadística. Guía de Estudio 2020* [en línea]. S.l.: s.n. [Consulta: 20 septiembre 2020]. Disponible en: https://rdu.unc.edu.ar/handle/11086/15055.

BOBILLO, A.G., 2019. Ciberasedio a Alibaba: Jack Ma dice que su tienda sufre todos los días 300 millones de ataques informáticos. *ComputerHoy* [en línea]. [Consulta: 16 septiembre 2020]. Disponible en: https://computerhoy.com/noticias/industria/ciberasedio-alibaba-jack-ma-dice-tienda-sufre-todos-dias-300-millones-ataques-informaticos-514787.

CAPARÓ, E.V., 2019. ¿CÓMO PLANTEAR LAS VARIABLES DE UNA INVESTIGACIÓN?: OPERACIONALIZACIÓN DE LAS VARIABLES. *Odontología Activa Revista Científica*, vol. 4, no. 1, pp. 15-20. ISSN 2588-0624. DOI 10.31984/oactiva.v4i1.289.

CONCEPCIÓN-TOLEDO, D.N., 2019. Metodología de la investigación: Origen y construcción de una tesis doctoral. *Revista Científica de la UCSA*, vol. 6, no. 1, pp. 76-87. ISSN 2409-8752.

CONDE ORTIZ, D., 2020. *Ethical Hacking Of An Industrial Control System* [en línea]. S.l.: s.n. [Consulta: 6 diciembre 2020]. Disponible en: http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-285573.

COOPER, M., 2016. Adventures in Ethical Hacking. *ITNOW*, vol. 58, no. 3, pp. 36-37. ISSN 1746-5702. DOI 10.1093/itnow/bww074.

CRUZ, por L. de la, 2019. DESCUBRE LOS PUERTOS QUE POSEE UNA COMPUTADORA. *Te confirmamos si tu sistema operativo aguanta un software* [en línea]. [Consulta: 21 octubre 2020]. Disponible en: https://siaguanta.com/c-tecnologia/puertos-de-una-computadora/.

CRUZ, T. y SIMOES, P., 2019. *ECCWS 2019 18th European Conference on Cyber Warfare and Security*. S.l.: Academic Conferences and publishing limited. ISBN 978-1-912764-29-7.

DEVI, R.S. y KUMAR, M.M., 2020. Testing for Security Weakness of Web Applications using Ethical Hacking. *2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184)*. S.l.: s.n., pp. 354-361. DOI 10.1109/ICOEI48184.2020.9143018.

DÍAZ DEL CASTILLO NÁDER, E., 2020. Herramientas y técnicas fundamentales del PMBOK V6, para recolección, análisis y representación de datos en la toma de decisiones gerenciales. En: Accepted: 2020-07-02T17:10:47Z [en línea], [Consulta: 20 septiembre 2020]. Disponible en: http://repository.unad.edu.co/handle/10596/35144.

DORDOIGNE, J., 2015. *Redes informáticas - Nociones fundamentales (5ª edición): (Protocolos, Arquitecturas, Redes inalámbricas, Virtualización, Seguridad, IP v6 ...)*. S.l.: Ediciones ENI. ISBN 978-2-7460-9733-9.

ENGEBRETSON, P., 2013. *The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy*. S.l.: Elsevier. ISBN 978-0-12-411641-2.

GEORG, T., OLIVER, B. y GREGORY, L., 2018. Issues of Implied Trust in Ethical Hacking. *The ORBIT Journal*, vol. 2, no. 1, pp. 1-19. ISSN 2515-8562. DOI 10.29297/orbit.v2i1.77.

GIANNONE, A.O., 2019. Método de inclusión de hacking ético en el proceso de testing de software. [en línea], [Consulta: 13 septiembre 2020]. Disponible en: http://ria.utn.edu.ar/xmlui/handle/20.500.12272/4068.

GÓMEZ, R. y CESAR, J., 2018. Formación de auditores internos ISO27001 y técnicas de Hacking ético. En: Accepted: 2019-01-11T23:30:21Z [en línea], [Consulta: 15 octubre 2020]. Disponible en: http://repository.unipiloto.edu.co/handle/20.500.12277/4648.

GRACIA, J.F.H., 2018. Tipos de Investigación. *Boletín Científico de la Escuela Superior Atotonilco de Tula* [en línea], vol. 5, no. 9. [Consulta: 15 septiembre 2020]. ISSN 2007-7831. DOI 10.29057/esat.v5i9.2885. Disponible en: https://repository.uaeh.edu.mx/revistas/index.php/atotonilco/article/view/2885.

GRANT, J., 2019. *Hackeo Ético: Guia complete para principiantes para aprender y comprender el concepto de hacking ético (Libro En Español/Ethical Hacking Spanish Book Version)*. S.l.: Independently Published. ISBN 978-1-71105-900-6.

GRAUS, G. y ENRIQUE, M., 2017. ESTADÍSTICA APLICADA A LA INVESTIGACIÓN CIENTÍFICA. En: Accepted: 2017-11-01T19:50:26Z [en línea], [Consulta: 15 septiembre 2020]. Disponible en: http://10.22.1.21:8080/jspui/handle/123456789/3667.

HIMANEN, P., 2015. La ética del hacker y el espíritu de la era de la información. En: Accepted: 2015-04-20T18:34:18Z [en línea], [Consulta: 13 septiembre 2020]. Disponible en: https://observatoriocultural.udgvirtual.udg.mx/repositorio/handle/123456789/199.

HURTADO SANDOVAL, M.E. y MENDAÑO MENDAÑO, L.A., 2016. Implementación de técnicas de hacking ético para el descubrimiento y evaluación de vulnerabilidades de la red de una cartera de Estado. En: Accepted: 2016-11-15T21:55:40Z [en línea], [Consulta: 15 octubre 2020]. Disponible en: http://bibdigital.epn.edu.ec/handle/15000/16836.

KERBEROS, J.R., 2015. CÓDIGOS DE ÉTICA Y RESPONSABILIDAD PROFESIONAL EN LA COMPUTACIÓN FORENSE. *aanndrade* [en línea]. [Consulta: 14 octubre 2020]. Disponible en: https://aanndrade.wordpress.com/2015/02/16/codigos-de-etica-y-responsabilidad-profesional-en-la-computacion-forense-2/.

KHAN, F., 2019. *Hands-On Penetration Testing with Python: Enhance your ethical hacking skills to build automated and intelligent systems*. S.l.: Packt Publishing Ltd. ISBN 978-1-78899-946-5.

MANSFIELD-DEVINE, S., 2017. Hiring ethical hackers: the search for the right kinds of skills. *Computer Fraud & Security*, vol. 2017, no. 2, pp. 15-20. ISSN 1361-3723. DOI 10.1016/S1361-3723(17)30016-7.

MATERO, I., 2020. Ethical Hacking: Research and Course Compilation. , pp. 49.

METSO, J., 2019. Penetration Testing : Ethical Hacking. En: Accepted: 2019-10-31T06:38:14Z [en línea]. [Consulta: 5 diciembre 2020]. Disponible en: http://www.theseus.fi/handle/10024/261658.

MOLDOVAN, A.-N. y GHERGULESCU, I., 2020. Leveraging Virtual Labs for Personalised Group-based Assessment in a Postgraduate Network Security and Penetration Testing Module. *2020 15th International Workshop on Semantic and Social Media Adaptation and Personalization (SMA*. S.l.: s.n., pp. 1-6. DOI 10.1109/SMAP49528.2020.9248457.

NAJERA-GUTIERREZ, G. y ANSARI, J.A., 2018. *Web Penetration Testing with Kali Linux: Explore the methods and tools of ethical hacking with Kali Linux, 3rd Edition*. S.l.: Packt Publishing Ltd. ISBN 978-1-78862-380-3.

NICHOLSON, S., 2019. How ethical hacking can protect organisations from a greater threat. *Computer Fraud & Security*, vol. 2019, no. 5, pp. 15-19. ISSN 1361-3723. DOI 10.1016/S1361-3723(19)30054-5.

OCHANG, P.A. y IRVING, P., 2017. Security Analysis of VoIP Networks Through Penetration Testing. En: R. DAMAŠEVIČIUS y V. MIKAŠYTĖ (eds.), *Information and Software Technologies*. Cham: Springer International Publishing, pp. 601-610. ISBN 978-3-319-67642-5. DOI 10.1007/978-3-319-67642-5_50.

ORDOÑEZ, I., 2016. Top 10 sistemas operativos favoritos de los hackers. *Taringa!* [en línea]. [Consulta: 20 septiembre 2020]. Disponible en: https://www.taringa.net/+ciencia_educacion/top-10-sistemas-operativos-favoritos-de-los-hackers_hrjhw.

PATIL, S., JANGRA, A., BHALE, M., RAINA, A. y KULKARNI, P., 2017. Ethical hacking: The need for cyber security. *2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI)*. S.l.: s.n., pp. 1602-1606. DOI 10.1109/ICPCSI.2017.8391982.

RADHOLM, F. y ABEFELT, N., 2020. *Ethical Hacking of an IoT-device: Threat Assessment and Penetration Testing : A Survey on Security of a Smart Refrigerator* [en línea]. S.l.: s.n. [Consulta: 5 diciembre 2020]. Disponible en: http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-280295.

RAKSHITHA, C.M., 2020. Scope and Limitations of Ethical Hacking and Information Security. *2020 International Conference on Electronics and Sustainable Communication Systems (ICESC)*. S.l.: s.n., pp. 613-618. DOI 10.1109/ICESC48915.2020.9155846.

ROBBERTS, C. y TOFT, J., 2019. *Finding Vulnerabilities in IoT Devices : Ethical Hacking of Electronic Locks* [en línea]. S.l.: s.n. [Consulta: 14 diciembre 2020]. Disponible en: http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-254667.

SABIH, Z., 2018. *Learn Ethical Hacking from Scratch: Your stepping stone to penetration testing*. S.l.: Packt Publishing Ltd. ISBN 978-1-78862-478-7.

SAHA, Sanchita, DAS, A., KUMAR, A., BISWAS, D. y SAHA, Subindu, 2020. Ethical Hacking: Redefining Security in Information System. En: M. CHAKRABORTY, S. CHAKRABARTI y V.E. BALAS (eds.), *Proceedings of International Ethical Hacking Conference 2019*. Singapore: Springer, pp. 203-218. ISBN 9789811503610. DOI 10.1007/978-981-15-0361-0_16.

SÁNCHEZ, VIVERO y BAROJA, 2020. Aplicación de una metodología de seguridad avanzada en redes inalámbricas - ProQuest. [en línea]. [Consulta: 15 octubre 2020]. Disponible en: https://search.proquest.com/openview/ba8fb554f72bbe6b3480064330dbaed4/1?pq-origsite=gscholar&cbl=1006393.

SCHÜTTE GONZÁLEZ, D., 2019. Hackear las bibliotecas. *Serie Bibliotecología y Gestión de Información* [en línea]. [Consulta: 13 septiembre 2020]. Disponible en: http://eprints.rclis.org/38951/.

SHEBLI, H.M.Z.A. y BEHESHTI, B.D., 2018. A study on penetration testing process and tools. *2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*. S.l.: s.n., pp. 1-7. DOI 10.1109/LISAT.2018.8378035.

SHREE J.P, 2019. Ethical Hacking: Tools and Techniques. *Journal of the Gujarat Research Society*, vol. 21, no. 2, pp. 181-185. ISSN 0374-8588.

SINHA, S., 2018. Setting Up a Penetration Testing and Network Security Lab. En: S. SINHA (ed.), *Beginning Ethical Hacking with Kali Linux: Computational Techniques for Resolving Security Issues* [en línea]. Berkeley, CA: Apress, pp. 19-40. [Consulta: 6 diciembre 2020]. ISBN 978-1-4842-3891-2. Disponible en: https://doi.org/10.1007/978-1-4842-3891-2_2.

Solvetic - Solución a los problemas informáticos. *Solvetic* [en línea], 2020. [Consulta: 14 octubre 2020]. Disponible en: https://www.solvetic.com/.

TAYAG, M.I. y DE VIGAL CAPUNO, M.E.A., 2019. Compromising Systems: Implementing Hacking Phases. [en línea]. SSRN Scholarly Paper. Rochester, NY: Social Science Research Network. [Consulta: 14 diciembre 2020]. ID 3391093. Disponible en: https://papers.ssrn.com/abstract=3391093.

THOMAS, G., BURMEISTER, O. y LOW, G., 2019. The Importance of Ethical Conduct by Penetration Testers in the Age of Breach Disclosure Laws. *Australasian Journal of Information Systems* [en línea], vol. 23. [Consulta: 14 diciembre 2020]. ISSN 1449-8618. DOI 10.3127/ajis.v23i0.1867. Disponible en: https://journal.acs.org.au/index.php/ajis/article/view/1867.

URQUIZO, S., LÓPEZ, K. y SANDOVAL, B., 2020. SOFTWARE ESTADÍSTICO PARA EL CÁLCULO DE LA MUESTRA Y LOS TIPOS DE MUESTREO. *FIMAQ Investigación y Docencia* [en línea], vol. 3, no. 1. [Consulta: 20 septiembre 2020]. ISSN 2602-8182. DOI 10.24133/fimaq.v3i1.1519. Disponible en: https://journal.espe.edu.ec/ojs/index.php/fimaq/article/view/1519.

V. VISOOTTIVISETH, AKARASIRIWONG, P., CHAIYASART, S. y CHOTIVATUNYU, S., 2017. PENTOS: Penetration testing tool for Internet of

Thing devices. *TENCON 2017 - 2017 IEEE Region 10 Conference*. S.l.: s.n., pp. 2279-2284. DOI 10.1109/TENCON.2017.8228241.

WALKER, B., [sin fecha]. *Hacking Ético: Guía completa para principiantes para aprender y entender los reinos del hacking ético*. S.l.: 2020.

WANG, Y. y YANG, J., 2017. Ethical Hacking and Network Defense: Choose Your Best Network Vulnerability Scanning Tool. *2017 31st International Conference on Advanced Information Networking and Applications Workshops (WAINA)*. S.l.: s.n., pp. 110-113. DOI 10.1109/WAINA.2017.39.

WHITAKER, A. y NEWMAN, D.P., 2005. *Penetration Testing and Network Defense: Penetration Testing _1*. S.l.: Cisco Press. ISBN 978-0-13-398784-3.

WOLF, G., 2014. Desarrollo seguro de aplicaciones con criptografía. *2° Congreso de Seguridad de la Información* [en línea]. conference. México D.F. [Consulta: 13 septiembre 2020]. Disponible en: http://ru.iiec.unam.mx/2579/.

WOLF, G., 2017. Independencia en el Ciberespacio. *Software Gurú*, no. 55, pp. 40-41. ISSN 1870-0888.

WOLF, G. y SORIA GUZMÁN, I., 2016. Ética Hacker, seguridad y vigilancia. [en línea]. [Consulta: 13 septiembre 2020]. Disponible en: http://ru.iiec.unam.mx/3483/.

YEVDOKYMENKO, M., MOHAMED, E. y ONWUAKPA, P., 2017. Ethical hacking and penetration testing using raspberry PI. *2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S T)*. S.l.: s.n., pp. 179-181. DOI 10.1109/INFOCOMMST.2017.8246375.

ANEXOS

Anexo N.º 1: Matriz de Operacionalización de Variables

Variable	Definición Conceptual	Definición Operacional	Indicadores	Escala de Medición
V.D. **Seguridad en la red de Comunicación de Inversiones Mayito**	"En la actual coyuntura tecnológica, las grandes redes informáticas en general, están conformadas por sistemas operativos y computadores, en su mayoría heterogéneos, que interactúan recurrentemente a través del Internet. De esta manera, la interconectividad ha tenido un aumento exponencial respecto de su arquitectura. Este tipo de crecimiento desmesurado, ha ocasionado que muchos ISP (Internet Service Provider), descuiden la protección de las redes y se encuentren altamente vulnerables a los ataques cibernéticos" Dordoigne (2015).	"Actualmente, las WLAN se han tornado en una infraestructura necesaria e indispensable. Ello ha traído como consecuencia una avalancha de personas muy afanosas por conseguir accesos no autorizados a estas redes para sustraer información confidencial vulnerando las estrategias de seguridad. Para ello es necesario implementar una metodología de seguridad continua y basado en buenas prácticas de seguridad informática" Sánchez et al. (2020).	Nivel de vulnerabilidad de la red de telecomunicaciones (Wifi). Nivel de vulnerabilidad de los discos HDD y/o SSD de la CPU de la red de telecomunicaciones. Nivel de vulnerabilidad de los de los puertos de la CPU. Nivel de capacidades y destrezas sobre el manejo del Hacking Ético del personal que interactúa directamente con la red de telecomunicaciones en la empresa.	De razón

Tabla N° 25: Operacionalización de la Variable Dependiente

Fuente: Elaboración propia

Tabla N° 26: Operacionalización de la Variable Independiente

Variable	Definición Conceptual	Definición Operacional	Indicadores	Escala de Medición
V.I. **Aplicación de Hacking Ético**	"El Hacking Ético se puede describir como aquella defensa que se puede implementar en contra de aquellas constantes amenazas provocadas por los ciberdelincuentes también conocidos como: "Hackers de Sombrero Negro", otorgándonos de esta manera, la posibilidad de mantenerlas bajo control, eliminándolas, rastreando su proveniencia, identificar a él o los autores de su ejecución, así como también determinar su ubicación física. En este sentido, también debemos describir a estas amenazas como un evento o una acción que busca vulnerar la seguridad de los sistemas. Análogamente, podemos describir a las vulnerabilidades como las debilidades que pueden llegar a provocar una acción subrepticia, la misma que puede devenir en un comportamiento inesperado respecto de la seguridad de los sistemas digitales informáticos", (Gómez (2018).	"La aplicación de las normas y procedimientos para el empleo del Hacking Ético, tiene muy bien definidas sus fases procedimentales, las cuales son: a) Reconocimiento b) Escaneo c) Obtención del acceso d) Elaboración del Informe, y e) Entrega del Informe Final, Hurtado y Mendaño (2016).	Pruebas Funcionales	De razón

Fuente: Elaboración propia

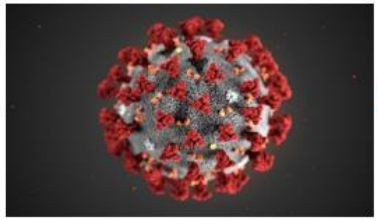
OBJETIVO GENERAL	Aplicar las técnicas empleadas en hacking ético para mejorar la seguridad de la red de telecomunicaciones de Inversiones Mayito

Objetivos Específicos	Indicador	Técnica / Instrumento	Tiempo Empleado	Modo de Cálculo
OE1: Mitigar la vulnerabilidad de la red de telecomunicaciones	Nivel de vulnerabilidad de la red de telecomunicaciones (Wifi)	Escaneo con software forense	Mensual	$$NVR = \frac{NRV}{n} * 100$$ Donde: NVR = Nivel de vulnerabilidad de la red NRV = Número de redes vulnerables n = Número de total redes
OE2: Mitigar la vulnerabilidad de los discos HDD y/o SSD de la CPU principal de la red	Nivel de vulnerabilidad de los discos HDD y/o SSD de la CPU principal de la red de telecomunicaciones			$$NVD = \frac{NDV}{n} * 100$$ Donde: NVD = Nivel de vulnerabilidad de los discos NDV = Número de discos vulnerables n = Número total de discos de almacenamiento
OE3: Mitigar la vulnerabilidad de los de los puertos de la CPU principal de la red de telecomunicaciones	Nivel de vulnerabilidad de los de los puertos de la CPU principal de la red de telecomunicaciones			$$NVP = \frac{NPV}{n} * 100$$ Donde: NVP = Nivel de vulnerabilidad de los puertos NPV = Número de puertos vulnerables n = Número total de puertos
OE4: Mejorar las capacidades y destrezas sobre la aplicación del Hacking Ético del personal que interactúa con la red	Nivel de capacidades y destrezas sobre la aplicación del Hacking Ético del personal que interactúa directamente con la red de telecomunicaciones	Charla de capacitación (Aula Virtual)		$$NCP = \frac{NPA}{n} * 100$$ Donde: NCP = Nivel de capacidad del personal NPA = Número preguntas acertadas n = Número total de preguntas

Anexo N.º 2: Realidad problemática

Realidad problemática: Aumento de Ciberdelincuencia

Crecimiento del uso del Internet



Pandemia del Covid-19

Transformación Digital

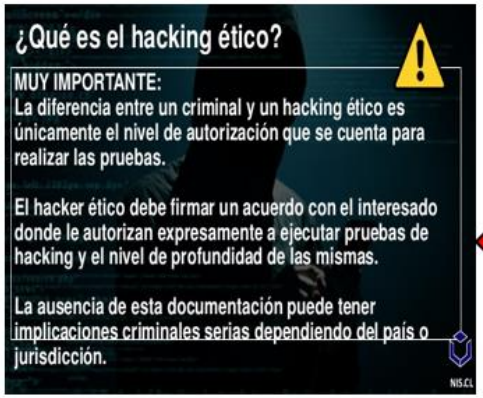
Crecimiento del Ciberdelito

Perú es el tercer país de Latinoamérica más afectado por ataques informáticos

Fuente: https://www.bitdefenderperu.com/peru-es-el-tercer-pais-de-latinoamerica-mas-afectado-por-ataques-informaticos/

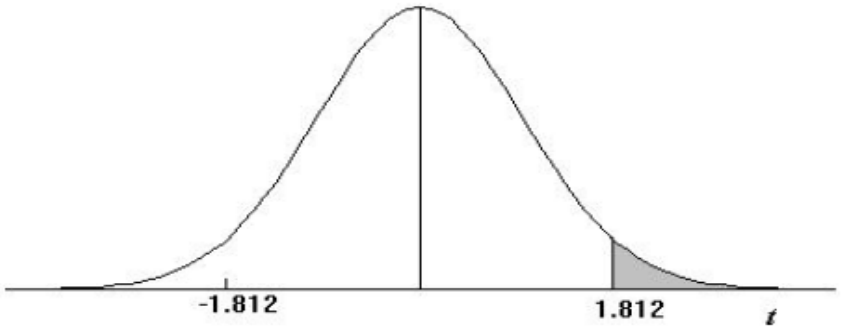
Crecimiento Ciberseguridad

Nivel Doméstico - Empresarial



Anexo N.º 3: Tabla de T- Student

Puntos de porcentaje de la distribución t



Ejemplo

Para $\phi = 10$ grados de libertad:

$P[t > 1.812] = 0.05$
$P[t < -1.812] = 0.05$

α / r	0,25	0,2	0,15	0,1	0,05	0,025	0,01	0,005	0,0005
1	1,000	1,376	1,963	3,078	6,314	12,706	31,821	63,656	636,578
2	0,816	1,061	1,386	1,886	2,920	4,303	6,965	9,925	31,600
3	0,765	0,978	1,250	1,638	2,353	3,182	4,541	5,841	12,924
4	0,741	0,941	1,190	1,533	2,132	2,776	3,747	4,604	8,610
5	0,727	0,920	1,156	1,476	2,015	2,571	3,365	4,032	6,869
6	0,718	0,906	1,134	1,440	1,943	2,447	3,143	3,707	5,959
7	0,711	0,896	1,119	1,415	1,895	2,365	2,998	3,499	5,408
8	0,706	0,889	1,108	1,397	1,860	2,306	2,896	3,355	5,041
9	0,703	0,883	1,100	1,383	1,833	2,262	2,821	3,250	4,781
10	0,700	0,879	1,093	1,372	1,812	2,228	2,764	3,169	4,587
11	0,697	0,876	1,088	1,363	1,796	2,201	2,718	3,106	4,437
12	0,695	0,873	1,083	1,356	1,782	2,179	2,681	3,055	4,318
13	0,694	0,870	1,079	1,350	1,771	2,160	2,650	3,012	4,221
14	0,692	0,868	1,076	1,345	1,761	2,145	2,624	2,977	4,140
15	0,691	0,866	1,074	1,341	1,753	2,131	2,602	2,947	4,073
16	0,690	0,865	1,071	1,337	1,746	2,120	2,583	2,921	4,015
17	0,689	0,863	1,069	1,333	1,740	2,110	2,567	2,898	3,965
18	0,688	0,862	1,067	1,330	1,734	2,101	2,552	2,878	3,922
19	0,688	0,861	1,066	1,328	1,729	2,093	2,539	2,861	3,883
20	0,687	0,860	1,064	1,325	1,725	2,086	2,528	2,845	3,850
21	0,686	0,859	1,063	1,323	1,721	2,080	2,518	2,831	3,819
22	0,686	0,858	1,061	1,321	1,717	2,074	2,508	2,819	3,792
23	0,685	0,858	1,060	1,319	1,714	2,069	2,500	2,807	3,768
24	0,685	0,857	1,059	1,318	1,711	2,064	2,492	2,797	3,745
25	0,684	0,856	1,058	1,316	1,708	2,060	2,485	2,787	3,725
26	0,684	0,856	1,058	1,315	1,706	2,056	2,479	2,779	3,707
27	0,684	0,855	1,057	1,314	1,703	2,052	2,473	2,771	3,689
28	0,683	0,855	1,056	1,313	1,701	2,048	2,467	2,763	3,674
29	0,683	0,854	1,055	1,311	1,699	2,045	2,462	2,756	3,660
30	0,683	0,854	1,055	1,310	1,697	2,042	2,457	2,750	3,646
40	0,681	0,851	1,050	1,303	1,684	2,021	2,423	2,704	3,551
60	0,679	0,848	1,045	1,296	1,671	2,000	2,390	2,660	3,460
120	0,677	0,845	1,041	1,289	1,658	1,980	2,358	2,617	3,373
∞	0,674	0,842	1,036	1,282	1,645	1,960	2,326	2,576	3,290

EVALUACIÓN DE INSTRUMENTOS DE RECOLECCIÓN DE DATOS

1.- **IDENTIFICACIÓN DEL EXPERTO**

NOMBRE DEL EXPERTO : Jaime Antenor Risco Mozo

DNI : 18085558 **PROFESIÓN :** Estadística

LUGAR DE TRABAJO : Gerencia RALL - EsSalud

CARGO QUE DESEMPEÑA : Estadístico de D&G

DIRECCIÓN : Calle Santa Clara Nro 190

TELÉFONO FIJO : _____ **TELÉFONO MOVIL :** 954992877

DIRECCIÓN ELECTRÓNICA : jaime.risco@essalud.gob.pe

FECHA DE EVALUACIÓN : 28/12/20

FIRMA

Lic. Jaime Antenor Risco Mozo
JEFE DE [illegible]

2.- **PLANILLA DE VALIDACIÓN DEL INSTRUMENTO**

CRITERIOS	APRECIACIÓN CUALITATIVA			
	EXCELENTE	BUENO	REGULAR	DEFICIENTE
Presentación del Instrumento	X			
Claridad en la redacción de los items.	X			
Pertinencia de las variables con los indicadores.	X			
Relevancia del contenido.	X			
Factibilidad de la aplicación.	X			

Anexo Nº 4: Abstract Certificado

ABSTRACT

In this research, applied research and experimental design were used, techniques such as observation and surveys for workers were used, and instruments such as questionnaires and information sheets were also applied. The vulnerability level of the telecommunications network was mitigated from 9.33 to 1.5 attacks, reaching a reduction of 7.83 represented in 83.93%. The second indicator, the level of vulnerability of HDD and SSD disks was 3.67 infections and through the implementation of the ethical hacking application it is now 0.5, reducing by 3.17 infections, represented by 86.38%. The third vulnerability indicator of the main CPU ports was 4 intrusions and through the implementation of ethical hacking it was lowered to 0.67 intrusion, achieving a reduction of 3.33 intrusion represented in 83.25%. Finally, with the Likert scale of 1 to 5 points, in order to measure the level of capacity and dexterity on the management of ethical hacking of the personnel who interact directly with the telecommunications network, before the implementation it was 9.5 points and through the implementation is now 23.33 points, obtaining an increase of 13.83 points.

Keywords: Ethical Hacking, vulnerability, communication network.

This document has been translated by the Translation and Interpreting Service of Cesar Vallejo University and it has been revised by the English native speaker: Mark Stables.

Mg. Ana Gonzales Castañeda
Professor of the School of Languages

Anexo Nº 5: Contrato de Auditoría y Confidencialidad

CONTRATO DE AUDITORIA INFORMÁTICA Y CONFIDENCIALIDAD

En la ciudad de Trujillo, La Libertad, a los 05 días del mes de setiembre del 2020;

REUNIDOS DE UNA PARTE, Doña Roxana Maribel, **AQUINO MÉNDEZ**, mayor de edad, con **D.N.I.** Nº: 26960595, en nombre y representación de la **EMPRESA INVERSIONES MAYITO**, en adelante, el **"CLIENTE"**, con domicilio fiscal en Calle Julio Chiriboga Nº 1259 con **RUC N° 10269605958**, la misma que se dedica a la distribución de productos farmacológicos, así como de **Agente Bancario del Banco de Crédito del Perú (BCP)**; y **DE OTRA PARTE**, Don Pedro Oswaldo **BELTRÁN CANESSA**, mayor de edad, con **D.N.I.** Nº: 17939348, en nombre y representación de **SÍ MISMO**, en adelante, el **"PROVEEDOR"**, domiciliado en el Jr. Agustín Gamarra Nº 327, Cercado de Trujillo, acuerdan en los términos y condiciones señaladas en las siguientes cláusulas:

El **CLIENTE** y el **PROVEEDOR**, en adelante, podrán ser denominadas, individualmente, **"la Parte"** y, conjuntamente, **"las Partes"**, reconociéndose mutuamente capacidad jurídica y de obrar suficiente para la celebración del presente Contrato, y:

EXPONEN

PRIMERO: Que el **CLIENTE** está interesado en la contratación de los servicios de:

a) Auditoria de los sistemas de telecomunicaciones (Wifi).

b) Realización de un informe detallado sobre la situación de los sistemas informáticos, con un plan que garantice el óptimo nivel de operatividad de los mismos.

c) Otros servicios consistentes en: Auditoría Forense de sus dispositivos de almacenamiento magnético digitales, recuperación de la toda la información que sea posible rescatar de los dispositivos en cuestión.

d) Elaborar un Plan de Seguridad Informática con los elementos y procedimientos que a su mejor criterio profesional sean posibles de implementar en función de las fallas detectadas, así como brindar la capacitación necesaria al personal responsable del área de facturación y cobranzas.

El **CLIENTE** está interesado en contratar dichos servicios para conocer la situación y la operatividad de sus sistemas informáticos, software y hardware para implementar soluciones correctivas y preventivas a los mismos con la finalidad de detectar y mitigar las vulnerabilidades de su infraestructura informática.

SEGUNDO: Que el **PROVEEDOR** es una empresa especializada en la prestación de servicios de Auditoria, seguimiento, conservación de sistemas informáticos, formación y capacitación.

TERCERO: Que las Partes están interesadas en celebrar un contrato de **PRESTACIÓN DE SERVICIOS INFORMÁTICOS** en virtud del cual el **PROVEEDOR** preste al **CLIENTE** los servicios de:

a) Auditoria de los sistemas de telecomunicaciones (Wifi).

b) Realización de un informe detallado sobre la situación de los sistemas informáticos, con un plan que garantice el óptimo nivel de operatividad de los mismos.

c) Otros servicios consistentes en: Auditoría Forense de sus dispositivos de almacenamiento magnético digitales, recuperación de la toda la información que sea posible rescatar de los dispositivos en cuestión.

d) Elaborar un Plan de Seguridad Informática con los elementos y procedimientos que a su mejor criterio profesional sean posibles de implementar en función de las fallas detectadas, así como brindar la capacitación necesaria al personal responsable del área de facturación y cobranzas.

e) Que las Partes reunidas en la sede social del **CLIENTE**, acuerdan celebrar el presente contrato de **PRESTACIÓN DE SERVICIOS INFORMÁTICOS**, en adelante, el "Contrato", de acuerdo con las siguientes:

CLÁUSULAS

PRIMERA: OBJETO

En virtud del Contrato el **PROVEEDOR** se obliga a prestar al **CLIENTE** los servicios de auditoria de los sistemas informáticos del **CLIENTE** y la ***realización posterior de un informe detallado***, para conocer la situación y la operatividad de sus sistemas informáticos, software y hardware, con un plan que garantice el óptimo nivel de los sistemas informáticos, en

adelante: **"los Servicios",** en los términos y condiciones previstos en el Contrato y en todos sus Anexos.

SEGUNDA: TÉRMINOS Y CONDICIONES GENERALES Y ESPECÍFICOS DE PRESTACIÓN DE LOS SERVICIOS

2.1. Los Servicios se prestarán en los siguientes términos y condiciones generales:

2.1.1. El **PROVEEDOR** responderá de la calidad del trabajo desarrollado con la diligencia exigible a una empresa experta en la realización de los trabajos objeto del Contrato.

2.1.2. El **PROVEEDOR** se obliga a gestionar y obtener, a su cargo, todas las licencias, permisos y autorizaciones administrativas que pudieren ser necesarias para la realización de los Servicios.

2.1.3. El **PROVEEDOR** se hará cargo de la totalidad de los tributos, cualquiera que sea su naturaleza y carácter, que se devenguen como consecuencia del Contrato, así como cualesquiera operaciones físicas y jurídicas que conlleve, salvo el Impuesto General a las Ventas (IGV) o su equivalente, que el **PROVEEDOR** repercutirá al **CLIENTE**.

2.1.4. El **PROVEEDOR** guardará confidencialidad sobre la información que le facilite el **CLIENTE** en o para la ejecución del Contrato o que por su propia naturaleza deba ser tratada como tal. Se excluye de la categoría de información confidencial toda aquella información que sea divulgada por el **CLIENTE**, aquella que haya de ser revelada de acuerdo con las leyes o con una resolución judicial o acto de autoridad competente. Este deber se mantendrá durante un plazo de tres años a contar desde la finalización del servicio.

2.1.5. En el caso de que la prestación de los Servicios suponga la necesidad de acceder a datos de carácter personal, el **PROVEEDOR**, como encargado del tratamiento, queda obligado al cumplimiento de la Leyes de Protección de Datos de Carácter Personal, conforme lo estipulan los Códigos Civiles y Penales de nuestro país. El **PROVEEDOR** responderá, por tanto, de las infracciones en que pudiera incurrir en el caso de que destine los

datos personales a otra finalidad, los comunique a un tercero, o en general, los utilice de forma irregular, así como cuando no adopte las medidas correspondientes para el almacenamiento y custodia de los mismos. A tal efecto, se obliga a indemnizar al **CLIENTE**, por cualesquiera daños y perjuicios que sufra directamente, o por toda reclamación, acción o procedimiento, que traiga su causa de un incumplimiento o cumplimiento defectuoso por parte del **PROVEEDOR** de lo dispuesto tanto en el Contrato como lo dispuesto en la normativa reguladora de la protección de datos de carácter personal. Asimismo, y según la normatividad vigente, el **PROVEEDOR** únicamente tratará los datos de carácter personal a los que tenga acceso conforme a las instrucciones del **CLIENTE** y no los aplicará o utilizará con un fin distinto al objeto del Contrato, ni los comunicará, ni siquiera para su conservación, a otras personas. En el caso de que el **PROVEEDOR** destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del Contrato, será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente. El **PROVEEDOR** deberá adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

2.1.6. El **PROVEEDOR** responderá de la corrección y precisión de los documentos que aporte al CLIENTE en ejecución del Contrato y avisará sin dilación al CLIENTE cuando detecte un error para que pueda adoptar las medidas y acciones correctoras que estime oportunas.

2.1.7. El **PROVEEDOR** responderá de los daños y perjuicios que se deriven para el **CLIENTE** y de las reclamaciones que pueda realizar un tercero, y que tengan su causa directa en errores del **PROVEEDOR**, o de su personal, en la ejecución del Contrato o que deriven de la falta de diligencia referida anteriormente.

2.1.8. Las obligaciones establecidas para el **PROVEEDOR** por la presente cláusula serán también de obligado cumplimiento para sus posibles empleados, colaboradores, tanto externos como internos, y subcontratistas, por lo que el **PROVEEDOR** responderá frente al **CLIENTE** si tales obligaciones son incumplidas por tales empleados.

2.2. El **PROVEEDOR** prestará los Servicios en los siguientes términos y condiciones específicas:

2.2.1. El **PROVEEDOR** realizará una auditoria de los sistemas

informáticos del **CLIENTE** para conocer la situación exacta en que se encuentran los sistemas informáticos del **CLIENTE**, software y hardware.

2.2.2. Una vez realizada la auditoria, los técnicos encargados de la misma realizarán un informe detallado de la situación, con un plan que garantice el óptimo nivel de los sistemas informáticos en el día a día y que planifique las necesidades que van surgiendo en el **CLIENTE**, atendiendo a las nuevas tecnologías y su constante evolución. Dicho plan podrá llevar a la contratación de otros servicios prestados por el **PROVEEDOR**.

2.2.3. Para la realización de la auditoria se desplazarán a la sede del **CLIENTE** dos técnicos del **PROVEEDOR**, uno como analista de sistemas y otro como asesor informático.

2.2.4. Los técnicos del **PROVEEDOR** realizarán su trabajo durante el horario **NO** comercial del **CLIENTE**, tales como los días domingos y feriados por un lapso de **08 horas diarias**.

2.2.5. El **CLIENTE** con la asistencia del **PROVEEDOR** realizará las copias necesarias de la programación, información, etc., para evitar su desaparición en el transcurso de la auditoria.

2.2.6. El **PROVEEDOR** realizará controles remotos, para elaborar un diagnóstico a través de soporte con una P.C. o por teléfono, de los sistemas informáticos del **CLIENTE**.

2.2.7. El encargado de los sistemas informáticos del **CLIENTE** estará en todo momento a disposición de los técnicos del **PROVEEDOR** para la realización de la auditoria y facilitará las claves y passwords necesarios para comprobar todos los sistemas y la descripción de los mismos.

2.2.8. Realizada la auditoria y antes de finalizar el informe completo, sin el plan para garantizar el óptimo nivel, se entregará al **CLIENTE** una copia del informe, en su estado, para su estudio.

2.2.9. Una vez estudiado por el **CLIENTE** el informe y antes de elaborar el plan que garantice el óptimo nivel de los sistemas, el encargado de los sistemas informáticos del **CLIENTE** tendrá las reuniones necesarias con los técnicos del **PROVEEDOR** para concretar las necesidades del CLIENTE. Cada parte llevará a las reuniones una propuesta. Una vez concretadas las necesidades, los técnicos del **PROVEEDOR** realizarán el plan.

2.2.10. Los plazos de entrega del informe y del plan se entregarán conforme la cláusula 5ª de este contrato. Una vez entregado el informe incluyendo el plan, el contrato estará cumplido

2.2.11. El contrato podrá ser ampliado para realizar los servicios necesarios para llevar el plan a buen término. Dicha ampliación será por acuerdo escrito entre las partes y el documento se unirá al presente contrato.

2.2.12. El **PROVEEDOR** ejecutará el Contrato realizando de manera competente y profesional los Servicios, cumpliendo los niveles de calidad exigidos y cuidando diligentemente los materiales del **CLIENTE** que tuviera que utilizar como consecuencia del Contrato.

TERCERA: POLÍTICA DE USO

3.1 El **CLIENTE** es el único responsable de determinar si los servicios que constituyen el objeto de este Contrato se ajustan a sus necesidades, por lo que el **PROVEEDOR** no garantiza que los servicios contratados se ajusten a las necesidades específicas del **CLIENTE**.

CUARTA: PRECIO Y FACTURACIÓN

4.1 El precio del Contrato es de **S/. 40.00 (Cuarenta y 00/100 Soles/Hora), sin incluir el IGV por 06 (seis) sesiones de 08 (ocho) horas cada una**, tal como se consignó en párrafo precedente.

4.2 El pago de las facturas o boletas (según sea el caso), se realizará, tras la aceptación de los trabajos por el **CLIENTE**, mediante transferencia bancaria a los 30 días de la fecha de recepción de la factura o boleta a la siguiente cuenta de débito de titularidad del **PROVEEDOR**: CCI: 63956473442425352276.

QUINTA: DURACIÓN DEL CONTRATO

5.1 El plazo de realización de la auditoria es de seis sesiones de 08 horas cada una

5.2 El plazo de entrega del informe para su estudio es de seis semanas como máximo.

5.3 El plazo de entrega del informe definitivo es de siete semanas como máximo a partir de la fecha referida en el encabezamiento del Contrato.

SEXTA: ACUERDO DE NIVEL DE SERVICIO

6.1 Todos los Servicios prestados por el **PROVEEDOR** se realizarán por personal especializado en cada materia. El personal del **PROVEEDOR** acudirá previsto de todo el material necesario, adecuado y actualizado, para prestar los Servicios.

6.2 El **PROVEEDOR** deberá cumplir los plazos de entrega que se acuerden con el **CLIENTE**. Se considerará un incumplimiento de los plazos cuando se superen las seis semanas para la auditoría y siete semanas para la entrega del Informe Final y en ese caso el **CLIENTE** podrá exigir al PROVEEDOR el pago de los daños y perjuicios que corresponda.

SÉPTIMA: MODIFICACIÓN

Las Partes podrán modificar el contrato de mutuo acuerdo y por escrito.

OCTAVA: RESOLUCIÓN

Las Partes podrán resolver el Contrato, con derecho a la indemnización de daños y perjuicios causados, en caso de incumplimiento de las obligaciones establecidas en el mismo.

NOVENA: NOTIFICACIONES

Las notificaciones que se realicen las Partes deberán realizarse por escrito con acuso de recibo en las direcciones descritas inicialmente en el presente contrato.

DÉCIMA: REGIMEN JURÍDICO

El presente contrato tiene carácter mercantil, no existiendo en ningún caso vínculo laboral alguno entre el **CLIENTE** y el personal del **PROVEEDOR** que preste concretamente los Servicios.

El incumplimiento de cualquiera de las obligaciones estipuladas en la presente cláusula facultará a la parte perjudicada a solicitar a la otra parte la resolución del presente contrato por incumplimiento, conforme a lo estipulado en el artículo 1430° del Código Civil Peruano, sin perjuicio de exigir el pago de la indemnización por daños y perjuicios a que hubiese lugar.

Firma del cliente:	**Firma del proveedor:**
	 ***Pedro O. Beltrán Canessa*** ***Docente Nombrado – Computación e Informática*** ***IESTP – "TRIJILLO"*** ***Ing. Industrial y de Sistemas*** ***CIP: 35960***

Anexo Nº 6: Fichas de registro de los indicadores en términos porcentuales

INVESTIGADOR:	BELTRÁN CANESSA, PEDRO OSWALDO	INDICADOR	NIVEL DE VULNERABILIDAD DE LA RED DE TELECOMUNICACIONES		
		FÓRMULA	$NVRT = \frac{NRV}{n} * 100$		
LUGAR:	INVERSIONES MAYITO TRUJILLO	FECHA DE INICIO		FECHA DE FIN	

INVESTIGADOR:	BELTRÁN CANESSA, PEDRO OSWALDO	INDICADOR	NIVEL DE VULNERABILIDAD DE LOS DISCOS DE LA RED DE TELECOMUNICACIONES		
		FÓRMULA	$NVDRT = \frac{NDV}{n} * 100$		
LUGAR:	INVERSIONES MAYITO TRUJILLO	FECHA DE INICIO		FECHA DE FIN	

INVESTIGADOR:	BELTRÁN CANESSA, PEDRO OSWALDO	INDICADOR	NIVEL DE VULNERABILIDAD DE LOS PUERTOS DE LA RED DE TELECOMUNICACIONES		
		FÓRMULA	$NVPRT = \frac{NPV}{n} * 100$		
LUGAR:	INVERSIONES MAYITO TRUJILLO	FECHA DE INICIO		FECHA DE FIN	

INVESTIGADOR:	BELTRÁN CANESSA, PEDRO OSWALDO	INDICADOR	NIVEL DE CAPACIDAD Y DESTREZA SOBRE EL MANEJO DE HACKING ÉTICO DE LA RED DE TELECOMUNICACIONES		
		FÓRMULA	$NCDSMHE = \frac{SPR}{120} * 100$		
LUGAR:	INVERSIONES MAYITO TRUJILLO	FECHA DE INICIO		FECHA DE FIN	

ANEXO Nº 7: Encuesta sobre capacidades y destrezas del personal involucrado en la seguridad de la red de telecomunicaciones

1. ¿Conoce Ud. sobre las buenas prácticas de la Seguridad Informática?

A: Desconozco

B: He escuchado algo

C: He leído algo

D: Tengo conocimiento, pero no lo practico

E: Tengo conocimiento y lo practico

2. ¿Conoce Ud. alguna técnica para proteger las redes Wifi de la empresa?

A: Desconozco

B: He escuchado algo

C: He leído algo

D: Tengo conocimiento, pero no lo practico

E: Tengo conocimiento y lo practico

3. ¿Conoce Ud. alguna técnica para proteger los puertos del servidor de la empresa?

A: Desconozco

B: He escuchado algo

C: He leído algo

D: Tengo conocimiento, pero no lo practico

E: Tengo conocimiento y lo practico

4. ¿Conoce Ud. alguna técnica para proteger los discos HDD o SSD del servidor de la empresa?

A: Desconozco

B: He escuchado algo

C: He leído algo

D: Tengo conocimiento, pero no lo practico

E: Tengo conocimiento y lo practico

5. ¿Conoce Ud. las técnicas del Hacking Ético para proteger las redes de telecomunicación?

A: Desconozco

B: He escuchado algo

C: He leído algo

D: Tengo conocimiento, pero no lo practico

E: Tengo conocimiento y lo practico

<u>Tabulación</u>:

Personal Inversiones Mayito		PREGUNTAS					SUMA
		1	2	3	4	5	
1							
2							
3							
4							
5							
6							

RESPUESTAS	VALORACIÓN
Desconozco	0
He escuchado	1
He leído	2
Conozco, pero no practico	3
Conozco y practico	4

INTERPRETACIÓN	
Nivel bajo	Suma < = 40
Nivel intermedio	40 < suma < 80
Nivel alto	Suma >= 80

Anexo Nº 8: Norma NTP-ISO/IEC 27001, código de buenas prácticas para la gestión de la seguridad de la información

La mejora continua y el proceso de análisis de riesgos se han suavizado, permitiendo otras formas más allá del PDCA, y no obligando a tener que identificar activos, amenazas y salvaguardas.

Contenido de la sesión:

1. Directrices de la NTP-ISO/IEC 27002 - I
   - Objeto y campo de aplicación
   - Términos y definiciones
   - Estructura del estándar
   - Evaluación y tratamiento del riesgo
   - Política de seguridad de información
2. Directrices de la NTP-ISO/IEC 27002 – II
   - Organización de la seguridad de información
   - Seguridad en recursos humanos
   - Gestión de activos
   - Control de acceso
   - Criptografía
   - Seguridad física y ambiental
   - Seguridad de operaciones
   - Gestión de comunicaciones
3. Directrices de la NTP-ISO/IEC 27002 - III
   - Adquisición, desarrollo y mantenimiento de sistemas
   - Relación con proveedores
   - Gestión de incidentes en la seguridad de información

- Aspectos de seguridad de información en la gestión de continuidad del negocio
- Cumplimiento

Objeto y Campo de Aplicación:

- ✓ Se ofrecen recomendaciones para la gestión de la seguridad de información.
- ✓ Busca proporcionar una base común para desarrollar normas de seguridad en las organizaciones.
- ✓ Puede servir como guía práctica para desarrollar estándares de seguridad.

Términos y Definiciones:

Activo: Algo que tenga valor para la organización.

Control: Herramienta de la gestión de riesgo, incluido políticas, pautas, estructuras organizacionales, que pueden ser de naturaleza administrativa, técnica, gerencial o legal.

Seguridad de información: Preservación de la confidencialidad, integridad y disponibilidad de la información, así mismo, otras propiedades como la autenticidad, no rechazo, contabilidad y confiabilidad también pueden ser consideradas.

Incidente de seguridad de información: Es indicado por una a varias series de incidentes inesperados y no deseados que tiene una gran probabilidad de comprometer las operaciones de negocios y de amenazar la seguridad de información.

Política: Dirección general y formal expresada por la gerencia.

Riesgo: Combinación de la probabilidad de un evento y sus consecuencias.

Gestión de riesgos: Actividades coordinadas para dirigir y controlar una organización considerando el riesgo.

Amenaza: Causa potencial de un incidente no deseado que puede resultar en daño al sistema u organización.

Vulnerabilidad: Debilidad de un activo o grupo de activos que pueden ser explotados por una o más amenazas.

Estructura del Estándar

Cláusulas

Categorías principales de seguridad:

- ✓ Descripción del objetivo de control.
- ✓ Controles que deben aplicarse.

Evaluación y Tratamiento del Riesgo

Evaluación de riesgos de seguridad:

Identificar, cuantificar y priorizar.

Tratamiento de riesgos de seguridad:

Reducir, aceptar, evitar, transferir.

Políticas de Seguridad:

- ✓ Política de seguridad de la información
- ✓ Documento de política de Seguridad de la Información
- ✓ Revisión de la política de Seguridad de la Información

Organización de la Seguridad de la Información:

- ✓ Organización Interna
- ✓ Roles y responsabilidades en la seguridad de información
- ✓ Segregación de funciones
- ✓ Contacto con autoridades
- ✓ Contacto con grupos de interés
- ✓ Seguridad de información en la gestión de proyectos
- ✓ Dispositivos Móviles y Teletrabajo
- ✓ Política para dispositivo móvil
- ✓ Teletrabajo

Seguridad en los Recursos Humanos:

- ✓ Previo al empleo
- ✓ Investigación de antecedentes
- ✓ Términos y condiciones del empleo
- ✓ Durante el empleo
- ✓ Responsabilidades de la gerencia
- ✓ Concientización, educación y entrenamiento en la seguridad de la información
- ✓ Proceso disciplinario
- ✓ Finalización o cambio de empleo
- ✓ Finalización de responsabilidades

Gestión de Activos:

- ✓ Responsabilidad de los activos
- ✓ Inventario de activos
- ✓ Propiedad de activos
- ✓ Uso adecuado de activos
- ✓ Devolución de activos
- ✓ Clasificación de la información
- ✓ Etiquetado de la información
- ✓ Manejo de activos
- ✓ Gestión de medios removibles
- ✓ Eliminación de medios
- ✓ Transferencia de medios físicos

Control de Acceso:

- ✓ Requerimientos de negocio para el control del acceso
- ✓ Política de control de acceso
- ✓ Acceso a redes y servicios de red
- ✓ Gestión de accesos de usuarios
- ✓ Registro de usuarios
- ✓ Gestión de acceso de usuarios
- ✓ Gestión de accesos privilegiados
- ✓ Gestión de la información secreta de autenticación
- ✓ Revisión de los derechos de acceso de los usuarios
- ✓ Retiro de los permisos de acceso
- ✓ Responsabilidades de usuario
- ✓ Uso de información secreta de autenticación
- ✓ Control de acceso a la información y las aplicaciones
- ✓ Restricción de acceso a la información
- ✓ Procedimiento de inicio de sesión seguro
- ✓ Sistema de gestión de contraseña
- ✓ Uso de utilidades del sistema
- ✓ Control de acceso al código fuente del programa

Criptografía:

- ✓ Controles criptográficos

- ✓ Política en el uso de controles de cifrado
- ✓ Administración de llaves

Seguridad Física y del Entorno:

- ✓ Áreas seguras
- ✓ Perímetro de seguridad física
- ✓ Controles físicos de entrada
- ✓ Seguridad en oficinas, cuartos y edificios
- ✓ Protección contra amenazas externas y ambientales
- ✓ Trabajo en áreas seguras
- ✓ Áreas de acceso pública, carga y entrega
- ✓ Equipamiento
- ✓ Ubicación y protección de equipamiento
- ✓ Suministros de soporte
- ✓ Seguridad en el cableado
- ✓ Mantenimiento de equipos
- ✓ Retiro de activos
- ✓ Seguridad de los equipos fuera de las instalaciones
- ✓ Desecho o rehúso seguro de los equipos
- ✓ Equipos de usuarios desatendidos
- ✓ Política de escritorio y pantalla limpia

Seguridad de las Operaciones:

- ✓ Responsabilidades y procedimientos operacionales
- ✓ Procedimientos operacionales documentados
- ✓ Administración de cambios
- ✓ Gestión de la capacidad
- ✓ Separación de ambientes
- ✓ Protección contra código malicioso
- ✓ Controles contra software malicioso
- ✓ Respaldo
- ✓ Copia de respaldo de información
- ✓ Registro y monitoreo
- ✓ Registro de eventos
- ✓ Protección de la información de registros

- ✓ Registros del administrador y operador
- ✓ Sincronización de relojes
- ✓ Control de software operacional
- ✓ Instalación de software sobre el sistema operativo
- ✓ Gestión de vulnerabilidades técnicas
- ✓ Gestión de vulnerabilidades técnicas
- ✓ Restricciones en la instalación de software
- ✓ Consideraciones de auditoria de sistemas de información
- ✓ Controles de auditoría de los sistemas de información

Seguridad de las Comunicaciones:

- ✓ Gestión de la seguridad en la red
- ✓ Controles en la red
- ✓ Seguridad de los servicios de la red
- ✓ Segregación en redes
- ✓ Transferencia de información
- ✓ Políticas y procedimientos de transferencia de información
- ✓ Acuerdos de transferencia
- ✓ Mensajería electrónica
- ✓ Acuerdos de confidencialidad o no revelación

Adquisición, Desarrollo y Mantenimiento de Sistemas:

- ✓ Requerimientos de seguridad de los sistemas de información
- ✓ Análisis y especificaciones de los requerimientos de seguridad
- ✓ Seguridad de servicios aplicativos sobre redes públicas
- ✓ Protección de transacciones aplicativas
- ✓ Seguridad en el desarrollo y soporte de procesos
- ✓ Política de desarrollo seguro
- ✓ Procedimientos de control de cambios
- ✓ Revisión técnica de aplicaciones después de cambios al sistema operativo
- ✓ Restricciones en los cambios a los paquetes de software
- ✓ Principios de ingeniería de sistemas segura
- ✓ Ambiente de desarrollo seguro
- ✓ Desarrollo de software en outsourcing

- ✓ Prueba de seguridad del sistema
- ✓ Prueba de aceptación del sistema
- ✓ Datos de prueba
- ✓ Protección de los datos de prueba del sistema

Relaciones con Proveedores:

- ✓ Seguridad de información en relaciones con el proveedor
- ✓ Políticas de seguridad de información en las relaciones con el proveedor
- ✓ Gestión de la seguridad en los acuerdos con el proveedor
- ✓ Cadena de suministro de tecnología de información y comunicaciones
- ✓ Gestión de servicios por terceras partes
- ✓ Monitoreo y revisión de los servicios de terceros
- ✓ Administración de cambios en los servicios de terceros

Gestión de Incidentes en la Seguridad de Información:

- ✓ Informes de los eventos de seguridad de la información y vulnerabilidades
- ✓ Responsabilidades y procedimientos
- ✓ Reporte de eventos de seguridad de la información
- ✓ Reporte de debilidades de seguridad
- ✓ Evaluación y decisión sobre los eventos de seguridad de información
- ✓ Respuesta a incidentes de seguridad de información
- ✓ Aprender de los incidentes de seguridad de la información
- ✓ Recolección de evidencia

Seguridad de Información en Gestión de Continuidad de Negocio:

- ✓ Continuidad de la seguridad de información
- ✓ Planeamiento de la continuidad de la seguridad de información
- ✓ Implementación de la continuidad de la seguridad de información
- ✓ Verificación y evaluación de la continuidad de la seguridad de información
- ✓ Redundancias
- ✓ Disponibilidad de centro de procesamiento de datos

Cumplimiento:

- ✓ Cumplimiento de los requerimientos legales

- ✓ Identificación de la legislación aplicable
- ✓ Derechos de propiedad intelectual (IPR)
- ✓ Protección de los registros
- ✓ Protección y privacidad de la información personal
- ✓ Regulación de controles de cifrado
- ✓ Revisiones a la seguridad de información
- ✓ Revisión independiente de la seguridad de información
- ✓ Cumplimiento de políticas y estándares de seguridad
- ✓ Verificación del cumplimiento técnico

Certificación del SGSI:

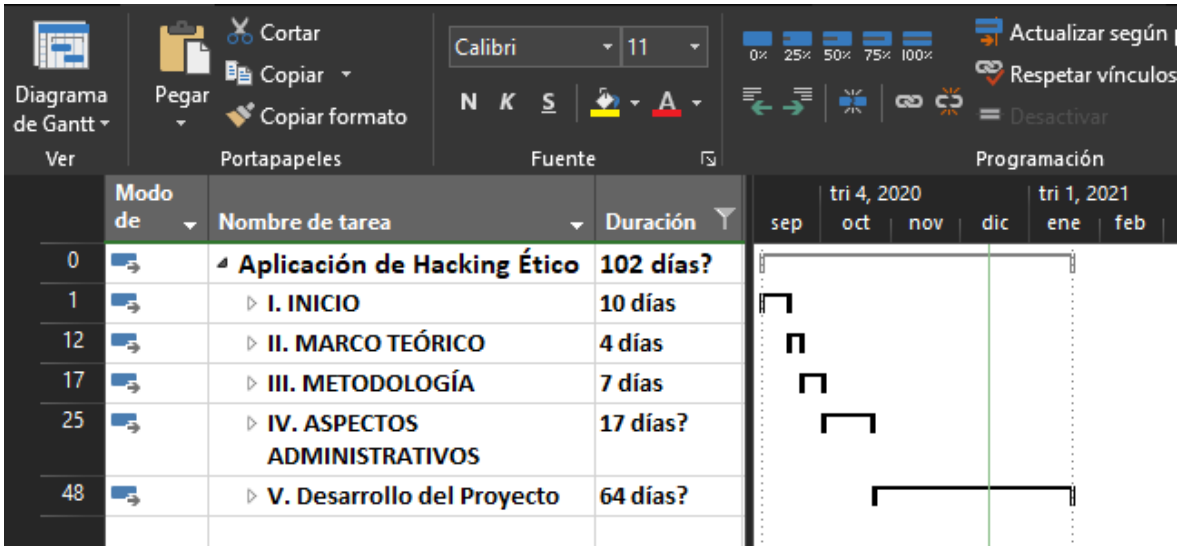
La certificación no implica que la organización ha obtenido determinados niveles de seguridad de la información para sus productos o servicios.

Las organizaciones certificadas pueden tener mayor confianza es su capacidad para gestionar la seguridad de la información, y por ende ayudará a asegurar a sus socios, clientes, y accionistas con quien hacen negocios.

Procesos análogos a los de las normas ISO 9001 e ISO 14000.

Certificado con duración de 3 años.

Anexo Nº 9: Cronograma de ejecución colapsado



Fuente: Elaboración propia

Anexo Nº 10: Cronograma de ejecución expandido

Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
Aplicación de Hacking Ético	**102 días**	**sáb 5/9/20**	**mar 19/1/21**	
I. INICIO	**10 días**	**sáb 5/9/20**	**mié 16/9/20**	
Inicio	1 día	sáb 5/9/20	sáb 5/9/20	
Introducción	1 día	lun 7/9/20	lun 7/9/20	2
Planteamiento Realidad Problemática	1 día	mar 8/9/20	mar 8/9/20	3
Investigar Objeto de Estudio y Campo de Acción	1 día	mié 9/9/20	mié 9/9/20	4
Definir Título del Proyecto	1 día	jue 10/9/20	jue 10/9/20	5
Formulación del Problema	1 día	vie 11/9/20	vie 11/9/20	6
Planteamiento de la Hipótesis	1 día	dom 13/9/20	dom 13/9/20	7
Definir Objetivo General	1 día	lun 14/9/20	lun 14/9/20	8
Definir Objetivos Específicos	1 día	mar 15/9/20	mar 15/9/20	9
Redacción Justificación del Proyecto	1 día	mié 16/9/20	mié 16/9/20	10
II. MARCO TEÓRICO	**4 días**	**jue 17/9/20**	**mar 22/9/20**	
Definición Marco Teórico	1 día	jue 17/9/20	jue 17/9/20	11
Búsqueda Antecedentes dela Investigación	1 día	vie 18/9/20	vie 18/9/20	13
Investigar Metodologías Existentes	1 día	lun 21/9/20	lun 21/9/20	14
Investigar Metodologías Pertinentes	1 día	mar 22/9/20	mar 22/9/20	15
III. METODOLOGÍA	**7 días**	**mié 23/9/20**	**jue 1/10/20**	
Definir Tipo y Diseño de Investigación	1 día	mié 23/9/20	mié 23/9/20	16
Definir Tipo y Diseño de Investigación	1 día	jue 24/9/20	jue 24/9/20	18
Definir Tipo y Diseño de Investigación	1 día	vie 25/9/20	vie 25/9/20	19
Definir Tipo y Diseño de Investigación	1 día	lun 28/9/20	lun 28/9/20	20
Definir Tipo y Diseño de Investigación	1 día	mar 29/9/20	mar 29/9/20	21
Definir Tipo y Diseño de Investigación	1 día	mié 30/9/20	mié 30/9/20	22
Definir Tipo y Diseño de Investigación	1 día	jue 1/10/20	jue 1/10/20	23
IV. ASPECTOS ADMINISTRATIVOS	**17 días**	**vie 2/10/20**	**vie 23/10/20**	
Identificar Aspectos Administrativos	1 día	vie 2/10/20	vie 2/10/20	24

Elaborar Recursos y Presupuestos	1 día	lun 5/10/20	lun 5/10/20	26
Elaborar el Financiamiento	1 día	mar 6/10/20	mar 6/10/20	27
Elaborar Cronograma de Ejecuciones	1 día	mié 7/10/20	mié 7/10/20	28
Validación en Turnitin	1 día	jue 8/10/20	jue 8/10/20	29
Levantar Observaciones del Turnitin	1 día	vie 9/10/20	vie 9/10/20	30
Realizar las Referencia de la Investigación	1 día	lun 12/10/20	lun 12/10/20	31
Primera Revisión del Asesor del Proyecto	1 día	mar 13/10/20	mar 13/10/20	32
Segunda Revisión del Asesor del Proyecto	1 día	mié 14/10/20	mié 14/10/20	33
Primera Revisión del Asesor Estadístico	2 días	jue 15/10/20	vie 16/10/20	34
Segunda Revisión del Asesor Estadístico	2 días	dom 18/10/20	lun 19/10/20	35
Elaboración de Diapositivas	2 días	mar 20/10/20	mié 21/10/20	36
Sustentación del Proyecto	2 días	jue 22/10/20	vie 23/10/20	37
V. Desarrollo del Proyecto				
Escaneo de Redes	9 días	dom 25/10/20	mié 4/11/20	38
Escaneo de Puertos	9 días	jue 5/11/20	mar 17/11/20	39
Escaneo de Discos	9 días	mié 18/11/20	lun 30/11/20	40
Implementación Aula virtual	10 días	mar 1/12/20	lun 14/12/20	41
Conclusiones	3 días	mar 15/12/20	jue 17/12/20	42
Recomendaciones	3 días	vie 18/12/20	mar 22/12/20	43
Discusión	1 día	mié 23/12/20	mié 23/12/20	44
Entrega para Revisión	2 días	jue 24/12/20	vie 25/12/20	45
Subsanación de Observaciones	10 días	lun 28/12/20	vie 8/1/21	46
Sustentación de Tesis	8 días	sáb 9/1/21	mar 19/1/21	47

Fuente: Elaboración propia

Anexo Nº 11: Aspectos administrativos

11.1. Recursos de personal

Código	Recursos humanos	Unidad	Cantidad	Costo Unitario (S/.)	Sub Total (S/.)
Subvenciones a Personas Naturales					
2.5.3.1.1.1	Investigador	Unidad	01	3.750	3,750.00
2.5.3.1.1.2	Asesor	Unidad	01	2.000	2,000.00
				Total	**5,750.00**

Fuente: Elaboración propia

11.2. Recursos materiales para la investigación

Código	Descripción	Unidad	Cantidad	Costo Unitario (S/.)	Sub Total (S/.)
Útiles de Escritorio					
71.60.0004 .0089	Lápices negros 2B	Unidad	02	1.50	3.00
71.60.0001 .0231	Bolígrafos de tinta seca color negro	Unidad	03	0.70	2.10
71.50.0022 .0029	Tajador de metal para lápiz	Unidad	01	2.50	2.50
71.11.0003 .0001	Corrector liquido tipo lapicero	Unidad	02	2.00	4.00
71.50.0011 .0014	Engrapador de metal mediano	Unidad	01	7.00	7.00
71.06.0004 .0052	Folder manila tamaño oficio	Unidad	01	1.00	1.00
71.72.0001 .0050	Block de papel bond tamaño A2 x100 hojas	Unidad	01	12.00	12.00
76.74.0004 .0152	Disco DVD grabable de 3.2 GB	Unidad	05	3.50	17.50
71.50.0025 .0068	Porta CD de plástico tipo cartuchera	Unidad	01	8.50	8.50
				Total	**57.60**

Fuente: Elaboración propia

11.3. Bienes para la investigación

Código	Descripción	Unidad	Cantidad	Costo Unitario (S/.)	Depreciación %	Sub Total (S/.)
Adquisición de maquinarias, equipo y mobiliario						
74.64.3847 .0001	Escritorio de madera	Unidad	01	450.00	5	22.50
74.64.8187 .0029	Silla giratoria	Unidad	01	150.00	5	7.50
76.75.0012 .0672	Mousepad	Unidad	01	15.00	3	0.45
76.75.0012 .0923	Cooler	Unidad	01	35.00	3	1.05
76.75.0059 .0004	Memoria USB	Unidad	05	15.00	3	2.25
95.22.8325 .0017	Smart Phone	Unidad	01	1,000.00	5	50
74.08.0500 .0001	Laptop	Unidad	01	6,000.00	3	180.00
14.04.0003 .0177	Licencia de SO Windows	Unidad	01	1000.00	1	10.00
					Total	**273.75**

Fuente: Elaboración propia

11.4. Pago de servicios para la investigación

Código	Descripción	Unidad	Cantidad	Costo Unitario (S/.)	Sub Total (S/.)
Útiles de escritorio					
87.05.0003 .0019	Servicio de internet / mes	Unidad	06	90.00	540.00
87.05.0001 .0001	Servicio de telefonía móvil / mes	Unidad	06	90.00	540.00
90.10.0006 .0017	Servicio de movilidad	Unidad	20	7.00	140.00
50.01.0005 .1553	Servicio de fotocopiado. Impresiones y escaneado	Unidad	30	1.00	30.00
				Total	**1,250.00**

Fuente: Elaboración propia

11.5. Presupuesto de la investigación

Nº	Descripción	Unidad	Cantidad	Sub Total (S/.)
1	Recursos humanos	Unidad	02	5,750.00
2	Recursos materiales	Unidad	09	57.60
3	Bienes	Unidad	08	273.75
4	Servicios	Unidad	07	1,250.00
			Total	**7,331.35**

Fuente: Elaboración propia

11.6. Financiamiento de la investigación

Entidad Financiadora	Monto (S/.)	Porcentaje (%)
Universidad César Vallejo SAC	5,750.00	78.43
Investigador	1,581.35	21.57

Fuente: Elaboración propia

Anexo Nº 12: Instalación y virtualización del software

En cuanto a la implementación de un Laboratorio de Hacking Ético, primeramente, se instaló una ***infraestructura básica***, teniendo como host de hospedaje una máquina virtual (VirtualBox), como software de ataque a ***Kali Linux*** y como software víctima para la prueba de vulnerabilidades a ***Raspberry Debian***, tal como se muestra en la Figuras N° 7 y 8.

Luego pasamos a la virtualización de ***Kali Linux*** (Figuras N° 9 y 10).

Finalmente, y para concluir la infraestructura básica, virtualizaremos ***Raspbian Debian*** (Figuras N° 11 y 12).

Por último, mostraremos el VirtualBox virtualizado (Figura N° 13).

Todo este software fue instalado en sus últimas versiones.

Figura N° 7: VirtualBox. Fuente: https://www.virtualbox.org

Figura 8: Instalación y Configuración de VirtualBox.

Fuente: https://www.virtualbox.org

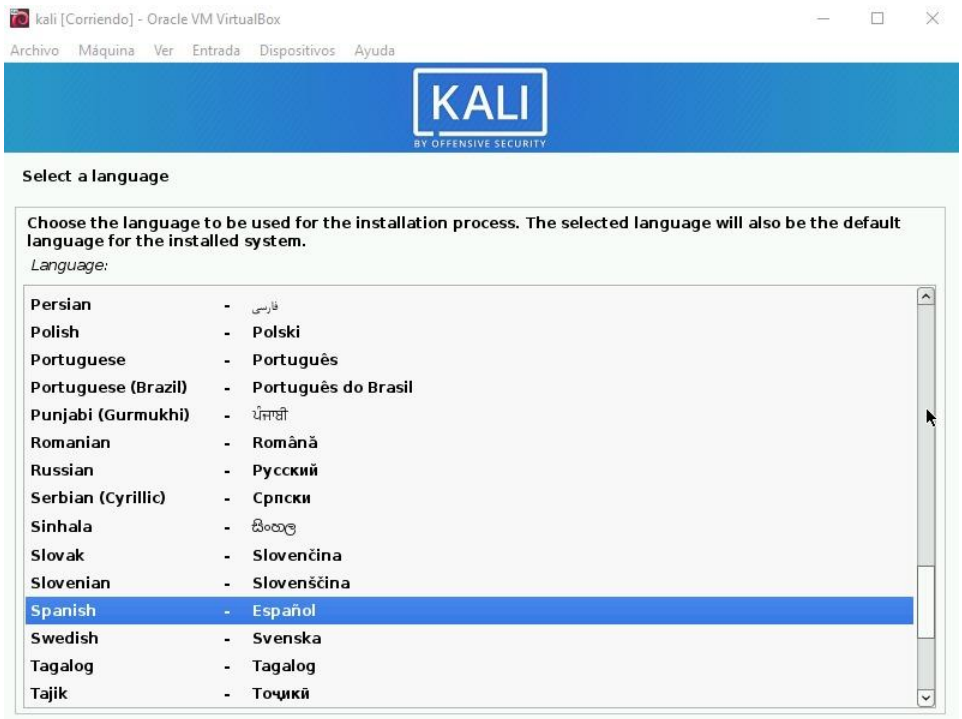


Figura 9: Instalación y Configuración de Kali Linux. Fuente: https://www.kali.org

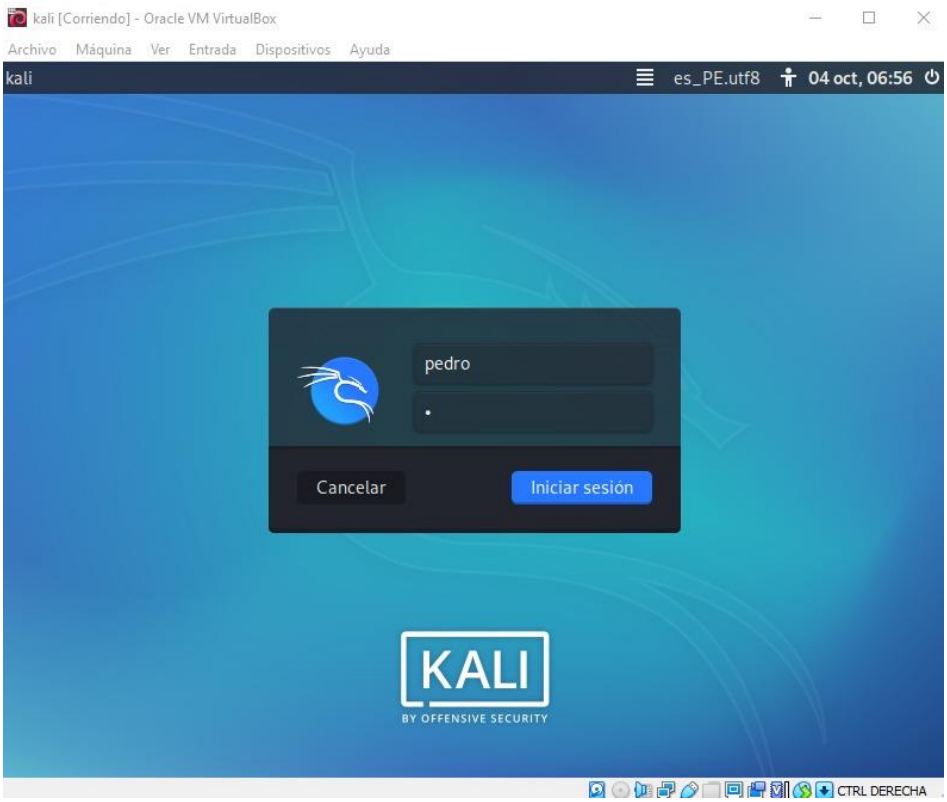


Figura 10: Virtualización de Kali Linux. Fuente: https://www.kali.org

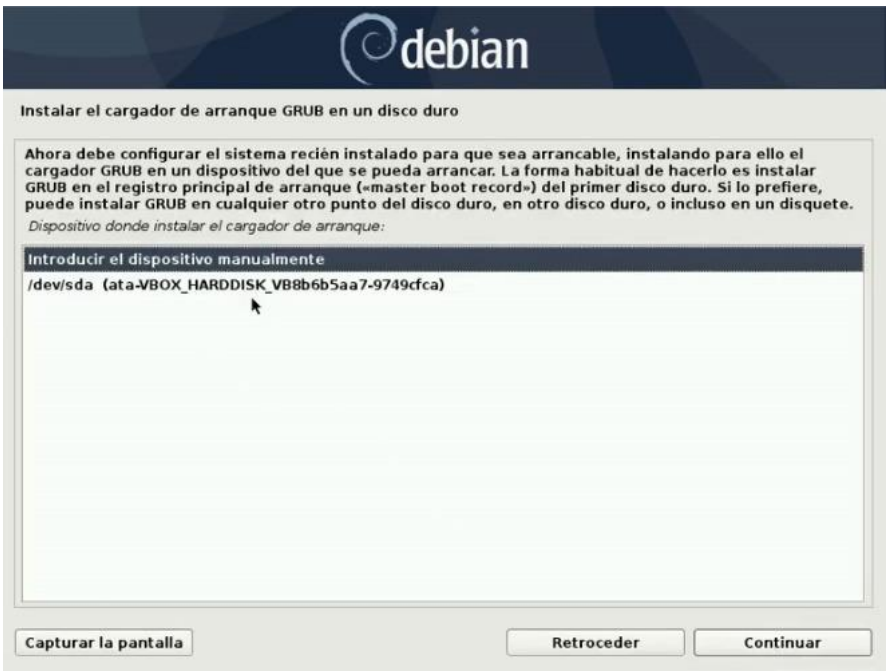


Figura 11: Instalación y Configuración de Raspbian. Fuente: https://www.raspbian.org

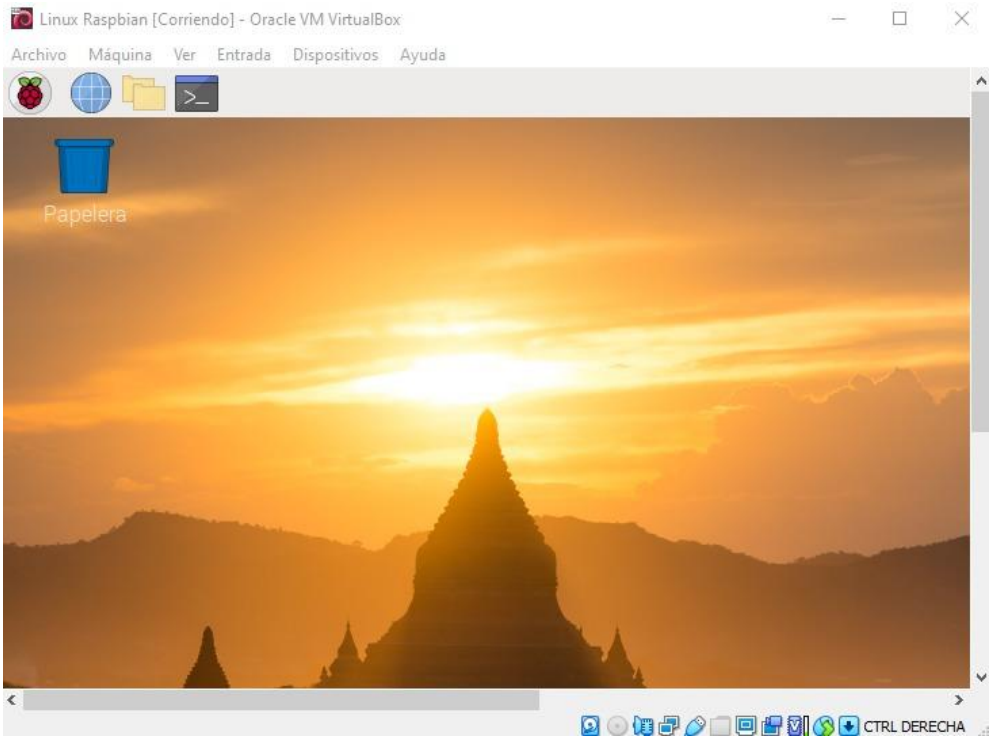


Figura 12: Virtualización de Raspbian Debian.

Fuente: https://www.raspbian.org

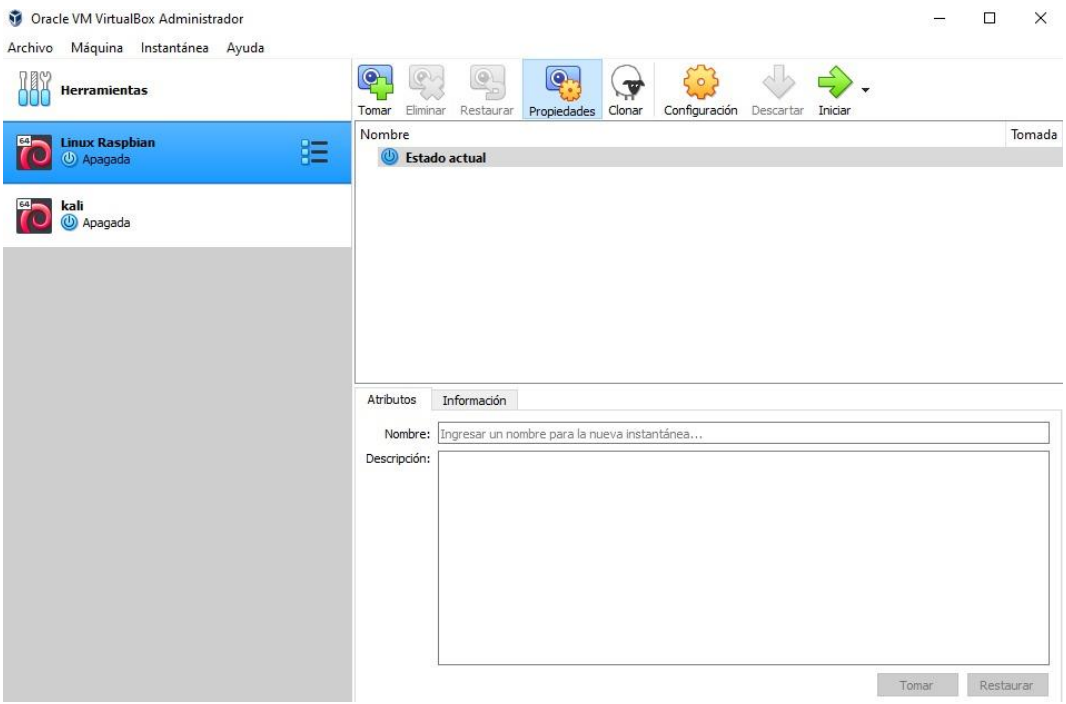


Figura 13: Kali y Raspbian Virtualizado.

Fuente: Elaboración Propia

Anexo Nº 13: Instalación y virtualización del software de ataque

Figura 15: Virtualización de Wifislax. Fuente: https://www.wifislax.com

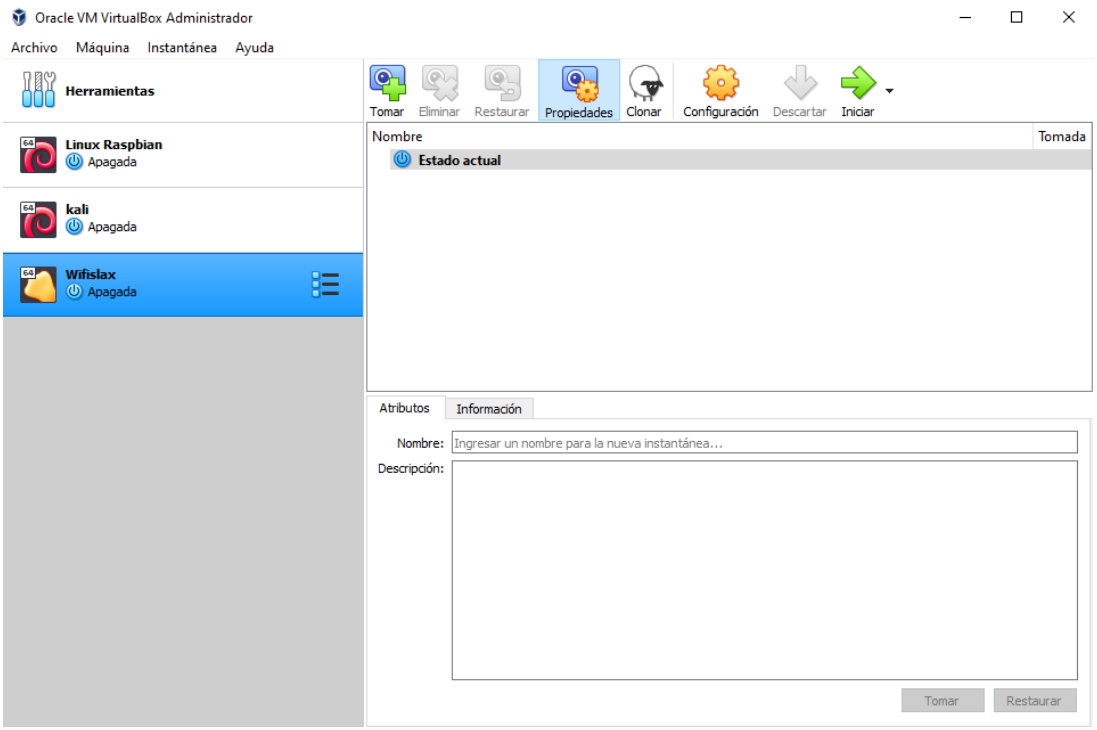


Figura 16: Wifislax Virtualizado. Fuente: Elaboración Propia

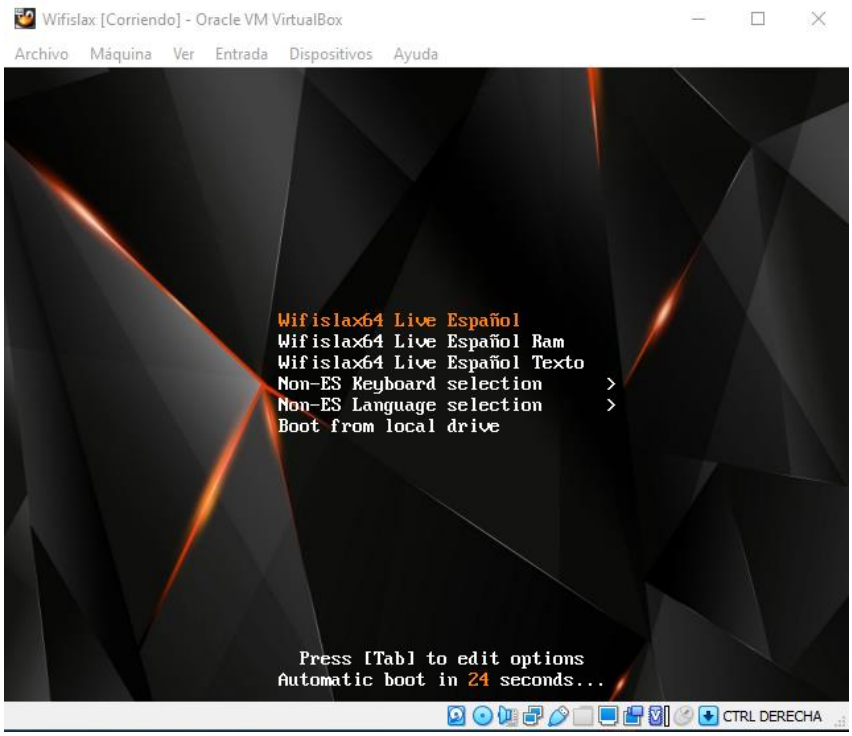


Figura N° 17: Cargando el Programa.
Fuente: Elaboración propia

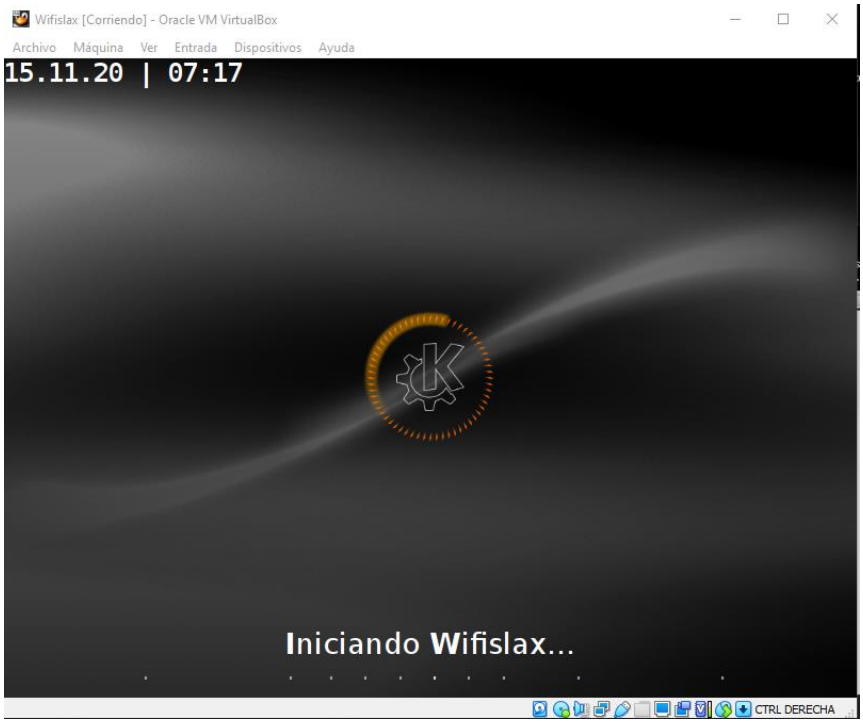


Figura N° 18: Verificando Hora del Sistema

Fuente: Elaboración propia

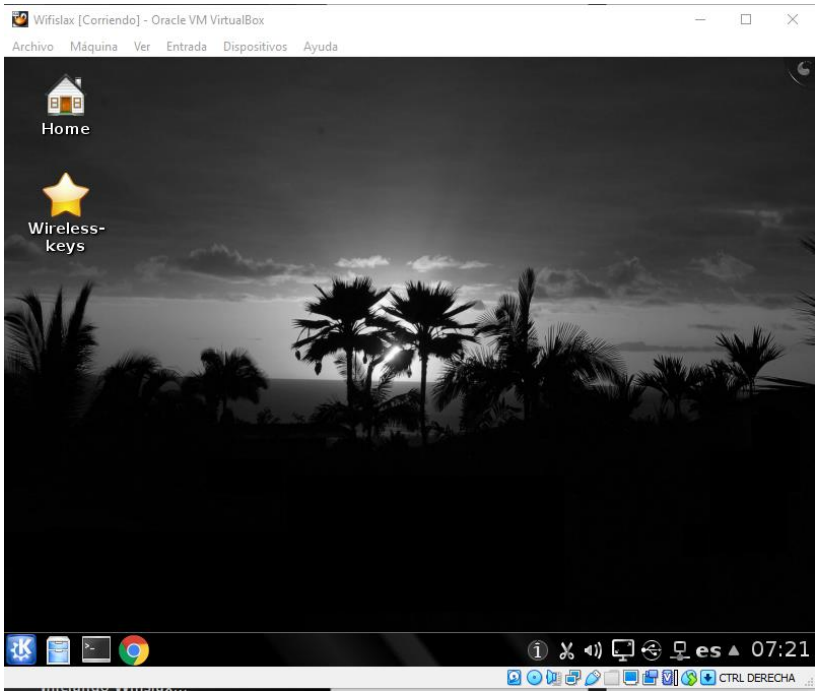


Figura N° 19: Interfaz del Programa

Fuente: Elaboración propia

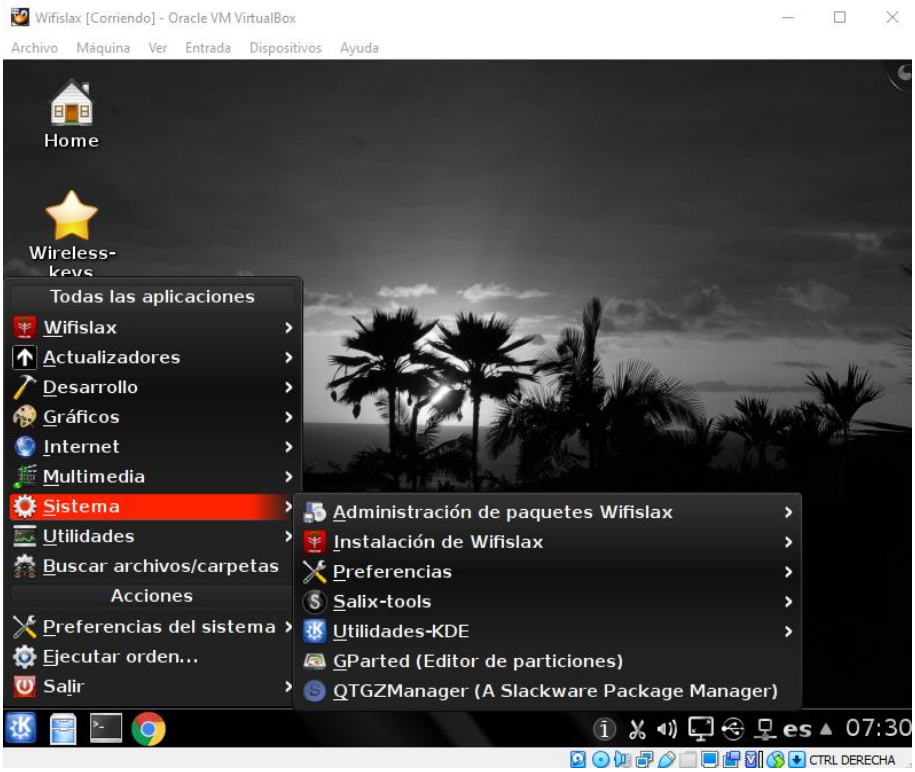


Figura N° 20: Editor de Particiones.
Fuente: Elaboración propia

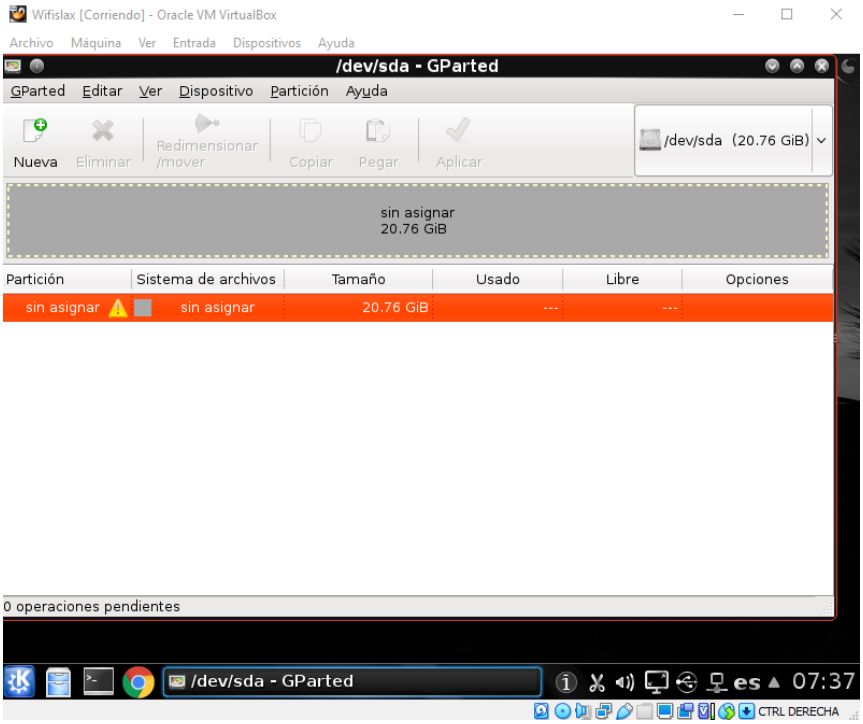


Figura N° 21: Tabla de Particiones.
Fuente: Elaboración propia

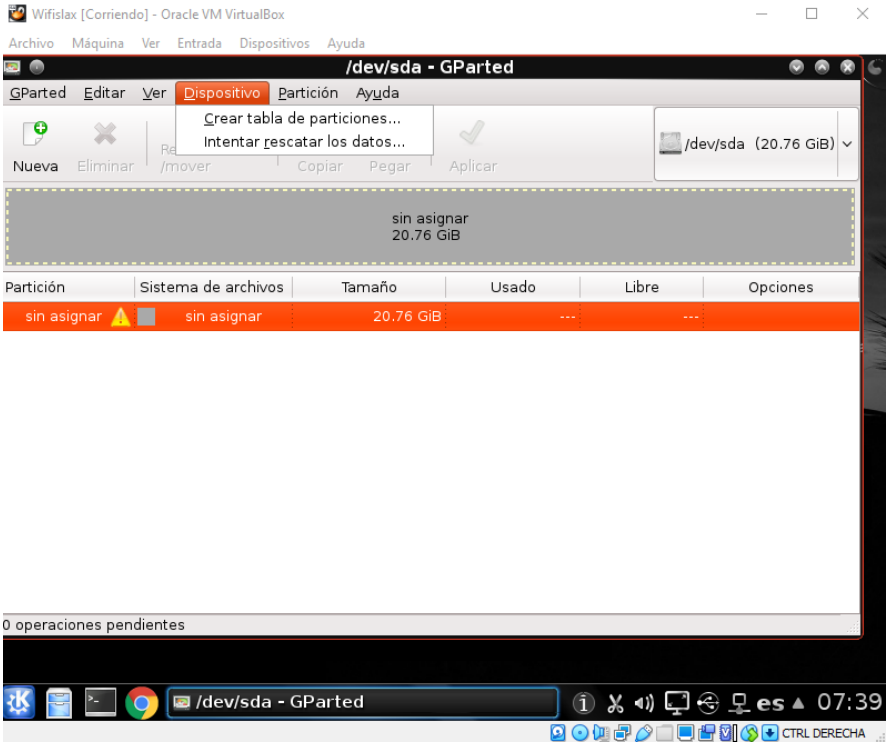


Figura N° 22: Selección del Dispositivo de Partición

Fuente: Elaboración propia

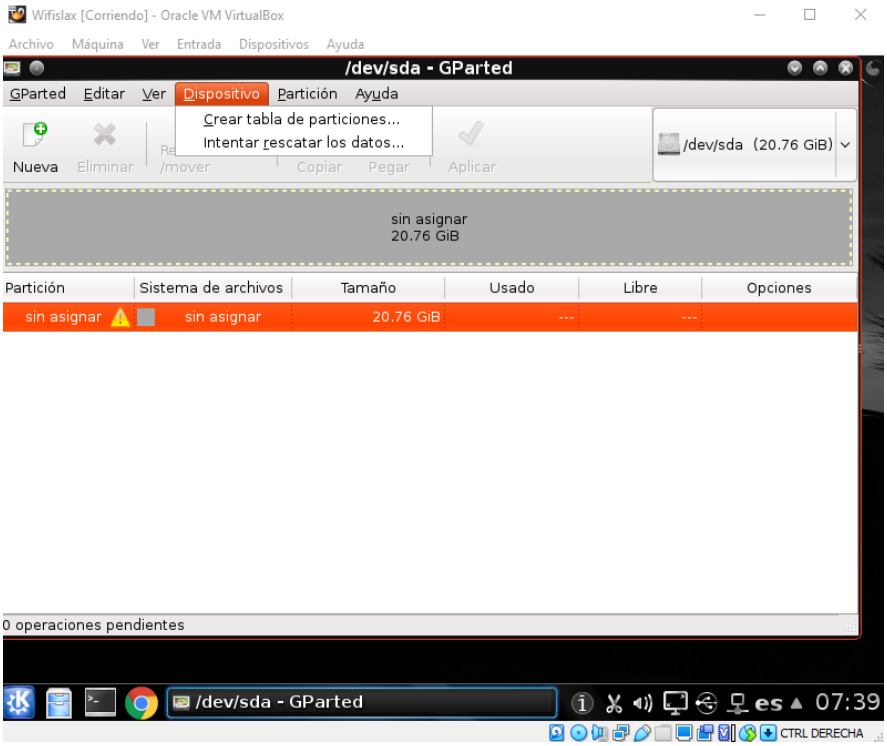


Figura N° 23: Creación de la Tabla de Particiones.
Fuente: Elaboración propia

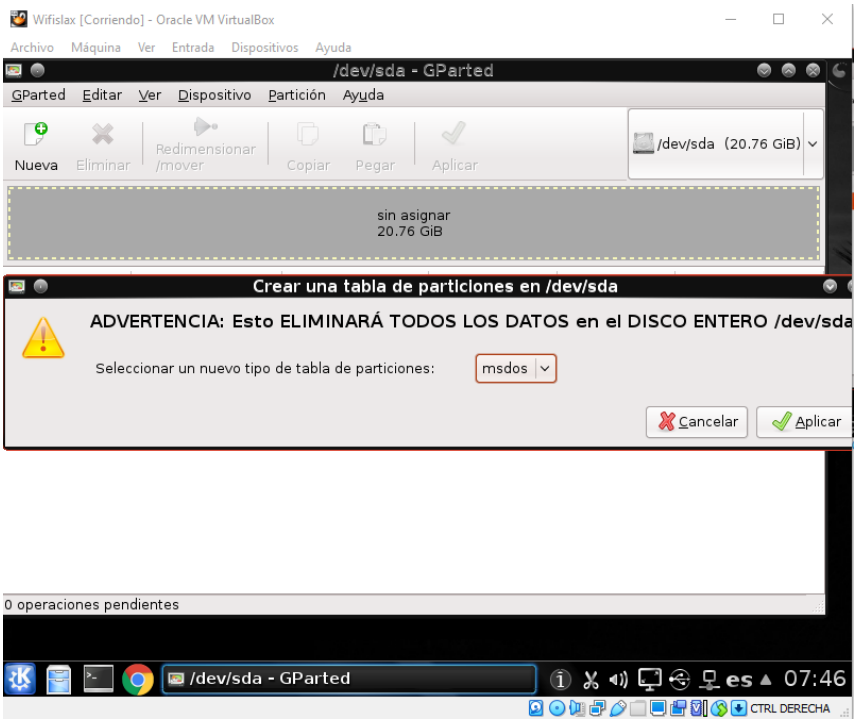


Figura N° 24: Formateo de la Partición.
Fuente: Elaboración propia

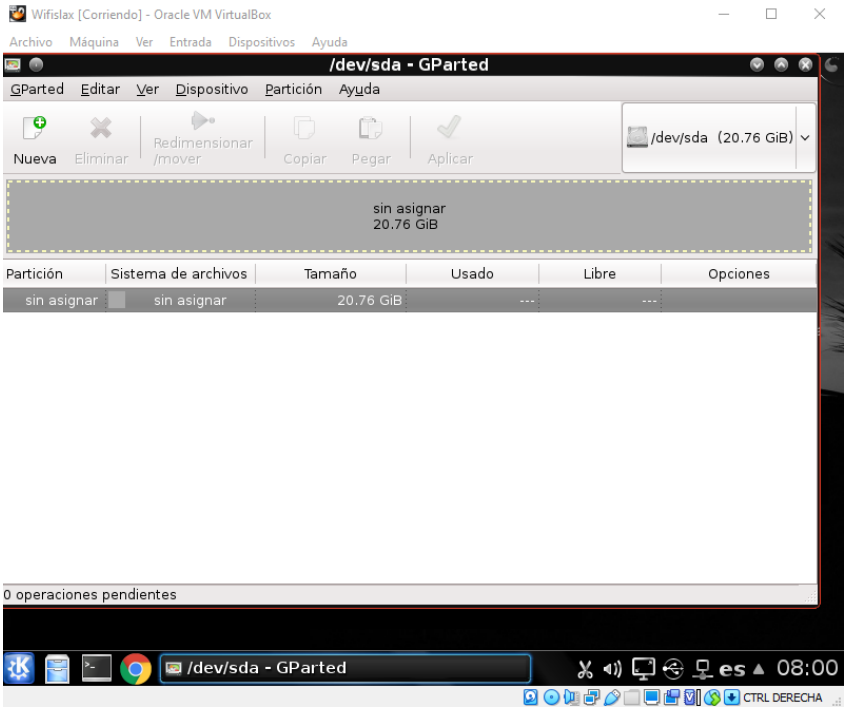


Figura N° 25: Partición sin Asignación.
Fuente: Elaboración propia

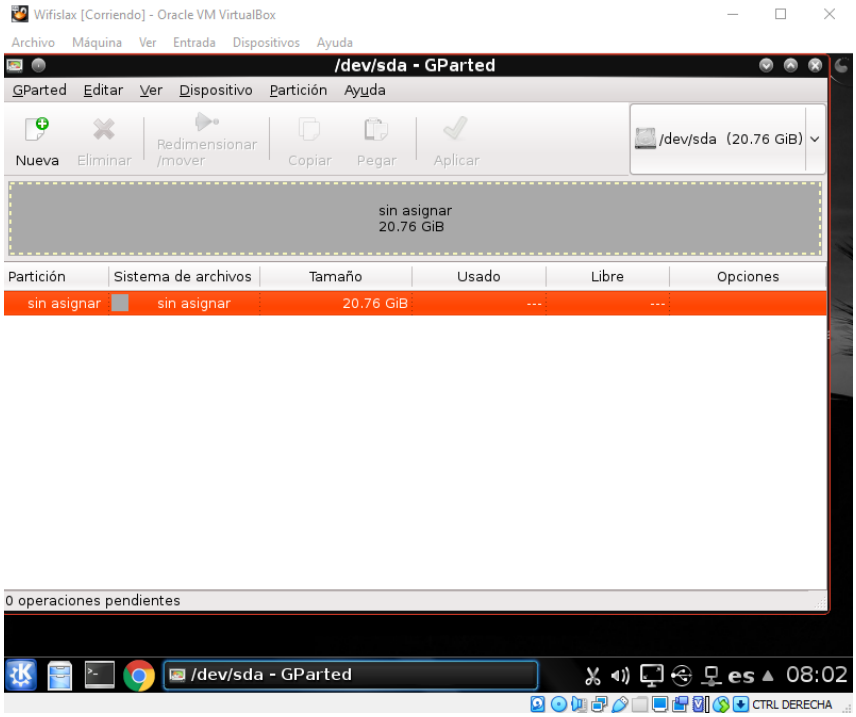


Figura N° 26: Asignación de la Partición.
Fuente: Elaboración propia

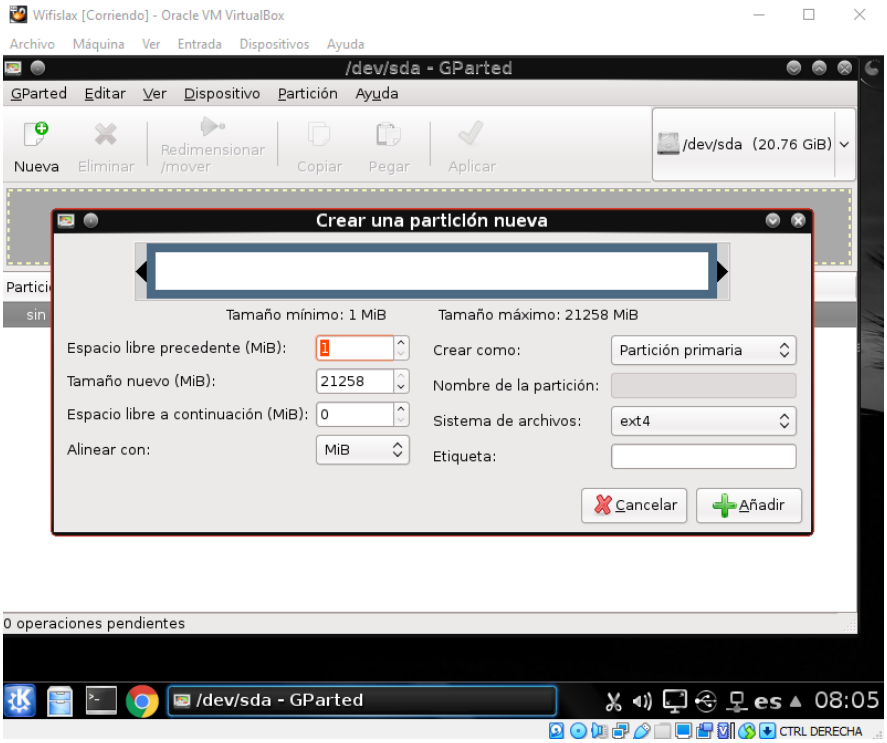


Figura N° 27: Edición de la Partición.
Fuente: Elaboración propia

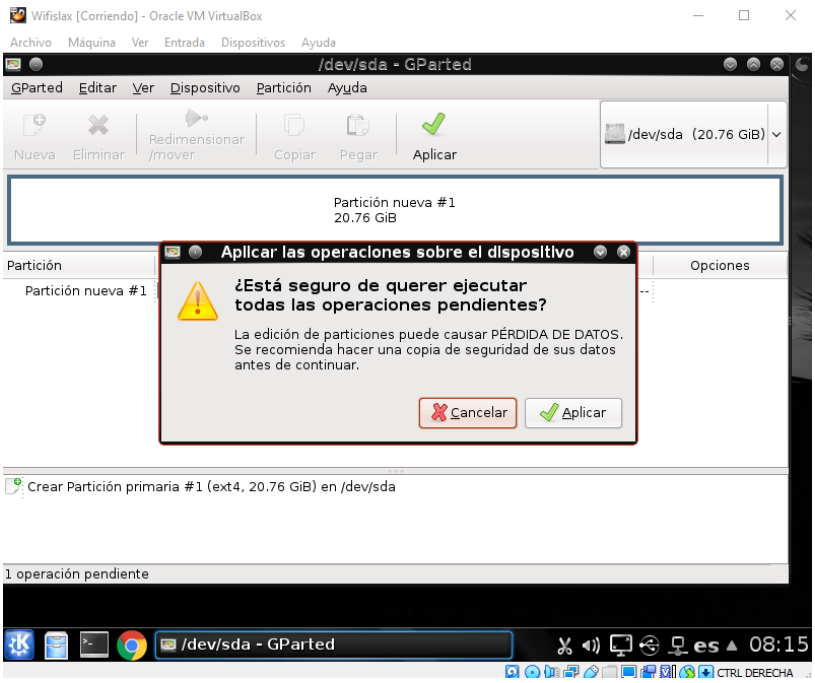


Figura N° 28: Ejecución de la Partición.
Fuente: Elaboración propia

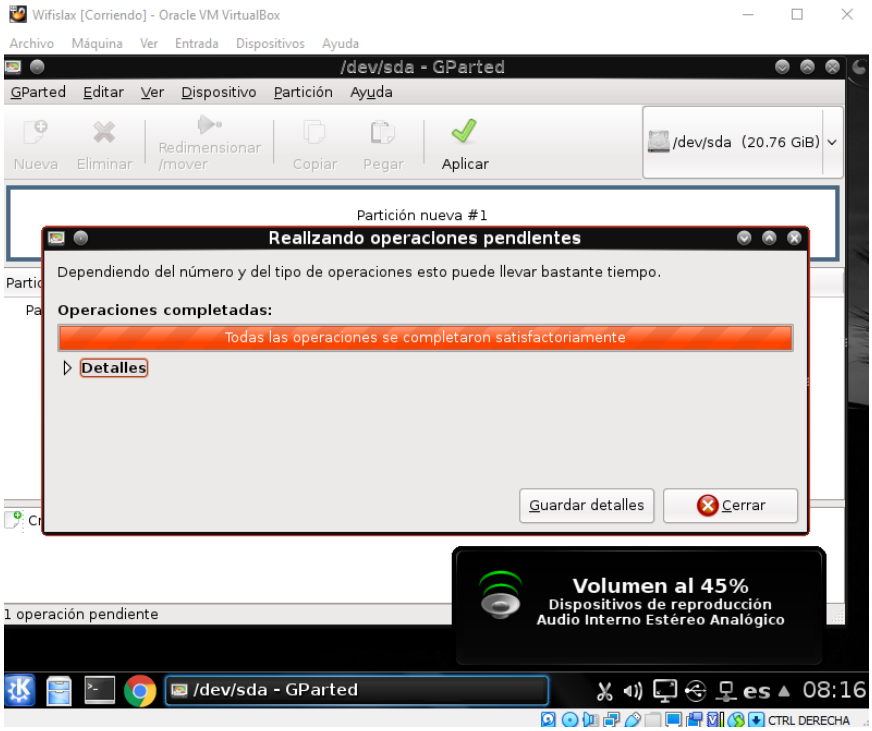


Figura N° 29: Ejecuciones Pendientes.
Fuente: Elaboración propia

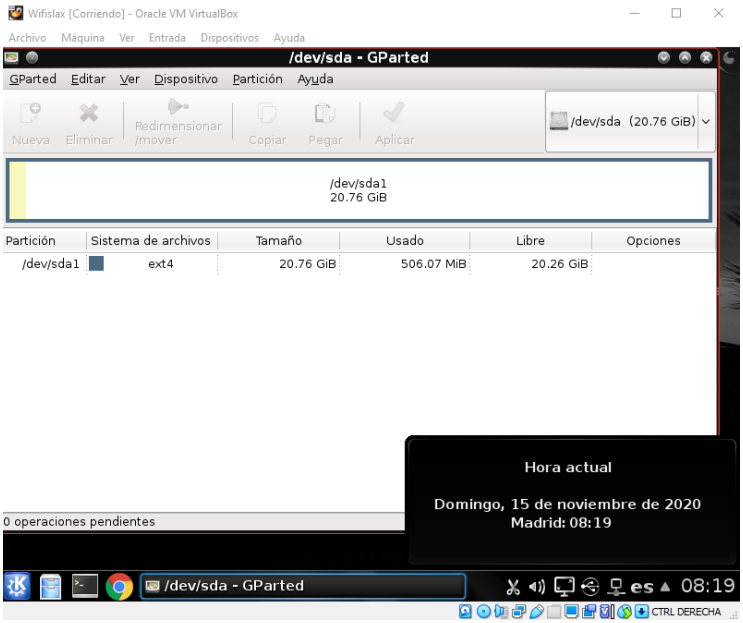


Figura N° 30: Culminación de la Partición.
Fuente: Elaboración propia

Figura N° 31: Instalación dentro de la Partición.
Fuente: Elaboración propia

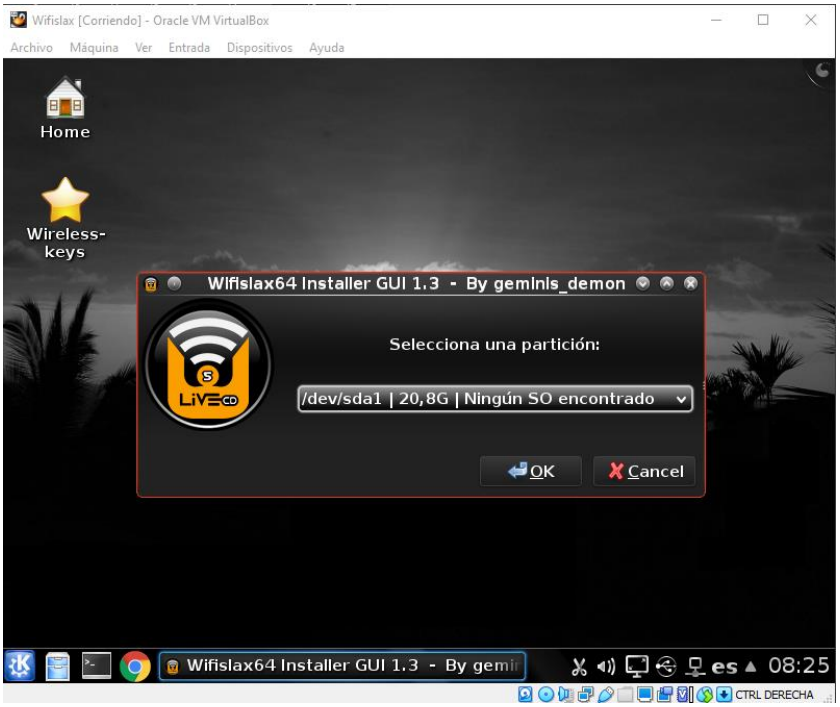


Figura N° 32: Selección del Instalador Gráfico y Partición.
Fuente: Elaboración propia

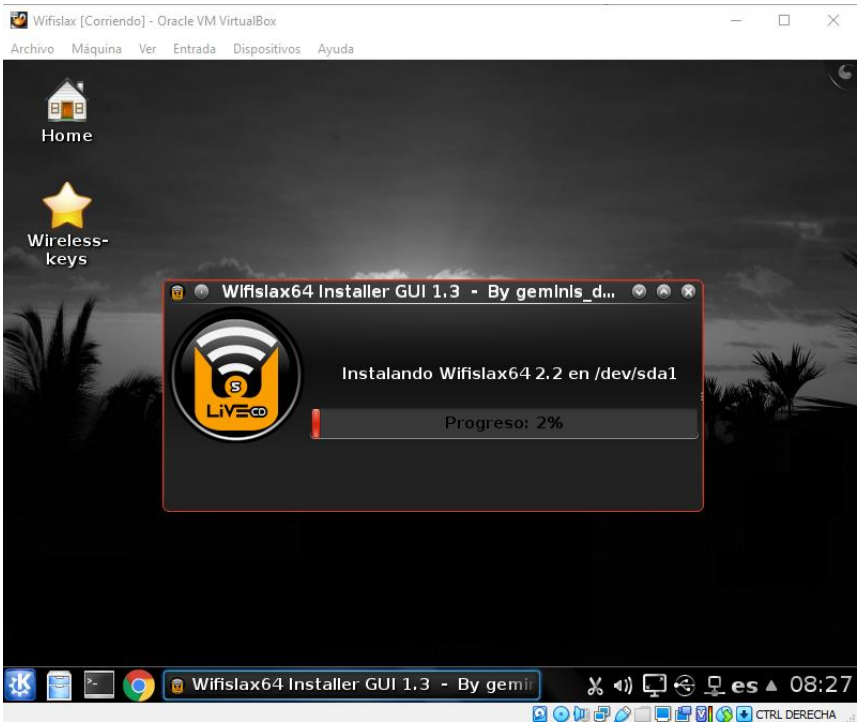


Figura N° 33: Instalación en Progreso.
Fuente: Elaboración propia

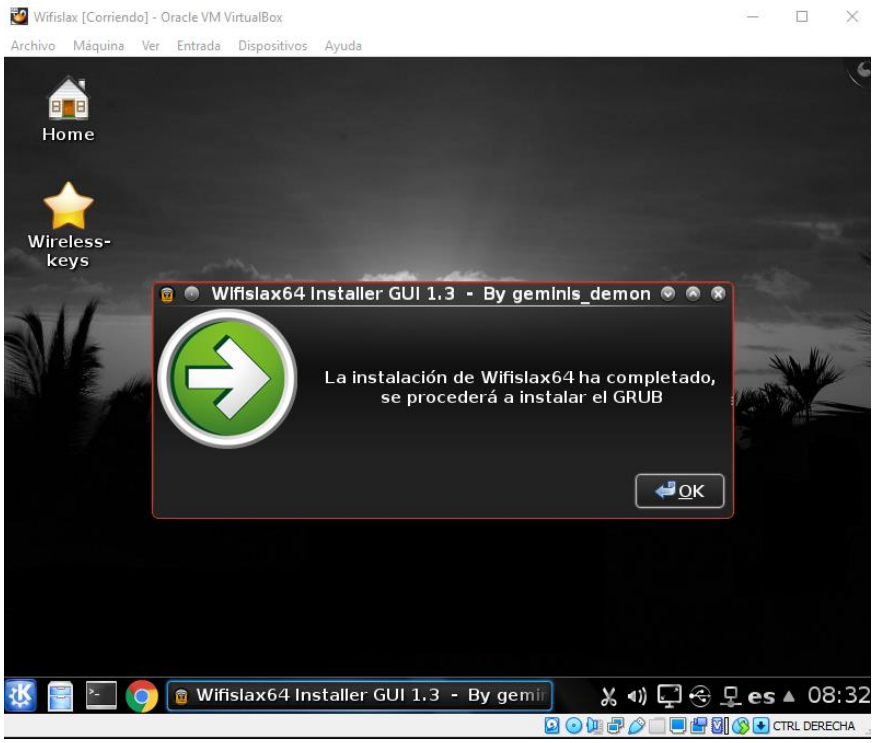


Figura N° 34: Instalación Completada.
Fuente: Elaboración propia

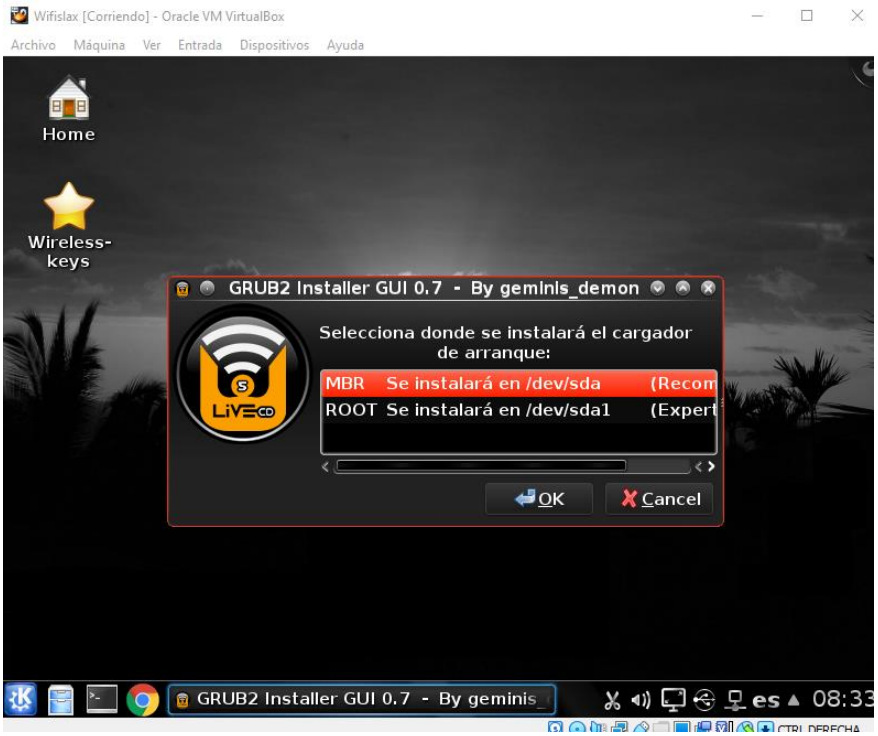


Figura N° 35: Instalación del grub (motor).
Fuente: Elaboración propia

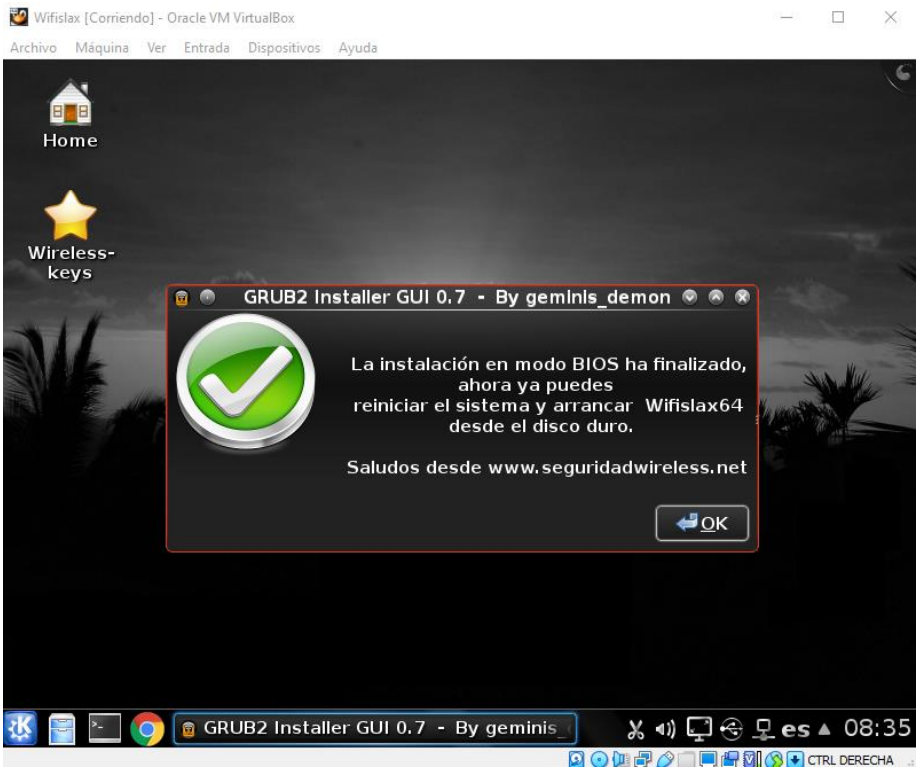


Figura N° 36: Instalación el Disco Duro (o Sólido).
Fuente: Elaboración propia

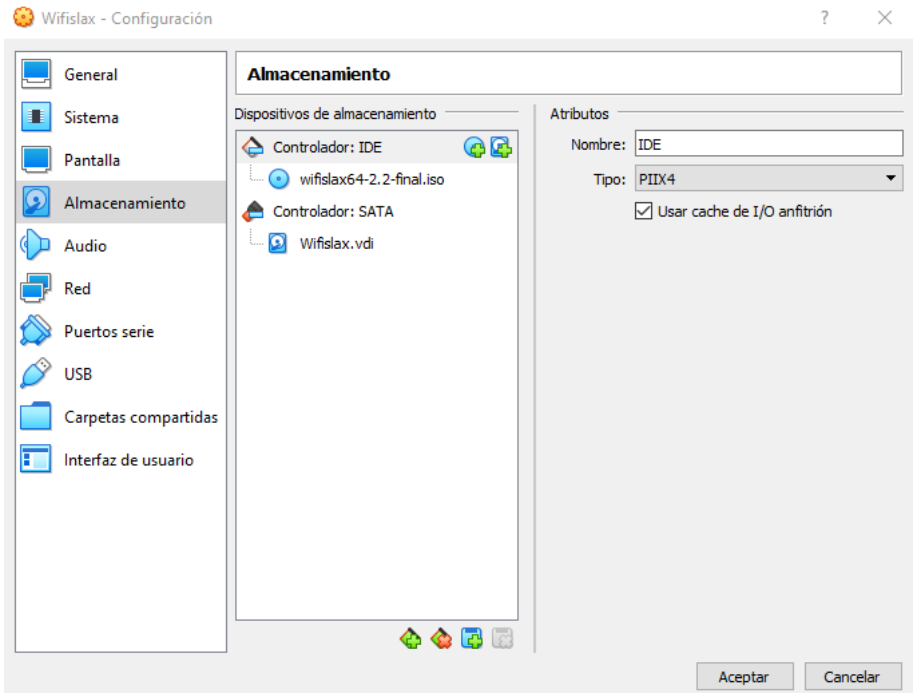


Figura N° 37: Almacenamiento en la máquina Virtual.
Fuente: Elaboración propia

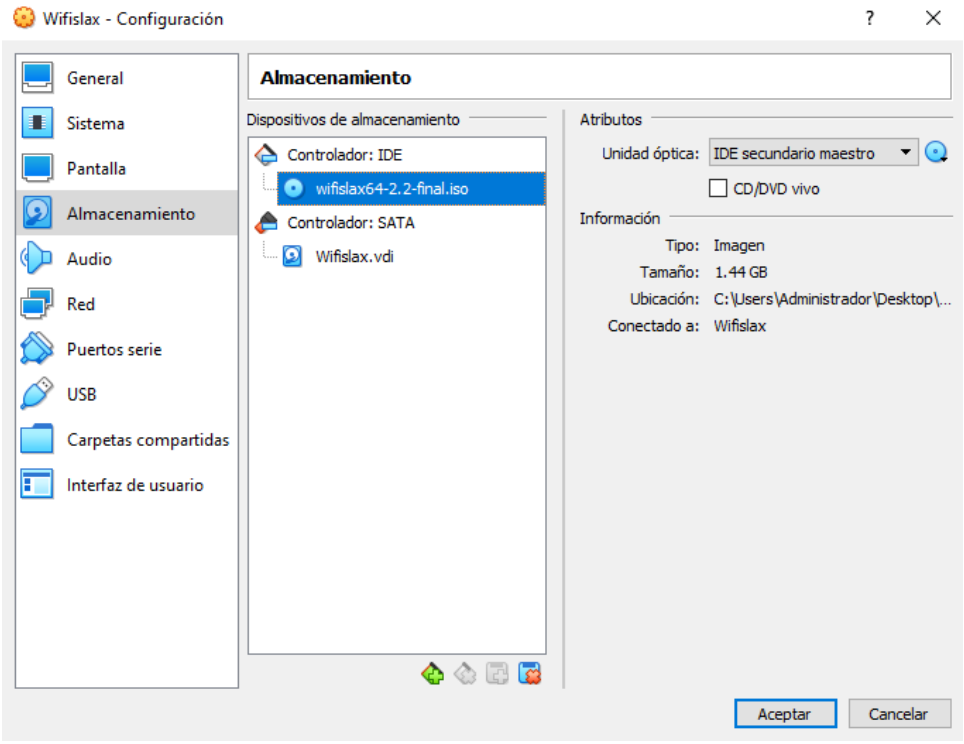


Figura N° 38: Eliminación de la Imagen ISO.
Fuente: Elaboración propia

Anexo Nº 14: Instalación y virtualización del OpenVAS

Figura N° 39: Instalación del OpenVAS. Fuente: https://openvas.org

Hasta este apartado, hemos tratado todo lo referente a las herramientas utilizadas comúnmente en el hacking ético de tipo local.

Sin embargo, es indispensable mencionar el uso de las herramientas de uso no local, es decir de las ***herramientas de uso remoto que utiliza el hacking ético***. Nos referimos explícitamente a aquellas que utilizan servidores que se encuentran en la nube y que requieren de algunas claves como las direcciones IP o contraseñas de las bases de datos para atacar al objetivo.

Entre los más populares tenemos al ***OpenVAS***, el cual es un software libre que puede correr en Kali Linux, tanto de manera local como remota.

¿Qué es el OpenVas y para qué sirve?

Traducido al español, significa literalmente: Escáner de Evaluación de Vulnerabilidad Abierta. Este resulta ser un escáner de vulnerabilidades con todas sus funcionalidades.

Las capacidades que incluye resultan ser tanto pruebas autenticadas como no autenticadas, protocolos de tipo industrial y cibernético, tanto de alto como de bajo nivel. Se puede programar para ejecutar escaneos de gran magnitud ya que posee internamente un lenguaje de programación muy robusto el mismo que se presta para la implementación de una prueba de vulnerabilidad, sea cual fuere su grado de dificultad.

Este escáner viene acompañado por un paquete de pruebas contra las vulnerabilidades, contando con una gran base de datos y constantes actualizaciones

diarias. Este software es administrado por la organización ***Greenbone***, la cual es una comunidad Open Source de código abierto.

Asimismo, este canal comunitario cuenta con más de 50,000 pruebas de pentesting. Este producto es constantemente desarrollado por ***Greebone Networks*** desde el año2009. Todas sus realizaciones son aportadas a la comunidad bajo la licencia GNU (Software Libre) en código abierto.

Greebone elabora OpenVas como un complemento de su gama de productos especializados en la gestión de vulnerabilidades de tipo comercial, también conocidas como: **"*Greebone Security Manager"*** (GSM).

Asimismo, OpenVAS es un producto que a la vez forma parte de una estructura más amplia. Cuando este se combina con módulos adicionales de código abierto, se convierte en el ***Greebone Vulnebility Management***, que viene a ser una gran solución para muchos problemas.

Basado en esto, todos los dispositivos relacionados con GSM, emplean a la vez fuentes de alimentación muy amplias, las mismas que cubren las necesidades de la organización. Un GVM que posea muchas funcionalidades adicionales con administración de una gran cantidad de dispositivos de hardware para arribar a un buen acuerdo final de servicio con un gran valor agregado de calidad viene a ser su objetivo terminal

Antecedentes del OpenVAS

Transcurría el año 2005 y sucedió que los programadores de los escáneres de vulnerabilidades de la prestigiosa organización ***NESSUS***, tomaron la decisión de terminar con el desarrollo de software de código abierto y optaron por desarrollar software privativo.

Frente a esta situación, los programadores de ***Intervation*** y ***DN-System***, que fueran las empresas que posteriormente fueran los fundadores de ***Greenbone Networks***, ya habían prestado servicios a ***NESSUS*** y se centraron específicamente en el desarrollo de herramientas de software a nivel cliente. Estos desarrollos fueron auspiciados por la **Oficina Federal de Alemania para la Seguridad de la Información (BSI)**.

Es así que durante el año 2006 y el 2007, tuvieron una actividad muy poco relevante, siendo que, a finales del año 2008, fundaron la organización ***Greenbone Networks GmbH***, la cual tuvo su sede en Osnabrück (Alemania) y desde entonces comenzaron a impulsar el desarrollo de OpenVAS. En este punto, la perspectiva de negocios de ***Greenbone*** tenía sus cimientos en tres soportes:

1. Ir más allá del simple escaneo de vulnerabilidades, para efectuar soluciones holísticas.
2. Crear un servicio al cual los clientes pudieran acceder con un determinado código de acceso.
3. Proseguir con los proyectos de software de código abierto a efectos de crear tecnología con seguridad y transparencia.

Posteriormente, en al año 2008 se aperturaron dos organizaciones más: la ***Secpod*** en la India y la ***Security Space*** en Canadá.

Las dos organizaciones tenían como meta el desarrollo de pruebas de pentesting y se aliaron a ***Greenbone*** para iniciar la producción de servicio de pruebas de vulnerabilidad muy fiables y constantemente actualizadas. De esta manera, se comenzaron a depurar aquellas pruebas de penetración que no eran del todo confiables o compatibles o que tenían problemas de licencia para iniciar un nuevo derrotero de partida limpio y transparente. Luego de ello el crecimiento comenzó a ser rápido y sostenido.

Seguidamente, ***Greenbone*** comenzó a construir los primeros núcleos adicionales para la elaboración de soluciones en el manejo de vulnerabilidades. Así también, la elaboración de su sitio web como su presentación se desplegaron desde cero e igualmente sucedió con el Core de sus productos.

De manera paralela, el escáner de OpenVAS, mejoró significativamente y de manera vertiginosa y dejó de ser compatible con sus anteriores versiones. Toda la producción de tipo Open Source fueron ofertados con la marca OpenVAS.

Es así que los primeros productos y servicios de hacking remoto como el ***Greebone Vulnerability Manager***, fueron introducidos al mercado a mediados del año 2010.

Desde los años 2010 hasta 2016 el nivel de comercialización aumentó y mejoró de manera sistemática al mismo tiempo que los productos de código abierto. El manejo de gestión de pentesting se incrementó para trasladar avisos de seguridad los cuales se actualizaban día a día y se ofreció al público un producto con una licencia compatible con GNU con certificación alemana, respaldadas por la **Oficina Federal de Alemania para la Seguridad de la Información (BSI)**, la cual respaldó a OpenVAS de manera sostenida y hasta la actualidad.

Ya en el mes de marzo del 2017, el llamado entorno OpenVAS llegó al nivel de su versión 9.0. Durante su campaña de promoción, se implementaron muchos nuevos núcleos con muchas nuevas funcionalidades. Así también, se desarrollaron cientos de miles de fragmentos de código los cuales fueron publicitados por un numeroso equipo de programadores los mismos que iban en aumento.

Fue durante el año 2017 que comenzó una nueva etapa para OpenVAS, principalmente porque ***Greenbone*** destacó como la fuerza propulsora de OpenVAS, clarificando la originalidad de la marca. Tanto es así, que hubo un cambio de nombre, se pasó de ***"Marco Openvas"*** a **"*Greebone Vulnerability Management"*** (GVM), en donde Escáner OpenVAS, forma parte.

Luego del lanzamiento de OpenVAS, versión 9.0 le sucedió el "(GVM-10), en donde no se realizaron cambios de licencia alguna y todos los núcleos mantuvieron su status de código abierto.

El siguiente gran cambio significativo ocurrió también en el año 2017, cuando las contribuciones de código abierto fueron ofrecidas por otras organizaciones relacionadas que compartían la misma tecnología y programación, haciendo pasar el software como si fuera de su propia autoría o sosteniendo que poseían una tecnología superior, que eran la mejor opción o que tenían el mejor precio, pero solo una pequeña minoría cumplía con los estándares GLP.

Actualmente, ya ninguna de esas empresas relacionadas trabaja con ***Greenbone***, lográndose de esta manera una mejor viabilidad de sus productos, ausencia de malentendidos y una mejor imagen de la producción de OpenVAS. Se cambió el

nombre al de ***"Greebone Community Feed"*** y se internalizó la programación del feed. Asimismo, las actualizaciones pasaron de ser de quincenales a diarias.

A inicios del 2018, vino el tercer gran cambio significativo cuando a su tecnología nativa se le incorporó la de GitHub y un foro de tipo comunitario. Toda esta transformación se concluyó durante el año 2018, aumentando tanto la producción como las acciones comunitarias.

Recientemente, en el año 2019, se concluyó con la escisión de las marcas y es por ello que ahora la letra "S" de OpenVAS, significa "Sistema" en vez del anterior "Escáner". Todo ello, siempre junto a su conocido logotipo recientemente actualizado y es por ello que el marco en donde se encuentra insertado el OpenVAS es conocido ahora como **"*Greebone Vulnerability Management"*** (GVM).

El actual OpenVas distribuido con el GVM-10 ha recibido gran cantidad de optimizaciones para optar así, por una mayor captación de vulnerabilidades al escanear blancos objetivos y redes cada vez más grades y proveídas de gran heterogeneidad.

El lanzamiento de OpenVAS conjuntamente con GVM-11, muestra significativos cambios sustanciales en su arquitectura en donde el anterior servicio **openvasd** se transforma solo en una línea de comando. Este entorno está administrado por una capa de operaciones **ospd.opevas**. Bajo esta nueva concepción, se opta ahora por eliminar al anterior **OTP** (Protocolo de transferencia de OpenVas) el cual tenía un estado constante y privativo por el **OSP** (Protocolo de Escaneo Abierto), el cual no posee un estado constante y está basado en programación XML con un veloz requerimiento de respuesta y totalmente de carácter genérico.

Figura N° 40: OpenVAS en Kali Linux.
Fuente: https://openvas.org

Evaluación de Vulnerabilidades

Es el proceso de ubicar y reportar las vulnerabilidades. Esto proporciona una manera de detectar y resolver los problemas de seguridad antes de la explotación de alguien o algo.

La razón de realizar este procedimiento es debido a ser un componente crítico en la infraestructura de seguridad de varias organizaciones, pues la habilidad de tener una instantánea de la seguridad de toda la red, apoya a diversos procesos de seguridad y administrativos.

Cuando se descubre una nueva vulnerabilidad, se puede realizar una evaluación para descubrir los sistemas vulnerables, iniciar el proceso para la instalación de parches. Después de esto, se debe realizar otra evaluación para verificar la solución de las vulnerabilidades.

Este ciclo de evaluar, parchar y verificar se ha convertido en un método estándar para manejar los temas de seguridad en varias organizaciones.

* OpenVAS: http://openvas.org/

Figura N° 41: Evaluación de Vulnerabilidades en OpenVAS. Fuente: https://openvas.org

Tipos de Evaluaciones

1. Evaluaciones de Host

Estas herramientas requieren instalar el software en cada sistema requerido a ser evaluado. Se evalúan vulnerabilidades a nivel del sistema como permisos de archivos inseguros, parches ausentes de software, políticas de seguridad para el cumplimiento de normas, e instalaciones de puertas traseras o troyanos.

2. Evaluaciones de Red

Implica localizar a todos los sistemas funcionando en la red, determinar los servicios de red utilizados, y analizarlos por probables vulnerabilidades. Este tipo de evaluaciones pueden ser escalables y eficientes en términos de requerimientos administrativos, y son el único método factible para estimar la seguridad de redes grandes y complejas sobre sistemas heterogeneos.

Figura N° 42: Tipo de Evaluaciones en OpenVAS. Fuente: https://openvas.org

El Proceso de Evaluación

Sin importar en gran medida cual es la solución utilizada para la evaluación de vulnerabilidades, es muy probable se realice el mismo proceso de evaluación.

- Detectar los Sistemas en Funcionamiento
- Identificar los Sistemas en Funcionamiento
- Enumerar los Servicios
- Identificar los Servicios
- Identificar las Aplicaciones
- Identificar las Vulnerabilidades
- Reportar las Vulnerabilidades

Figura N° 43: Proceso de Evaluación en OpenVAS. Fuente: https://openvas.org

OpenVAS

OpenVAS (Open Vulnerability Assessment System) o Sistema Abierto para la Evaluación de Vulnerabilidades; está constituido por varios servicios y herramientas los cuales proporcionan la capacidad para realizar un escaneo de vulnerabilidades muy completo y poderoso, además de ser una solución para la administración de vulnerabilidades.

El corazón de esta arquitectura es el Escaner OpenVAS orientada al servicio, asegurado utilizando SSL. Este muy eficiente escaner ejecuta los NVTs - Network Vulnerability Tests (Pruebas de Vulnerabilidad en Redes), los cuales son servidos con actualizaciones diarias mediante el OpenVAS NVT Feed o mediante el servicio comercial, con más de 30,000 de ellos en total.

Todos los productos OpenVAS son Software Libre. Y la mayoría de componentes tienen licencia GNU/GPL.

* OpenVAS: http://www.openvas.org/about.html

Figura N° 44 Siglas del OpenVAS.
Fuente: https://openvas.org

Características de OpenVAS

- **OpenVAS Scanner:** Escaneo de varios objetivos de manera concurrente. OpenVAS Transfer Protocol (OTP), Soporte SSL.

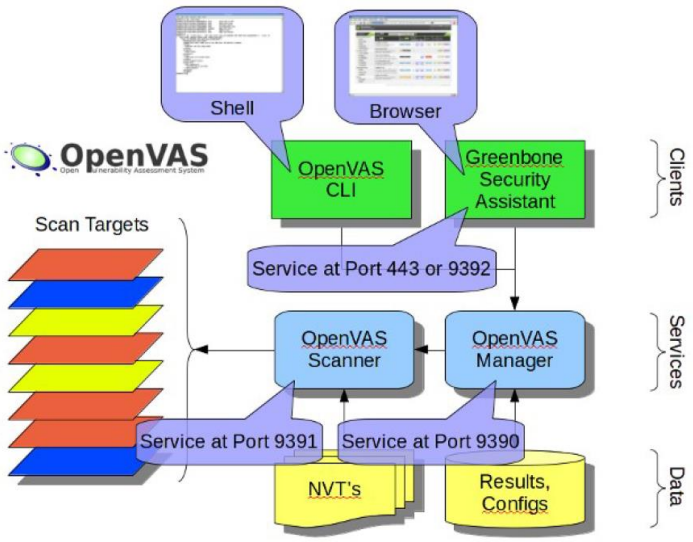
- **OpenVAS Manager:** OpenVAS Management Protocol (OMP), Base de Datos SQL (sqlite) para las configuraciones y resultados del escaneo, Soporte SSL para OMP (siempre), Varias tareas de escaneo concurrentes (Varios escaners OpenVAS), Gestor de notas para los resultados del escaneo, Gestor de falsos positivos para los resultados del escaneo. Escaneos programados, Detener, pausar y reiniciar tareas de escaneo. Modo Maestro-Esclabo para controlar varias instancias desde un nodo central, Reportes en varios formatos (XML, HTML, etc.), Gestor de usuarios, etc.

- **Greenbone Security Assistant (GSA):** Cliente para OMP y OAP, HTTP y HTTPS, Servidor web propio (microhttpd), no se requiere un servidor web adicional, Sistema de ayuda integrado en línea.

* Features Overview: http://www.openvas.org/software.html#feature_overview

Figura N° 45: Características del OpenVAS.
Fuente: https://openvas.org

Resumen de la Arquitectura de OpenVAS



* http://openvas.org/software.html

Figura N° 46: Arquitectura del OpenVAS.
Fuente: https://openvas.org

El Gestor de OpenVAS

Es el servicio central quién consolida el escaneo de vulnerabilidades en una solución completa para la gestión de vulnerabilidades.

El Manejador controla el Escaner mediante OTP - OpenVAS Transfer Protocol (Protocolo OpenVAS de Transferencia) y ofrece por si mismo OMP - OpenVAS Management Protocol (Protocolo de Gestión OpenVAS) basado en XML.

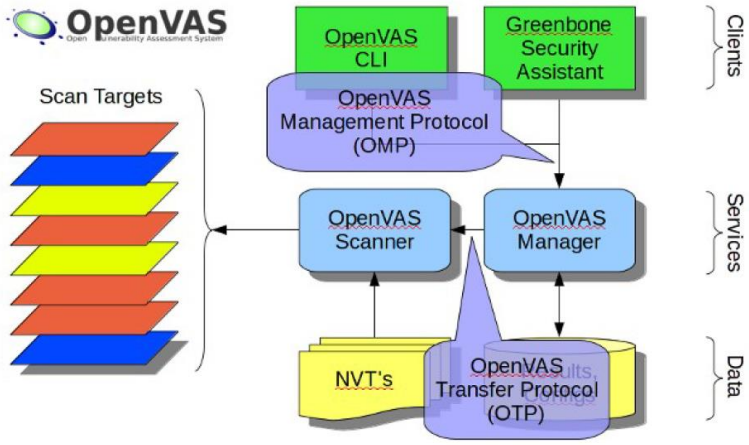
Toda la inteligencia es implementada en el Gestor, así es posible implementar varios tipos de clientes con un comportamiento similar, por ejemplo con relación al filtrado y ordenamiento de los resultados del escaneo.

El Gestor también controla una base de datos SQL (basada en sqlite) donde se almacenan de manera centralizada toda la configuración y resultados del escaneo. Finalmente el gestor también controla la gestión de los usuarios incluyendo controles de acceso con grupos y roles.

* http://www.openvas.org/software.html

Figura N° 47: Gestor del OpenVAS.
Fuente: https://openvas.org

El Gestor de OpenVAS (Cont.)



* http://www.openvas.org/software.html

Figura N° 48: Gestor del OpenVAS (Cont.).
Fuente: https://openvas.org

Clientes de OpenVAS

Están disponibles diferentes clientes OMP.

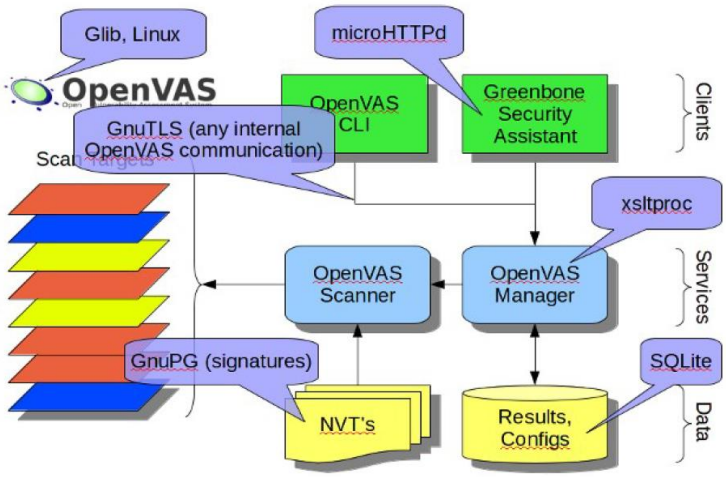
- **Greenbone Security Assistant (GSA)**: Es un servicio web el cual ofrece una interfaz de usuario para navegadores web. Este utiliza XSL (Extensible Stylesheet Language) el cual convierte las respuestas OMP en HTML.
- **OpenVAS CLI (Command-line Interface):** Contiene la herramienta en línea de comando “omp” el cual permite crear procesos batch (por lotes) para dirigir el Gestor de OpenVAS

La mayoría de las herramientas listadas comparten funcionalidad la cual esta añadida en las librerías OpenVAS.

El escaner OpenVAS ofrecen un protocolo de comunicación OTP (OpenVAS Transfer Protocol) el cual permite controlar la ejecución del escaneo.

Figura N° 49: Clientes del OpenVAS.
Fuente: https://openvas.org

Clientes OpenVAS (Cont.)



* http://openvas.org/software.html

Figura N° 50: Clientes del OpenVAS (Cont.).
Fuente: https://openvas.org

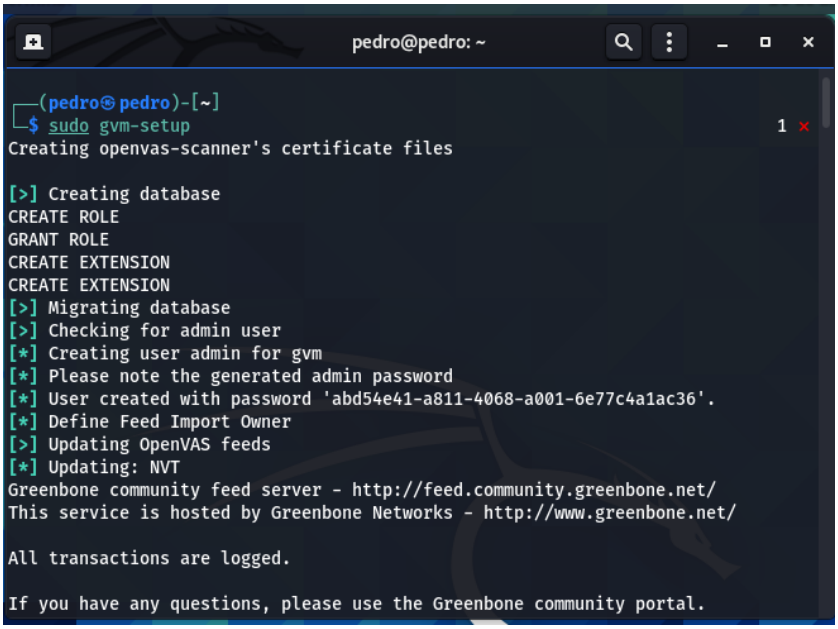


Figura N° 51: Instalación del OpenVAS en Kali Linux.
Fuente: https://openvas.org

Anexo Nº 15: Escaneo de la red

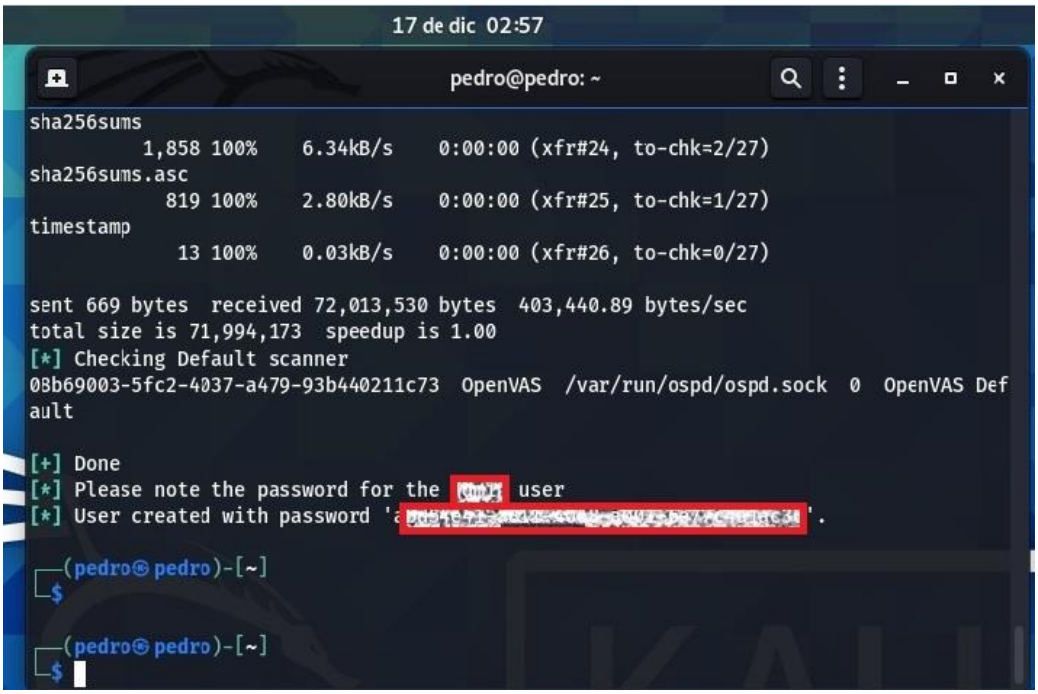


Figura N° 52: Generación del Usuario y Contraseña en OpenVAS - Kali Linux
Fuente: https://openvas.org

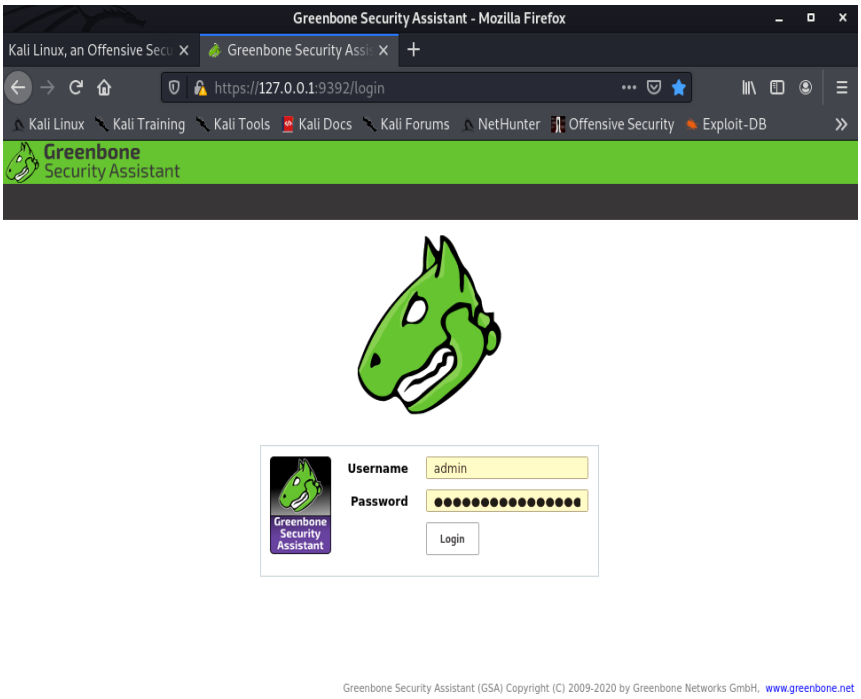


Figura N° 53: Ingresando a Greenbone en OpenVAS - Kali Linux.
Fuente: https://openvas.org

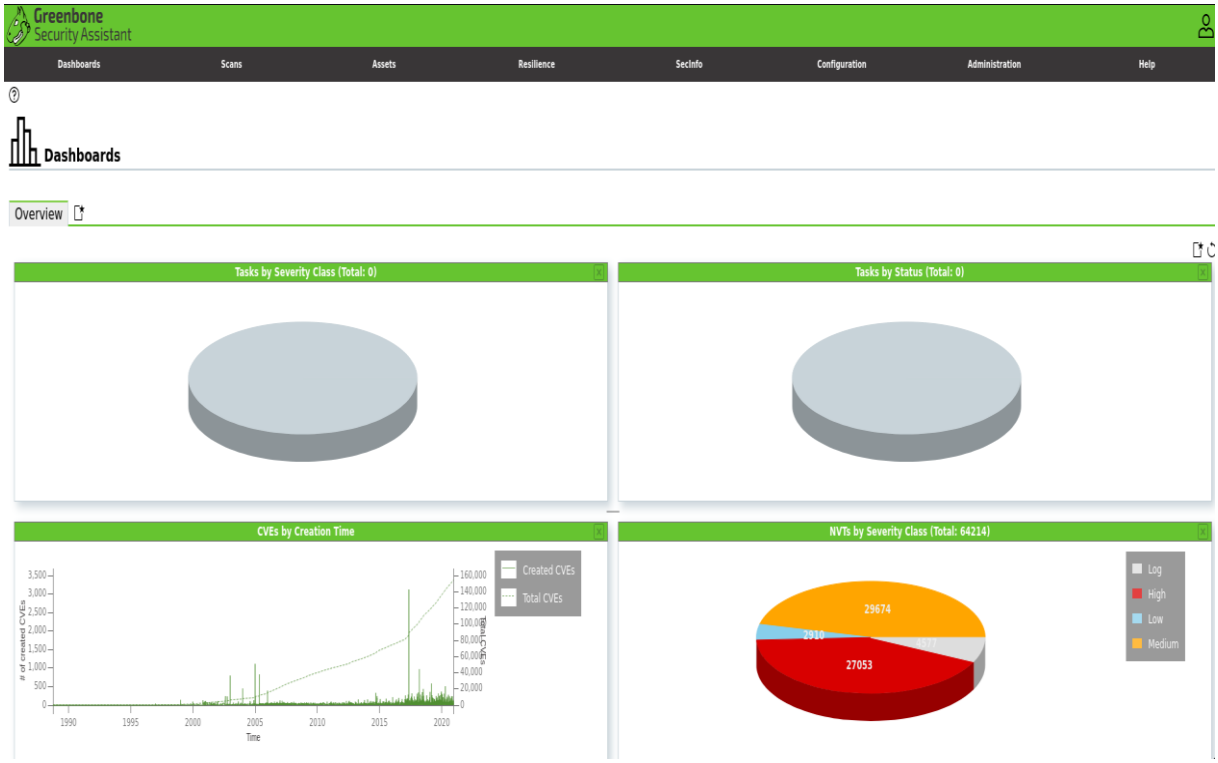


Figura N° 54: Dashboard de Vulnerabilidades de OpenVAS

Figura N° 55: Solicitud de tarea al Dashboard de Vulnerabilidades de OpenVAS

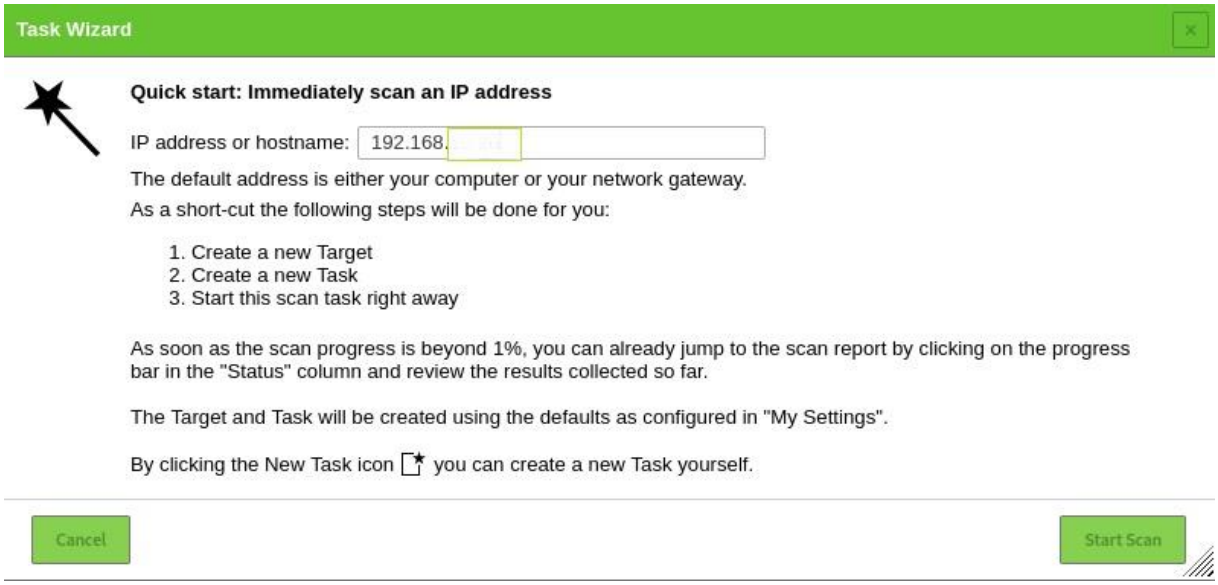


Figura N° 56: Colocando el IP Target al Dashboard de Vulnerabilidades de OpenVAS

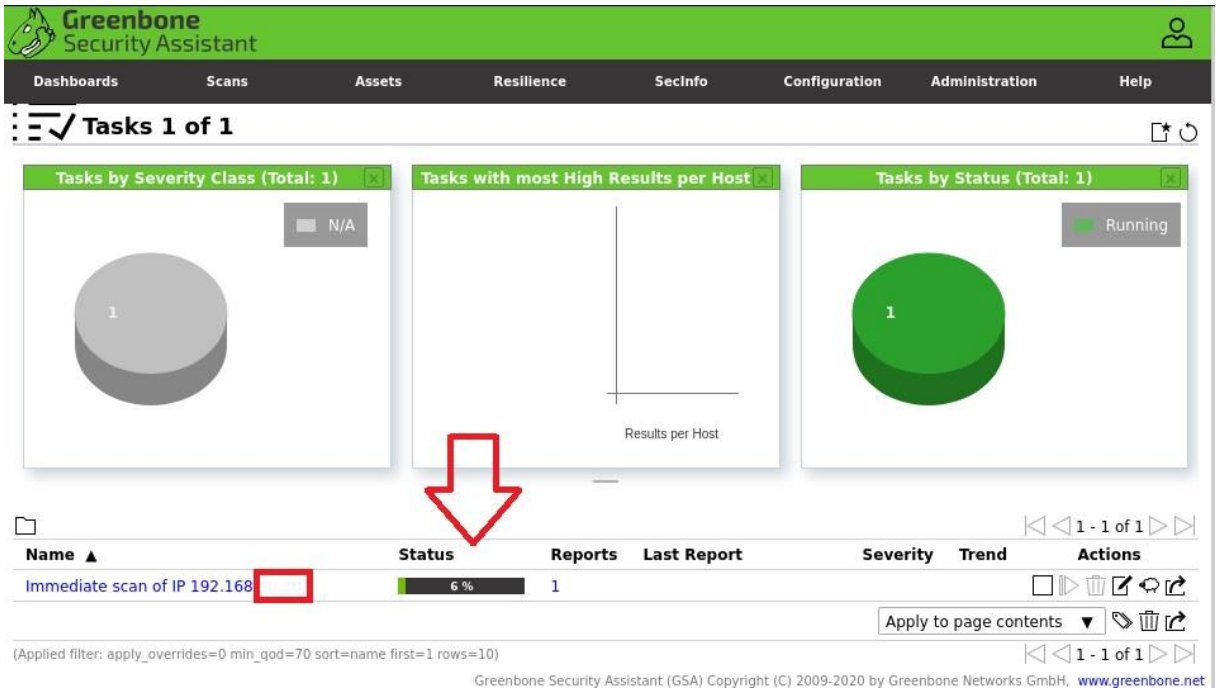


Figura N° 57: Progreso de escaneo en el Dashboard de Vulnerabilidades de OpenVAS

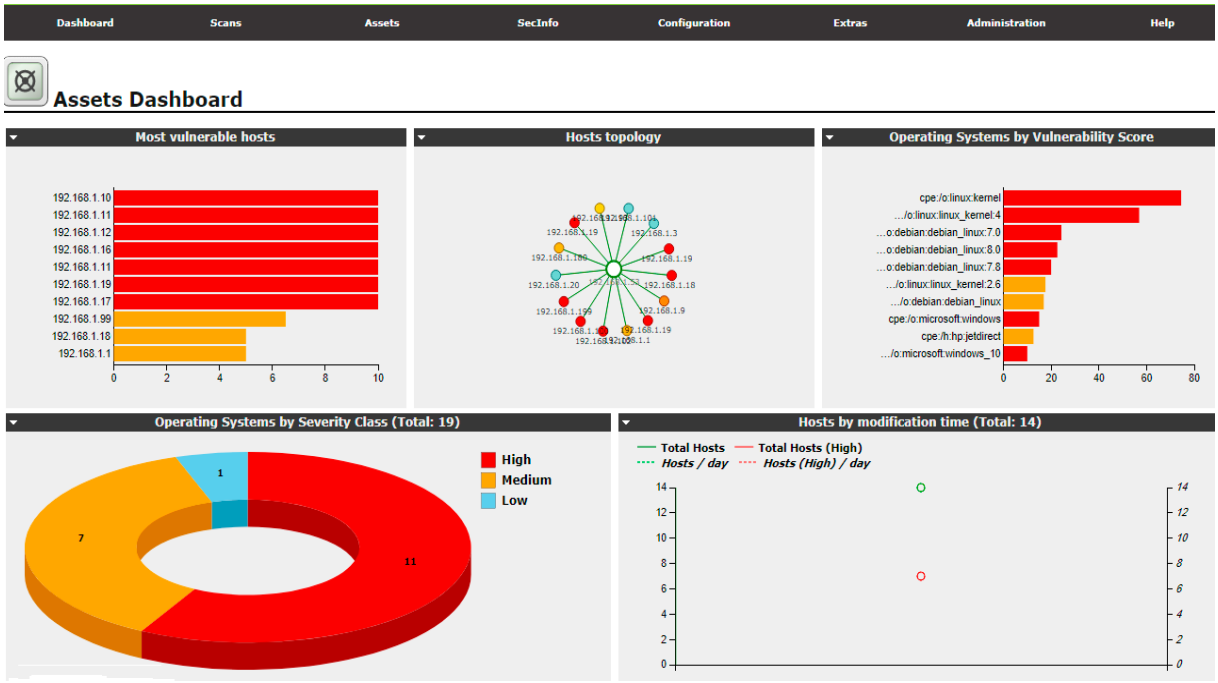


Figura N° 58: Resultados del escaneo en el Dashboard de Vulnerabilidades de OpenVAS

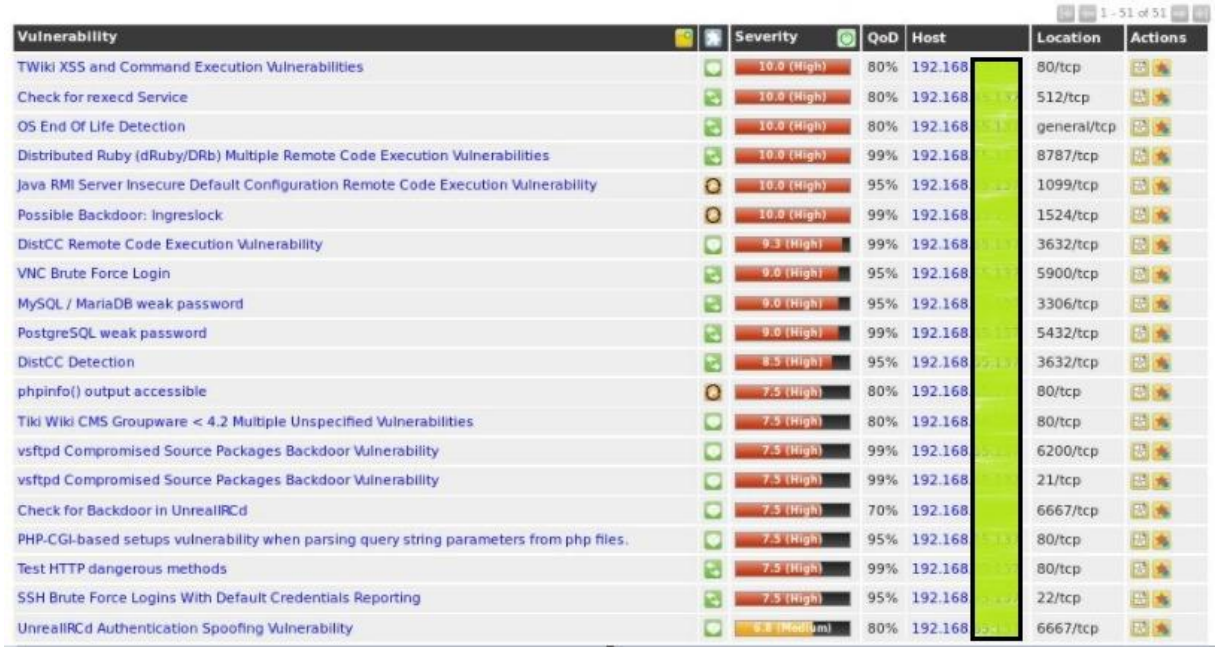


Figura N° 59: Reporte de Vulnerabilidades en OpenVAS

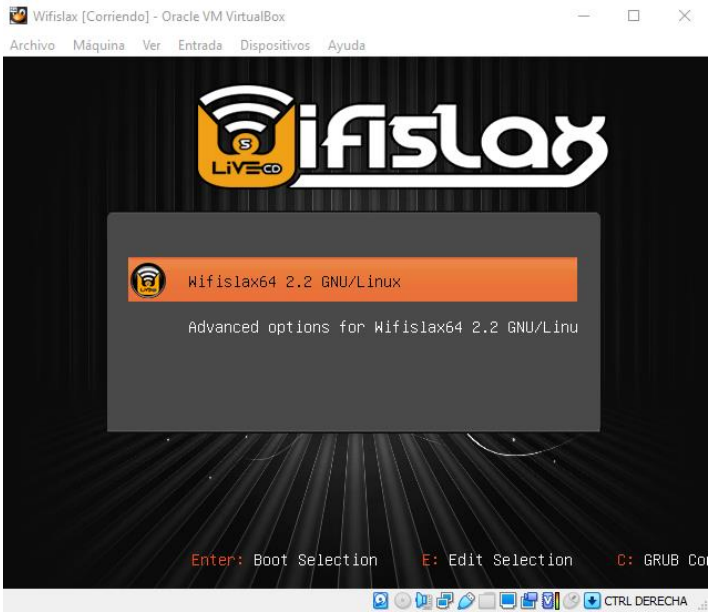


Figura N° 60: Levantamos el Sistema Operativo a Través de la Unidad Virtual (Partición Propia). Fuente: Elaboración propia

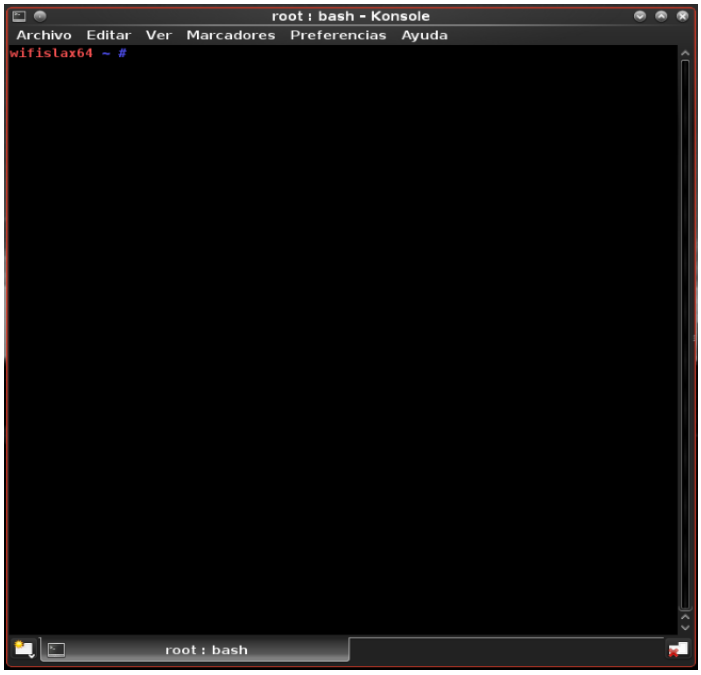


Figura N° 61: Prompt del Comando. Fuente: Elaboración propia

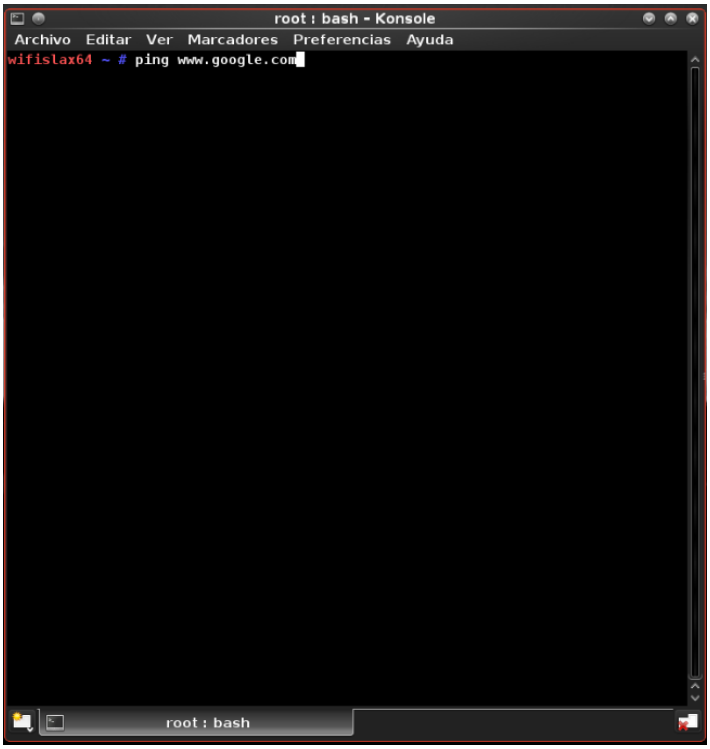


Figura N° 62: Prueba de Pineo. Fuente: Elaboración propia

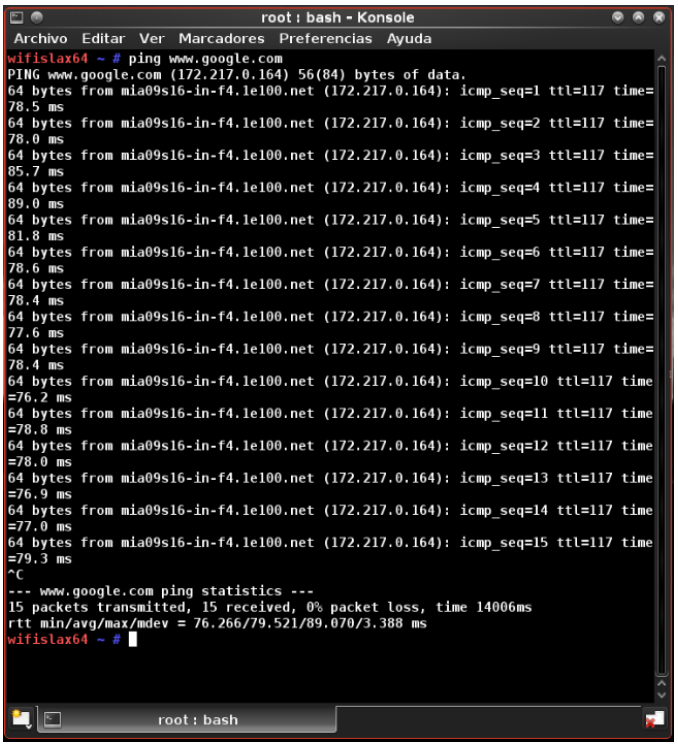


Figura N° 63: Pineo del Sistema. Fuente: Elaboración propia

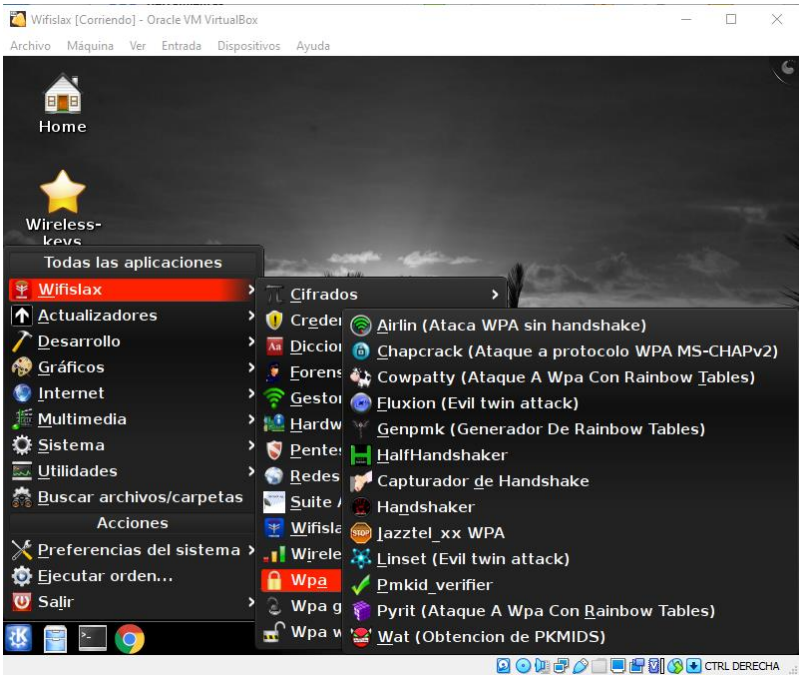


Figura N° 64: Selección de Linset.
Fuente: Elaboración propia

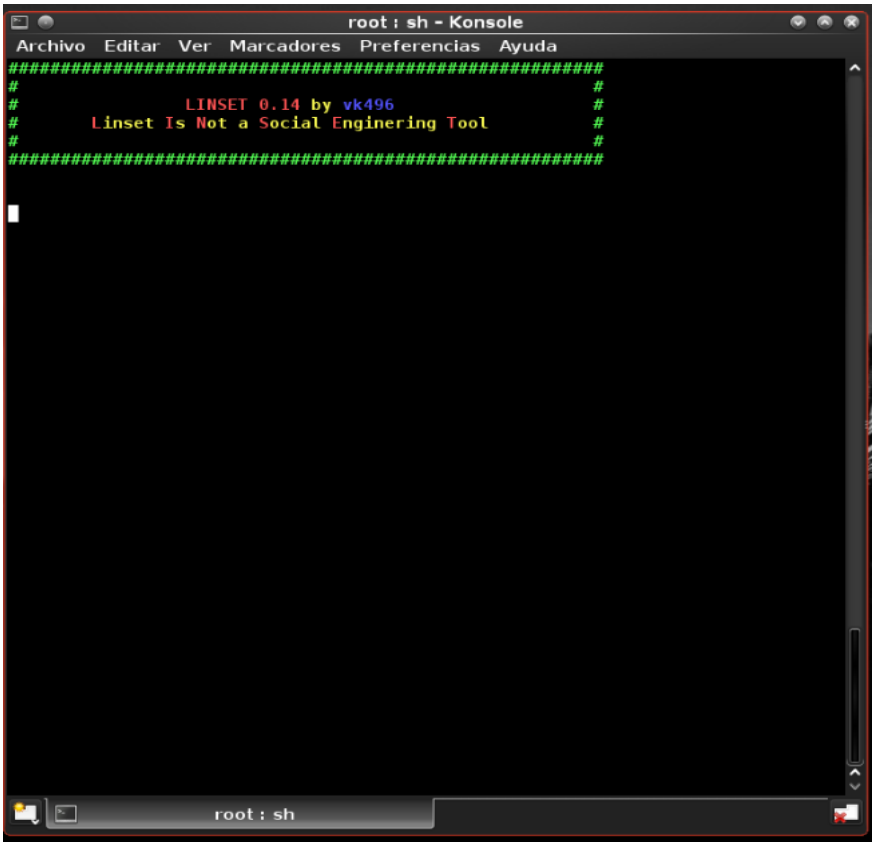


Figura N° 65: Interfaz de Linset. Fuente: Elaboración propia

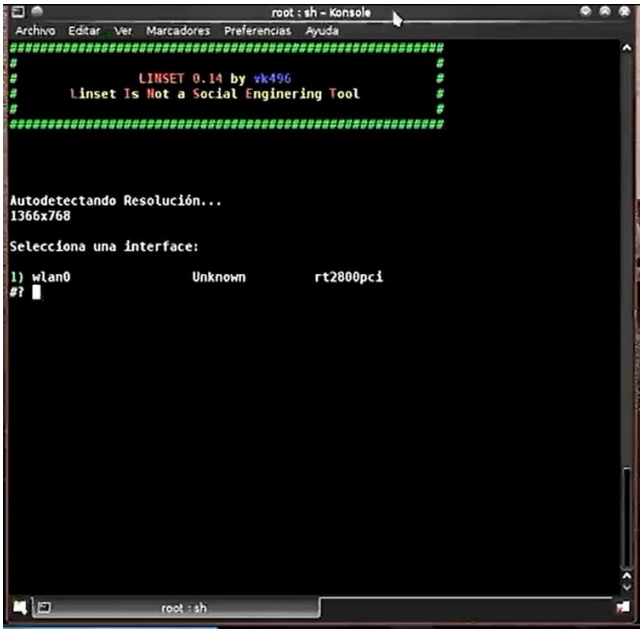


Figura N° 66: Selección de la Interfaz de Ataque.
Fuente: Elaboración propia

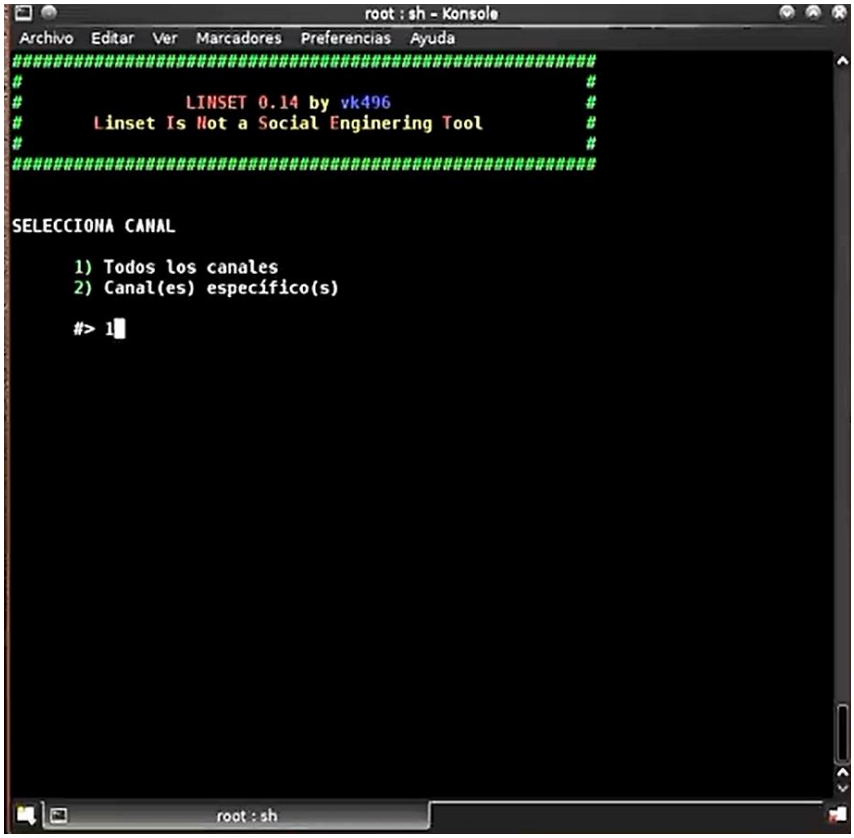
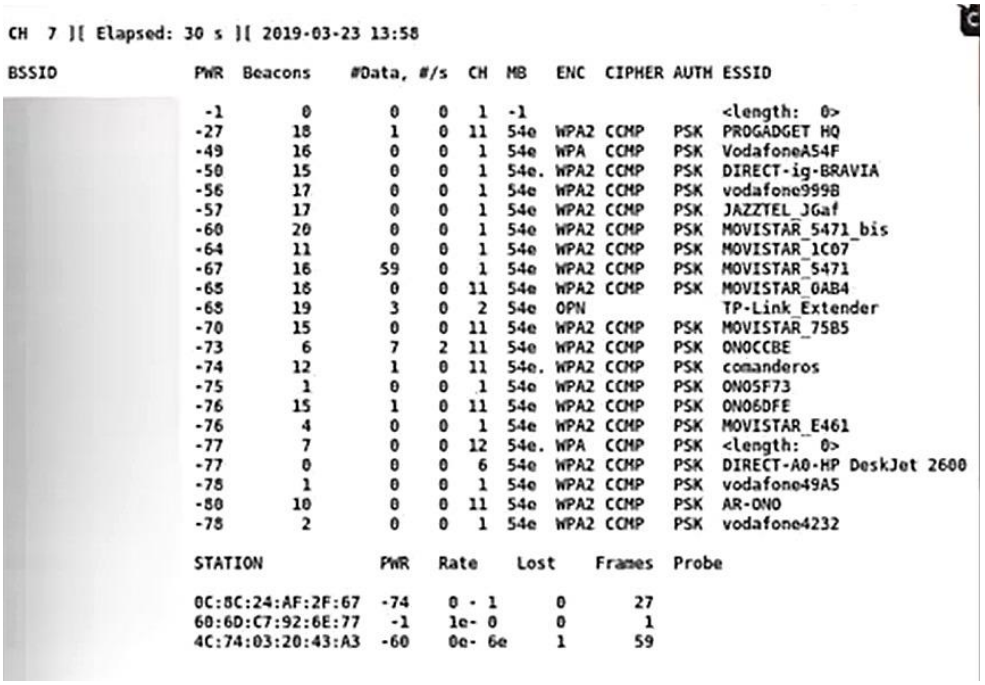
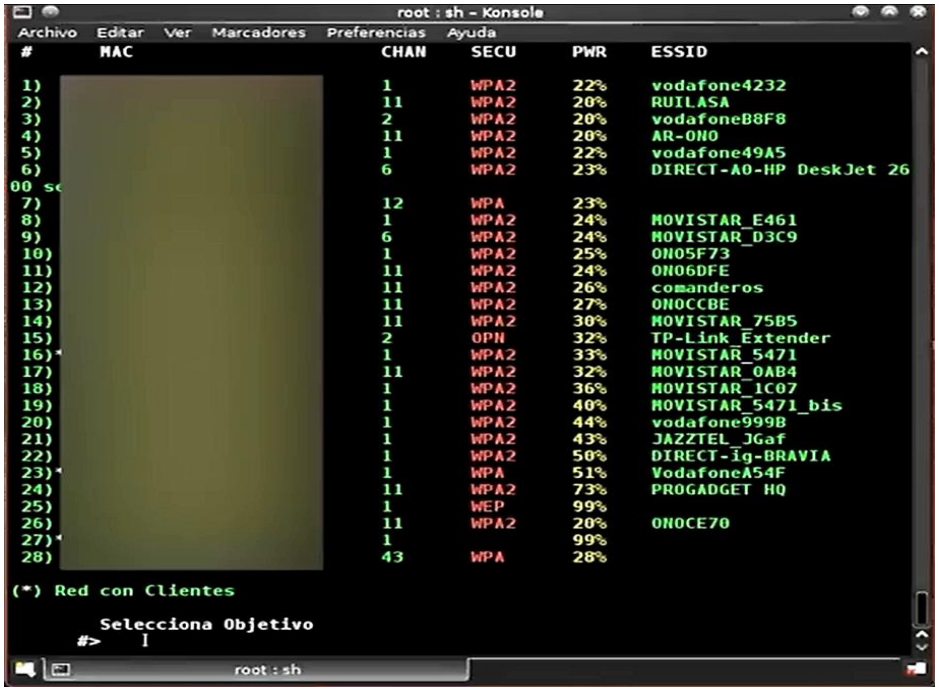


Figura N° 67: Selección del Canal.
Fuente: Elaboración propia



```
CH  7 ][ Elapsed: 30 s ][ 2019-03-23 13:58

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

                    -1        0        0    0   1  -1                    <length:  0>
                   -27       18        1    0  11  54e  WPA2 CCMP   PSK  PROGADGET HQ
                   -49       16        0    0   1  54e  WPA  CCMP   PSK  VodafoneA54F
                   -50       15        0    0   1  54e. WPA2 CCMP   PSK  DIRECT-ig-BRAVIA
                   -56       17        0    0   1  54e  WPA2 CCMP   PSK  vodafone999B
                   -57       17        0    0   1  54e  WPA2 CCMP   PSK  JAZZTEL_JGaf
                   -60       20        0    0   1  54e  WPA2 CCMP   PSK  MOVISTAR_5471_bis
                   -64       11        0    0   1  54e  WPA2 CCMP   PSK  MOVISTAR_1C07
                   -67       16       59    0   1  54e  WPA2 CCMP   PSK  MOVISTAR_5471
                   -65       16        0    0  11  54e  WPA2 CCMP   PSK  MOVISTAR_0AB4
                   -68       19        3    0   2  54e  OPN              TP-Link_Extender
                   -70       15        0    0  11  54e  WPA2 CCMP   PSK  MOVISTAR_75B5
                   -73        6        7    2  11  54e  WPA2 CCMP   PSK  ONOCCBE
                   -74       12        1    0  11  54e. WPA2 CCMP   PSK  comanderos
                   -75        1        0    0   1  54e  WPA2 CCMP   PSK  ONO5F73
                   -76       15        1    0  11  54e  WPA2 CCMP   PSK  ONO6DFE
                   -76        4        0    0   1  54e  WPA2 CCMP   PSK  MOVISTAR_E461
                   -77        7        0    0  12  54e. WPA  CCMP   PSK  <length:  0>
                   -77        0        0    0   6  54e  WPA2 CCMP   PSK  DIRECT-A0-HP DeskJet 2600
                   -78        1        0    0   1  54e  WPA2 CCMP   PSK  vodafone49A5
                   -80       10        0    0  11  54e  WPA2 CCMP   PSK  AR-ONO
                   -78        2        0    0   1  54e  WPA2 CCMP   PSK  vodafone4232

STATION            PWR   Rate    Lost    Frames  Probe

0C:8C:24:AF:2F:67  -74    0 - 1      0        27
60:6D:C7:92:6E:77   -1    1e- 0      0         1
4C:74:03:20:43:A3  -60    0e- 6e     1        59
```

Figura N° 68: Rastreo de Redes Wifi.
Fuente: Elaboración propia



```
root : sh - Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda
#       MAC                    CHAN    SECU     PWR    ESSID

 1)                            1       WPA2     22%    vodafone4232
 2)                            11      WPA2     20%    RUILASA
 3)                            2       WPA2     20%    vodafoneB8F8
 4)                            11      WPA2     20%    AR-ONO
 5)                            1       WPA2     22%    vodafone49A5
 6)                            6       WPA2     23%    DIRECT-A0-HP DeskJet 26
00 se
 7)                            12      WPA      23%
 8)                            1       WPA2     24%    MOVISTAR_E461
 9)                            6       WPA2     24%    MOVISTAR_D3C9
 10)                           1       WPA2     25%    ONO5F73
 11)                           11      WPA2     24%    ONO6DFE
 12)                           11      WPA2     26%    comanderos
 13)                           11      WPA2     27%    ONOCCBE
 14)                           11      WPA2     30%    MOVISTAR_75B5
 15)                           2       OPN      32%    TP-Link_Extender
 16)                           1       WPA2     33%    MOVISTAR_5471
 17)                           11      WPA2     32%    MOVISTAR_0AB4
 18)                           1       WPA2     36%    MOVISTAR_1C07
 19)                           1       WPA2     40%    MOVISTAR_5471_bis
 20)                           1       WPA2     44%    vodafone999B
 21)                           1       WPA2     43%    JAZZTEL_JGaf
 22)                           1       WPA2     50%    DIRECT-ig-BRAVIA
 23)                           1       WPA      51%    VodafoneA54F
 24)                           11      WPA2     73%    PROGADGET HQ
 25)                           1       WEP      99%
 26)                           11      WPA2     20%    ONOCE70
 27)                           1               99%
 28)                           43      WPA      28%

(*) Red con Clientes

      Selecciona Objetivo
    #>
root : sh
```

Figura N° 69: Captura de Redes Wifi.
Fuente: Elaboración propia

Figura N° 70: Filtrado de Wifi Objetivo. Fuente: Elaboración propia

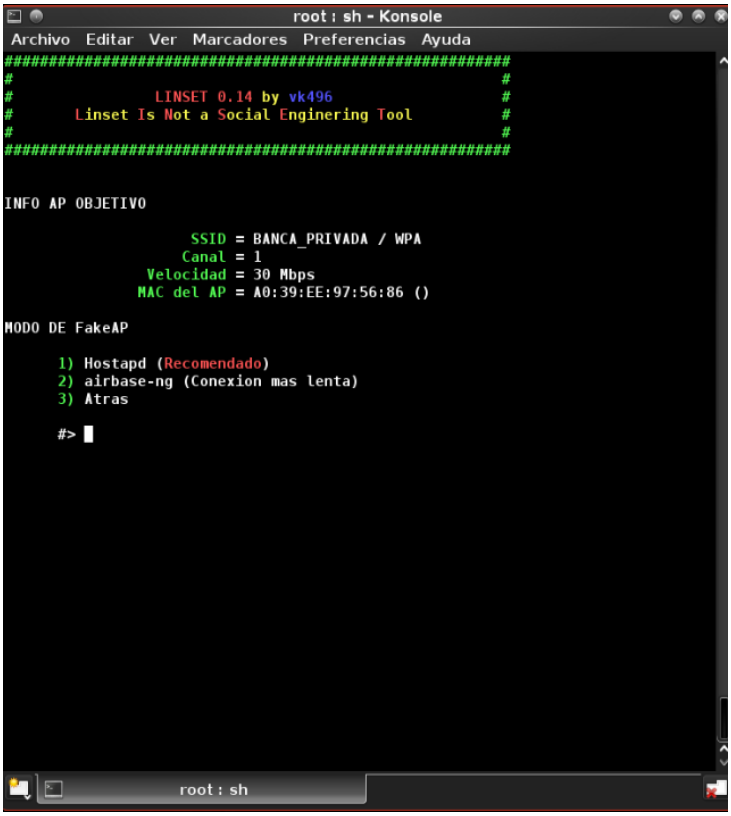


Figura N° 71: Información del Objetivo. Fuente: Elaboración propia

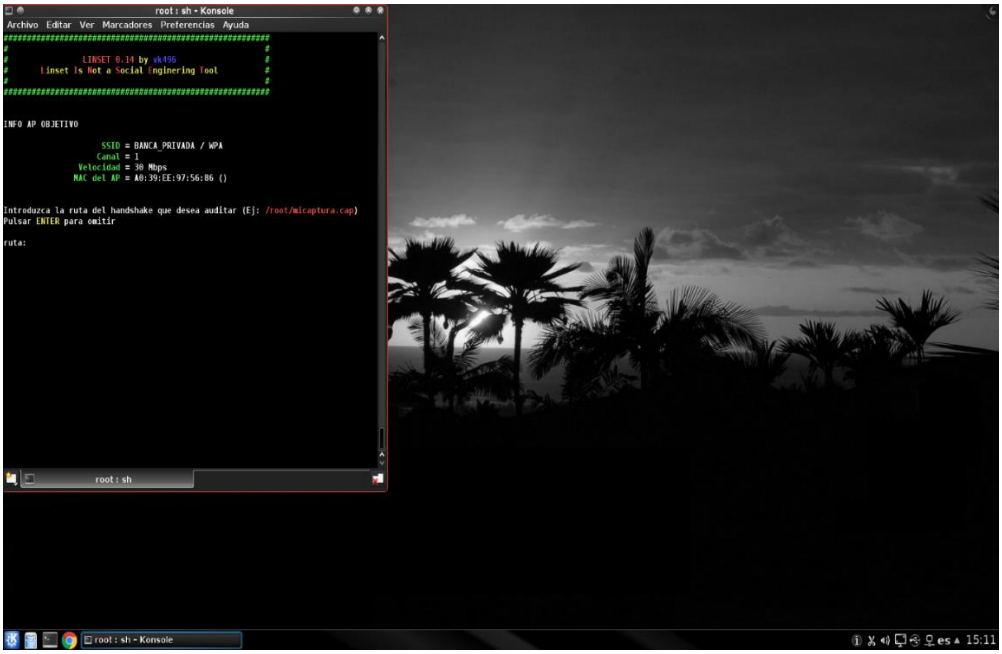


Figura N° 72: Introducción a la Ruta Handshake.

Fuente: Elaboración propia

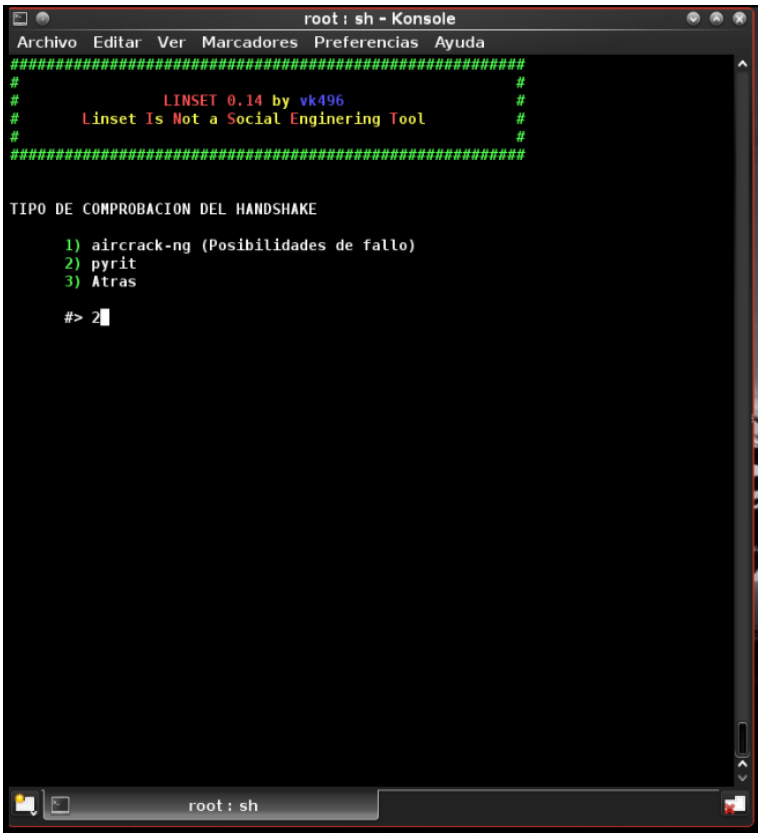


Figura N° 73: Comprobación del HandShake. Fuente: Elaboración propia

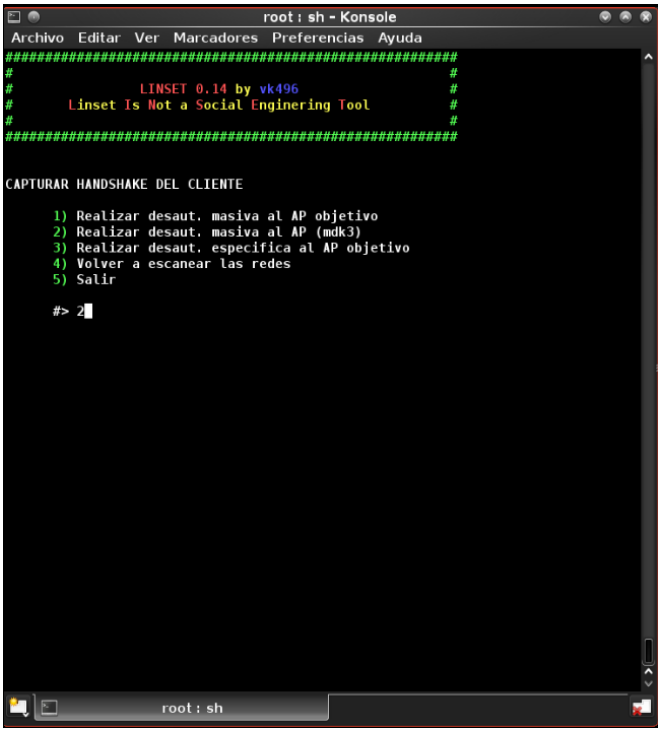


Figura N° 74: Captura del Handshake Objetivo. Fuente: Elaboración propia

Figura N°75: HandShake Objetivo.

Fuente: Elaboración propia

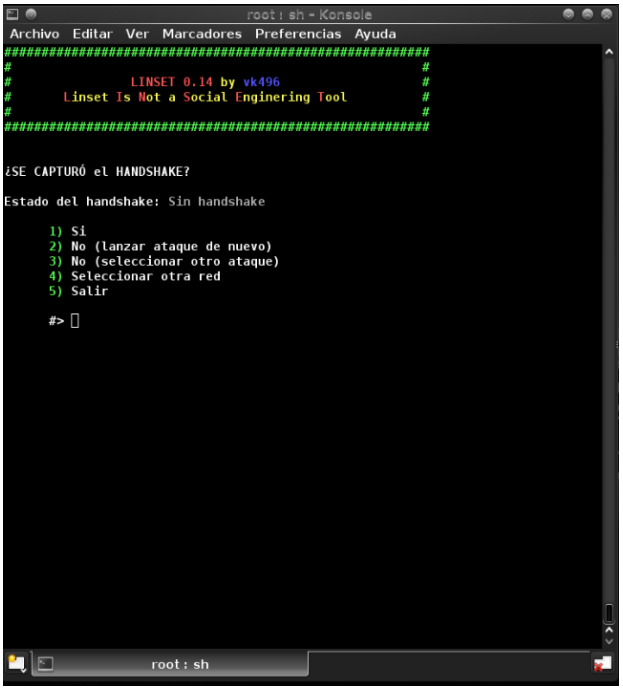


Figura N° 76: Confirmación Captura del HandShake. Fuente: Elaboración propia

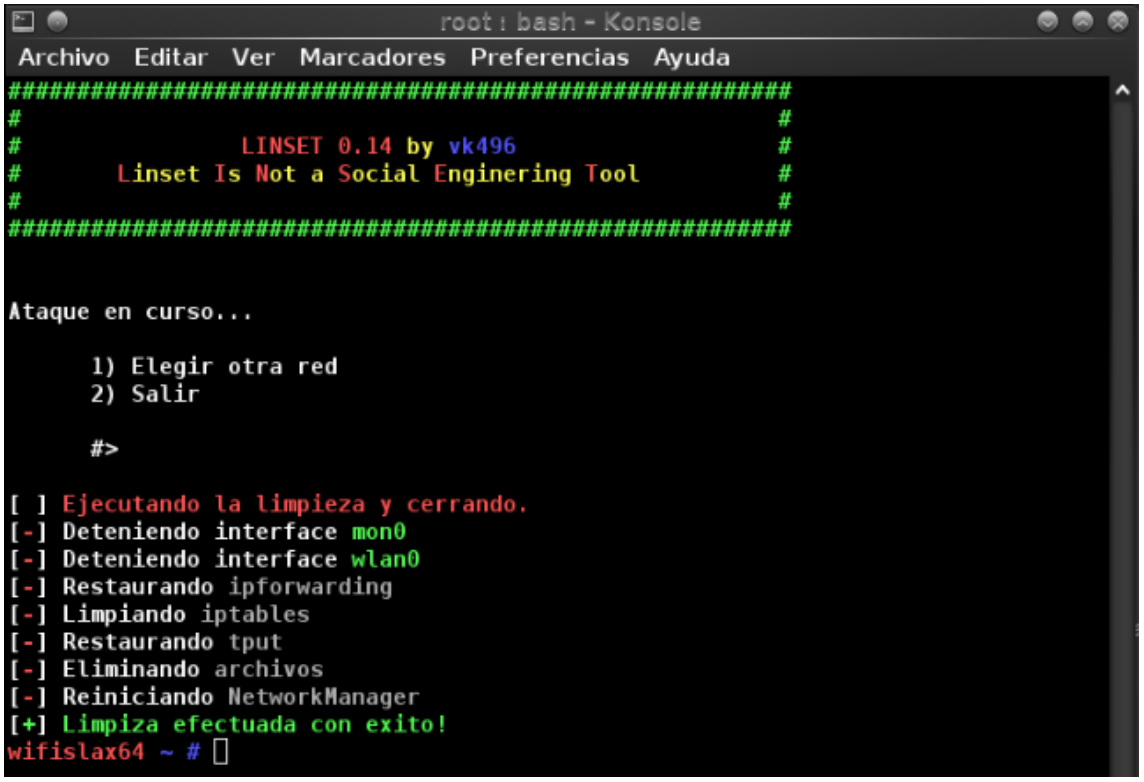


Figura N° 77: Ataque en Curso.

Fuente: Elaboración propia

Figura N° 78: En espera del Password.

Fuente: Elaboración propia

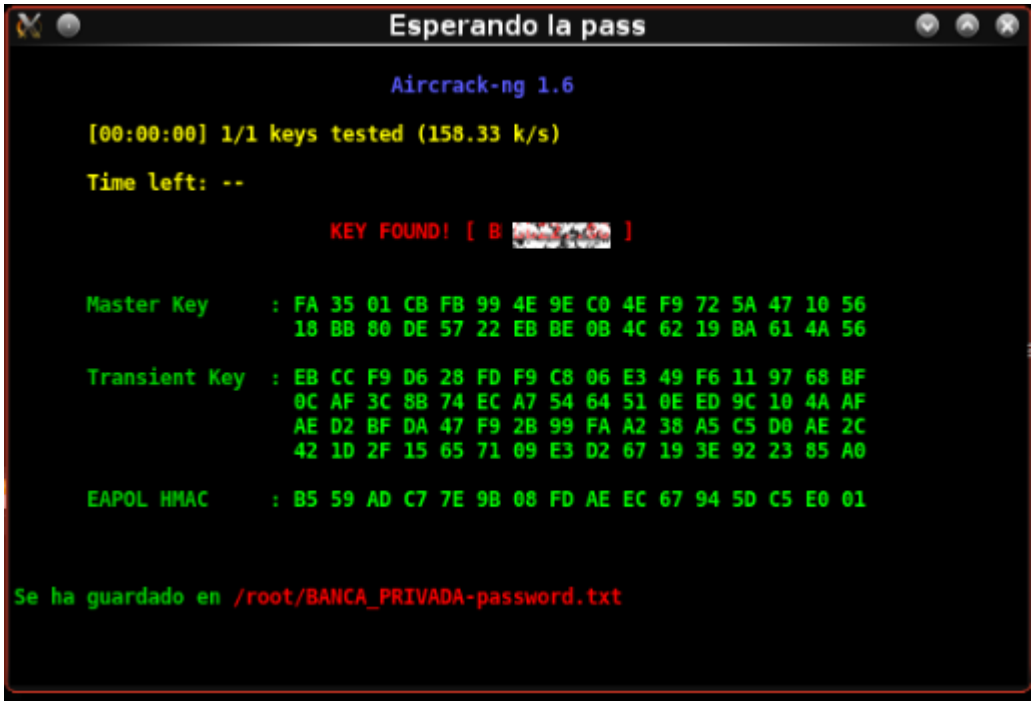


Figura N° 79: Key Found encontrado (Password).

Fuente: Elaboración propia

Anexo Nº 16: Escaneo de los puertos

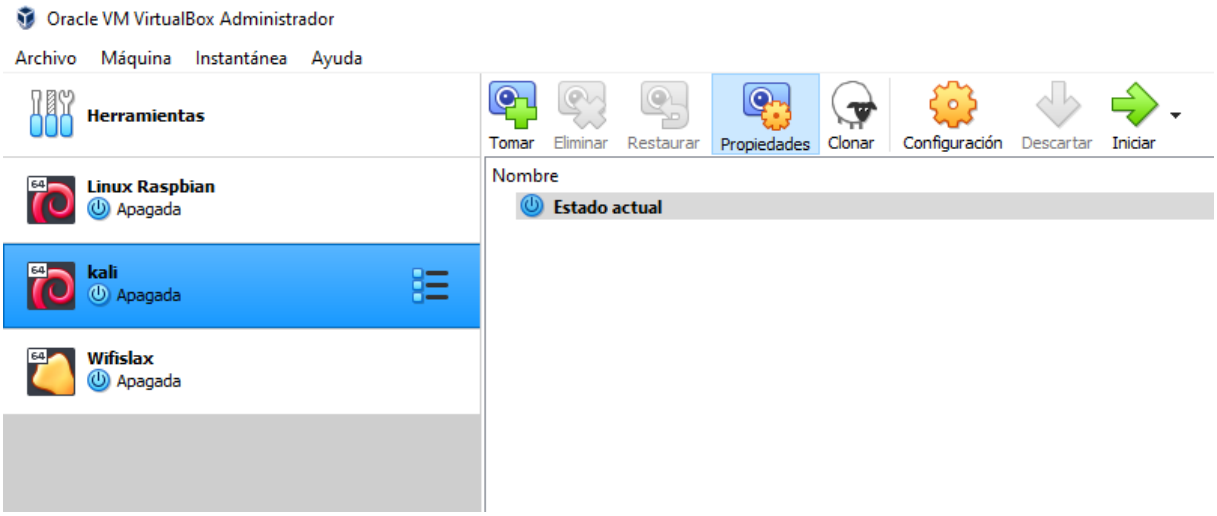


Figura Nº 80: Iniciando sesión en VirtualBox.

Fuente: Elaboración propia

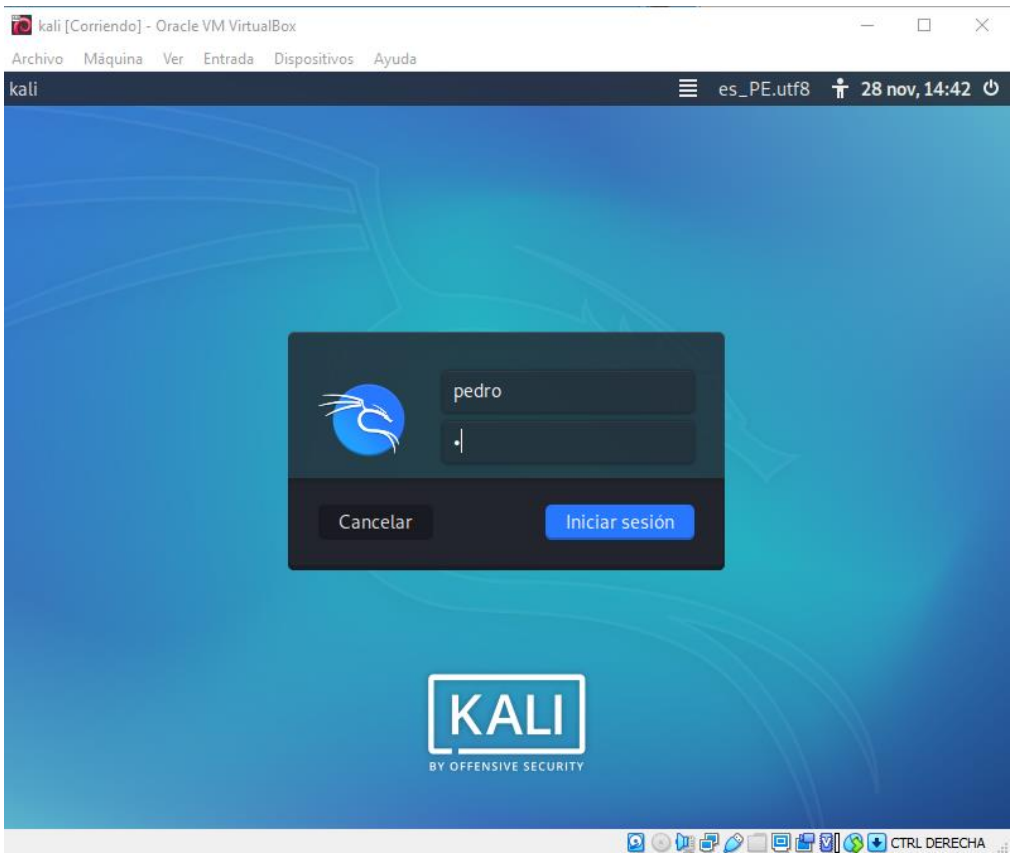


Figura Nº 81: Iniciando sesión en Kali Linux. Fuente: Elaboración propia

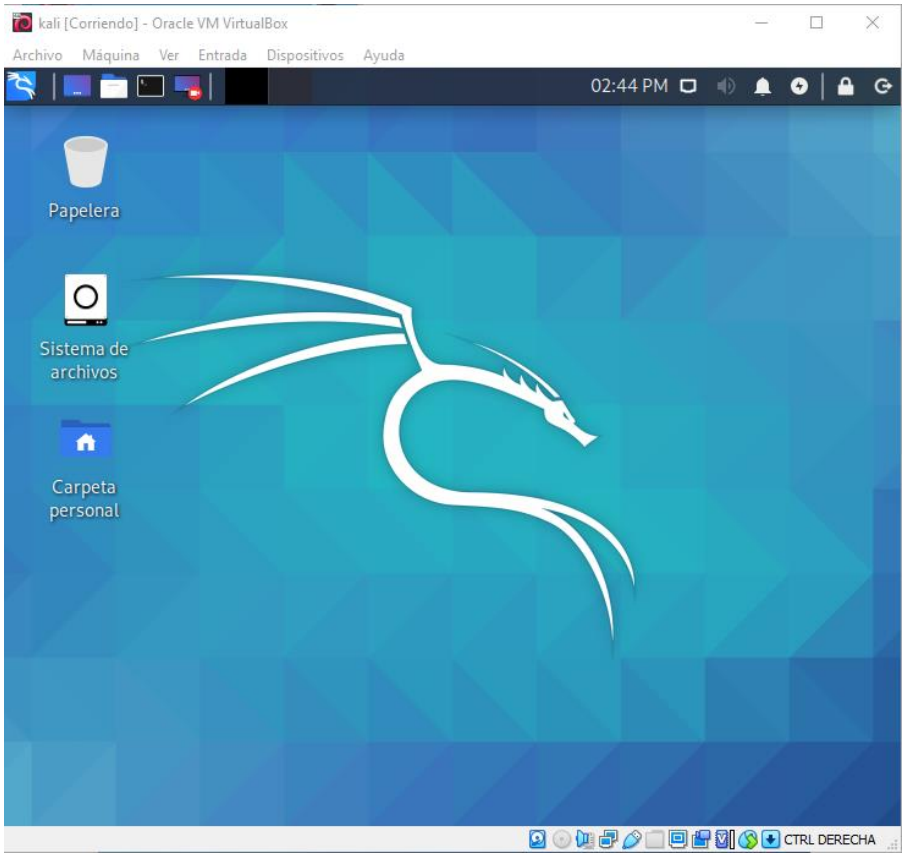


Figura Nº 82: Interfaz de usuario en Kali Linux. Fuente: Elaboración propia

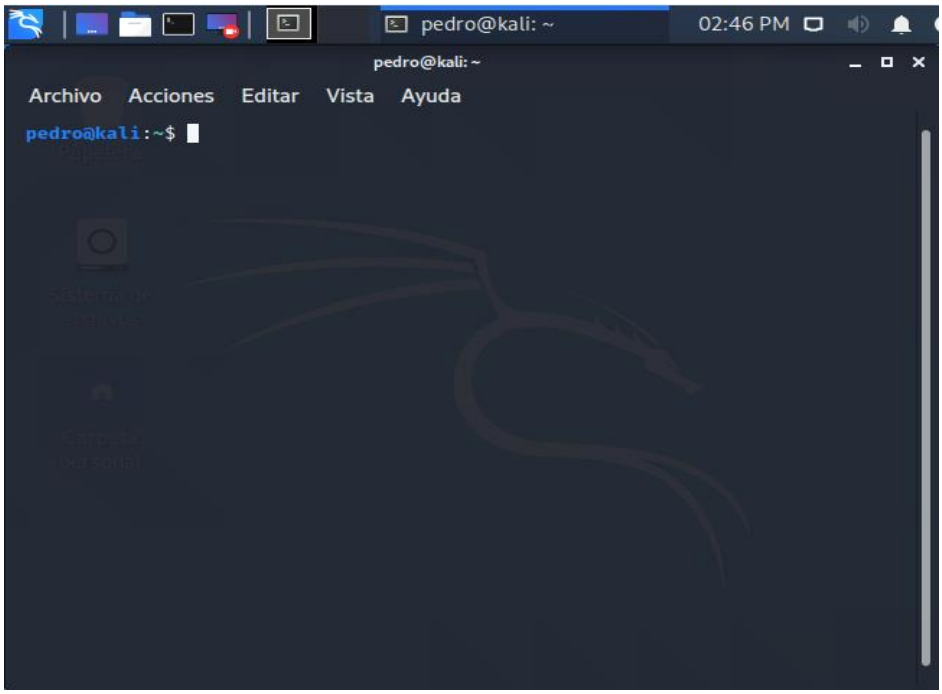


Figura Nº 83: Interfaz de usuario en Kali Linux. Fuente: Elaboración propia

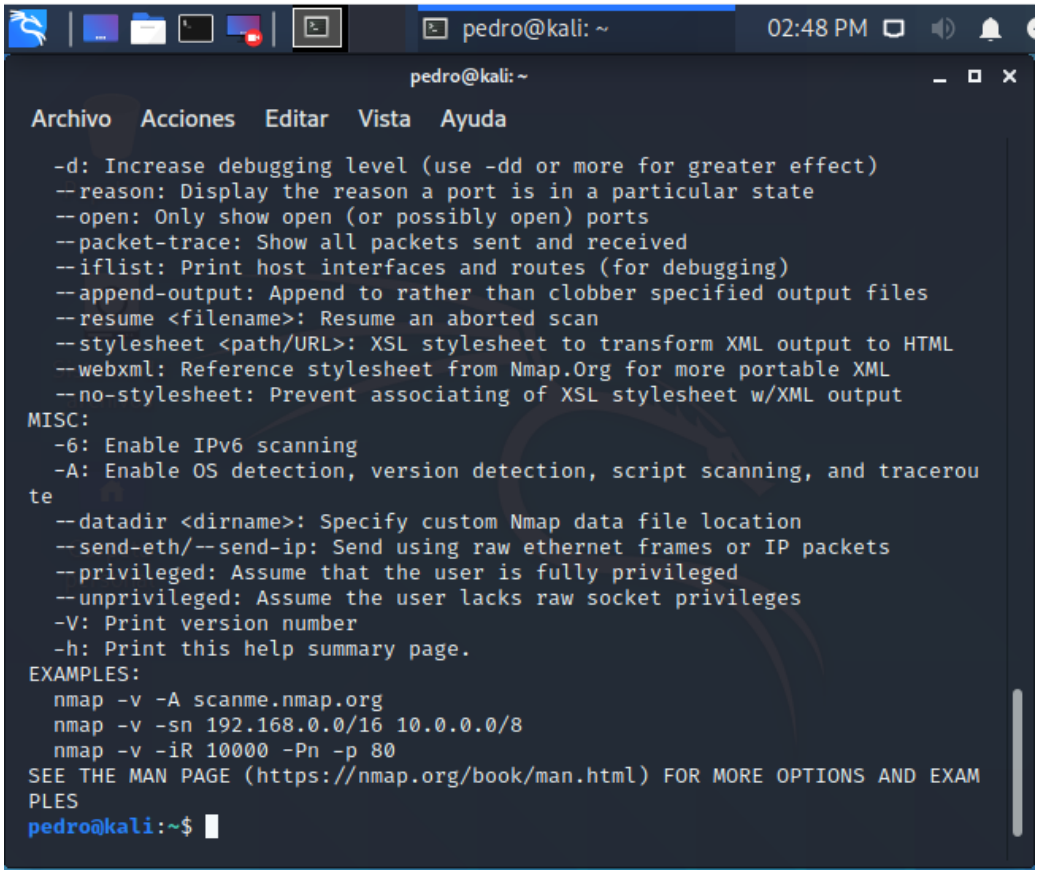


Figura Nº 84: Cargando paquetes en Kali Linux. Fuente: Elaboración propia

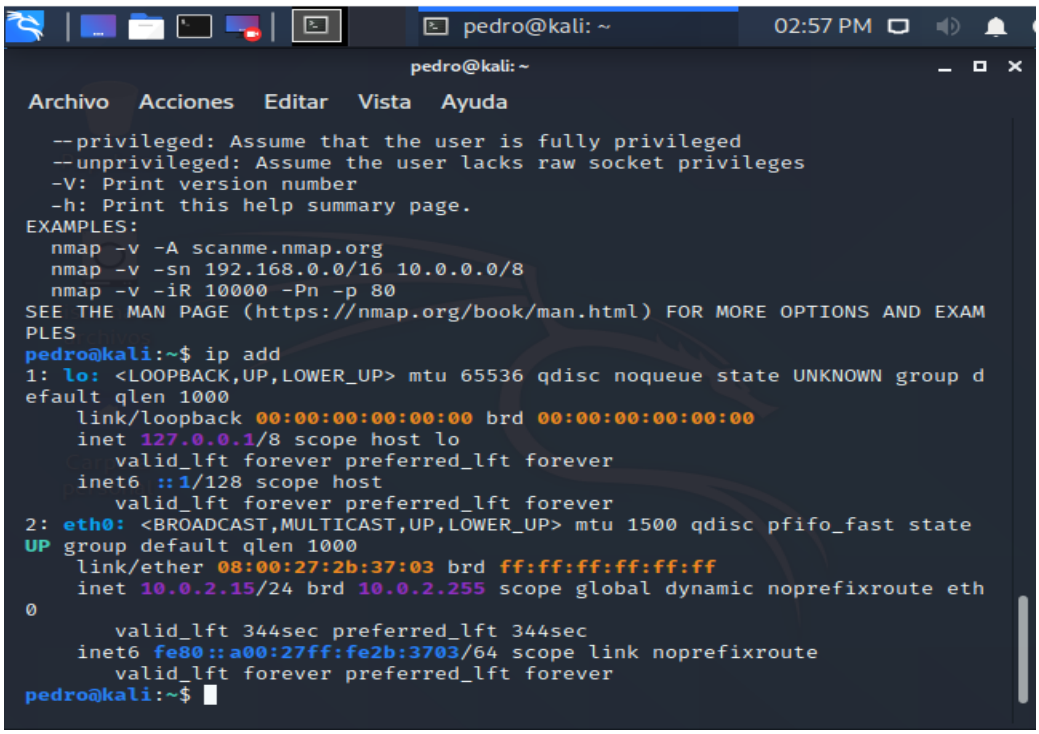


Figura Nº 85: Identificando la IP en Kali Linux. Fuente: Elaboración propia

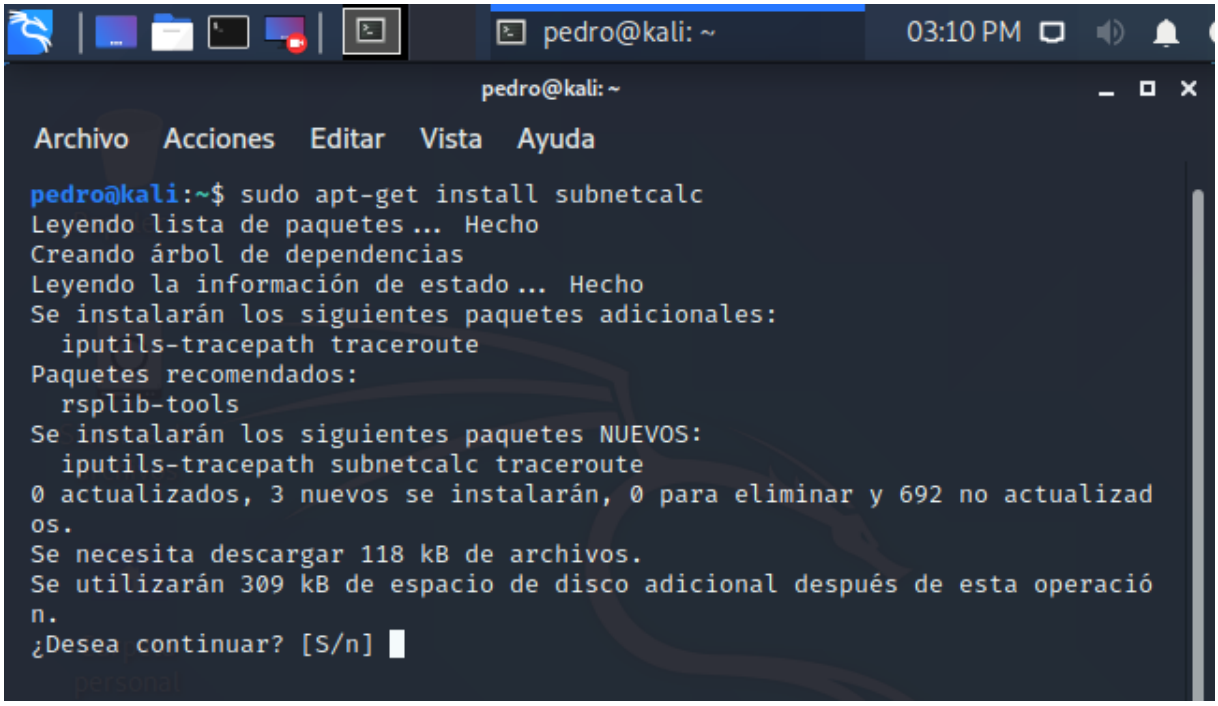


Figura Nº 86: Instalando SubNetCalc en Kali Linux. Fuente: Elaboración propia

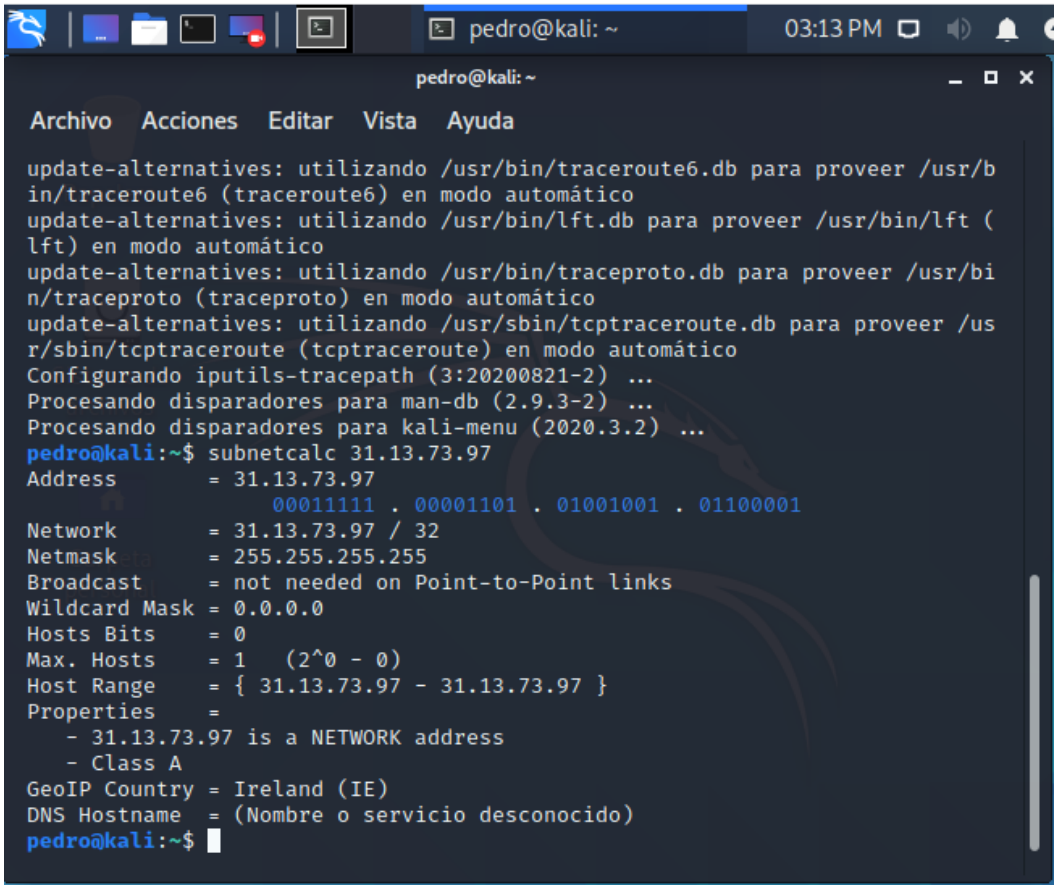


Figura Nº 87: Culminando la Instalando SubNetCalc en Kali Linux.

Fuente: Elaboración propia

En pantalla conseguiremos:

Dirección en valor binario

Dirección de la red con prefijo

Mascara de subred

Cuantos bits de la dirección pertenecen a host

y cuantos pertenecen a red

Cantidad máxima de host

Rango de host en esa red.

Figura Nº 88: Instalando SubNetCalc en Kali Linux.

Fuente: Elaboración propia

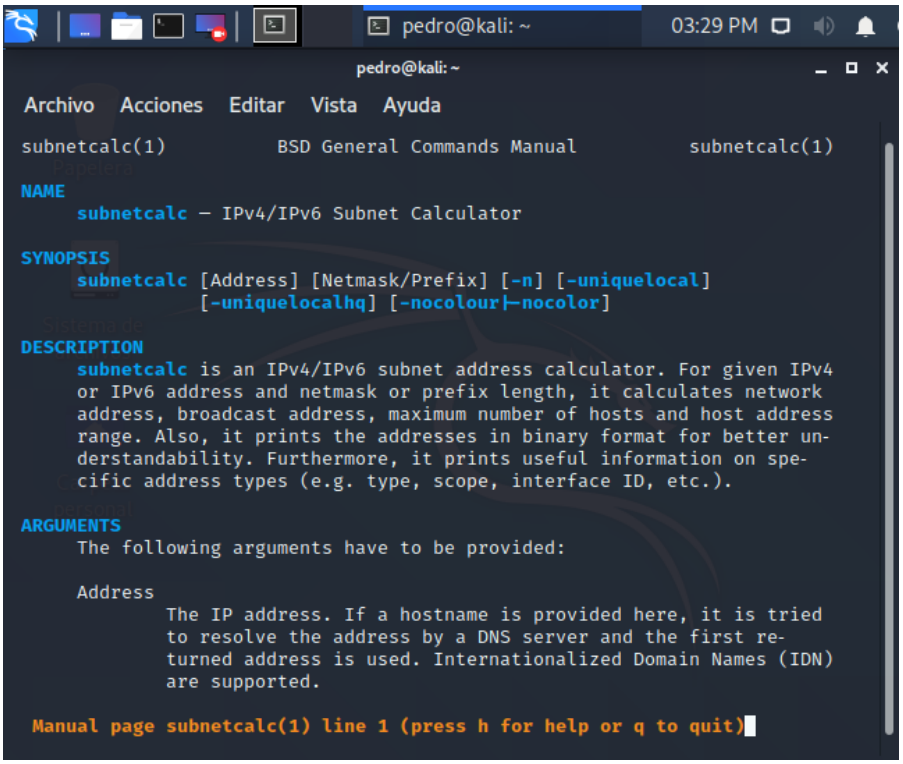


Figura Nº 89: Especificaciones de SubNetCalc en Kali Linux.

Fuente: Elaboración propia

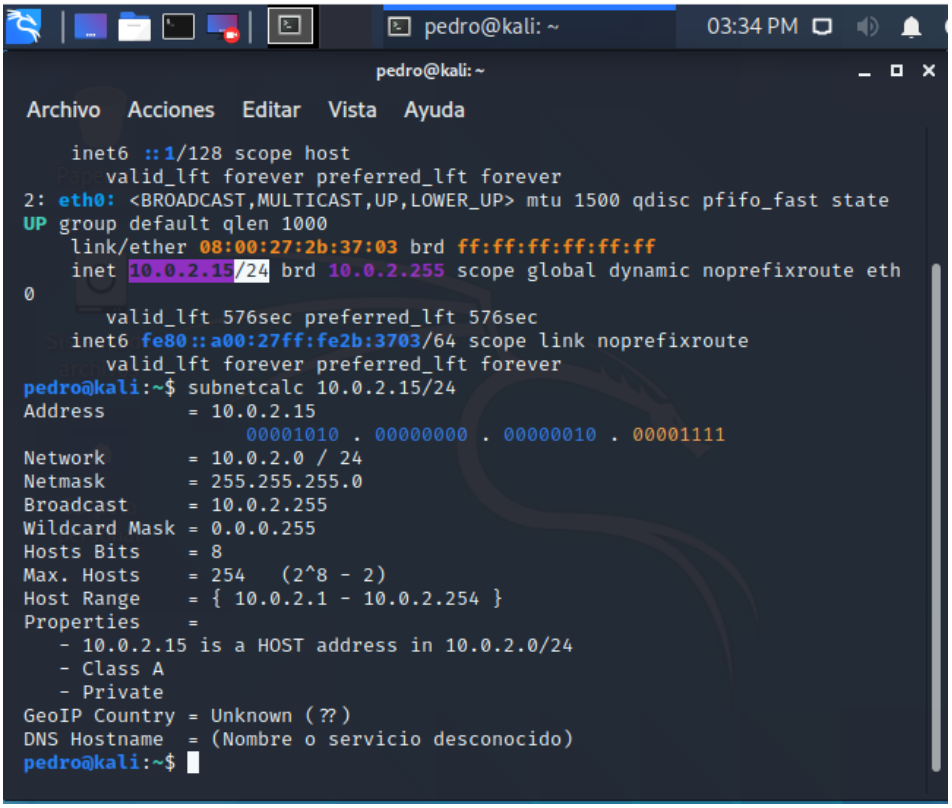


Figura Nº 90: Obteniendo dirección IP y Máscara de Sub Red.

Fuente: Elaboración propia

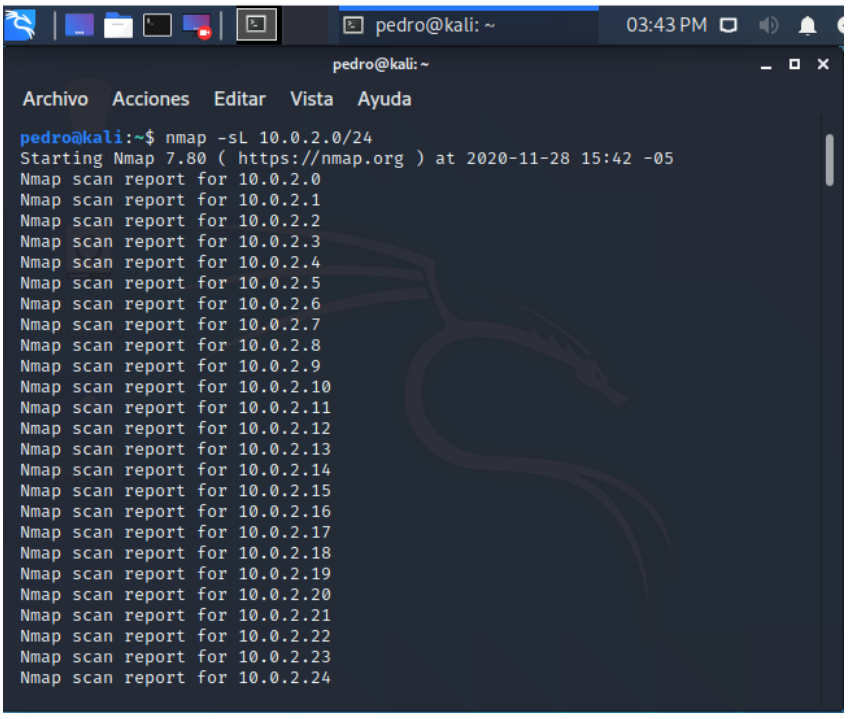


Figura Nº 91: Escaneo de puertos (no detectables por los administradores).
Fuente: Elaboración propia

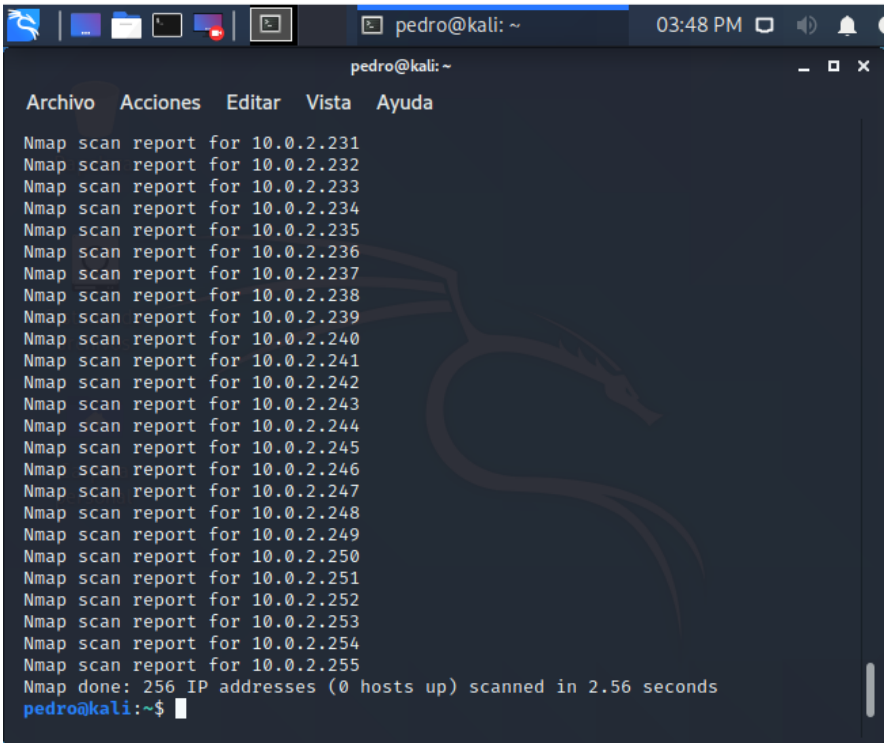


Figura Nº 92: Escaneo de Hosts levantados y Firewall (sin asignar).

Fuente: Elaboración propia

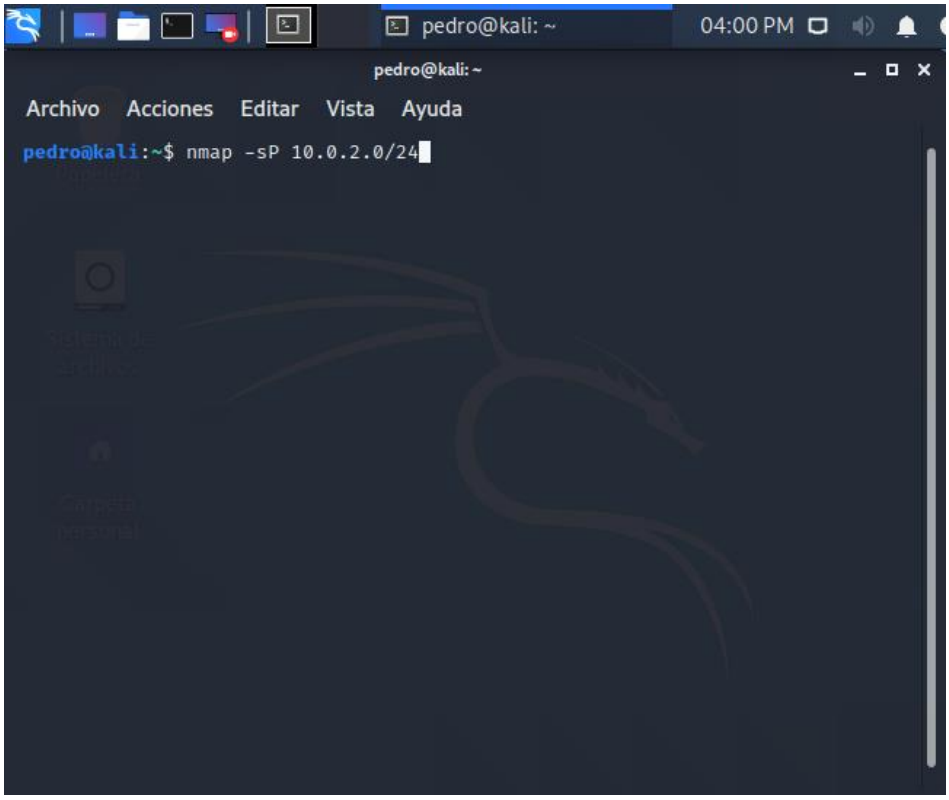


Figura Nº 93: Pineo de la Red. Fuente: Elaboración propia

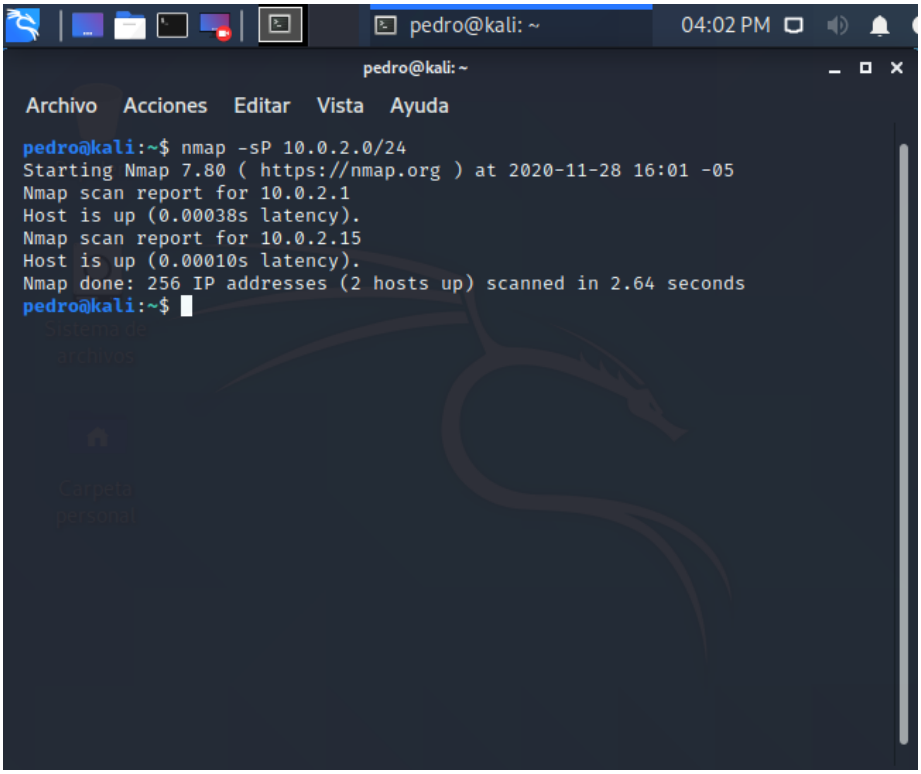


Figura Nº 94: Reporte de los puertos y hosts levantados.

Fuente: Elaboración propia

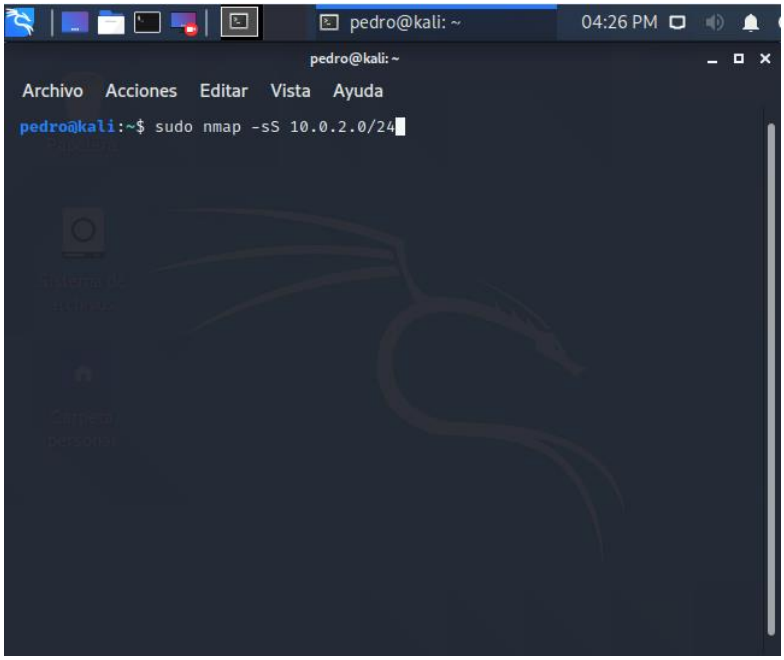


Figura Nº 95: Ataque tipo SYN (sincronizado).

Fuente: Elaboración propia

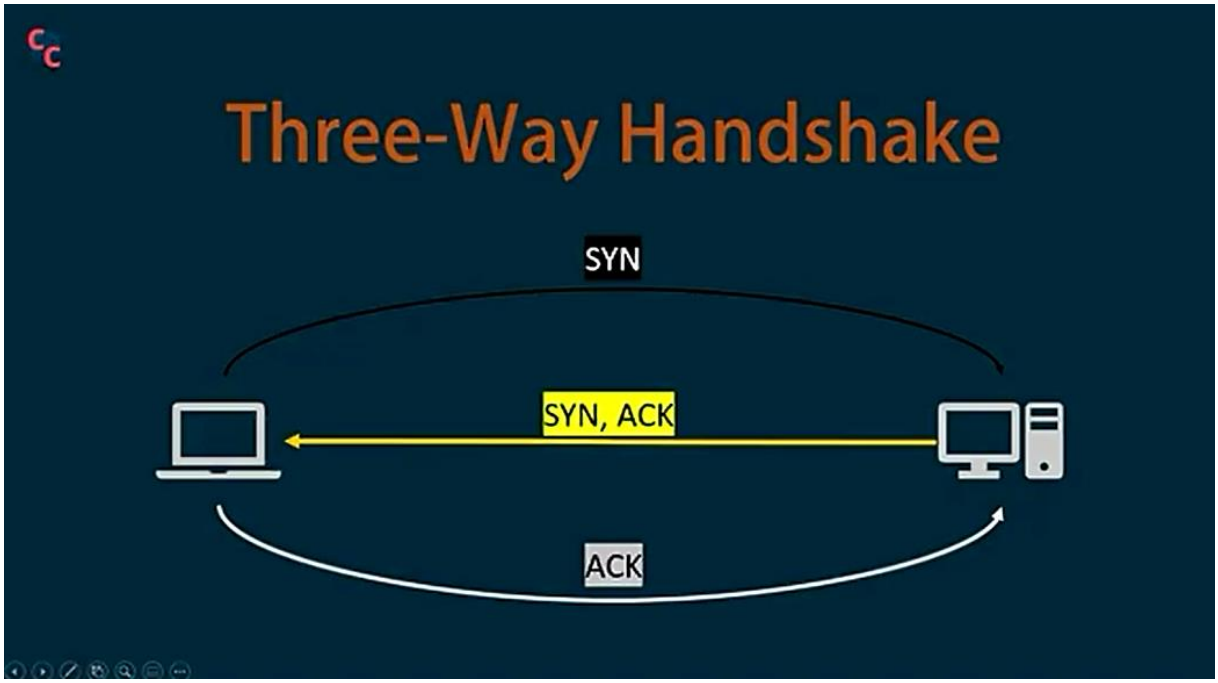


Figura Nº 96: Rutas del HadShake. Fuente: Elaboración propia

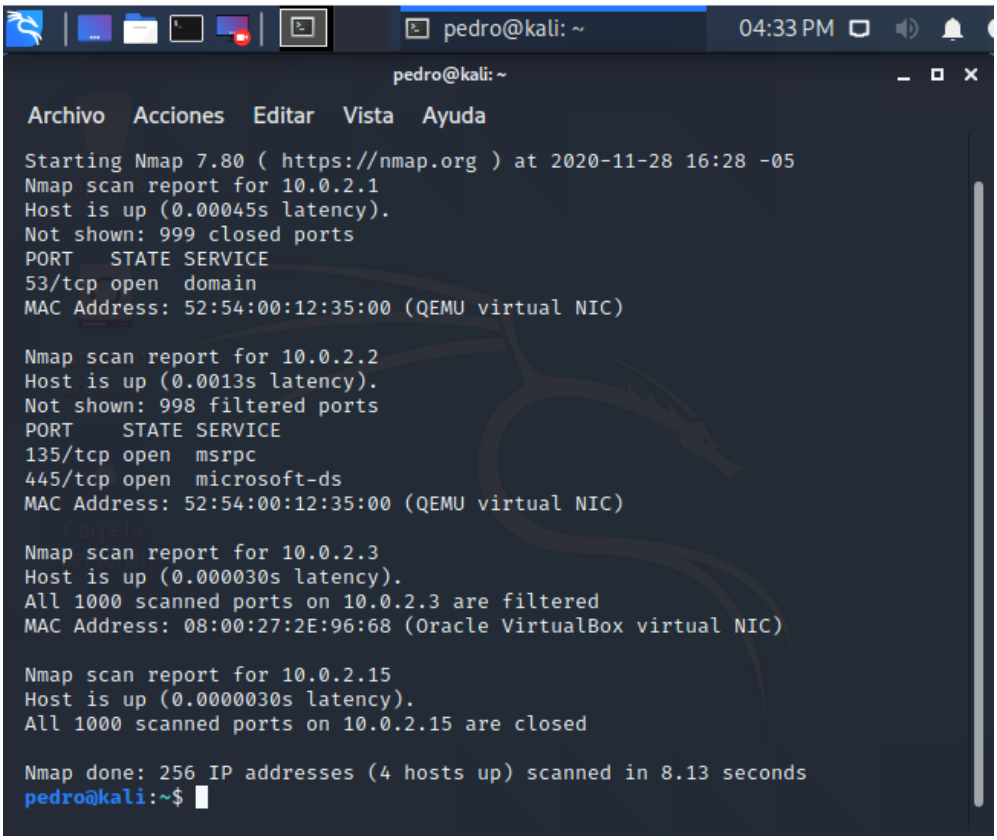


Figura Nº 97: Vulnerabilidad de los servidores (no se cierran ante un ataque). Fuente: Elaboración propia

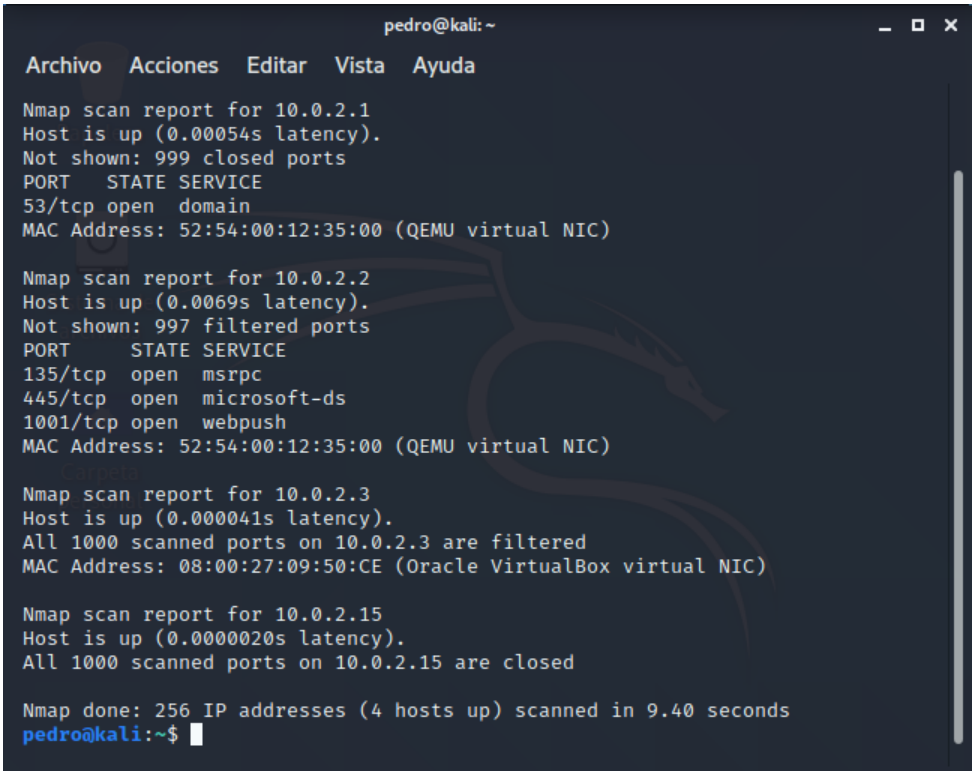


Figura Nº 98: Ataque a nivel de Capa 2 o nivel de direcciones.

Fuente: Elaboración propia

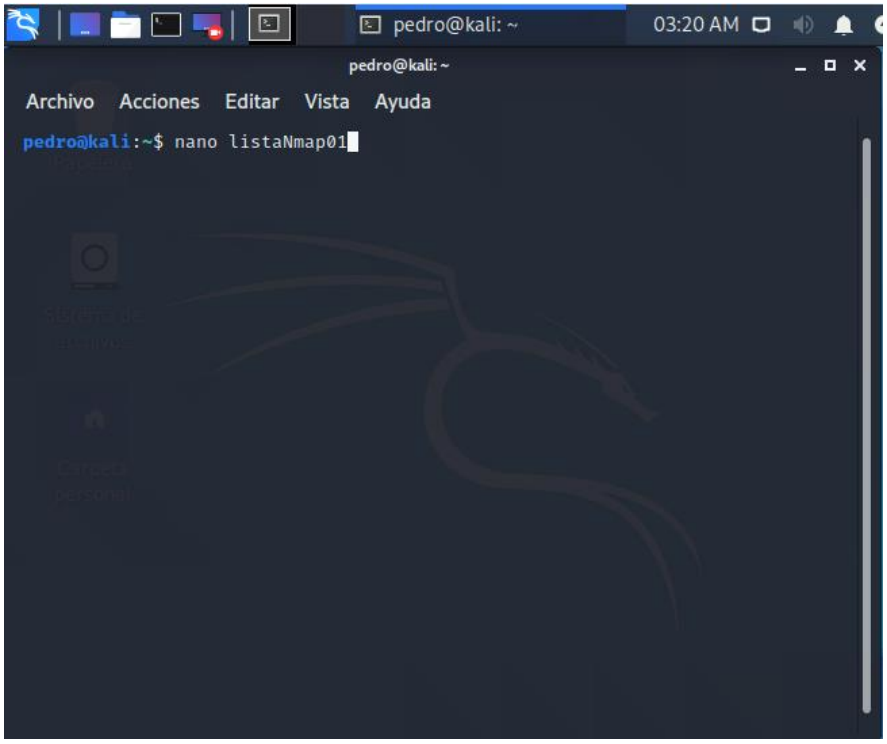


Figura Nº 99: Listado de Nmap con el editor Nano direcciones IP.
Fuente: Elaboración propia

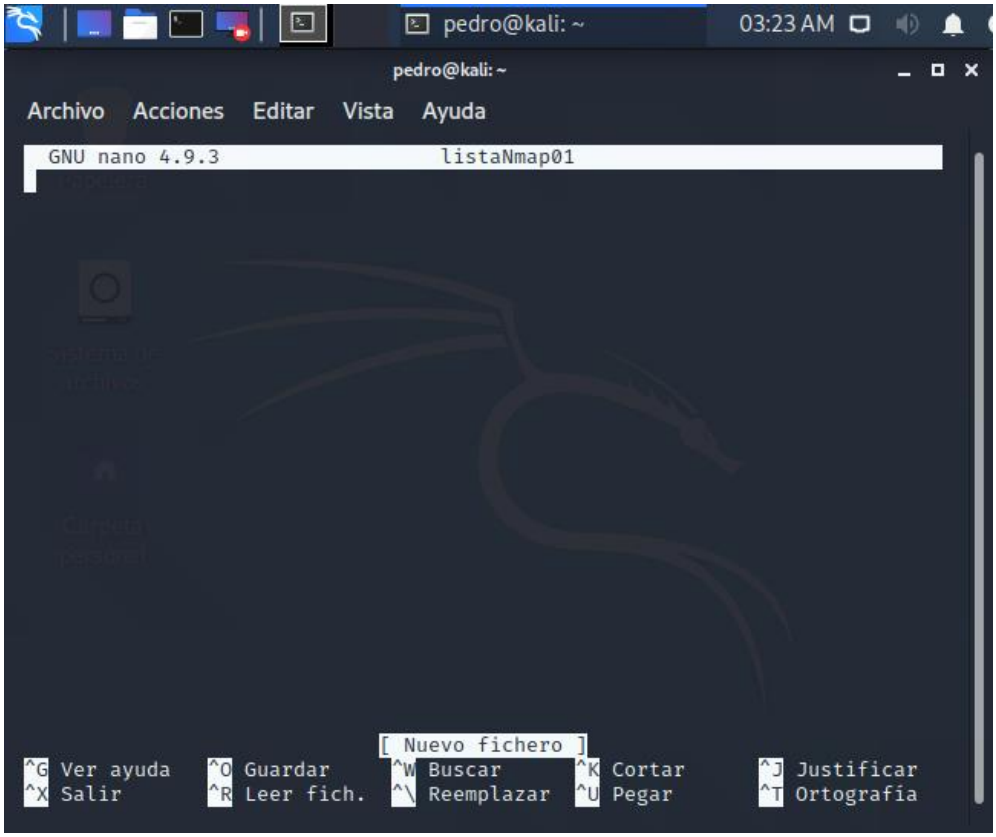


Figura Nº 100: Interfaz editor Nano direcciones IP. Fuente: Elaboración propia

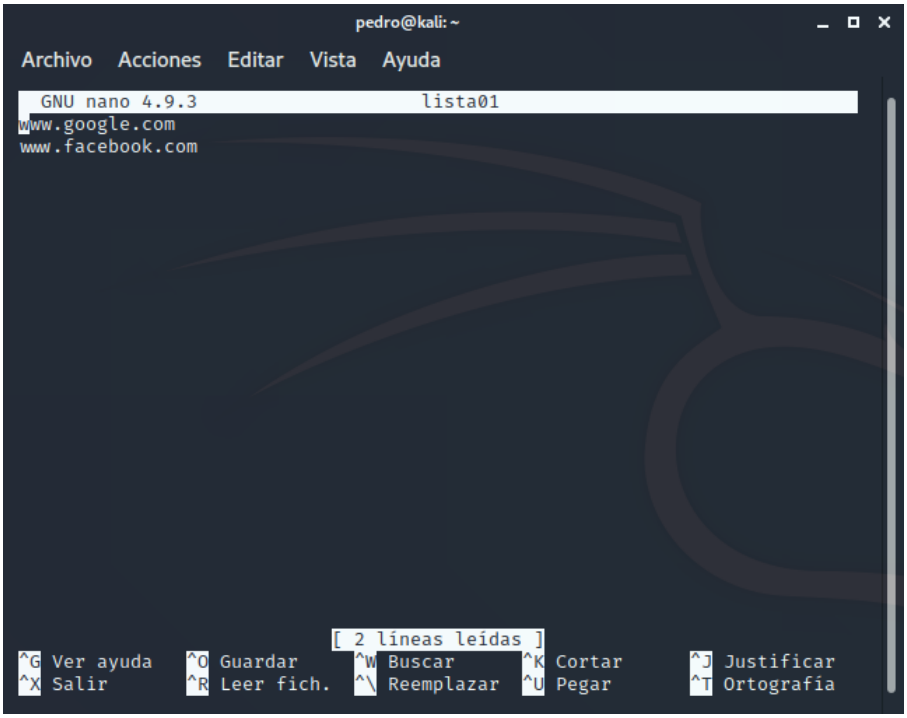


Figura Nº 101: Grabado de direcciones en Nano direcciones IP.

Fuente: Elaboración propia

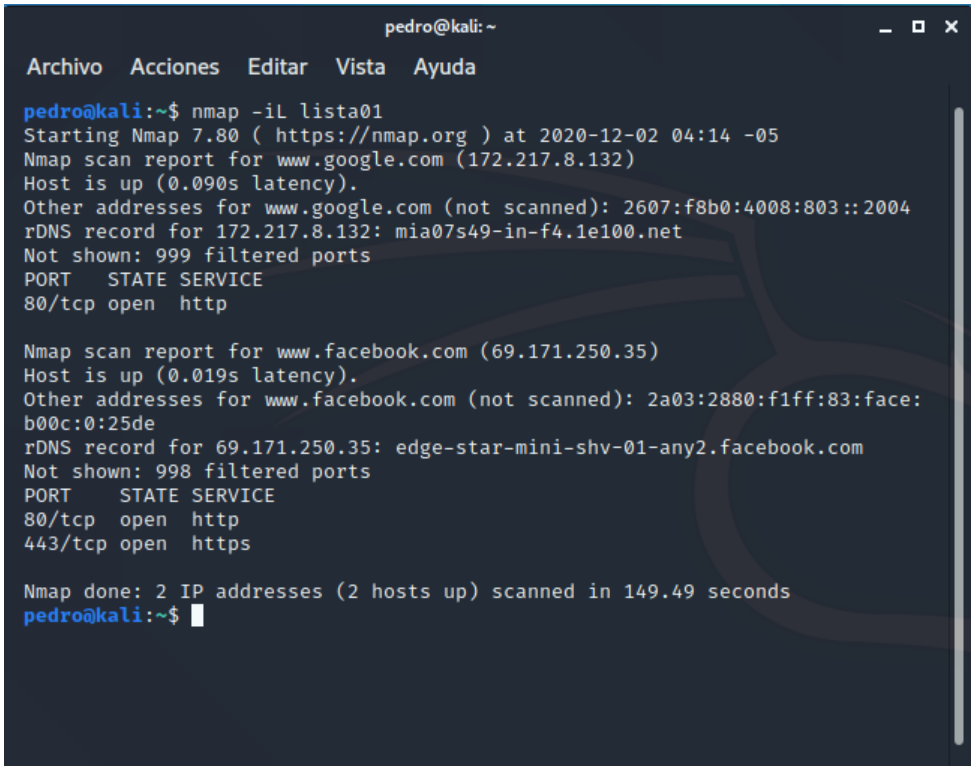


Figura Nº 102: Barrido de direcciones con Input List.

Fuente: Elaboración propia

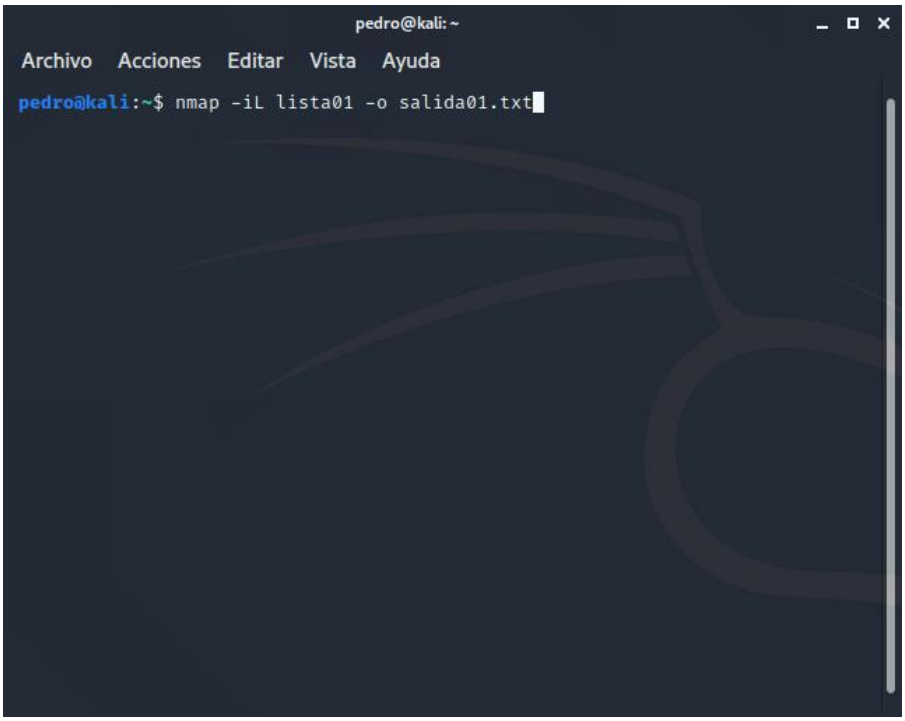


Figura Nº 103: Guardado de direcciones con OutPut List.

Fuente: Elaboración propia

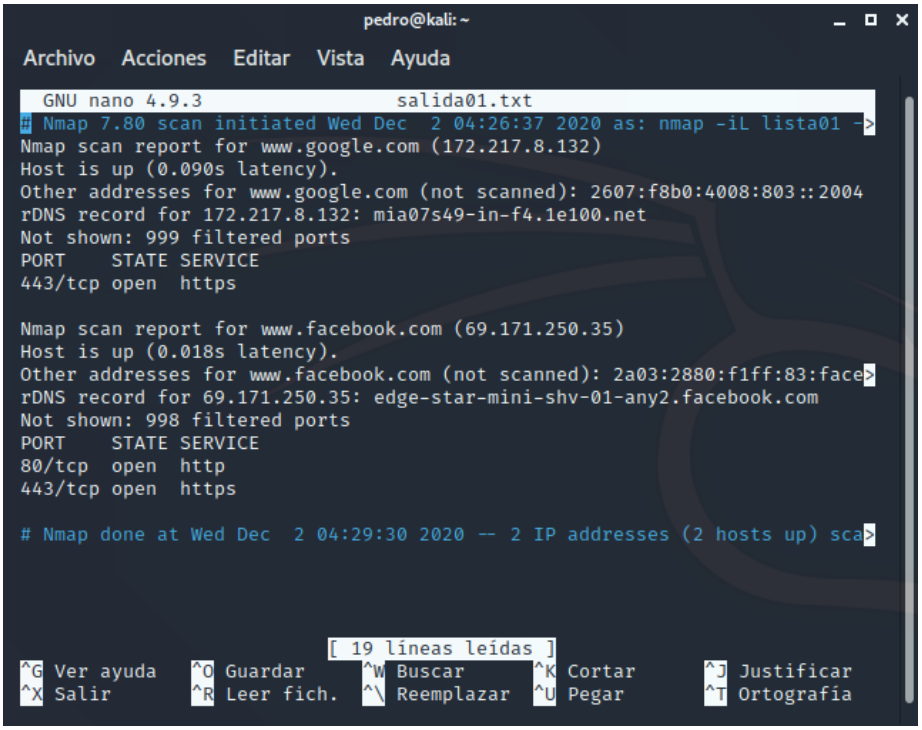


Figura Nº 104: Gabado de direcciones con formato TXT.

Fuente: Elaboración propia

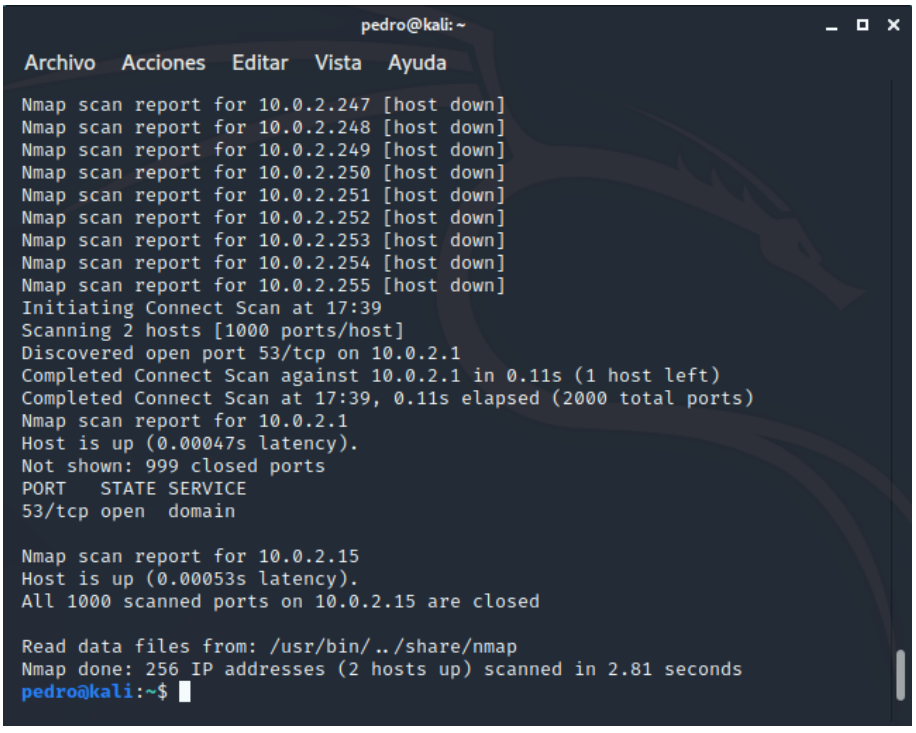


Figura Nº 105: Ampliando detalles de Nmap con -v. Fuente: Elaboración propia

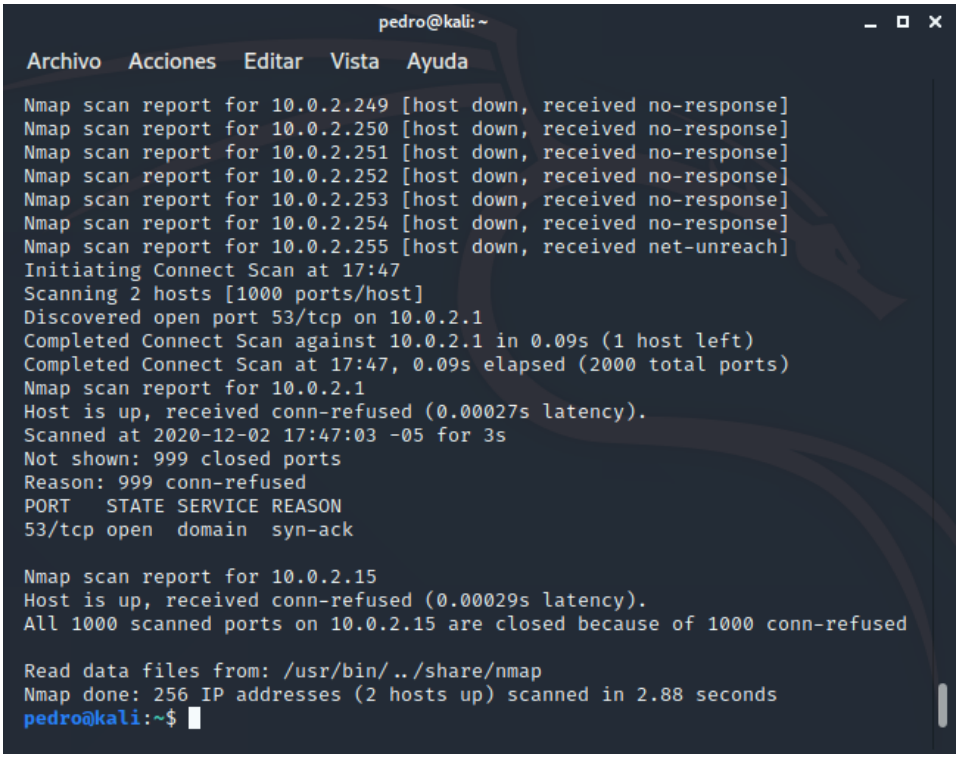


Figura Nº 106: Amplificando nivel de detalles de Nmap con -vv. Fuente: Elaboración propia

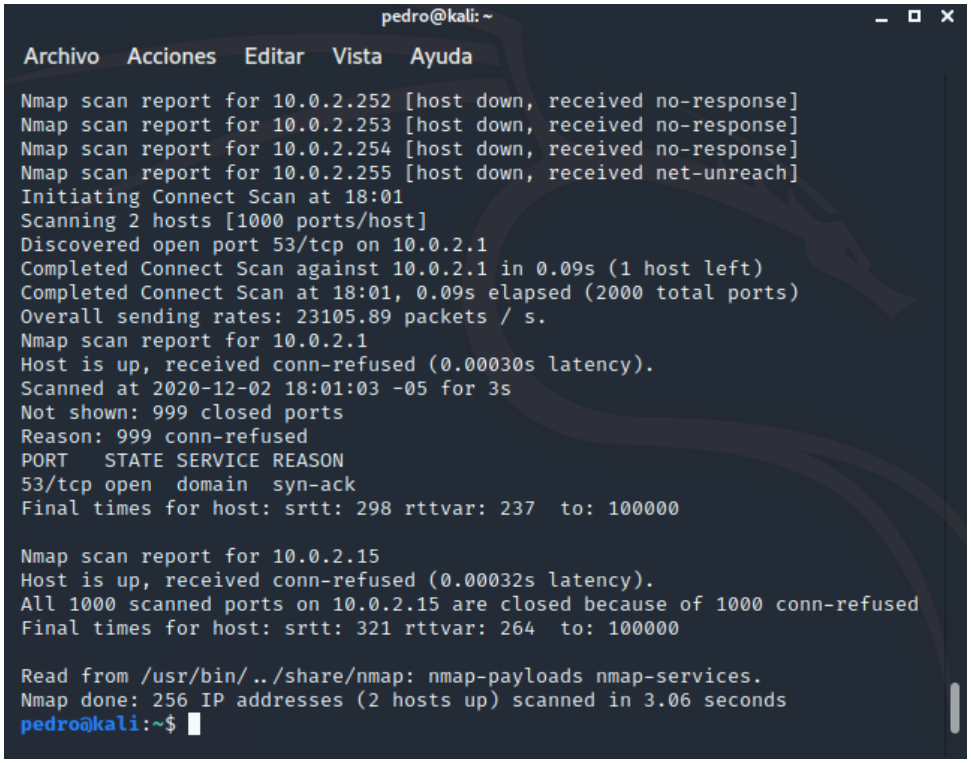


Figura Nº 107: Vulnerando a servidores con -d. Fuente: Elaboración propia

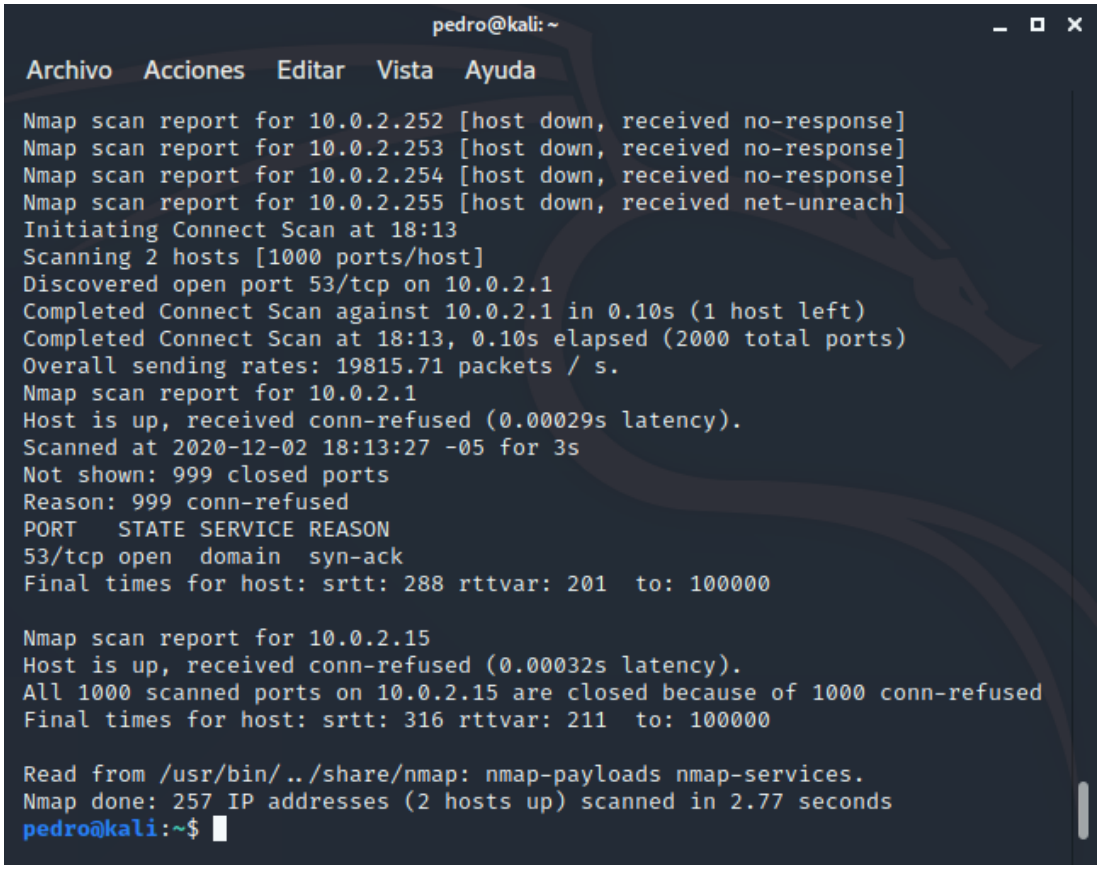


Figura Nº 108: Escaneamos puertos y hosts con -v.

Fuente: Elaboración propia

Anexo Nº 17: Escaneo de los discos

1. Para clonar una imagen forense del disco a analizar, vamos a descargar el software Access Data FTK Imager desde su página web (Forensics Tool Kit):

Figura Nº 109

Fuente: Elaboración propia

2. Luego instalamos el programa:

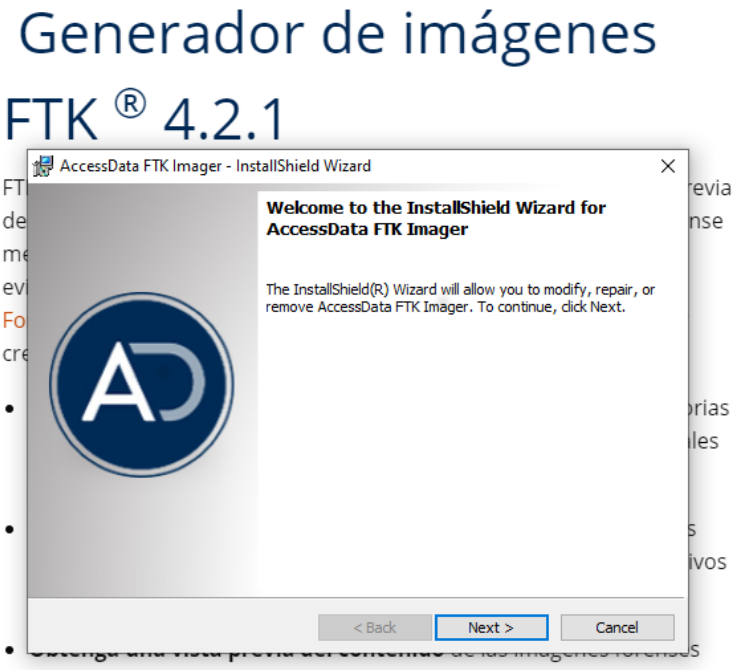


Figura Nº 110

Fuente: Elaboración propia

3. Visualizaremos la siguiente interfaz:

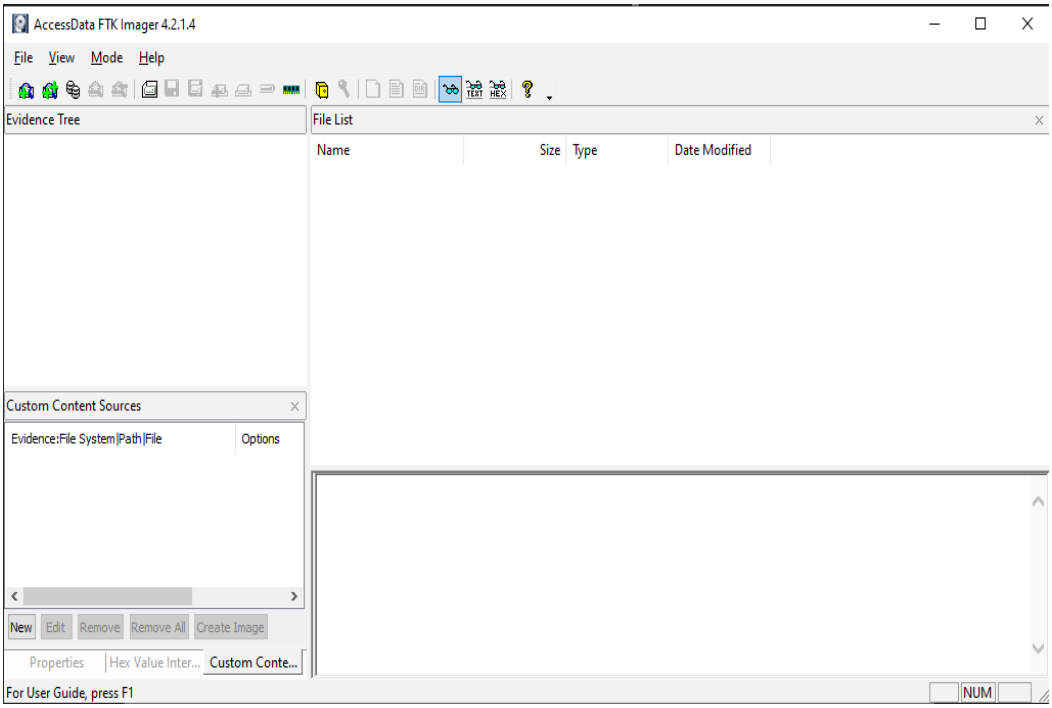


Figura Nº 111

Fuente: Elaboración propia

4. Seleccionaremos: Crear Imagen

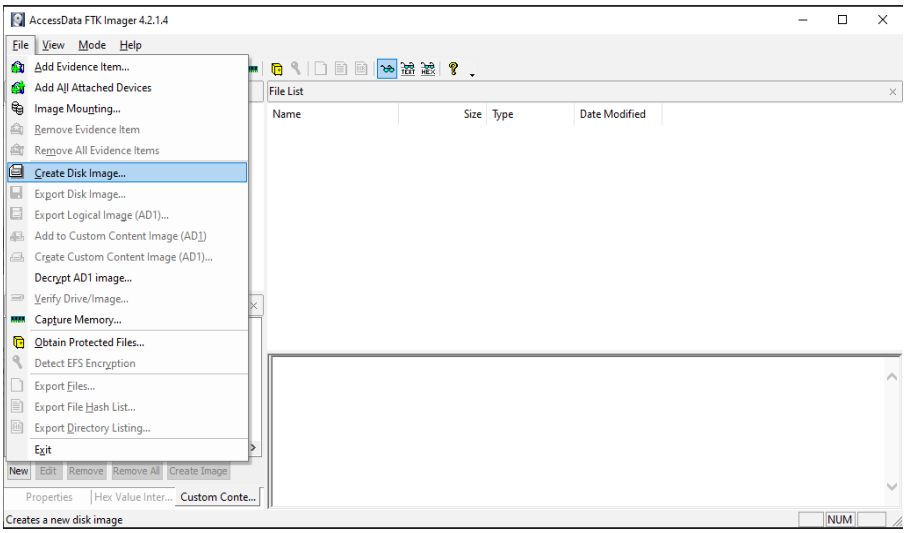


Figura Nº 112

Fuente: Elaboración propia

5. Luego seleccionamos: Crear evidencia física

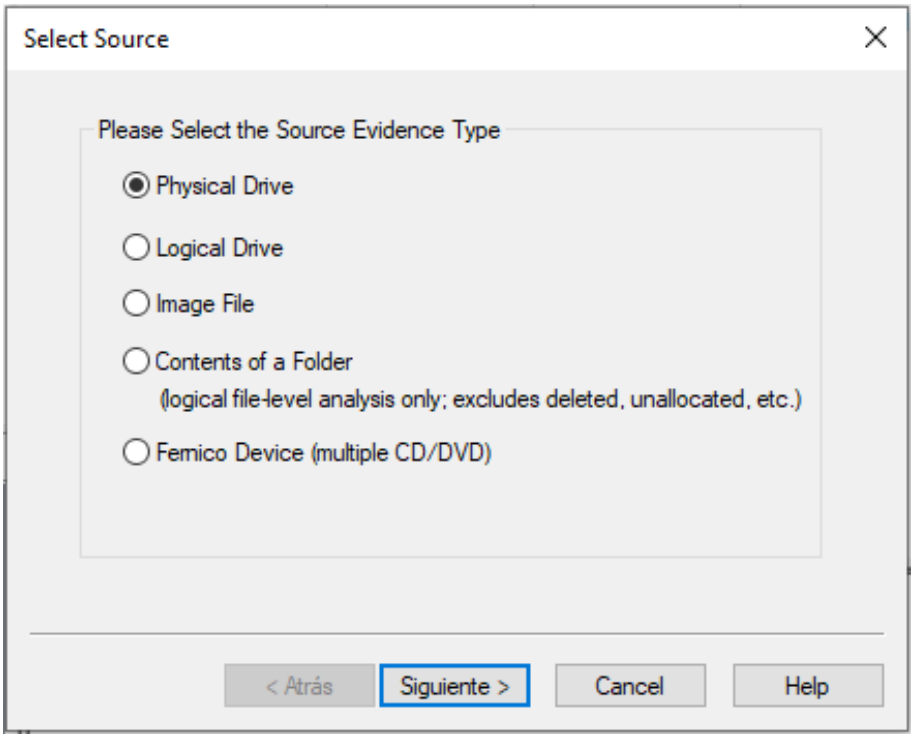


Figura Nº 113

Fuente: Elaboración propia

6. Seguidamente, seleccionamos la unidad fuente (C:)

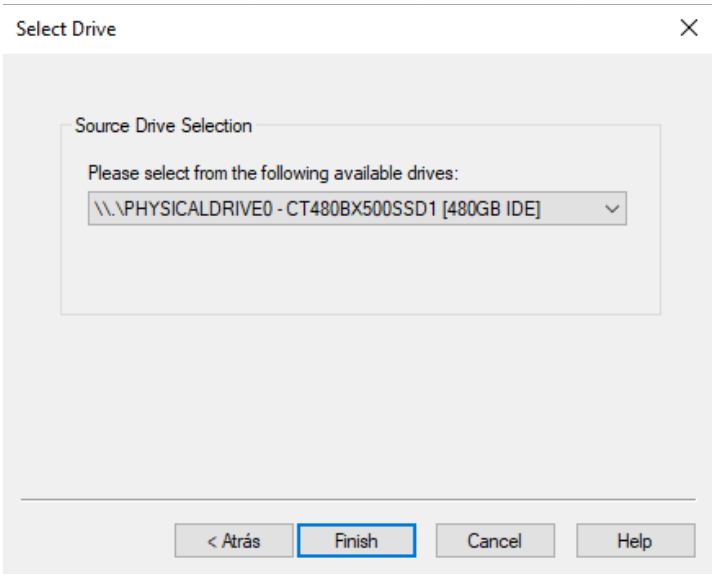


Figura Nº 114

Fuente: Elaboración propia

7. A continuación, seleccionamos como destino, una carpeta creada en otra unidad de almacenamiento:

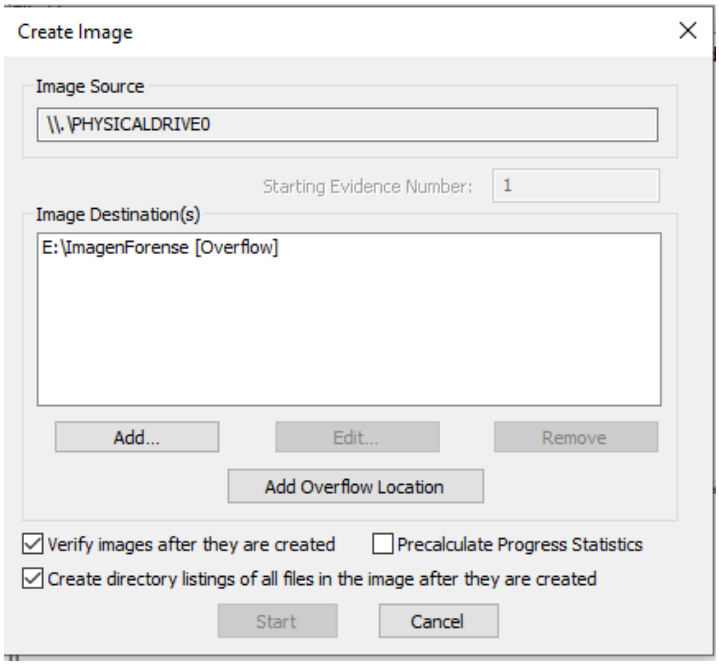


Figura Nº 115

Fuente: Elaboración propia

8. De esta manera, se iniciará la creación de la imagen forense:

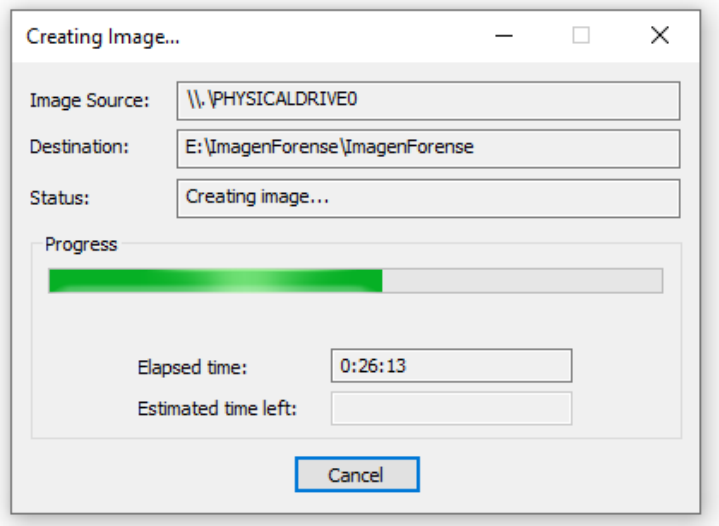


Figura Nº 116

Fuente: Elaboración propia

9. Asimismo, es conveniente tener en cuenta ciertas consideraciones sobre esta herramienta forense:

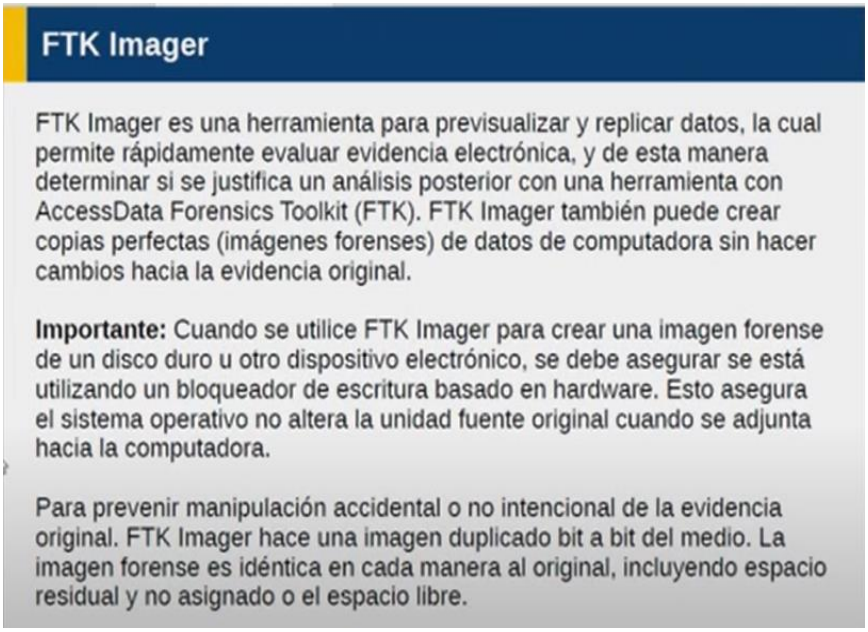


Figura Nº 117

Fuente: Elaboración propia

10. Cabe resaltar que se está trabajando con una computadora ACER PREDATOR Core i7 de Décima Generación:

Figura Nº 118

Fuente: Elaboración propia

11. A pesar de ello, la creación de la imagen forense, nos tomará casi una hora:

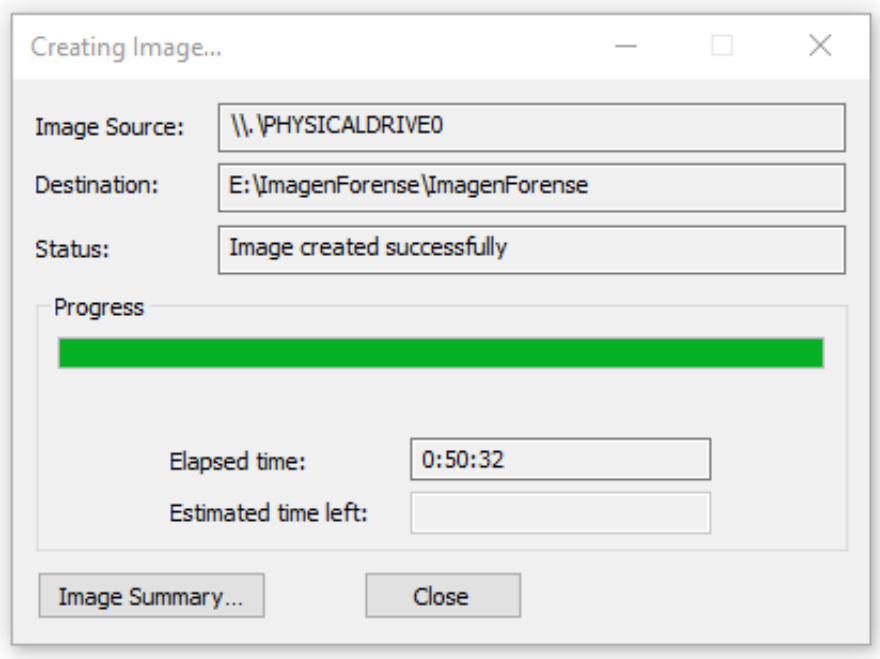


Figura Nº 119

Fuente: Elaboración propia

12. Posteriormente, la imagen forense quedará terminada e iniciará su verificación:

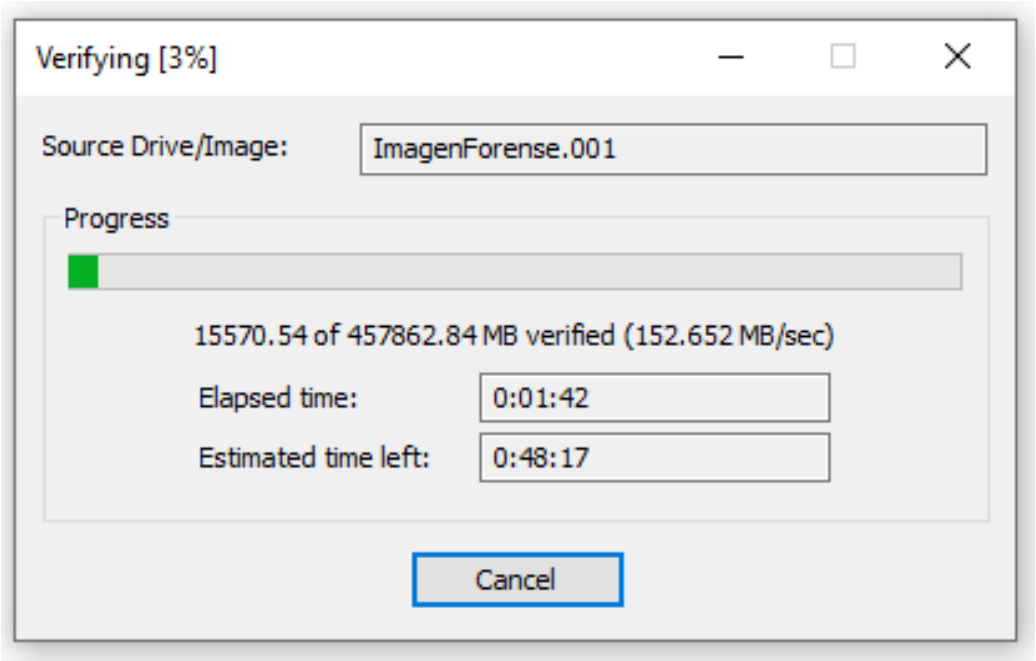


Figura Nº 120

Fuente: Elaboración propia

13. Por último, la verificación de la imagen forense mostrará que la imagen lograda es idéntica a la original (Match):

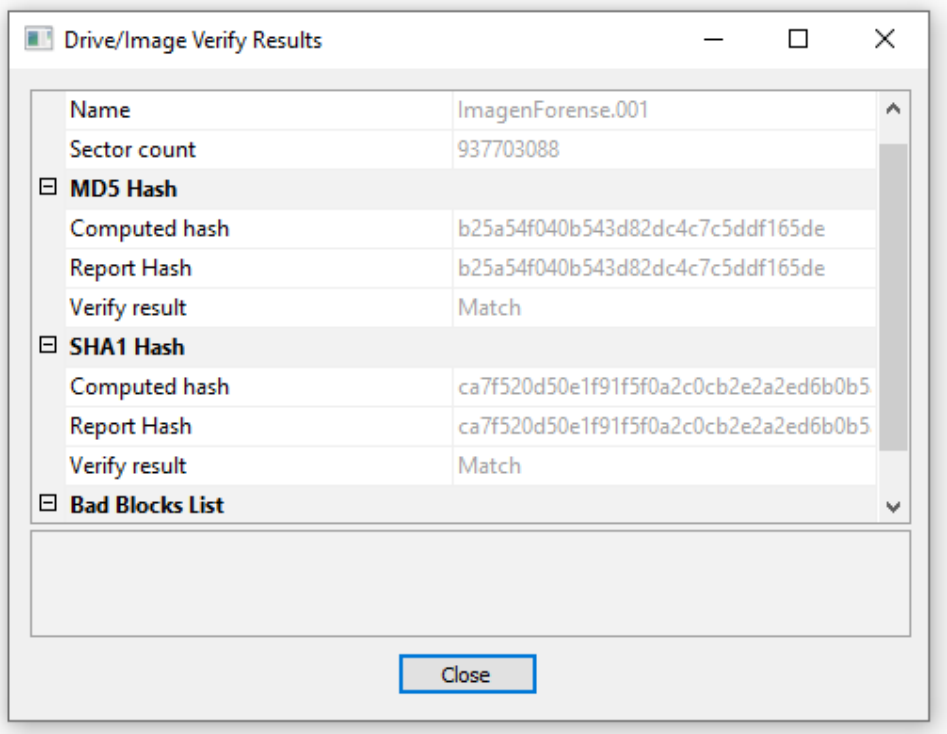


Figura Nº 121

Fuente: Elaboración propia

14. También mostrará que en la imagen clonada no se hallaron sectores defectuosos (No bad blocks found in image):

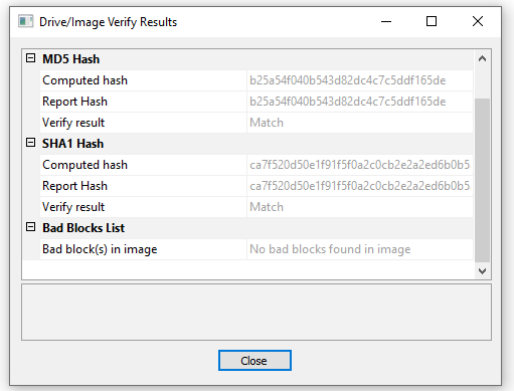


Figura Nº 122

Fuente: Elaboración propia

15. Ahora analizaremos algunas características de esta herramienta forense:

Figura Nº 123

Fuente: Elaboración propia

16. Vemos que nos permite crear también, encriptaciones:

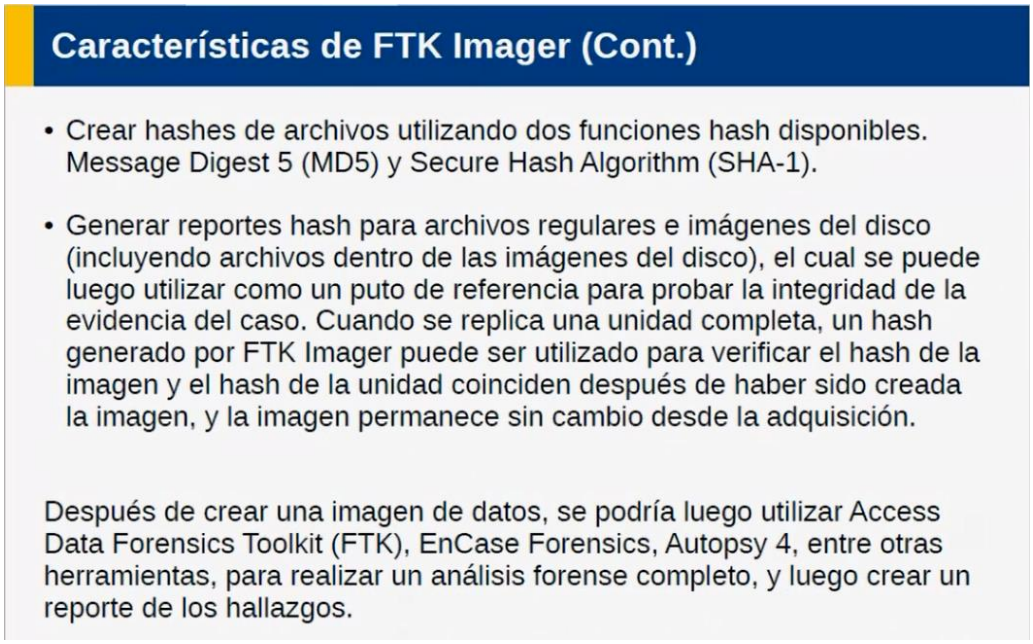


Figura Nº 124

Fuente: Elaboración propia

17. Luego pasaremos a obtener los archivos protegidos (Obtain Protected Files), para visualizar algún archivo sospechoso utilizando FTK y seleccionando la imagen forense:

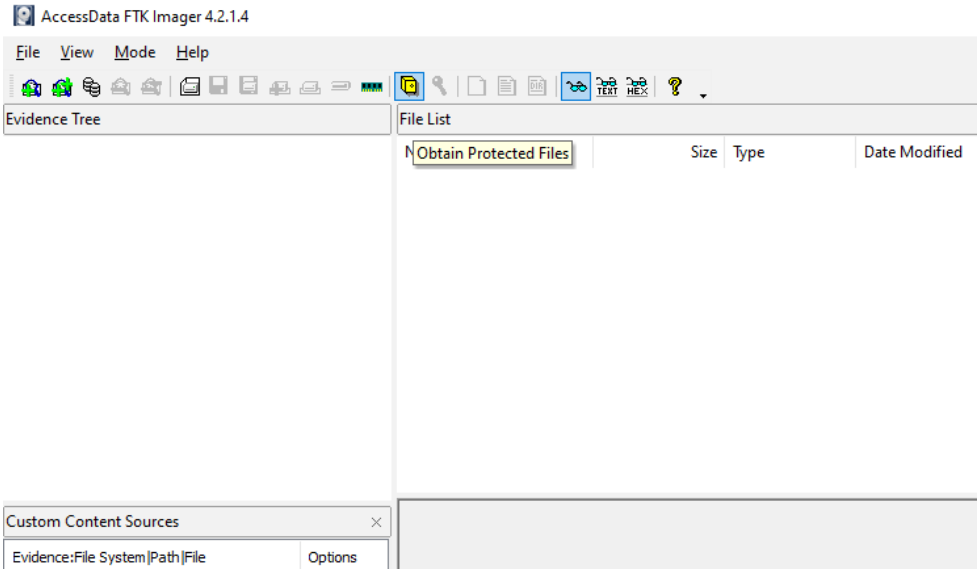


Figura Nº 125

Fuente: Elaboración propia

18. Previamente creamos en el escritorio una carpeta denominada Protegido, para exportar la información de búsqueda:

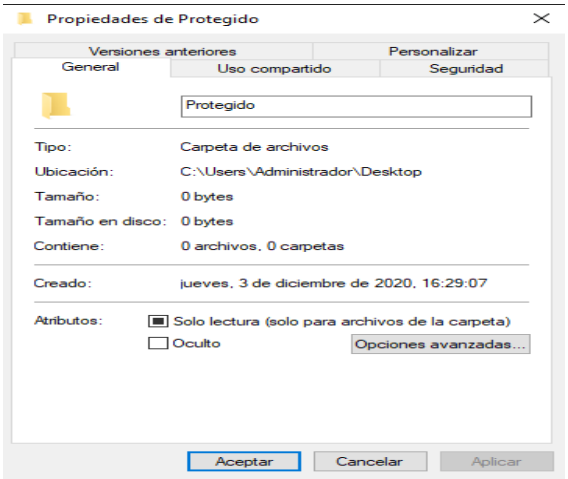


Figura Nº 126

Fuente: Elaboración propia

19. Seleccionamos esa carpeta como destino desde FTK:

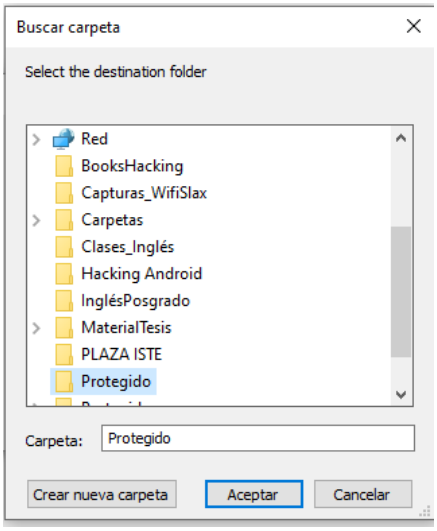


Figura Nº 127

Fuente: Elaboración propia

20. Pasamos ahora a realizar la búsqueda de la carpeta con FTK:

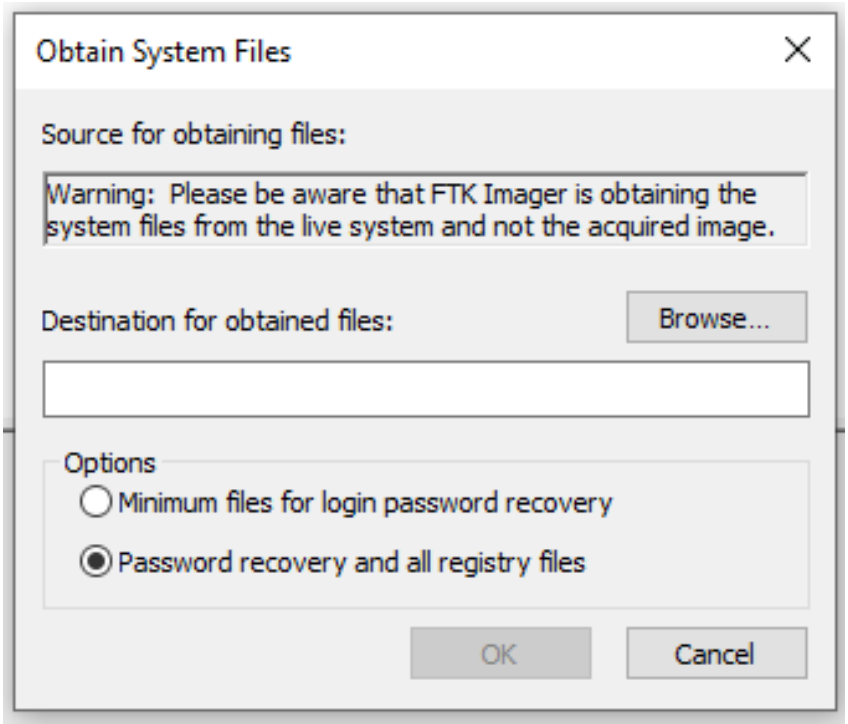


Figura Nº 128

Fuente: Elaboración propia

21. Direccionamiento a la carpeta Protegido:

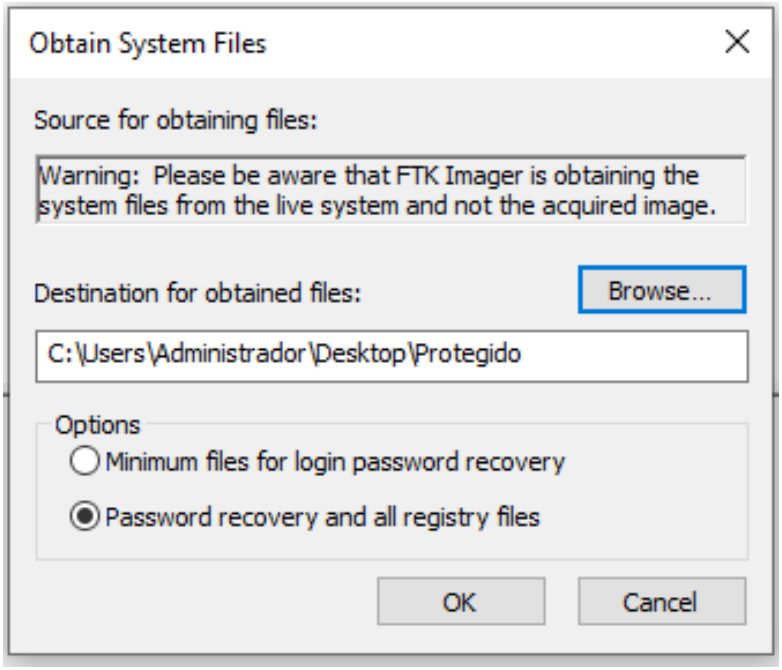


Figura Nº 129

Fuente: Elaboración propia

22. El escaneo se lleva a cabo:

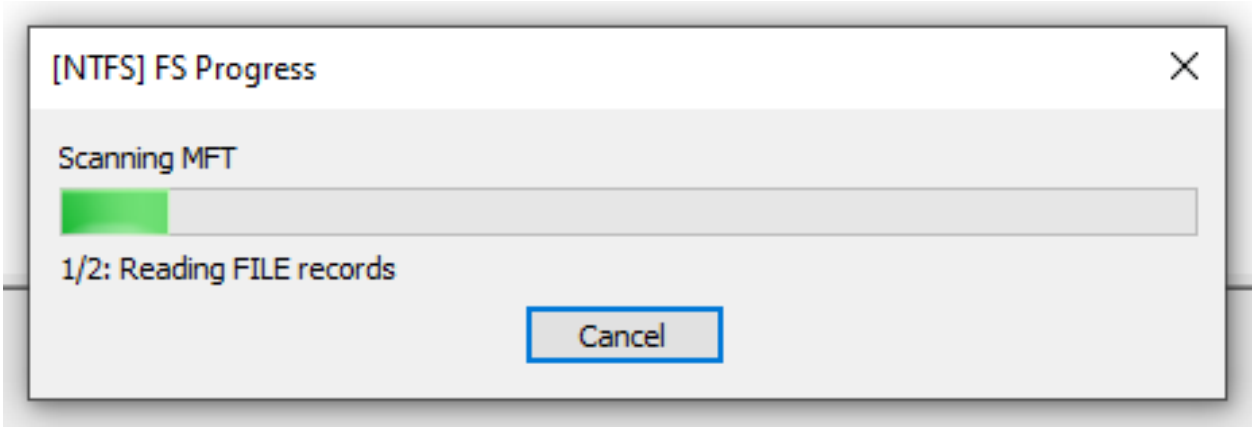


Figura Nº 130

Fuente: Elaboración propia

23. Una vez terminado el escaneo, vamos a verificar el contenido de la carpeta Protegido:

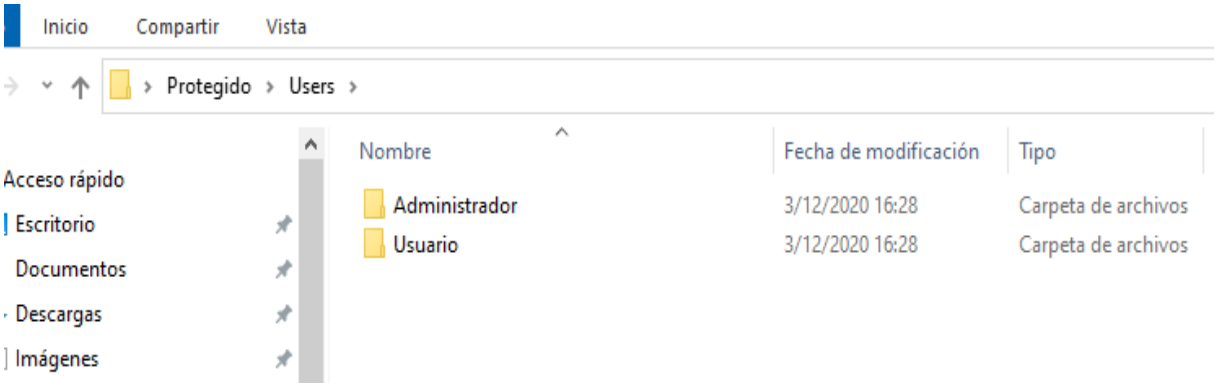


Figura Nº 131

Fuente: Elaboración propia

24. Aquí se aprecia que esta carpeta a su vez ha creado dos sub carpetas: Administrador y Usuario y la carpeta Administrador contiene a su vez a dos sub carpetas: Crypto y Protect:

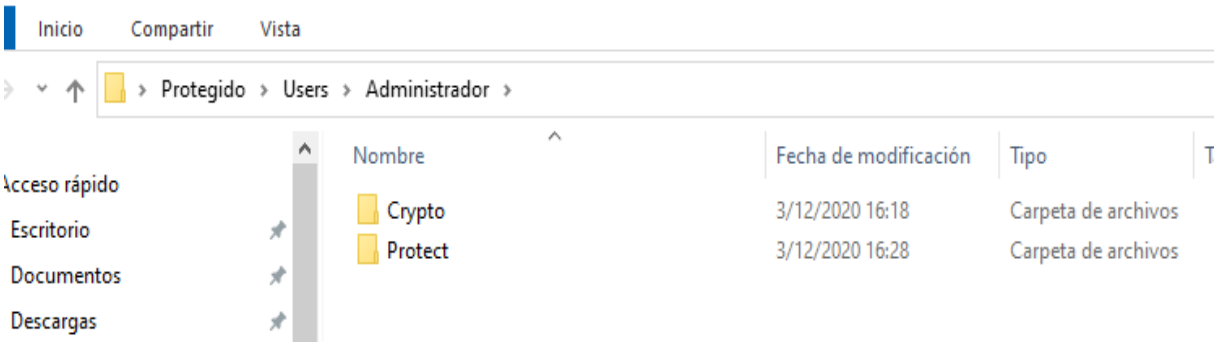


Figura Nº 132

Fuente: Elaboración propia

25. Verificamos el contenido de la carpeta Crypto y apreciamos que también a su vez, contiene dos sub carpetas: Keys y RSA

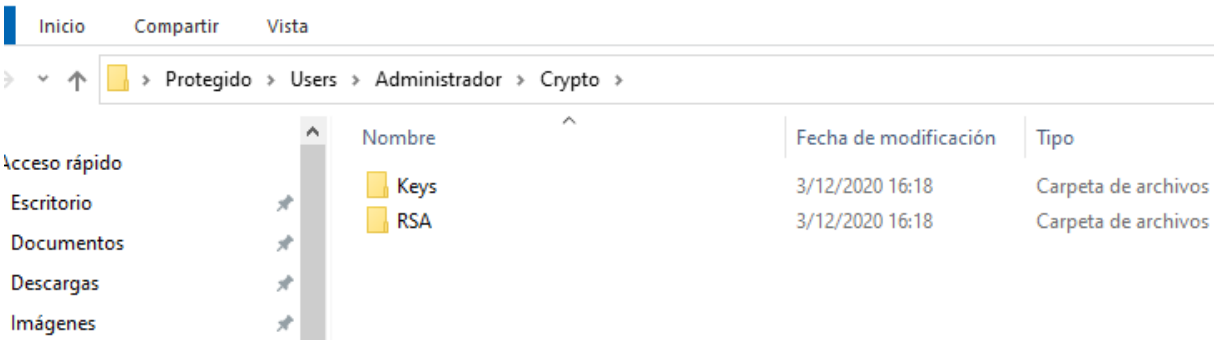


Figura Nº 133

Fuente: Elaboración propia

26. Podemos ver que la carpeta Keys solo tiene un archivo de sistema de 1 KB:

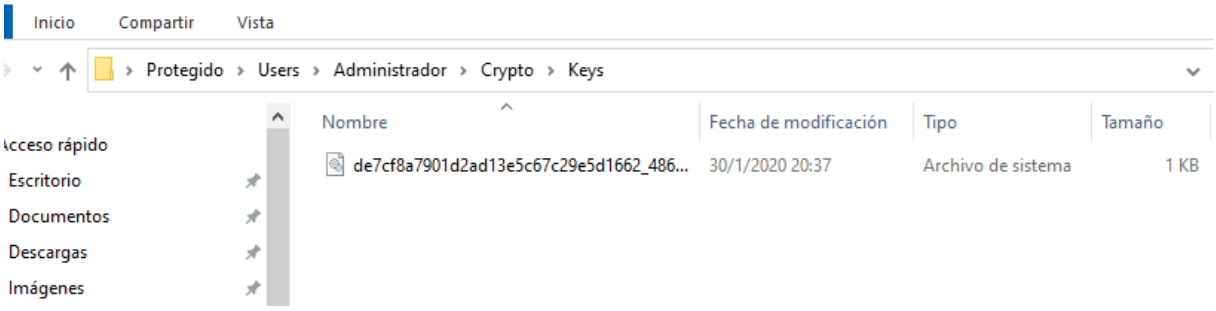


Figura Nº 134

Fuente: Elaboración propia

27. La carpeta RSA contiene a su vez otra carpeta numerada:

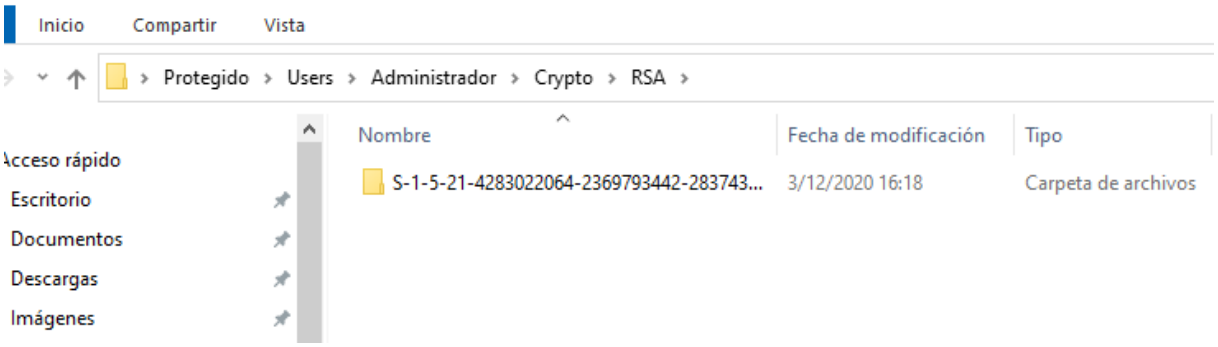


Figura Nº 135

Fuente: Elaboración propia

28. La carpeta numerada contiene solo archivos de sistema de 1 KB por lo tanto, se descarta la posibilidad de archivos encriptados maliciosos:

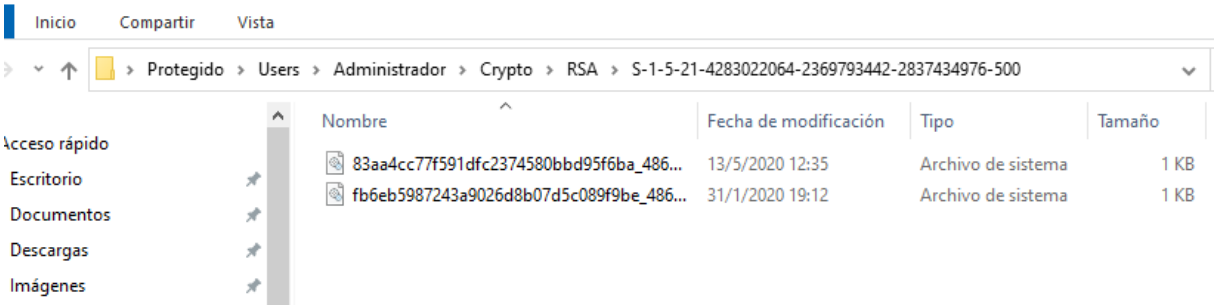


Figura Nº 136

Fuente: Elaboración propia

Anexo Nº 18: Capacitación de las destrezas y habilidades en Hacking Ético del personal involucrado en el manejo de la red de telecomunicaciones de Inversiones Mayito - Agente Bancario.

Medio audio visual: Aula Virtual

URLs: http://campus.pedrobeltrancanessa.org/

http://www.pedrobeltrancanessa.com/moodle/

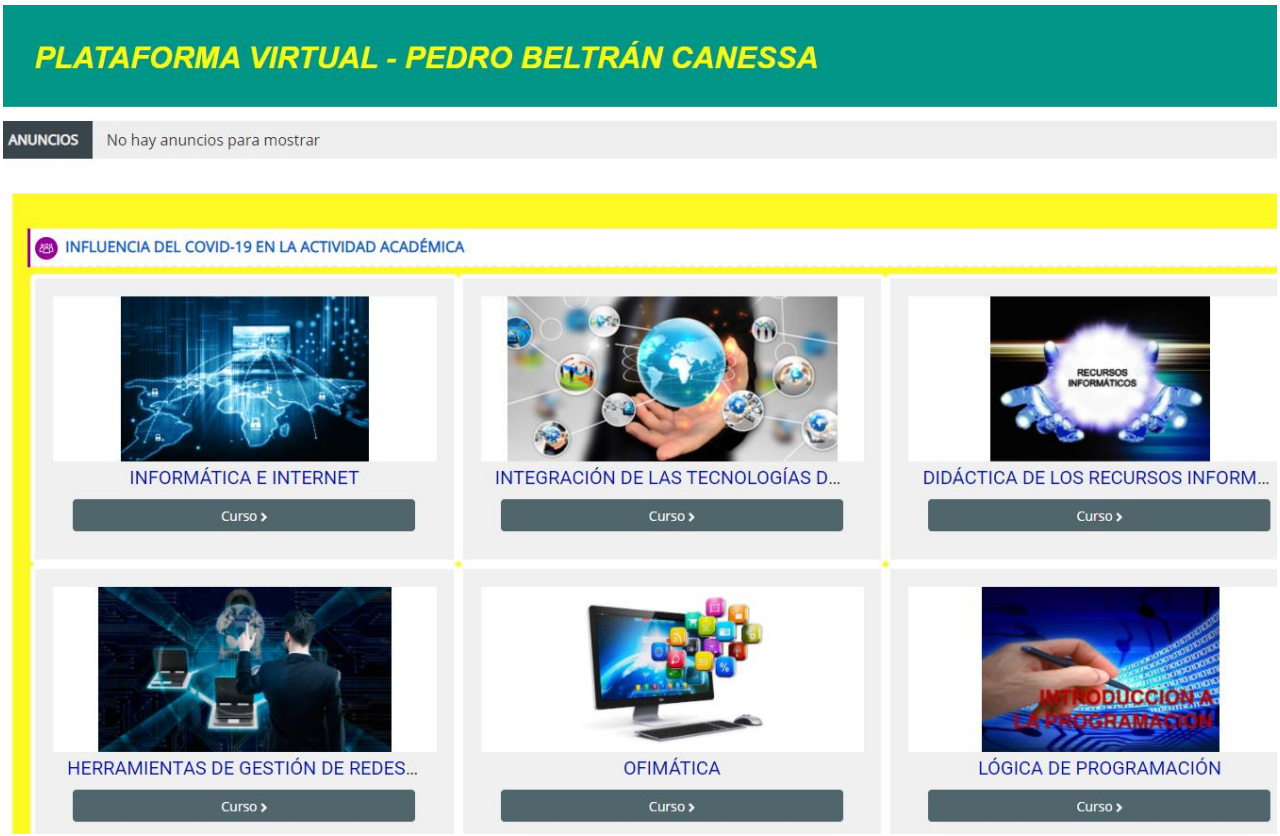


Figura Nº 137

Fuente: Elaboración propia

Anexo Nº 19: Teorías relacionadas

Figura N° 138: Definición Familia ISO 27000.

Fuente: es.sladishare.net

Figura N° 139: Definiciones de las Normas ISO 27000-2001-27002.

Fuente: es.sladishare.net

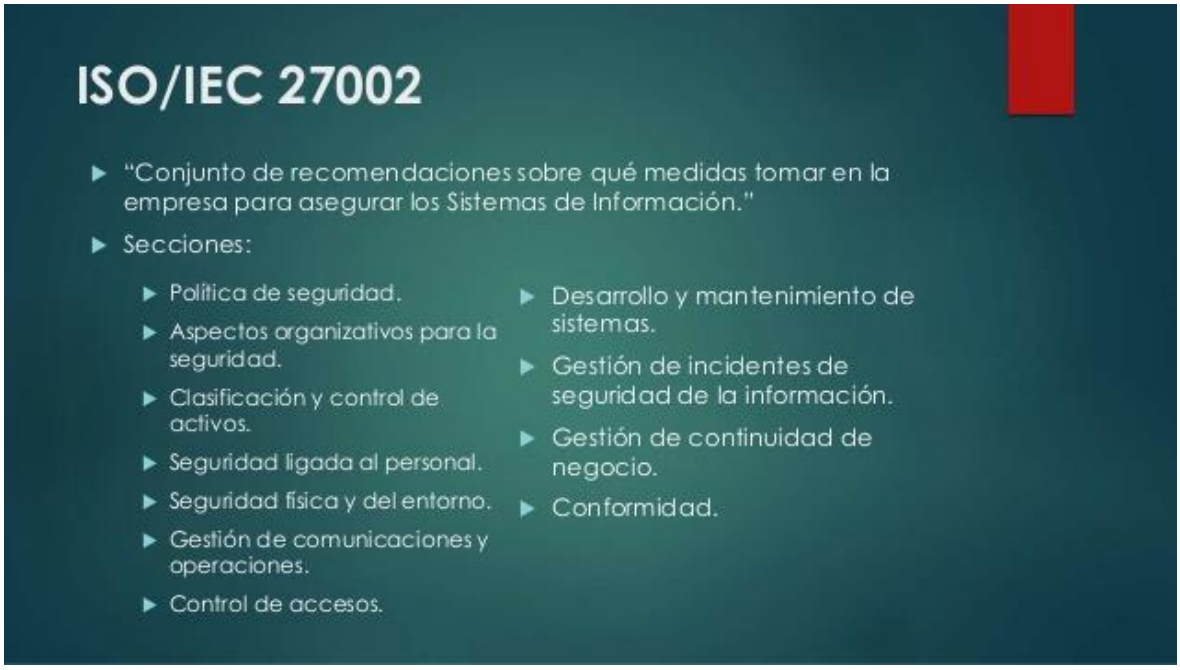


Figura N° 140: Definiciones de la Norma ISO 27002.

Fuente: es.sladishare.net

Figura N°141: Diferencias entre las Normas ISO 27001 e ISO 27002.

Fuente: es.sladishare.net

Según Toledo et al (2019), la metodología de la investigación tiene su fundamentación en la experiencia y conocimientos acumulados y adquiridos a través del tiempo, la misma que se constituye como una estrategia de trabajo de índole colectiva que hace las veces de un catalizador en la aceleración de la formación de profesionales de posgrado.

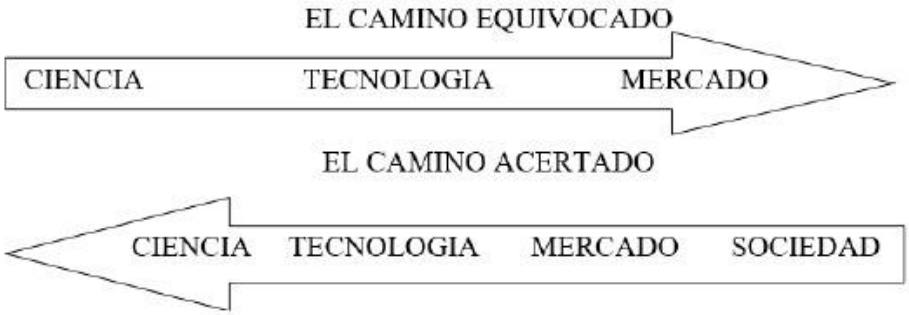


Figura N° 142: Respuesta científica a las reales demandas de la sociedad.

Fuente: Toledo et al (2019, p. 3)

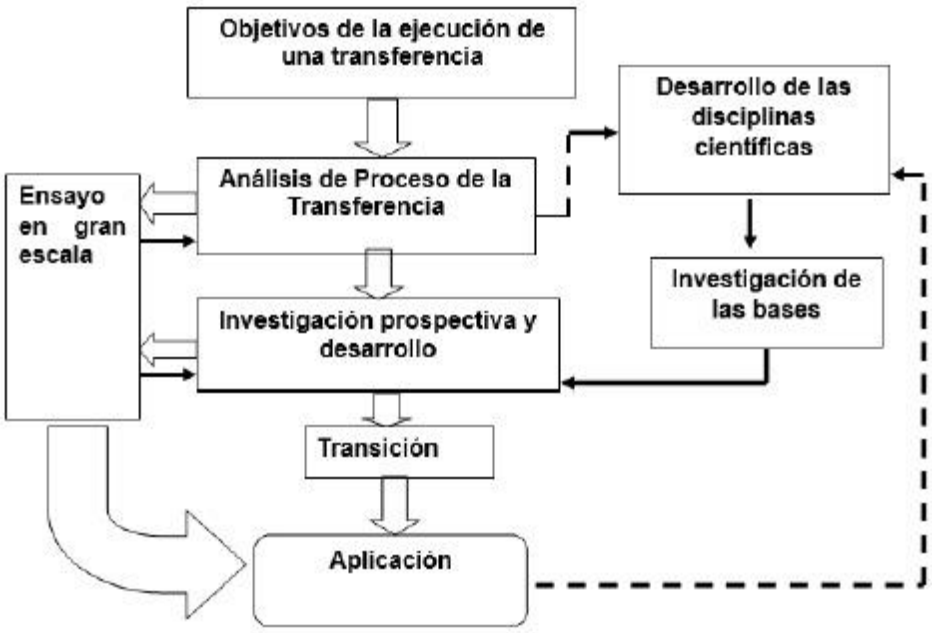


Figura N° 143: El proceso de las transferencias de las tecnologías en la interacción con las demandas de conocimientos nuevos

Fuente: Toledo et al. (2019, p. 10)

METODOLOGÍA EXPERIMENTAL	METODOLOGÍA NO EXPERIMENTAL
Se provocan (manipulan) los efectos	Los efectos ya se han producido
Se modifica la variable independiente y observamos los cambios (efectos) en la variable dependiente	No se modifican, sólo se seleccionan y observan
Orientación hacia el futuro	Orientación hacia el pasado
Aleatorización de grupos	Grupos naturales ya formados

Figura N° 144: Cuadro comparativo entre la Metodología Experimental y No experimental. Fuente: Elaboración propia

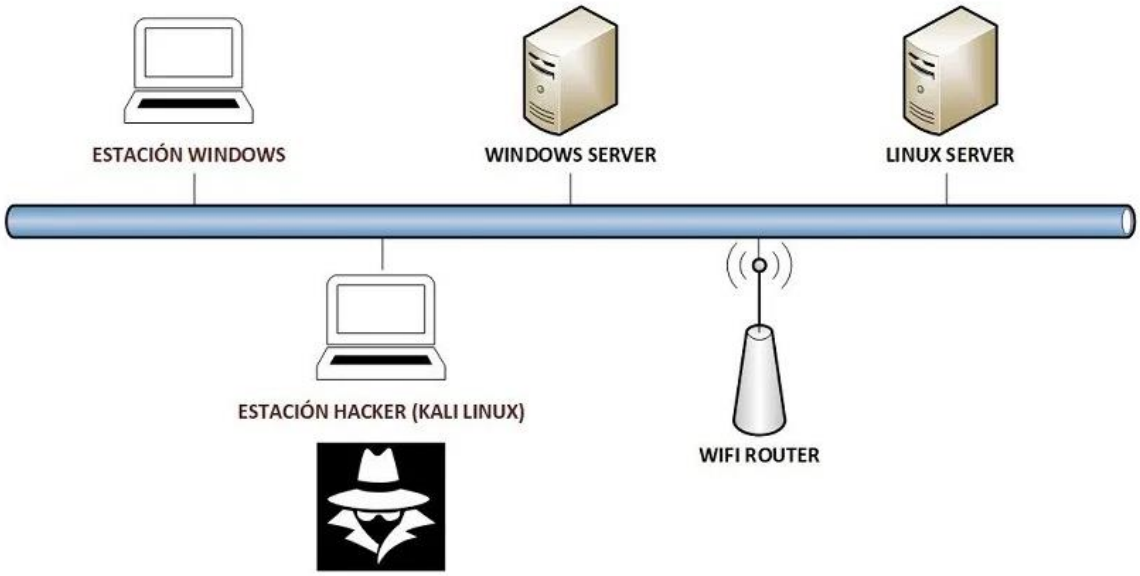


Figura N° 145: Laboratorio de Aplicaciones de Hacking Ético.

Fuente: Astudillo (2019)

Figura N° 146: Descarga gratuita de Plataformas Virtuales de Microsoft.

Fuente: Astudillo (2019)

- **Vulnerable by Design: https://www.vulnhub.com/**
- **Buggy Web App: http://www.itsecgames.com/**
- **Damn Vulnerable iOS Application: http://damnvulnerableiosapp.com/**
- **Game of Hacks: http://www.gameofhacks.com/**
- **Hack This Site!: https://www.hackthissite.org/**

Figura N° 147: Direcciones web de software gratuito para fines experimentales.

Fuente: Astudillo (2019)

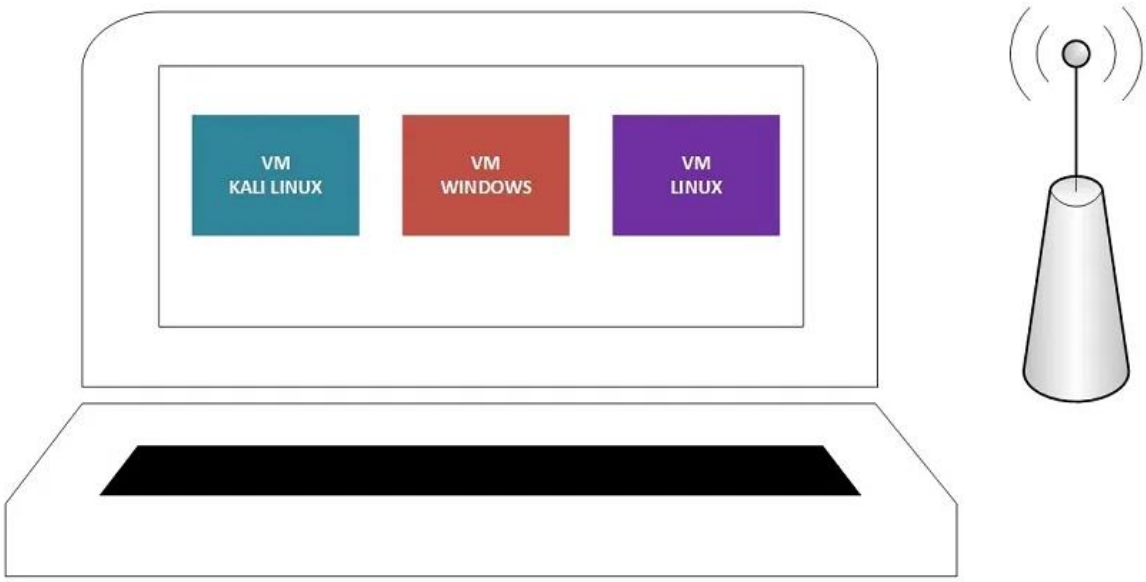


Figura N° 148: Laboratorio de Hacking Ético.

Fuente: Astudillo (2019)

Matriz de aspectos de la información-impacto-control

Aspecto de la información	Impacto	Control
Confidencialidad	➢ Pérdida de competitividad ➢ Divulgación de información protegida por leyes de privacidad	➢ Control de acceso ➢ Permisos en las carpetas o archivos ➢ Encriptación
Integridad	➢ Inexactitud ➢ Decisiones erróneas ➢ Fraude	➢ Control de acceso ➢ Firmas digitales ➢ Encriptado ➢ Hashes
Disponibilidad	➢ Pérdida del tiempo productivo ➢ Interfiere con los objetivos de la Organización ➢ Pérdida de la funcionalidad operativa	➢ Redundancia ➢ Copias de respaldo ➢ Controles de acceso

Figura N° 149: Matriz de Información-Impacto.

Fuente: Astudillo (2017)

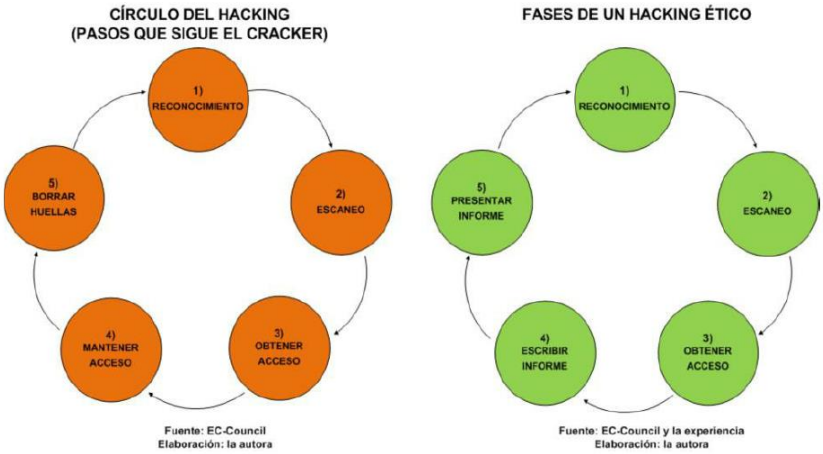


Figura N° 150: Fases del Hacking.

Fuente: Astudillo (2017)

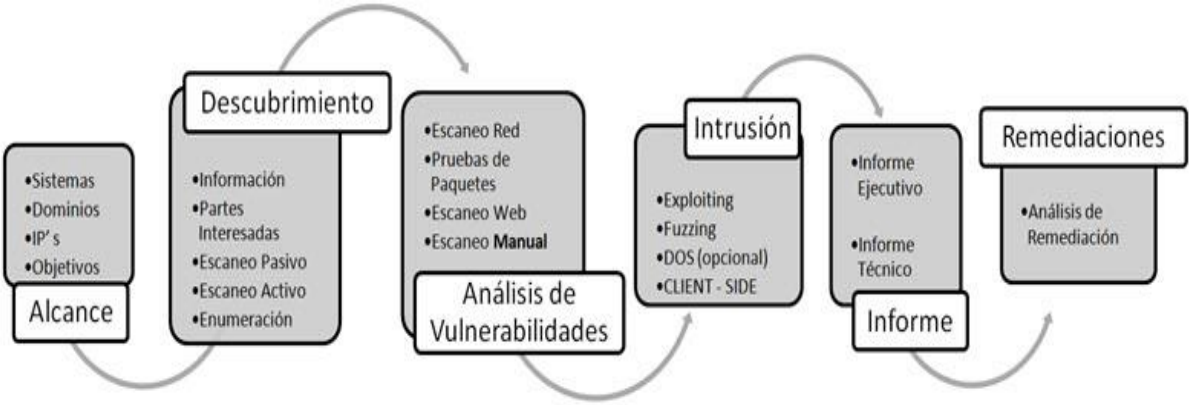


Figura N° 151: Fases del Hacking Ético.

Fuente: Pedraza (2014)

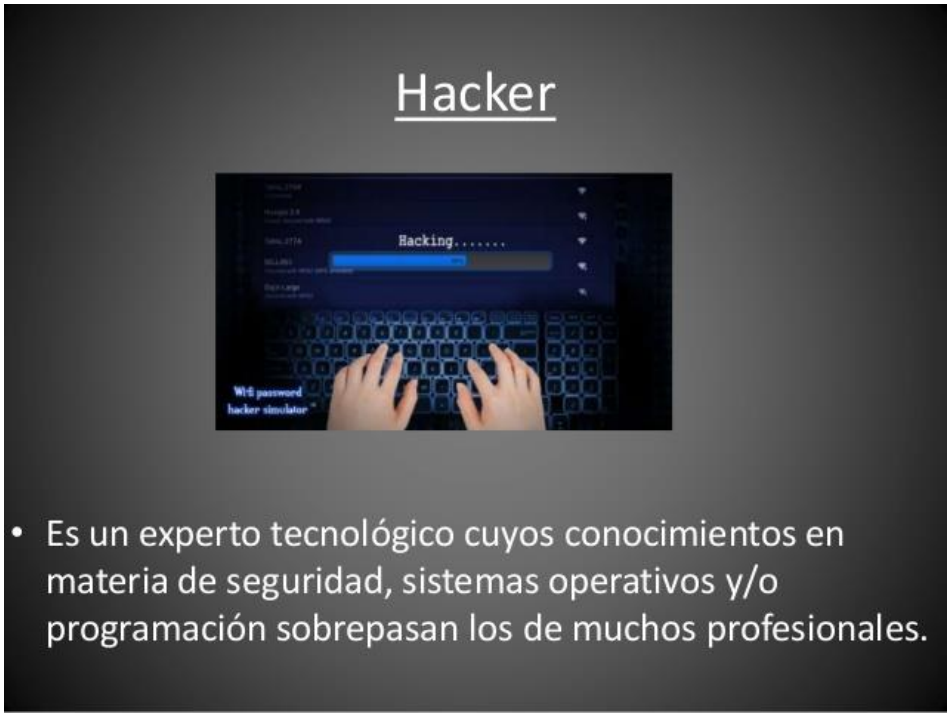


Figura N° 152: Definición de Hacker.

Fuente: Internet

Figura Nº 153: Fases del Hacking No Ético.

Fuente: Pedraza (2014)

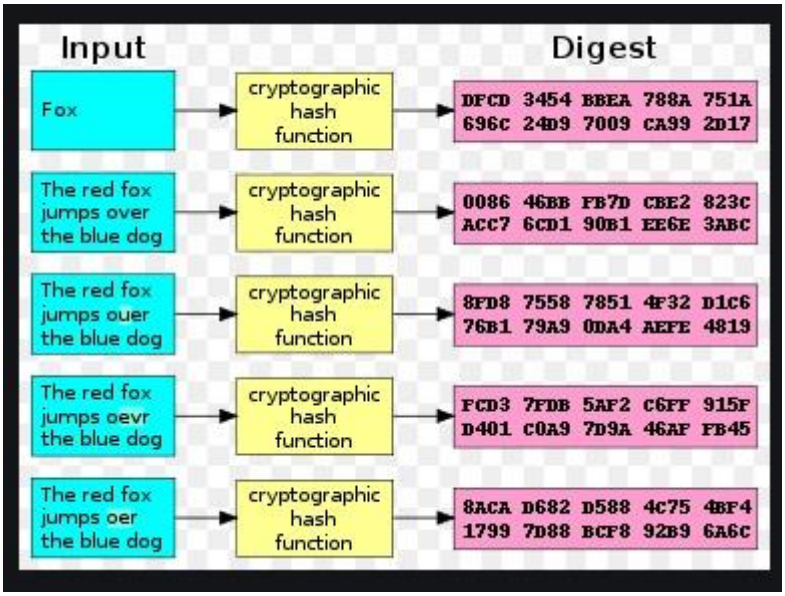


Figura N°154: Conversión Hash.

Fuente: Gutiérrez (2013)

Figura Nº 155: Niveles de Investigación.

Fuente: Supo y Garay et al. (2012)

Figura Nº 156: Niveles de Investigación.

Fuente: Supo y Garay et al. (2012)

Figura Nº 157: Matriz – Impacto - Control

Fuente: Internet

Figura Nº 158: Análisis de evidencias digitales.

Fuente: Karina Astudillo (2020)