EVALUAR LAS HERRAMIENTAS DE SEGURIDAD INFORMÁTICA MÁS EFECTIVAS DEL SISTEMA OPERATIVO KALI LINUX, UTILIZADOS EN LOS PROCESOS DE AUDITORÍA INFORMÁTICA EN LOS SISTEMAS DE INFORMACIÓN Y COMUNICACIÓN DE LAS ORGANIZACIONES

ARTURO ENRIQUE RUIZ HERNÁNDEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CÚCUTA
2022

EVALUAR LAS HERRAMIENTAS DE SEGURIDAD INFORMÁTICA MÁS EFECTIVAS DEL SISTEMA OPERATIVO KALI LINUX, UTILIZADOS EN LOS PROCESOS DE AUDITORÍA INFORMÁTICA EN LOS SISTEMAS DE INFORMACIÓN Y COMUNICACIÓN DE LAS ORGANIZACIONES

ARTURO ENRIQUE RUIZ HERNÁNDEZ

Proyecto de Grado – Monografía presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

JOHN FREDDY QUINTERO TAMAYO
Director de Proyecto

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CÚCUTA
2022

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

Firma del Presidente de Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Ciudad., Fecha sustentación

DEDICATORIA

El presente trabajo es dedicado a mi Familia: mi esposa Margarita Caballero y mis hijas Ana Karina y Ana Lucía, por su paciencia, comprensión, fortaleza y me animan a cada momento a ser mejor persona; igualmente a mis Padres, hermanos y demás familiares, de una u otra manera están atentos apoyándome y acompañándome en cada momento de mi vida.

AGRADECIMIENTOS

Agradezco a Dios, por su infinito amor y misericordia; a Margarita quien continuamente me anima a seguir perseverando en las buenas ideas; Karina y Lucía que con sus continuas y bellas sonrisas me inspiran a ser mejor. A la Universidad Nacional Abierta y a Distancia UNAD, por su metodología y pionera en este método de estudios, por otro lado, a cada uno de los tutores y asesores que me acompañaron en el proceso les reconozco que sin su apoyo y colaboración éste logro no hubiera sido posible.

CONTENIDO

LISTA DE TABLAS

PÁG.

LISTA DE FIGURAS

PÁG.

GLOSARIO

Amenaza. Circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor (INCIBE, 2017).

Ataque de Fuerza Bruta. Un ataque de fuerza bruta es un procedimiento para averiguar una contraseña que consiste en probar todas las combinaciones posibles hasta encontrar la combinación correcta (INCIBE, 2017).

Auditoría de seguridad. Es el estudio que comprende el análisis y gestión de sistemas llevado a cabo por profesionales en tecnologías de la información (TI) con el objetivo de identificar, enumerar y describir las diversas vulnerabilidades que pudieran presentarse en una revisión exhaustiva de las estaciones de trabajo, redes de comunicaciones, servidores (INCIBE, 2017).

Brecha de seguridad. Violaciones de la seguridad que ocasionan la destrucción, pérdida o alteración accidental o deliberada de datos personales cuando están siendo transmitidos, están almacenados o son objeto de otros tratamientos (INCIBE, 2017).

Ciberdelincuente. Persona que realiza actividades delictivas en la red contra personas o sistemas informáticos, pudiendo provocar daños económicos o reputacionales mediante robo, filtrado de información, deterioro de software o hardware, fraude y extorsión. Casi siempre están orientados a la obtención de fines económicos (INCIBE, 2017).

Confidencialidad. Confidencialidad es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información (INCIBE, 2017).

Cortafuegos. Sistema de seguridad compuesto o bien de programas (software) o de dispositivos hardware situados en los puntos limítrofes de una red que tienen el objetivo de permitir y limitar, el flujo de tráfico entre los diferentes ámbitos que protege sobre la base de un conjunto de normas y otros criterios (INCIBE, 2017).

Denegación de servicios. Se entiende como denegación de servicio, en términos de seguridad informática, a un conjunto de técnicas que tienen por objetivo dejar un servidor inoperativo. Mediante este tipo de ataques se busca sobrecargar un servidor y de esta forma impedir que los usuarios legítimos puedan utilizar los servicios por prestados por él (INCIBE, 2017).

Disponibilidad. Se trata de la capacidad de un servicio, un sistema o una información, a ser accesible y utilizable por los usuarios o procesos autorizados cuando éstos lo requieran (INCIBE, 2017).

Informática forense. La informática forense consiste en un proceso de investigación de los sistemas de información para detectar toda evidencia que pueda ser presentada como prueba fehaciente en un procedimiento judicial (INCIBE, 2017).

Integridad. La Integridad es la propiedad de la información, por la que se garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada, por errores de software o hardware o por condiciones medioambientales (INCIBE, 2017).

Inyección SQL. Es un tipo de ataque que se aprovecha de una vulnerabilidad en la validación de los contenidos introducidos en un formulario web y que puede permitir la obtención de forma ilegítima de los datos almacenados en la base de datos del sitio web, entre ellos las credenciales de acceso (INCIBE, 2017).

Pentest. Una prueba de penetración es un ataque a un sistema software o hardware con el objetivo de encontrar vulnerabilidades (INCIBE, 2017).

Ransomware. El ciberdelincuente, toma control del equipo infectado y «secuestra» la información del usuario cifrándola, de tal forma que permanece ilegible si no se cuenta con la contraseña de descifrado (INCIBE, 2017).

Sniffer. Un sniffer es un programa que monitoriza la información que circula por la red con el objeto de capturar información (INCIBE, 2017).

Vulnerabilidad. Debilidad o fallo de un sistema que puede ser aprovechado con fines maliciosos (normalmente mediante un programa que se denomina exploit) (INCIBE, 2017).

RESUMEN

El sistema operativo *Kali Linux* tiene gran popularidad entre los profesionales de seguridad informática y actualmente es uno de los más comunes ya que como sistema integra una gran número de herramientas de seguridad para auditoría y *pentest* lo cual tiene gran relevancia, pero existe el problema que en este sistema operativo no se tiene mucha destreza y habilidades para su ejecución pues en nuestro medio existe poca información bibliográfica y de la que se dispone está en idiomas diferentes al español, y por lo tanto para cualquier consulta se debe recurrir a las páginas oficiales que a través de artículos y pruebas contribuyen a la actualización pero la gran mayoría de esto se encuentra en el idioma inglés.

En el presente trabajo se evalúan 10 herramientas de auditoría integradas en el sistema operativo *Kali Linux*, cuyo conocimiento y referencia contribuyen en gran medida para iniciarse en el mundo de la seguridad informática, teniendo en cuenta su valor bibliográfico y su aporte a futuros trabajos de grado. Además, se definen casos en las que las herramientas tienen utilidad a la hora de realizar test de intrusión y se elabora la documentación pertinente de las herramientas seleccionadas.

ABSTRACT

The Kali Linux operating system has great popularity among computer security professionals and is currently one of the most common because as a system integrates a large number of security tools for auditing and pentest which has great relevance, But there is the problem that in this operating system there is not much skill and abilities for its execution because in our environment there is little bibliographic information and that which is available is in languages other than Spanish, and therefore for any consultation must resort to the official pages that through articles and tests contribute to the update but the vast majority of this is in the English language.

In the present work, 10 auditing tools integrated in the Kali Linux operating system are evaluated, whose knowledge and reference contribute greatly to getting started in the world of computer security, taking into account their bibliographic value and their contribution to future degree works. In addition, cases are defined in which the tools are useful when performing intrusion tests and the relevant documentation of the selected tools is prepared.

INTRODUCCIÓN

El sistema operativo Kali Linux tiene gran relevancia en cuanto a los analistas de seguridad o pentester, puesto que ofrece un gran número de herramientas relacionadas con la seguridad, además de esto ha ganado aceptación en el mundo de la seguridad informática y hoy se puede decir que es el sistema operativo líder relacionado con el tema de seguridad informática; no es el único software que se utiliza para realizar los test de intrusión, existen otras herramientas que aunque ofrecen casi las mismas capacidades y herramientas, Kali Linux tiene la ventaja sobre ellos por su grado de popularidad y la comunidad que constantemente ha estado incluyendo actualizaciones y mejoras al software. Una de las grandes ventajas es que siendo un Linux es un software libre de distribución gratuita y descarga e instalación en cualquier equipo, ya sea de escritorio, portátil, USB, smartphone y hasta en Raspberry PI.

Además de esto, en nuestro medio son muy pocos los profesionales en seguridad informática que tienen la destreza y manejo que este gran software nos ofrece, y más aún el usuario final que aunque este sistema operativo no es tanto para trabajo de escritorio sino más orientado a realizar actividades de test de intrusión, no tiene gran aceptación hacia este último puesto que su entorno siendo gráfico, al actualizar y requerir de su manejo generalmente se realiza por la Terminal y en modo línea de comando, razón por la cual un usuario que no tenga la destreza sobre este ambiente lo verá como algo sin sentido y no comprenderá muy bien la gran utilidad que ofrece.

Por otra parte, antes de Kali Linux el software se llamó Bactrack y ofrecía la misma funcionalidad, ya siendo hoy en día con su entorno gráfico más amigable que la comunidad ha estado desarrollando y continúa aplicando mejoras y nuevas actualizaciones. En cuanto a documentación, la comunidad de Kali Linux, los foros, videotutoriales y libros mantienen actualizados a los futuros profesionales en esta área lo relacionado con el manejo y la destreza del gran número de herramientas que ofrece.

Se requiere que esta herramienta logre aceptación en nuestro medio y que obtenga gran popularidad para que sea utilizada de una manera ética, responsable y con destreza, puesto que, aunque tiene popularidad no es muy común encontrarla en ambientes de hogar y corporativos y como es un sistema operativo basado en Debian Linux su grado de adaptación requiere tiempo, perseverancia y cuidado al momento de llevar a cabo cualquier tarea.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

Se presentan los antecedentes del problema planteado, referenciar estadísticas del problema, entre otros.

Ochoa Guevara Frey Marín (2018) en su Tesis de grado: “Estudio de seguridad en las bases de datos, mediante metodologías de *pen test*, *ethical hacking* en la secretaria de hacienda municipal de los patios”, para las pruebas se utilizó varios sistemas operativos con la metodología UNIX bajo LINUX, con software sofisticado como lo es Kali Linux que permite con cada una de las herramientas internas hacer escaneo de puertos, pruebas de penetración y un número significativo de implementaciones logrando los objetivos de vulnerabilidades que afecten los diferentes Sistemas Operativos.

Osorio Carrero John Edward (2020), en su tesis: “Análisis y Valoración de Vulnerabilidades de la Infraestructura Cibernética de la Empresa Nostradamus S.A.S “, la cual se desarrolló mediante la ejecución de un enfoque técnico referente a la realización de pruebas de penetración usando la distribución Kali Linux para obtener un ambiente controlado en el que se pudieron recrear los ataques ocurridos en la organización.

Marmolejo Serrano Javier y Pastrana Franco Adrián (2018), en su tesis: “Pruebas de penetración a la infraestructura tecnológica de la empresa taller industrial Alkan S.A.S de la ciudad Guadalajara de Buga, valle para identificar vulnerabilidades” En este documento se encuentra la valoración del estado de la infraestructura cibernética de la empresa NOSTRADAMUS S.A.S la cual se desarrolló mediante la ejecución de un enfoque técnico referente a la realización de pruebas de penetración usando la distribución Kali Linux para obtener un ambiente controlado en el que se pudieron recrear los ataques ocurridos en

la organización. Kali Linux es un sistema operativo referente a nivel mundial en el ámbito de la seguridad defensiva y ofensiva, puesto que cuenta con gran cantidad de herramientas diseñadas para la auditoria y seguridad informática.

Ballen León, Diego Francisco (2019), en sus tesis: “Análisis de Vulnerabilidades al Servidor de Pruebas del Departamento de Sistemas de la E.S.E. Hospital Marco Felipe Afanador del Municipio de Tocaima Cundinamarca Generando las Recomendaciones para Realizar un Proceso de Hardening“. Otra de las herramientas que fueron de gran ayuda fue la suite de seguridad informática KALI LINUX, al igual que openvas, esta distribución es totalmente gratuita y sirve como complemente perfecto para realizar pentesting reconociendo posibles fallas a diferentes niveles y objetivos que posiblemente los analizadores de vulnerabilidades puedan pasar por alto, lo que demuestra que al igual que la infraestructuras los métodos de análisis no son perfectos y pueden necesitar complementos adicionales para dar una visión adicional al escenario analizado.

1.2 FORMULACIÓN DEL PROBLEMA

Se propone a partir de lo anterior una pregunta problema alineada a lo presentado en el ítem anterior.

¿Cuáles herramientas de la distribución Kali Linux podrían mejorar la auditoria de seguridad informática en un entorno empresarial?

1.3 JUSTIFICACIÓN

En la actualidad aunque en la página oficial Kali.org hay información sostenible de la operación correcta del sistema operativo Kali Linux, está en gran parte es utilizada por personal que se ha capacitado a través de muchos años en seguir la trayectoria de cómo implementar Linux tanto en equipos personales como en servidores; en otras palabras, es un lenguaje muy complejo para las personas que están iniciándose en el mundo de la

ciberseguridad y además la página oficial se encuentra en inglés, todas estas dificultades hacen que no sea muy común en nuestro medio el manejo y la destreza en este sistema operativo, además comercialmente no es atractivo y no es de fácil implementación en empresas que cuentan con años en la destreza y manejo de sistemas operativos comerciales. Además de esto, la interfaz gráfica no resulta de gran atractivo para el usuario final que ve la búsqueda de sus iconos, carpetas y archivos no son de fácil acceso y resulta poco comprensible y hasta difícil adquirir nuevamente destreza y manejo para acostumbrarse a la nueva interfaz gráfica del software.

Por otro lado, resulta comprensible para los nuevos usuarios del sistema operativo Linux que aunque ha ganado popularidad en muchas comunidades, la gran cantidad de distribuciones resulten un poco confusas para seleccionar la mejor y la más adecuada para su entorno de trabajo, esto tanto para lo personal como para la laboral, a pesar de esto las comunidades adscritas a realizar mejoras de estos sistemas se han encargado de promover su uso de una manera amigable introduciendo tutoriales, foros, videos de instalación y configuración, soporte técnico y libros entre otros, a quien se quiera iniciar en este sistema operativo.

Por tanto, el proyecto a realizar busca que se documenten algunas herramientas de seguridad informática en español para hacerlas más efectivas y más accesibles al usuario que se está iniciando en seguridad informática, que pueda aumentar sus habilidades, destrezas y que le permitan un oportuno y buen manejo en la realización de pruebas de intrusión y auditorías informáticas con este software. Finalmente, la ejecución de este proyecto se convertirá en un buen material de consulta para los estudiantes de la especialización en seguridad informática de la Universidad Nacional Abierta y a Distancia – UNAD interesados en seguir este tema.

2. OBJETIVOS

2.1 OBJETIVOS GENERAL

Evaluar diez herramientas de auditoría integradas en el Sistema Operativo Kali Linux.

2.2 OBJETIVOS ESPECÍFICOS

Definir el estado del arte y casos de éxito sobre auditorías que hagan uso de herramientas especializadas implícitas en Kali Linux.

Documentar el funcionamiento de las herramientas de auditoría articuladas al Sistema Operativo Kali Linux.

Ejecutar una PoC por cada herramienta documentada a modo de manual de uso.

Elaborar manual con tres escenarios los cuales se resuelven haciendo uso de la auditoría y sus herramientas.

3. MARCO REFERENCIAL

3.1 MARCO TEÓRICO

La seguridad de TI es un conjunto de estrategias de ciberseguridad que evita el acceso no autorizado a los activos de la organización, como computadoras, redes y datos. Mantiene la integridad y confidencialidad de la información sensible, bloqueando el acceso de hackers sofisticados (Mason Andrew, 2001).

Debido a que la tecnología de la información se ha convertido en la frase de moda corporativa aceptada que significa, básicamente, "computadoras y cosas relacionadas", a veces se puede ver que la seguridad de la información y la ciberseguridad se usan indistintamente. Estrictamente hablando, la ciberseguridad es la práctica más amplia de defender los activos de TI de los ataques , y la seguridad de la información es una disciplina específica bajo el paraguas de la ciberseguridad. La seguridad de la red y la seguridad de las aplicaciones son prácticas hermanas de la seguridad de la información, que se centran en las redes y el código de la aplicación, respectivamente.

Como se puede ver, en la definición de ambas se presenta cierta superposición de conceptos, la cual se puede aclarar teniendo en cuenta que la ciberseguridad está por encima de las demás; no puede proteger los datos transmitidos a través de una red insegura o manipulados por una aplicación con fugas. Además, hay mucha información que no se almacena electrónicamente y que también debe protegerse. Por tanto, el cometido del profesional en ciberseguridad es necesariamente amplio.

3.1.1 Principios de Seguridad de la Información

Los componentes básicos de la seguridad de la información se resumen con mayor frecuencia en la llamada tríada CIA: Confidencialidad, integridad y disponibilidad. La confidencialidad es quizás el elemento de la tríada que más inmediatamente le viene a la

mente cuando piensa en la seguridad de la información. Los datos son confidenciales cuando solo pueden hacerlo aquellas personas que están autorizadas a acceder a ellos; Para garantizar la confidencialidad, debe poder identificar quién está tratando de acceder a los datos y bloquear los intentos de quienes no tienen autorización. Las contraseñas, el cifrado, la autenticación y la defensa contra ataques de penetración son técnicas diseñadas para garantizar la confidencialidad (Frühling Gallardo, 2012).

Integridad significa mantener los datos en su estado correcto y evitar que sean modificados indebidamente, ya sea por accidente o maliciosamente. Muchas de las técnicas que garantizan la confidencialidad también protegerán la integridad de los datos; después de todo, un pirata informático no puede cambiar los datos a los que no puede acceder, pero existen otras herramientas que ayudan a brindar una defensa de la integridad en profundidad: las sumas de comprobación pueden ayudarlo a verificar los datos la integridad, por ejemplo, y el software de control de versiones y las copias de seguridad frecuentes pueden ayudarlo a restaurar los datos a un estado correcto si es necesario. La integridad también cubre el concepto de no repudio : debe poder demostrar que ha mantenido la integridad de sus datos, especialmente en contextos Legales (Frühling Gallardo, 2012).

La disponibilidad es la imagen reflejada de la confidencialidad: Si bien debe asegurarse de que usuarios no autorizados no puedan acceder a sus datos, también debe asegurarse de que puedan acceder a ellos quienes tengan los permisos adecuados. Asegurar la disponibilidad de los datos significa hacer coincidir los recursos informáticos y de red con el volumen de acceso a los datos que espera e implementar una buena política de respaldo para fines de recuperación ante desastres (Areitio Bertolín, 2008). La seguridad de la información, a menudo denominada InfoSec, se refiere a los procesos y herramientas diseñados e implementados para proteger la información empresarial confidencial de modificaciones, interrupciones, destrucción e inspección (Areitio Bertolín, 2008).

¿Cuál es la diferencia entre ciberseguridad y seguridad de la información? La seguridad de la información y la ciberseguridad a menudo se confunden. InfoSec es una parte crucial de la ciberseguridad, pero se refiere exclusivamente a los procesos diseñados para la seguridad de los datos. La ciberseguridad es un término más general que incluye InfoSec (Gago, 2017).

¿Qué certificaciones se necesitan para trabajos de ciberseguridad? Las certificaciones para trabajos de ciberseguridad pueden variar. Para algunas empresas, su director de seguridad de la información (CISO) o el gerente de seguridad de la información certificado (CISM) pueden requerir capacitación específica del proveedor. De manera más general, las organizaciones sin fines de lucro como el Consorcio Internacional de Certificación de Seguridad de Sistemas de Información brindan certificaciones de seguridad ampliamente aceptadas. Las certificaciones pueden variar desde CompTIA Security + hasta Certified Information Systems Security Professional (CISSP) (Gago, 2017).

3.1.2 Tipos de Seguridad Informática (INFOSEC)

3.1.2.1 Seguridad de la Aplicación. La seguridad de las aplicaciones es un tema amplio que cubre las vulnerabilidades del software en aplicaciones web y móviles e interfaces de programación de aplicaciones (API). Estas vulnerabilidades se pueden encontrar en la autenticación o autorización de los usuarios, la integridad del código y las configuraciones, y las políticas y procedimientos maduros. Las vulnerabilidades de las aplicaciones pueden crear puntos de entrada para infracciones importantes de InfoSec. La seguridad de las aplicaciones es una parte importante de la defensa del perímetro de InfoSec.

3.1.2.2 Seguridad en la Nube. La seguridad en la nube se centra en la creación y el alojamiento de aplicaciones seguras en entornos de nube y en el consumo seguro de aplicaciones en la nube de terceros. "Nube" simplemente significa que la aplicación se

ejecuta en un entorno compartido. Las empresas deben asegurarse de que exista un aislamiento adecuado entre los diferentes procesos en entornos compartidos.

3.1.3 Criptografía

Cifrar los datos en tránsito y los datos en reposo ayuda a garantizar la confidencialidad e integridad de los datos. Las firmas digitales se utilizan comúnmente en criptografía para validar la autenticidad de los datos. La criptografía y el cifrado se han vuelto cada vez más importantes. Un buen ejemplo de uso de la criptografía es el Estándar de cifrado avanzado (AES). El AES es un algoritmo de clave simétrica que se utiliza para proteger información gubernamental clasificada.

3.1.4 Seguridad de la Infraestructura

La seguridad de la infraestructura se ocupa de la protección de redes internas y extranet, laboratorios, centros de datos, servidores, computadoras de escritorio y dispositivos móviles.

3.1.5 Respuesta a Incidentes

La respuesta a incidentes es la función que monitorea e investiga el comportamiento potencialmente malicioso. En preparación para las infracciones, el personal de TI debe tener un plan de respuesta a incidentes para contener la amenaza y restaurar la red. Además, el plan debe crear un sistema para preservar las pruebas para el análisis forense y el posible enjuiciamiento. Estos datos pueden ayudar a prevenir más infracciones y ayudar al personal a descubrir al atacante (Tibaquira Cortes, 2015).

3.1.6 Categorías de Seguridad Informática

La seguridad de la red es la práctica de proteger una red informática de intrusos, ya sean atacantes dirigidos o malware oportunista.

La seguridad de las aplicaciones se centra en mantener el software y los dispositivos libres de amenazas. Una aplicación comprometida podría proporcionar acceso a los

datos que está diseñada para proteger. La seguridad exitosa comienza en la etapa de diseño, mucho antes de que se implemente un programa o dispositivo.

La seguridad de la información protege la integridad y privacidad de los datos, tanto en almacenamiento como en tránsito. Por su parte, la seguridad operativa incluye los procesos y decisiones para manejar y proteger los activos de datos. Los permisos que tienen los usuarios cuando acceden a una red y los procedimientos que determinan cómo y dónde se pueden almacenar o compartir los datos caen bajo este paraguas.

La recuperación ante desastres y la continuidad del negocio definen cómo responde una organización a un incidente de seguridad cibernética o cualquier otro evento que provoque la pérdida de operaciones o datos. Las políticas de recuperación ante desastres dictan cómo la organización restaura sus operaciones e información para volver a la misma capacidad operativa que tenía antes del evento. La continuidad del negocio es el plan al que recurre la organización mientras intenta operar sin ciertos recursos.

La educación del usuario final aborda el factor de seguridad cibernética más impredecible: las personas. Cualquiera puede introducir accidentalmente un virus en un sistema que de otro modo sería seguro si no sigue las buenas prácticas de seguridad. Enseñar a los usuarios a eliminar archivos adjuntos de correo electrónico sospechosos, no a conectar unidades USB no identificadas, y otras lecciones importantes es vital para la seguridad de cualquier organización (Gamboa Suarez, 2020).

3.1.7 Hacking Ético y Pentesting

Ciertamente, a lo largo de los años el llamado “hacking ético” ha tenido adeptos y contrincantes. Ello ha estado relacionado fundamentalmente por la combinación de estos dos vocablos: ético (se refiere a algo correcto, bueno), hacking (indica lo contrario). El desconocimiento del rol que juega el hacking ético es la principal causa de esta problemática.

El hacking ético no entra en los sistemas informáticos para robar o alterar información, sino para encontrar vulnerabilidades y fallos. También es conocido como prueba de intrusión o pentest, o sea, es “el arte de comprobar la existencia de vulnerabilidades de seguridad en una organización, para posteriormente, a través de un informe, revelar aquellos fallos de seguridad encontrados, mitigarlos a la brevedad posible y evitar fugas de información y ataques informáticos”. A aquellos que realizan las pruebas de intrusión o pentest se les denomina pentester (Rodríguez Llerena, 2020).

La labor de los pentester siempre está ligada a las necesidades y preocupaciones que pueda tener una entidad. Por ello, cada prueba de intrusión será diferente y su éxito dependerá de las habilidades y experiencias que tenga el profesional. Existen tres tipos de pentesting, los cuales están relacionados con la cantidad de información que se posea sobre la entidad a auditar y la manera en que se vayan a realizar las pruebas de intrusión (Rodríguez Llerena, 2020).

Caja blanca (White box): Es el más completo, debido a que parte de un análisis integral. Con este se evalúa toda la infraestructura de la red. El pentester tiene conocimiento sobre todos los aspectos de seguridad de la entidad (medidas, estructura de la red, contraseñas, etcétera) (Rodríguez Llerena, 2020).

Caja gris (Grey box): Es el más recomendado por los especialistas. A diferencia del anterior, el pentester no posee la información específica para realizar el test de penetración, por eso, requiere de tiempo y recursos para identificar la información necesaria acerca de las posibles vulnerabilidades existentes (Rodríguez Llerena, 2020).

Caja negra (Black box): En este caso no hay información sobre la entidad y se actúa de forma similar a un ciberdelincuente para tratar de reconocer fallos en la estructura de la red.

3.1.8 Conocimientos Indispensables para un Especialista en Seguridad Informática para el Pentesting

Un especialista en seguridad informática debe estar preparado como hacker ético para poder tener una mayor visibilidad y un total control sobre el sistema de la entidad. Es necesario que dicho especialista cuente con un título en Informática o afín, y tenga un conocimiento avanzado en redes (LAN, WAN), en los protocolos (TCP/IP-IPv4-IPv6), en sistemas operativos y servicios estándares empleados en casi todas las empresas (DNS, Ldap, Squid, mySql, FTP); todo ello para poder interpretar los datos que dan las herramientas empleadas en el escaneo de las vulnerabilidades y su explotación.

3.1.8.1 Linux. Se trata de un sistema operativo de 32 bits de libre distribución, desarrollado originalmente por Linus Torvalds, un estudiante de la universidad finlandesa de Helsinki, quien, en 1991, se abocó a la tarea de reemplazar a Minix, un clon de Unix de pequeñas proporciones y finalidad académica desarrollado años antes por Andrew Tannenbaun (Corbet, Rubini y Kroah-Hartman, 2005).

A medida que avanzaba en su desarrollo, Linus fue dejando el código fuente de las sucesivas versiones del kernel y utilidades de Linux a disponibilidad de los usuarios de Internet. Este fue sin duda un gran acierto, ya que hizo posible que una multitud de desarrolladores de todo el mundo se familiarizaran con el código, lo cual en primera instancia significó un gran aporte de sugerencias, evolucionado luego hacia un espectacular ejemplo de desarrollo distribuido de software: centenares de desarrolladores independientes, desde diferentes puntos del planeta tomaron a su cargo la producción de software para Linux, ya sea escribiéndolo desde cero o portándolo desde otras plataformas Unix. Esta modalidad de desarrollo continua aún hoy y ha permitido a Linux alcanzar un alto nivel de desarrollo y madurez, así también como un amplio grado de aceptación (Fernández, 2011).

3.1.8.1.1 ¿En qué se diferencia Linux de otros sistemas operativos? En muchos sentidos, Linux es similar a otros sistemas operativos que puede haber usado antes, como Windows, macOS (anteriormente OS X) o iOS. Como otros sistemas operativos, Linux tiene una interfaz gráfica y los mismos tipos de software a los que está acostumbrado, como procesadores de texto, editores de fotos, editores de video, etc. En muchos casos, el creador de un software puede haber creado una versión para Linux del mismo programa que usa en otros sistemas. En resumen: si puede usar una computadora u otro dispositivo electrónico, puede usar Linux (Wolf, 2015).

Pero Linux también se diferencia de otros sistemas operativos en muchos aspectos importantes. Primero, y quizás lo más importante, Linux es un software de código abierto. El código utilizado para crear Linux es gratuito y está disponible para que el público lo vea, edite y, para los usuarios con las habilidades adecuadas, para contribuir (Wolf, 2015).

Linux también es diferente en eso, aunque las piezas centrales del sistema operativo Linux son generalmente comunes, hay muchas distribuciones de Linux, que incluyen diferentes opciones de software. Esto significa que Linux es increíblemente personalizable, porque no solo se pueden cambiar las aplicaciones, como los procesadores de texto y los navegadores web. Los usuarios de Linux también pueden elegir componentes centrales, como qué sistema muestra gráficos y otros componentes de la interfaz de usuario (Wolf, 2015).

3.1.8.1.2 ¿Quién usa Linux? Probablemente ya uses Linux, lo sepas o no. Dependiendo de la encuesta de usuarios que mire, entre uno y dos tercios de las páginas web en Internet son generadas por servidores que ejecutan Linux (Pascuale Darío, 2004).

Las empresas y las personas eligen Linux para sus servidores porque es seguro, flexible y puede recibir un excelente soporte de una gran comunidad de usuarios, además de

empresas como Canonical, SUSE y Red Hat, cada una de las cuales ofrece soporte comercial.

Muchos dispositivos que probablemente posea, como teléfonos y tabletas Android y Chromebooks, dispositivos de almacenamiento digital, grabadoras de video personales, cámaras, dispositivos portátiles y más, también ejecutan Linux. Su automóvil tiene Linux funcionando bajo el capó. Incluso Microsoft Windows incluye componentes de Linux, como parte del Subsistema de *Windows* para Linux (*WSL*) (Pascuale Darío, 2004).

3.1.8.1.3 ¿Quién "posee" Linux? En virtud de su licencia de código abierto, Linux está disponible gratuitamente para cualquier persona. Sin embargo, la marca comercial del nombre “Linux” pertenece a su creador, Linus Torvalds. El código fuente de Linux está protegido por los derechos de autor de sus numerosos autores individuales y tiene la licencia GPLv2 (Kirch Olaf, 2000).

El término "Linux" técnicamente se refiere solo al kernel de Linux. La mayoría de la gente se refiere a todo el sistema operativo como "Linux" porque para la mayoría de los usuarios, un sistema operativo incluye un paquete de programas, herramientas y servicios (como un escritorio, un reloj, un menú de aplicaciones, etc.). Algunas personas, en particular los miembros de la Free Software Foundation , se refieren a esta colección como GNU / Linux, porque muchas de las herramientas vitales incluidas son componentes GNU. Sin embargo, no todas las instalaciones de Linux usan componentes GNU como parte del sistema operativo: Android , por ejemplo, usa un kernel de Linux pero depende muy poco de las herramientas GNU.

3.1.8.1.4 ¿Cuál es la diferencia entre Unix y Linux? Es posible que haya oído hablar de Unix, que es un sistema operativo desarrollado en la década de 1970 en Bell Labs por Ken Thompson, Dennis Ritchie y otros. Unix y Linux son similares en muchos aspectos y, de hecho, Linux fue creado originalmente para ser indistinguible de Unix. Ambos tienen herramientas similares para interactuar con el sistema, herramientas de programación,

diseños del sistema de archivos y otros componentes clave. Sin embargo, no todos los Unix son gratuitos y de código abierto. A lo largo de los años, se han creado varios sistemas operativos diferentes que intentaron ser "similares a Unix" o "compatibles con Unix", pero Linux ha sido el más exitoso, superando con creces a sus predecesores en popularidad (Fernández Moya, 1998).

3.1.9 Distribuciones de Linux Centradas en la Seguridad para el Hacking Ético y el Pentesting

DracOS Linux (Dragon Comodo OS) se creó sobre la base de LFS (linux desde cero) y se utiliza para realizar pruebas de seguridad con cientos de herramientas esenciales para cubrir pruebas de penetración, análisis forense e ingeniería inversa. Lo interesante de DracOS Linux es que este sistema operativo no tiene un entorno GUI, solo puede acceder a la herramienta mediante CLI (interfaz de línea de comandos). Bugtraq OS es otra distribución de Linux para pruebas de penetración basada en Debian o Ubuntu (Meller y Liberzon, 2016).

DEFT es la abreviatura de Digital Evidence & Forensics Toolkit, es una distribución de Linux hecha para análisis forense informático y respuesta a incidentes. DEFT Linux fue construido en base a Xubuntu, que usaba LXDE como entorno de escritorio. DEFT Linux se ejecuta en Live Mode, que una vez que inicia el sistema y comienza a usarlo. CAINE, abreviatura de Computer Aided Investigative Environment es otra distribución de Linux Live para análisis forense digital. CAINE se creó en base a Ubuntu y utilizó el entorno de escritorio MATE y LightDM. CAINE está repleto de herramientas para ayudar al investigador o auditor de TI a encontrar puntos de datos y pistas que se necesitan para el análisis forense de seguridad informática. (Meller y Liberzon, 2016).

Network Security Toolkit es una distribución de Linux basada en Fedora Live-CD diseñada para seguridad de red y pruebas de penetración de red. NST tiene como objetivo el diagnóstico de redes y la supervisión de servidores. NST incluye un arsenal de herramientas de seguridad de red, a las que se puede acceder a la mayoría de las

tareas a través de la interfaz de usuario web (WUI). BackBox Linux es una distribución de Linux basada en Ubuntu para realizar pruebas de penetración y evaluación de seguridad. BackBox ofrece estabilidad y rapidez, está configurado con el entorno de escritorio XFCE. La idea del diseño era el mínimo consumo de recursos y maximizar el rendimiento.

BackBox Linux cargado con herramientas de análisis y seguridad conocidas cubre una amplia gama de temas, evaluación de seguridad de aplicaciones web, análisis de redes y análisis forense informático. Backbox Linux tiene herramientas muy bien organizadas, que evitan herramientas de funcionalidad redundantes y similares BlackArch Linux es otra distribución de pruebas de penetración de Linux basada en Arch Linux. Las interesantes entre las herramientas de BlackArch es que hay aplicaciones integradas para el análisis de seguridad de drones, como Snoppy, Skyjack y Mission Planner (Meller y Liberzon, 2016).

Parrot Security OS es un sistema operativo forense y de pruebas de penetración basado en Debian. Lo interesante de ParrotSec OS es que tiene un modo anónimo. Al activar el modo anónimo, ParrotSec enrutará automáticamente todo el tráfico a través de TOR. ParrotSec proporciona una amplia gama de herramientas de pentesting, análisis forense digital, ingeniería inversa y herramientas de generación de informes. ParrotSec también se envió con herramientas destinadas a realizar criptografía y programación (Meller y Liberzon, 2016).

Finalmente, además de la mejor distribución de Linux para pruebas de penetración está Kali Linux, la cual es una distribución de Linux basada en Debian para auditorías de seguridad y principalmente para pruebas de penetración. Esta su vez está destinada para ser utilizada en tareas relacionadas con la seguridad. Kali Linux viene con una gran cantidad de herramientas de prueba de penetración de varios campos y herramientas de análisis forense digital. Kali Linux es compatible con una amplia gama de dispositivos, incluidos i386, amd64 y la plataforma ARM (Ramadhan y Putra, 2018).

3.1.10 Kali Linux

Kali es una distribución de Linux basada en Debian, diseñada para la auditoría de seguridad, los tests de intrusión y la informática forense, por tanto, se puede hacer todo como se realice en este sistema operativo. La instalación de paquetes es la misma, y la configuración es análoga. Los documentos y la información que se puede encontrar en Internet sobre Debian nos valen para Kali (Hertzog, O'Gorman y Aharoni, 2017).

Kali está mantenida por una empresa –Offensive Security Ltd.–. Utiliza paquetes GPL, por lo que el código fuente está disponible. Su desarrollo está muy focalizado en un grupo pequeño de desarrolladores de confianza, que firman los paquetes con GPG para evitar troyanos en la distribución. Kali incluye más de 600 aplicaciones para auditoría de seguridad e informática forense; incluyendo escáneres de puertos –como NMAP–, *sniffers* – como *Wireshark*–, suites de crackeo Wifi –como *Aircrackng*–, suites para construir troyanos y *exploits* –como *Metasploit*–, o programas para descubrir claves –como *John the Ripper*–. Incluye también un modo forense de arranque, en el que el disco duro no se utiliza en absoluto: aunque encuentre una partición swap no se usa ni se monta, no se monta ninguna partición del disco, y se desactiva el automontado. Tampoco levanta de forma automática las tarjetas de red. Kali utilizado desde un llavero USB o desde un CD es una herramienta forense excepcional (Hertzog, O'Gorman y Aharoni, 2017).

Antes de entrar en cómo utilizar Kali linux para realizar un test de intrusión, se recomienda que esta prueba de intrusión no solicitado o autorizado se constituye como delito. Un test de intrusión, test de penetración, o penetration test, o pentest, es un procedimiento de auditoría de seguridad activa en el que, con autorización del propietario de un sistema de información, el auditor de seguridad analiza el susodicho sistema buscando de forma proactiva agujeros de seguridad vulnerables.

El test de intrusión puede terminar al encontrar una vulnerabilidad, aunque solo sea explotable teóricamente; puede precisar el desarrollo de una prueba de concepto para

validar que la vulnerabilidad encontrada es explotada, o puede incluso llegar a requerir que se demuestre la vulneración llegando a explotar la vulnerabilidad. El test de intrusión no está enfocado a una máquina, sino a un sistema de información concreto.

Esto involucra los servidores, los ordenadores de sobremesa y el software de sistemas. Pero -y esto se olvida con frecuencia-, involucra también al personal, a las mecánicas y los procedimientos de la empresa, y a la gestión de la información en su sentido más amplio. Esto quiere decir que un test de intrusión puede ser realmente realizado mediante técnicas de ingeniería social, o mediante cualquier otra técnica que no sea necesariamente tecnológica.

A diferencia de los escaneos automatizados, que son indiscriminados, el test de intrusión requiere un análisis previo de los sistemas de información de un cliente. Esto supone que es muy importante recoger información del cliente, analizarla, y antes de comenzar a trabajar ya tener una idea clara de las vulnerabilidades. Los tests de intrusión son especialmente útiles si se realizan después de una auditoría de seguridad de la familia de normas ISO/IEC 27000; ya que, al terminarla, el auditor tiene una idea muy clara de cómo funciona un sistema, de dónde están sus vulnerabilidades, y aunque estrictamente hablando se haya pasado la norma ISO/IEC 27001, el auditor puede deducir a partir de la información extraída cómo atacaría el sistema, y hasta dónde podría llegar en caso de proceder al ataque. El test de intrusión, en este escenario, no dejaría de ser la validación empírica de lo encontrado después de una auditoría previa de seguridad (Armendáriz López, 2017).

Es importante recordar que la familia de normas ISO/IEC 27000 se centra en procedimientos: se puede tener un sistema que pase la ISO/IEC 27001 y que tenga vulnerabilidades que sean verificables a través de tests de intrusión; igualmente se puede tener un sistema que, sin pasar la ISO/IEC 27001, no tenga vulnerabilidades. Son, pues, análisis complementarios que se pueden realizar en el mismo pedido del cliente; en cuyo caso es recomendable realizar primero la auditoría completa ISO/IEC 27001:

desaparecerán las vulnerabilidades de proceso, y se obtiene mucha información que permite al auditor ir directamente por las vulneraciones de software, servidores y redes (Armendáriz López, 2017).

Cabe destacar que un test de intrusión es un tema que legalmente es delicado, y es fácil realizar actos delictivos de buena fe. Hay que tener en cuenta que, a diferencia de una auditoría de seguridad común en la que se valida el cumplimiento de una norma a partir de pruebas documentales y de la observación directa con el beneplácito y delante del observado, un test de intrusión no deja de ser una validación de la seguridad a partir de la ruptura de esta. Y las rupturas de la seguridad en sistemas informáticos son de entrada ilegales en nuestro ordenamiento jurídico. Aunque algunos lo puedan considerar como "emocionante", realizar tests de intrusión es legalmente delicado, y en muchos casos es ilegal hasta con la aprobación expresa y explícita de la propiedad. Cuando se habla de "propiedad", se hace referencia al dueño de la empresa, persona o personas con el nivel máximo ejecutivo (Armendáriz López, 2017).

Se debe tener mucho cuidado y estar atento que la persona que contrate el servicio pueda legalmente autorizar la realización de la intrusión: ya que se puede dar el caso que quien contrate, aunque oficialmente sea el "director de sistemas", no tenga autorización real para permitir una intrusión. También se debe tener en cuenta que por mucho que el propietario autorice la intervención en su sistema de información, eso no significa que sea legal: por ejemplo, no se puede leer correos electrónicos o intervenir comunicaciones. En el caso de sistemas tipo *cloud* o en los que se haya alquilado una máquina virtual o una máquina física a un proveedor, es posible que muchas de las cosas que se puedan hacer no supongan intromisión en los sistemas del cliente, sino en los del proveedor, lo que podría constituirse como delito. Además, algunas operaciones concretas de la mecánica de los tests de intrusión pueden ser delictivas en algunas jurisdicciones legales.

Aunque el planteamiento de las fases es lineal, es importante tener claro que en cualquier momento se puede volver a fases anteriores. Por ejemplo, al redactar el alcance y las

condiciones del test de intrusión podría descubrirse que realmente se tienen que hacer cosas distintas de las presupuestadas, y ajustar el presupuesto acorde a ello. Al realizar las validaciones legales, puede que se tenga que reducir el alcance o alterar las condiciones de los tests de intrusión, lo que probablemente cambie los permisos que se necesitan. Al recoger la información se puede descubrir cosas del sistema que se desconocían – especialmente si no se ha auditado el sistema respecto a la norma con anterioridad–, lo que obliga a analizar la legalidad de hacer *pentesting* sobre lo descubierto, cambiar el alcance y las condiciones del test, y probablemente pedir nuevos permisos. Al analizar las vulnerabilidades se puede obtener información nueva que nos obligue a rehacer pasos anteriores, y al explotar las vulnerabilidades logra encontrar otras nuevas que requieran análisis y los pasos anteriores.

Finalmente, al presentar los resultados al propietario esta nos puede solicitar ampliar el ámbito inicialmente contratado, y al capacitar a los trabajadores se logra detectar asuntos que requieran ser comunicados al propietario. Se debe interpretar, por lo tanto, las fases principalmente en el contexto de que unas cosas van antes que otras, y que todas las fases deben cubrirse. Habitualmente, algunas fases más de una vez (Santo Orcero, 2018).

3.1.10.1 ¿Debería usar Kali Linux? Kali Linux está específicamente diseñado para cumplir con los requisitos de las pruebas de *pentesting* profesionales y la auditoría de seguridad. Para lograr esto, se han implementado varios cambios centrales en Kali Linux que reflejan estas necesidades: Servicios de red deshabilitados de forma predeterminada: Kali Linux contiene enlaces *systemd* que deshabilitan los servicios de red de forma predeterminada (Santo Orcero, 2018).

Un conjunto mínimo y confiable de repositorios: dados los objetivos y metas de Kali Linux, mantener la integridad del sistema como un todo es absolutamente clave. Con ese objetivo en mente, el conjunto de fuentes de software ascendentes que utiliza Kali se mantiene al mínimo absoluto . Muchos usuarios nuevos de Kali se ven tentados a

agregar repositorios adicionales a su *sources. list*, pero hacerlo corre un riesgo muy serio de romper su instalación de Kali Linux (Santo Orcero, 2018).

3.1.11¿Es el sistema operativo Kali Linux el más apropiado para ser utilizado como usuario?

Es de esperar que se recomiende que utilicen Kali Linux. Sin embargo, el hecho es que Kali es una distribución de Linux dirigida específicamente a probadores de *pentesting* profesionales y especialistas en seguridad, y dada su naturaleza única, NO es una distribución recomendada si no está familiarizado con Linux o está buscando una distribución general. -Distribución de escritorio Linux de propósito para desarrollo, diseño web, juegos, etc. Incluso para los usuarios experimentados de Linux, Kali puede presentar algunos desafíos. Aunque Kali es un proyecto de código abierto, que no es un gran proyecto de código-abierto, por razones de seguridad. El equipo de desarrollo es pequeño y confiable, los paquetes en los repositorios están firmados tanto por el responsable individual como por el equipo y, lo que es más importante, el conjunto de repositorios ascendentes de los que se obtienen las actualizaciones y los nuevos paquetes es muy pequeño. Agregar repositorios a sus fuentes de software que no hayan sido probados por el equipo de desarrollo de Kali Linux es una buena manera de causar problemas en su sistema.

Si bien Kali Linux está diseñado para ser altamente personalizable , no espere poder agregar paquetes y repositorios aleatorios no relacionados que estén "fuera de banda" de las fuentes de software regulares de Kali y que funcionen.

En particular, no hay absolutamente ningún soporte para el comando *apt-add-repository, LaunchPad* o *PPA*. Intentar instalar *Steam* en tu escritorio Kali Linux es un experimento que no terminará bien. Incluso conseguir un paquete tan común como *NodeJS* en una instalación de Kali Linux puede requerir un poco de esfuerzo y retoques adicionales. Si no está familiarizado con Linux en general, si no tiene al menos un nivel básico de competencia en la administración de un sistema, si está buscando una distribución de

Linux para usar como herramienta de aprendizaje para familiarizarse con Linux, o si desea una distribución que pueda usar como una instalación de escritorio de propósito general, Kali Linux probablemente no sea lo que está buscando.

Además, el uso indebido de las herramientas de prueba de seguridad y penetración dentro de una red, particularmente sin una autorización específica, puede causar daños irreparables y tener consecuencias personales y / o legales importantes. "No entender lo que estaba haciendo" no funcionará como excusa. Sin embargo, si es un probador de *pentesting* profesional o está estudiando pruebas de intrusión con el objetivo de convertirse en un profesional certificado, no hay mejor conjunto de herramientas, a cualquier precio, que Kali Linux (Blanco Esquerra, 2014).

3.2 MARCO CONCEPTUAL

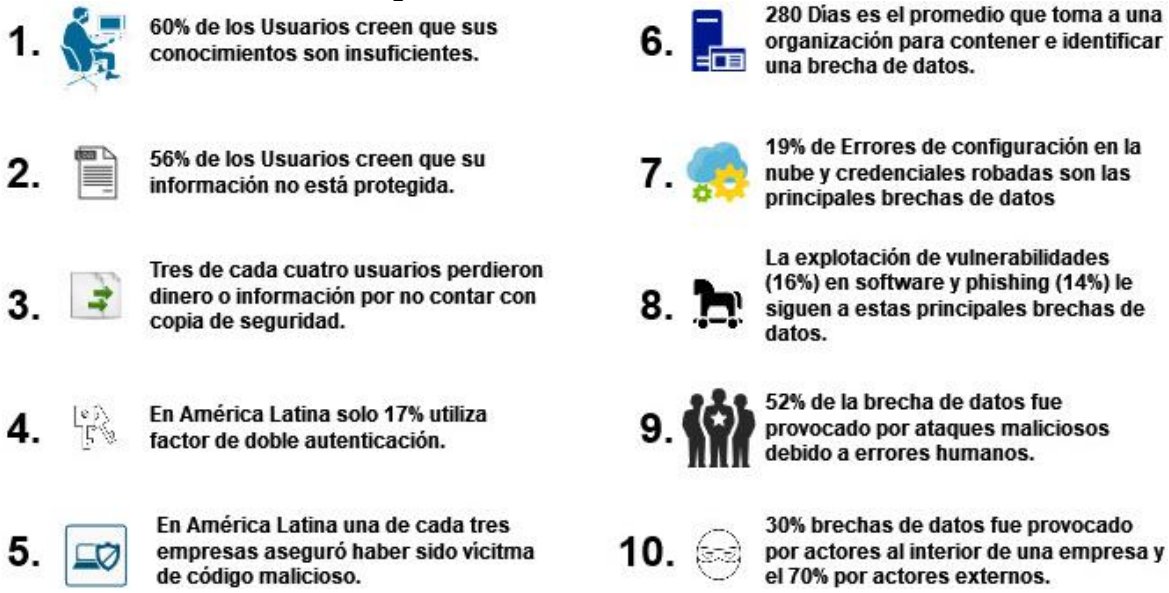
Según el autor Álvaro Gómez Vieites en su libro Seguridad Informática Básico se puede definir la seguridad informática como cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan conllevar daños sobre la información, comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios autorizados al sistema (Gómez Vieites, 2011). Según Kaspersky y Furnell (2014), la ciberseguridad es la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos.

También se conoce como seguridad de tecnología de la información o seguridad de la información electrónica. Por otra parte, la auditoría informática es el proceso metodológico ejecutado por especialistas del área de auditoría y de informática. Está orientada a la verificación y aseguramiento de que las políticas y procedimientos establecidos para el manejo y uso adecuado de la tecnología de la información, se lleven a cabo de manera oportuna y eficiente (Fernández Arcentales y Casas Caycedo, 2017).

3.3 ANTECEDENTES O ESTADO ACTUAL

En su artículo: Diez datos sobre el estado de la ciberseguridad tras la pandemia de la Revista Semana (2020) la firma de seguridad informática ESET, compañía especializada en detección de amenazas informáticas, publicó un informe sobre la aceleración que tuvo el uso de la tecnología durante la pandemia del coronavirus, lo que generó cambios en los hábitos de los usuarios e incidencias en el accionar de los cibercriminales en Latinoamérica. Dinero expone 10 de los principales datos publicados por ESET en el marco de un escenario tecnológico atípico por cuenta de la coyuntura sanitaria y económica.

Figura 1 Diez datos sobre ciberseguridad



Fuente Revista Semana (2020).

Por otra parte, Estrada García Carlos Román, en su trabajo de grado: Análisis y pruebas de las herramientas de hacking ético incluidas en el sistema operativo Kali Linux, implementado en un *Raspberry* Pi 3, aplicadas en la empresa Fishcorp S.A., concluyen que los futuros profesionales en seguridad informática y sus auditores deben estar en constante actualización de manejo y uso de técnicas para contrarrestar las medidas que utilizan los ciberdelincuentes, además, utilizan el sistema operativo Kali Linux como

herramienta fundamental para la prueba de auditoría ejecutada en el presente proyecto de grado; también, en su desarrollo resaltan la importancia de implementar políticas de seguridad informática que permiten proteger sus activos informáticos (Estrada García, 2018).

Ochoa Guevara (2018), en su trabajo de grado titulado: Estudio de seguridad en las bases de datos, mediante metodologías de pen test, Ethical Hacking en la secretaria de hacienda municipal de Los Patios, menciona las carencias con los procesos de integridad y confidencialidad de la información de la entidad pública, razón por la cual se pueden ver afectadas las bases de datos, además para su desarrollo ejecuta la herramienta NMAP que se encuentra inmerso en el sistema operativo Kali Linux, recomienda además la virtualización para ejecutar pruebas de funcionamiento detectando puertos abiertos y establecer un sistema de control de usuarios a los sistemas de información, entre otras mejoras está el mantenimiento a la base de datos y un sistema antivirus en las estaciones de los usuarios.

Castro Maturana Yeimar Alonso en su trabajo de grado titulado: Seguridad informática en el sistema operativo Linux en sus diversas distribuciones aplicadas a las tecnologías de la información, concluye que la gran cantidad de sistemas operativos Linux sirven para llevar a cabo multitareas, su gran ventaja siendo *opensource* y ahorro para las empresas en la adquisición de software comercial, esto contando con las comunidades que están actualizando las diferentes versiones y en cuanto a la documentación si describe que es más bien difícil puesto que esta se rige por sus páginas centrales. Además, menciona a la distribución Kali Linux como parte fundamental para la construcción de su monografía y enfocada está a la seguridad o *Pentesting* (Castro Maturana, 1992).

Contreras Flórez (2017), en su trabajo de grado titulado: propuesta de auditoría a las aplicaciones web de la empresa C&M consultores aplicando herramientas de software libre, resalta que las empresas aún ven el proceso de seguridad informática como un costo y no como un valor agregado que redundará en la protección de sus activos de

información y por sobre todo la confianza con sus clientes, también, la importancia de los controles de acceso tanto a las instalaciones físicas y a su información esto para evitar la posible pérdida o fuga de información y comprometer los datos de la compañía, la importancia de las diferentes herramientas de seguridad informática para la detección de vulnerabilidades que son *opensource*, igualmente recomienda la inclusión de mecanismos de seguridad físicos y el desarrollo de políticas de seguridad para mitigar vulnerabilidades.

3.4 MARCO LEGAL

De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas de informáticos. En cuanto a la legislación actual y presente para el problema descrito se encuentra: la Ley 1273 de 2009 Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones, la Ley 1581 sobre el cual se dictan disposiciones generales para la protección de datos personales.

Por consiguiente y teniendo en cuenta que el Congreso de la República de Colombia (2009) en la Ley 1273 de 2009 los actos delictivos cometidos se registran a continuación:

Artículo 269A: Acceso abusivo a un sistema informático: donde se hace mención al acceso abusivo a un sistema informático porque se accede a los cajeros automáticos propiedad del banco y además se sustrae dinero de los ahorradores

Artículo 269D: Daño informático, alteraron el funcionamiento de los cajeros y borraron el rastro de las transacciones realizadas.

Artículo 269E: Uso de software malicioso: instalación de malware en los sistemas operativos de los cajeros.

Artículo 269F: Violación de datos personales, porque a través del malware instalado se obtiene las claves de acceso de los usuarios que están en las bases de datos.

Artículo 269H: Circunstancias de agravación punitiva: se realiza sobre redes y sistemas informáticos del sector financiero nacional y además la comete un funcionario de confianza que posee la información de clientes, obteniendo provecho para sí y para terceros, del banco donde trabaja.

En este caso el actuar delictivo de un expolicía en el cual se depositó la total confianza para ejercer dicha labor de seguridad informática en el banco, violando además el contrato laboral en el que se le exige confidencialidad y buen desempeño laboral acompañado de la ética profesional en el ejercicio de sus labores.

Articulo 269I: Hurto por medios informáticos y semejantes: porque viola medidas de seguridad a sistemas electrónicos y además suplanta a usuarios en los sistemas.

Artículo 269J: Transferencia no consentida de activos: porque con lucro y manipulación informática consigue obtener el dinero de los cajeros automáticos ubicados en varias ciudades del país.

De otro lado, y de acuerdo al Congreso de la República (2012) en la Ley 1581 de 2012, por el cual se dictan disposiciones generales para la protección de datos personales, se debe tener en cuenta puesto que existen disposiciones legales que han expuesto datos personales de clientes afectando el buen nombre de la entidad y por consiguiente la pérdida de credibilidad y confianza hacia el banco.

En esta parte se realiza mención en los Títulos: II – Principios Rectores, incisos c) y g).

c) Donde se hace mención al Principio de Libertad donde los datos personales no podrán ser obtenidos o divulgados sin previa autorización o en ausencia de mandato legal que revele el consentimiento.

g) Principio de seguridad: la información se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

Título VI – Deberes de los responsables del tratamiento y encargados del tratamiento, Artículo 17. Deberes de los responsables del tratamiento, inciso d), i), n).

d) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

i) Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular.

n) Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.

Artículo 18. Deberes de 'los Encargados del Tratamiento. Incisos b) y k)
b) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

k) Informar a la Superintendencia de Industria y Comercio cuando se l presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.

Ya en su capítulo 2, donde se refiere a los procedimientos y sanciones, en su artículo 23. Sanciones. La superintendencia de Industria y Comercio podrá imponer a los responsables del tratamiento y encargados del tratamiento las sanciones correspondientes en cuanto a multas de carácter personal e institucional, suspensión de las actividades, cierre temporal de las operaciones y cierre definitivo de la operación que involucre el tratamiento de datos sensibles.

4. HERRAMIENTAS UTILIZADAS PARA REALIZAR PRUEBAS DE INTRUSIÓN DEL SISTEMA OPERATIVO KALI LINUX

El sistema operativo Kali Linux ha ganado ventaja en relación a otros puesto que es el más adecuado y utilizado por los profesionales en seguridad informática para llevar a cabo los procesos de test de intrusión, aunque muchos de ellos y gran parte lleva la ventaja Linux como sistema operativo para ejecutar las herramientas de auditoría informática, no se puede dejar a un lado el sistema operativo Microsoft Windows, en el que también se pueden ejecutar estas herramientas y que inclusive su soporte por ser más de tipo comercial requiere de un pago, es por esto que los *pentester* recurren a las herramientas *open source* que además también cuentan con foros, grupos, capacitaciones y formación *on-line* y por supuesto las certificaciones que avalan como un experto en seguridad informática.

Por otra parte, la academia ha ganado gran importancia y hoy en día se encuentran muchas instituciones que son las líderes en certificaciones de gran importancia como CEH (*Certified Ethical Hacker*), *Computer Hacking Forensic Investigator* (CHFI), solo por mencionar algunas de ellas puesto que existen otras de mucha relevancia y que en la hoja de vida de un profesional en seguridad informática da un valor agregado y genera solidez y por sobre todo confianza puesto que lo acredita como una persona idónea, capacitada con sentido de ética profesional que actuará bajo la ley, con responsabilidad y compromiso para llevar a cabo las labores que se le encomiendan y que una vez finalizadas informará a través de un documento utilizando un lenguaje técnico y entendible para los que tengan acceso a estos reportes técnicos.

Las academias o instituciones educativas que son *partners* de estas empresas que certifican al profesional tienen en sus programas el entrenamiento y uso más práctico de ciertas herramientas para la ejecución de auditorías informáticas siendo una de las más utilizadas y más común para los *pentesters* como es *nmap* que es la herramienta líder

ideal para todo aquel que desee iniciarse en seguridad informática que viene instalada en el sistema operativo Kali Linux; igualmente, y como parte de los procesos de auditoría se puede mencionar a *Metasploit framework* por su facilidad de implementación y relación con otras herramientas como *nmap*.

También, es preciso mencionar las herramientas de criptografía, como ejemplo se puede citar a la consola del antivirus Kaspersky Total Security for Business, en la cual tiene en uno de sus módulos la implementación de cifrado para ejecutarse a un disco duro completo, carpetas y/o archivos, unidades extraíbles y que sirven para que la información contenida en estos medios no se vea comprometida su integridad; estos procesos de cifrado de la información que son ejecutadas en muchas entidades públicas y privadas protegen la información sensible y evitan en lo posible la fuga de información.

Por otro lado, están los llamados equipos de ciberseguridad *blue* y *red team*, mientras que el *blue team* son los encargados de establecer las defensas y protegerse de los ataques, es este equipo en el que entre sus tareas de respuesta está el análisis forense, analizar fallos de seguridad entre otros; además de este grupo están el *red team* que es el que ejecuta los ataques y es personal que puede ser externo a la empresa, este grupo es el encargado de probar la eficacia del programa de seguridad que tiene la empresa.

A continuación se realiza un breve resumen de las cuatro grandes fases de un ciclo de test de intrusión: Reconocimiento, Escaneo, Explotación y *Post-explotación*, dichas técnicas son muy utilizadas dentro del ámbito del sistema operativo Linux: William Khepri en sus artículos citados en la página web: Las 25 mejores herramientas de Kali Linux parte I y II, informa sobre las herramientas que se pueden ejecutar en el sistema operativo Kali Linux y llama a este como la “navaja Suiza” de los *pentester*, coincide además con Sebastián Bortnik en donde menciona las cinco herramientas para principiantes para realizar test de intrusión con Kali Linux, estos artículos guardan similitud en la selección de ciertas herramientas entre las que se pueden mencionar: *nmap, metasploit framework*, solo por mencionar estas dos puesto que para cualquier principiante o inclusive en niveles

más avanzados se debe adquirir conocimiento, destreza y habilidad para ejecutar un test de intrusión que todo profesional en ciberseguridad debe realizar en algún momento y que es preciso que el conocimiento y recomendación de estas herramientas se debe poseer.

Por otra parte, y referenciado la tesis del estudiante Álvarez Támara Ricardo Enrique, en la que crea un Manual de guía para el aprendizaje de Linux, se recalca la importancia de este sistema operativo para iniciarse como profesional en ciberseguridad y el cual es fundamental puesto que la mayoría de herramientas se ejecutan bajo este sistema operativo y son *open source*, aquí cabe recalcar que es necesario adquirir destrezas y habilidades para el manejo de Linux puesto que Kali como tal es un sistema que no es para instalarlo tanto a un PC de escritorio o portátil y que para la estación de usuario resultaría muy incómodo y poco agradable su labor, pero sí de gran valor y ayuda para aquel que se está iniciando en ciberseguridad y que actualmente es muy utilizada y ofrece un sinnúmero de herramientas con gran complemento de foros, cursos, videos para su respectiva ejecución.

También, en esta parte se coincide con la tesis de Almeida Coloma Cesar Leonardo y Pincay Párraga Jasson Alfredo en la implementación de un laboratorio de seguridad de informática para la realización de técnicas de ataque y defensa (pentesting) en un ambiente real controlado, utilizando una distribución de Kali Linux y el informe técnico de Nomesque Patiño Ana Delcy en su socialización: Capacidades técnicas, legales y de gestión para equipos Blue Team y Red Team, puesto que se sigue con la metodología y utilización de Kali Linux como sistema operativo líder, recomendado, de gran ayuda para realizar pruebas de intrusión y descubrir las vulnerabilidades de las organizaciones para posteriormente entregar un informe técnico y dar las respectivas soluciones; en estos trabajos se menciona la implementación en un ambiente controlado instalando como máquina virtual el sistema operativo Kali Linux y desde allí ejecutar el test de intrusión; citando además la tesis de Alex Daniel Vinueza Gualotuña en la Elaboración de Guías de prácticas de laboratorio para la asignatura seguridad de redes empleando Kali Linux,

se puede dar a conocer que como tal es el sistema operativo líder para los profesionales en seguridad informática y que además de poseer un sinnúmero de herramientas para detectar las vulnerabilidades presentes en una empresa, se puede conocer que al implementar sistemas estos en ocasiones se configuran sin precaución en el manejo de contraseñas o permisos a usuarios y que pueden ocasionar grandes riesgos para la organización.

Finalmente, y citando la página oficial de Kali Linux, en ella se puede encontrar desde la respectiva documentación, descarga de versiones a plataformas como vmware o virtualbox, live CD o USB, entre otros, pasando por el soporte de la comunidad y foros que involucran temas para principiantes hasta temas avanzados y por supuesto cursos que acreditarán y certificarán al profesional en seguridad informática en las habilidades, destrezas y manejo de este sistema operativo de gran popularidad para la ciberseguridad.

4.1 CASOS DE ÉXITO SOBRE AUDITORÍAS QUE HAGAN USO DE HERRAMIENTAS ESPECIALIZADAS IMPLÍCITAS EN KALI LINUX

Mujahid Tabassum, Saju Mohanan, Tripti Sharma, en su publicación: Ethical Hacking and Penetrate Testing using Kali and Metasploit Framework resalta la importancia de que los usuarios utilicen el filtrado en sus correos electrónicos para evitar el phishing, el deshabilitar páginas o sitios web falsos para que no se acceda a ellos y que los usuarios finales realicen el cambio periódico de contraseñas como un mecanismo seguro, resalta la importancia de que el personal de la empresa debe educarse para que estos conozcan los diferentes ataques a los que puede enfrentarse una organización y las restricciones que estos deben tener a la red corporativa. También, la configuración y administración del firewall para bloquear la IP de origen cuando se detecta un tráfico inadecuado a la red, estos deben cumplir las reglas de filtrado y evitar fuentes peligrosas, las empresas deben vigilar constantemente sus sistemas para evitar la pérdida de datos y se vea comprometida su buen nombre.

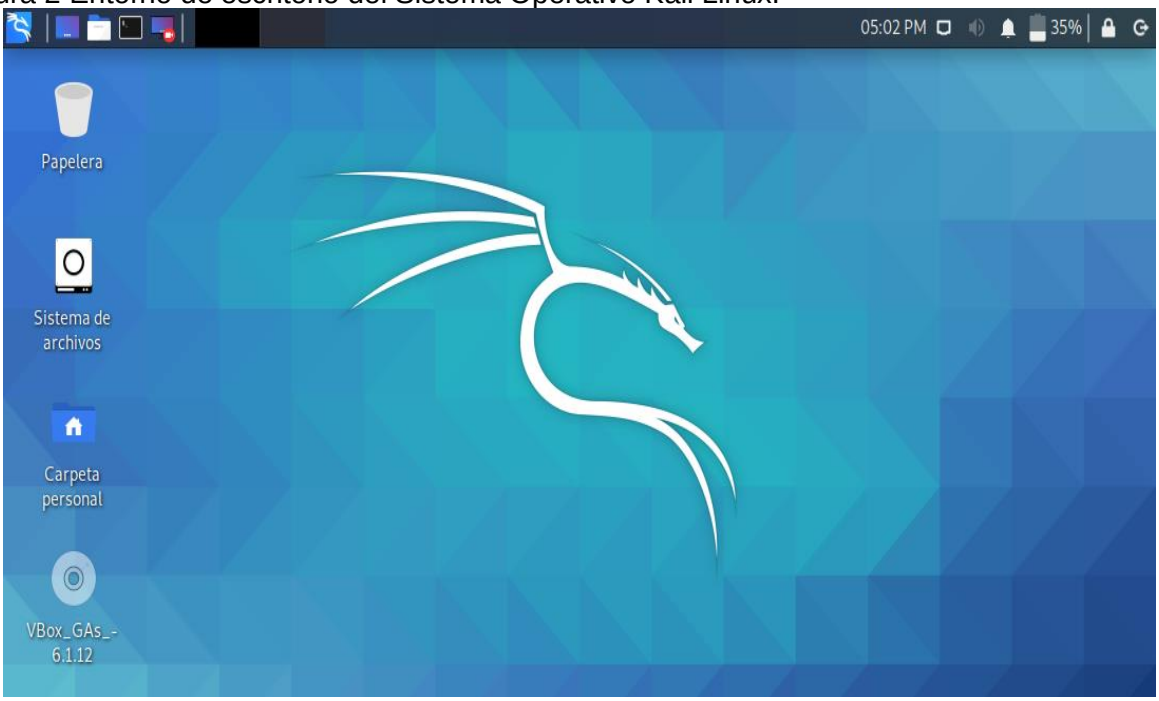
Entre los estudios ejecutados en trabajos de grado se puede mencionar a: Bravo Indacochea y Barrera Landires Fernando Aarón, que tiene como título: auditoría de seguridad informática en la red de datos de una empresa utilizando como mecanismo de hacking ético el sistema operativo kali linux previo a la propuesta de implementación del *firewall pfsense* y correlacionador de eventos *siem*, en el presente proyecto las herramientas utilizadas para su respectiva ejecución se utilizaron *nmap, foca, maltego, dmitry, ping, tracerouter* y *nslookup* el cual ayudaron a detectar vulnerabilidades y emitir recomendaciones para la respectiva protección de los activos de información.

Además de esto, es importante mencionar la ejecución a su infraestructura tecnológica en la que se aplicaron pruebas de *ethical hacking* para detectar vulnerabilidades, servicios desactualizados y con las respectivas configuraciones en las políticas de seguridad se logra corregir situaciones por medio de su firewall para proteger su infraestructura de las amenazas que pueden ocasionar daños a su red empresarial con la consecución de su pérdida de información sensible; además, recomiendan seguir efectuando auditorías de seguridad informática para que en ellas se detecten las posibles vulnerabilidades, riesgos y amenazas que puedan afectar a la organización y más específicamente a su infraestructura tecnológica. También, están las políticas de seguridad informática con su respectivo firewall que a través de una buena administración permite que los usuarios autorizados accedan con ciertos permisos a los datos de la organización.

5. PRUEBA DE CONCEPTO PARA CADA UNA DE LAS HERRAMIENTAS UTILIZADAS

En la Figura 2. Se puede visualizar el entorno de escritorio del sistema operativo Kali Linux.

Figura 2 Entorno de escritorio del Sistema Operativo Kali Linux.



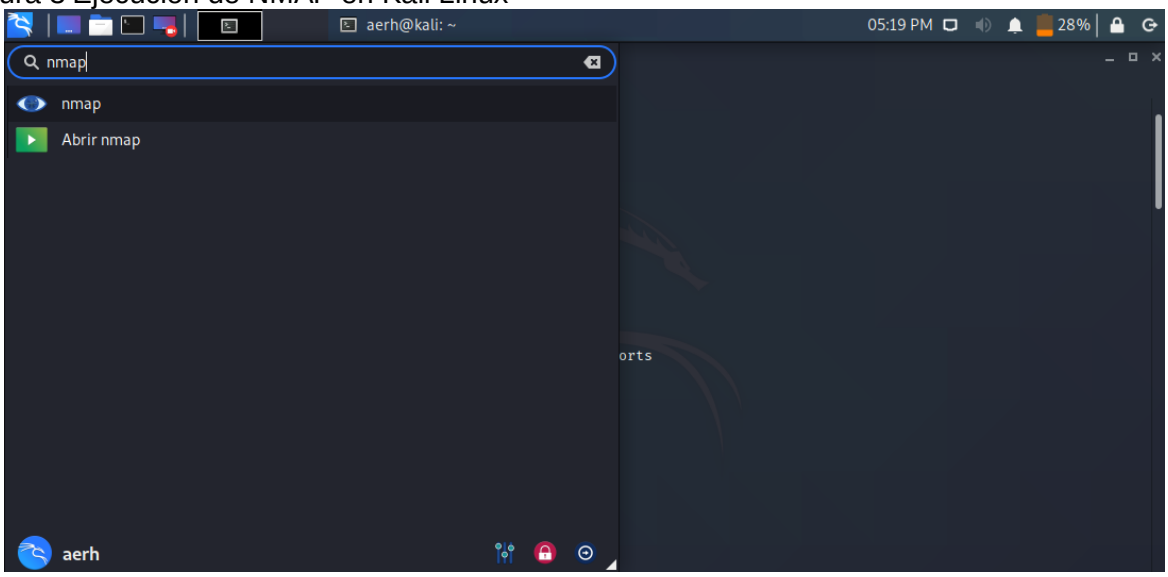
Fuente Arturo Ruiz

Se categorizan las siguientes herramientas:

5.1 NMAP

En la Figura 3. Se puede visualizar la búsqueda y ejecución del programa nmap.

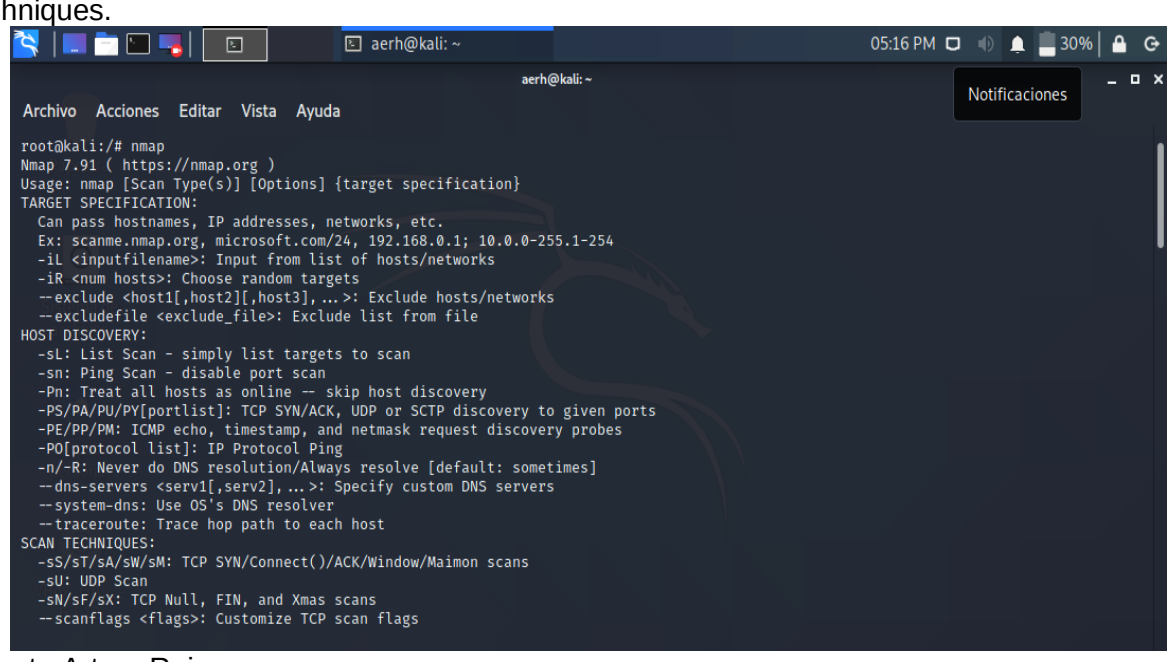
Figura 3 Ejecución de NMAP en Kali Linux



Fuente Arturo Ruiz

En la Figura 4. Se puede visualizar en la terminal la ejecución del comando *nmap* con su *target specification*, *host Discovery* y *scan techniques*.

Figura 4 Ejecución del comando nmap con su target specification, host Discovery y scan techniques.



Fuente Arturo Ruiz

5.1.1 Características

Flexible: Admite docenas de técnicas avanzadas para trazar redes llenas de filtros IP, cortafuegos, enrutadores y otros obstáculos. Esto incluye muchos mecanismos de escaneo de puertos (tanto TCP como UDP), detección de SO , detección de versiones , barridos de ping y más. Consulte la página de documentación (Lyon, 2008).

Potente: NMAP se ha utilizado para escanear enormes redes de literalmente cientos de miles de máquinas (Lyon, 2008).

Portátil: la mayoría de los sistemas operativos son compatibles, incluidos Linux, Microsoft Windows, FreeBSD, OpenBSD, Solaris, IRIX, Mac OS X, HP-UX, NetBSD, Sun OS, Amiga y más (Lyon, 2008).

Fácil: si bien NMAP ofrece un amplio conjunto de funciones avanzadas para usuarios avanzados, puede comenzar tan simplemente como "NMAP -v -A *aimthost* ". Tanto la línea de comandos tradicional como las versiones gráficas (GUI) están disponibles para adaptarse a sus preferencias. Los binarios están disponibles para aquellos que no deseen compilar NMAP desde la fuente (Lyon, 2008).

Gratis: El objetivo principal del Proyecto NMAP es ayudar a que Internet sea un poco más seguro y proporcionar a los administradores / auditores / piratas informáticos una herramienta avanzada para explorar sus redes. NMAP está disponible para descarga gratuita y también viene con el código fuente completo que puede modificar y redistribuir según los términos de la licencia (Lyon, 2008).

Bien documentado: Se ha realizado un esfuerzo significativo en páginas de manual completas y actualizadas, documentos técnicos, tutoriales e incluso un libro completo. Encuéntrelos en varios idiomas aquí (Lyon, 2008).

Compatible: Si bien NMAP no tiene garantía, está bien respaldado por una vibrante comunidad de desarrolladores y usuarios. La mayor parte de esta interacción ocurre en las LISTAS DE CORREO DE NMAP . La mayoría de los informes de errores y las preguntas deben enviarse a la lista NMAP-dev , pero solo después de leer las pautas. Se recomienda que todos los usuarios se suscriban a la lista de anuncios de NMAP-HACKERS DE bajo tráfico. También puede encontrar NMAP en Facebook y Twitter . Para chatear en tiempo real, únase al canal #nmap en Freenode o EFNet (Lyon, 2008).

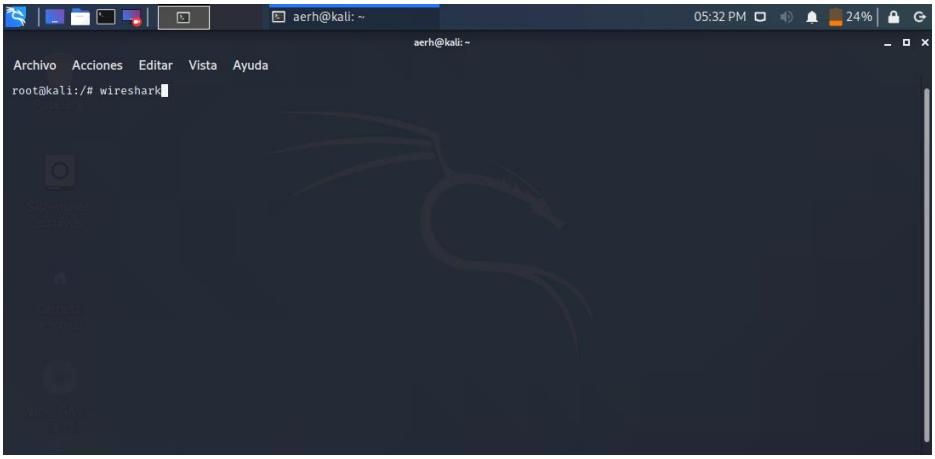
Aclamado: NMAP ha ganado numerosos premios, incluido el "Producto de seguridad de la información del año" por *Linux Journal, Info World* y *Codetalker Digest.* Ha aparecido en cientos de artículos de revistas, varias películas, docenas de libros y una serie de cómics. Visite la página de prensa para obtener más detalles (Lyon, 2008).

Popular: Miles de personas descargan Nmap todos los días, y está incluido en muchos sistemas operativos (Redhat Linux, Debian Linux, Gentoo, FreeBSD, OpenBSD, etc.). Se encuentra entre los diez mejores programas (de 30.000) en el repositorio Freshmeat.Net. Esto es importante porque le da a Nmap su desarrollo vibrante y comunidades de soporte al usuario (Lyon, 2008).

5.2 WIRESHARK

En la Figura 5. Se puede visualizar la ejecución del programa wireshark en la terminal.

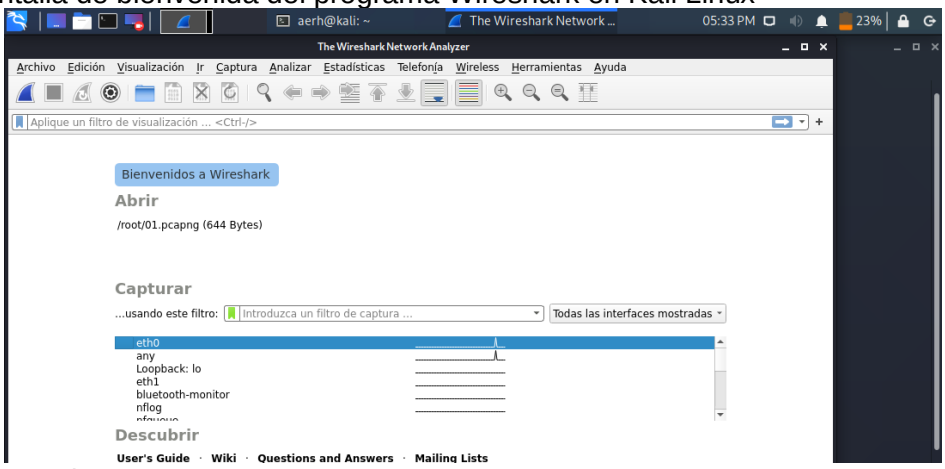
Figura 5 Ejecución de Wireshark en Kali Linux



Fuente Arturo Ruiz

En la Figura 6. Se puede visualizar la pantalla de bienvenida del programa wireshark y su menú de opciones.

Figura 6 Pantalla de bienvenida del programa Wireshark en Kali Linux



Fuente Arturo Ruiz

5.2.1 Características

Disponible para Linux y Windows

Captura de paquetes en vivo desde una interfaz de red

Muestra los paquetes con información detallada de los mismos

Abre y guarda paquetes capturados

Importar y exportar paquetes en diferentes formatos

Filtrado de información de paquetes

Resaltado de paquetes dependiendo el filtro

Crear estadísticas (Lamping y Warnicke, 2004).

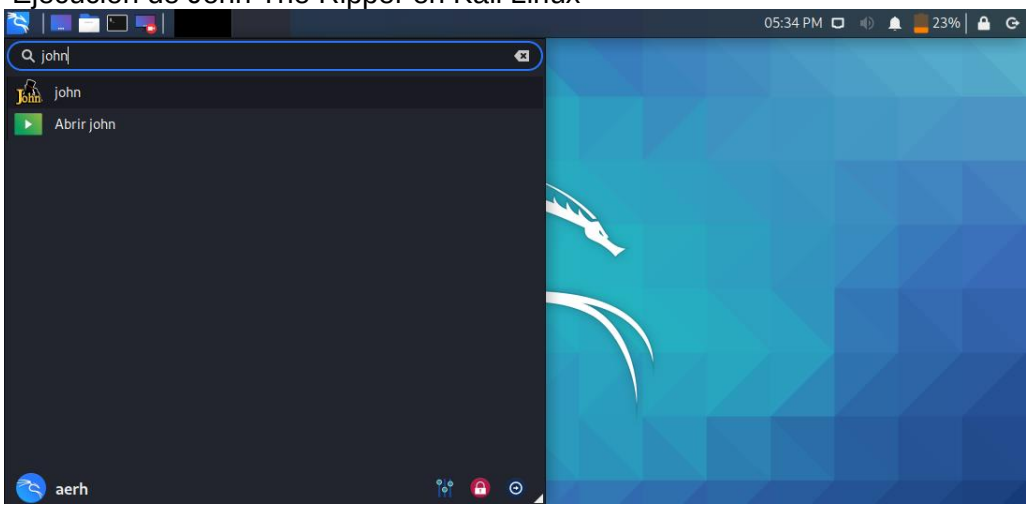
5.2.2 Ventajas

Entre sus cualidades se puede encontrar una enorme versatilidad que le lleva a soportar más de 480 protocolos distintos, además de la posibilidad de trabajar tanto con datos capturados desde una red durante una sesión con paquetes previamente capturados que hayan sido almacenados en el disco duro. Wireshark soporta el formato estándar de archivos tcpdump, es capaz de reconstruir sesiones TCP, y está apoyado en una completa interfaz gráfica que facilita enormemente su uso (Lamping y Warnicke, 2004).

5.3 JOHN THE RIPPER

En la Figura 7. Se puede visualizar la búsqueda y ejecución del programa John The Ripper (Anurag, 2021).

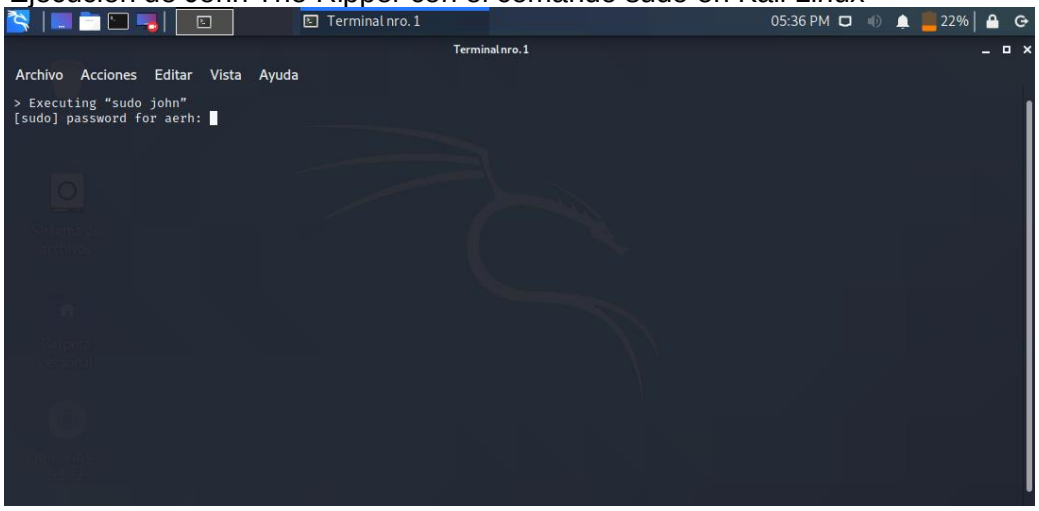
Figura 7 Ejecución de John The Ripper en Kali Linux



Fuente Arturo Ruiz

En la figura 8. Se puede visualizar la ejecución del programa John The Ripper con el comando sudo.

Figura 8 Ejecución de John The Ripper con el comando sudo en Kali Linux



Fuente Arturo Ruiz

5.3.1 Características

Optimizado para muchos modelos de procesador.

Funciona en muchas arquitecturas y sistemas operativos.

Ataques de diccionario y por fuerza bruta.

Muy personalizable (es software libre).

Permite definir el rango de letras que se usará para construir las palabras, y las longitudes.

Permite parar el proceso, y continuarlo más adelante.

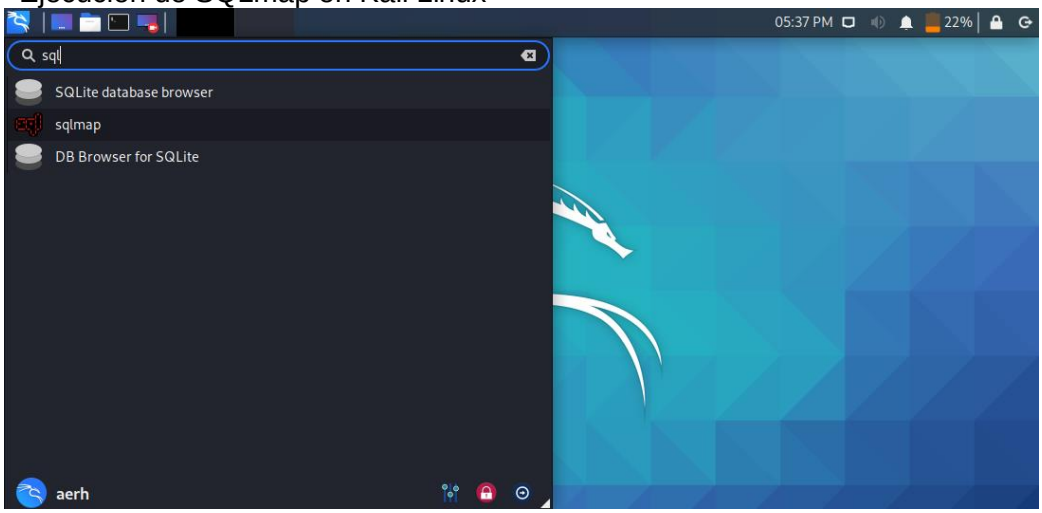
Permite incluir reglas en el diccionario para decir cómo han de hacerse las variaciones tipográficas.

Se utiliza en línea de comando y no tiene un entorno gráfico (Santo Orcero, 2018).

5.4 SQLMAP

En la Figura 9. Se puede visualizar la búsqueda y ejecución del programa *sqlmap*.

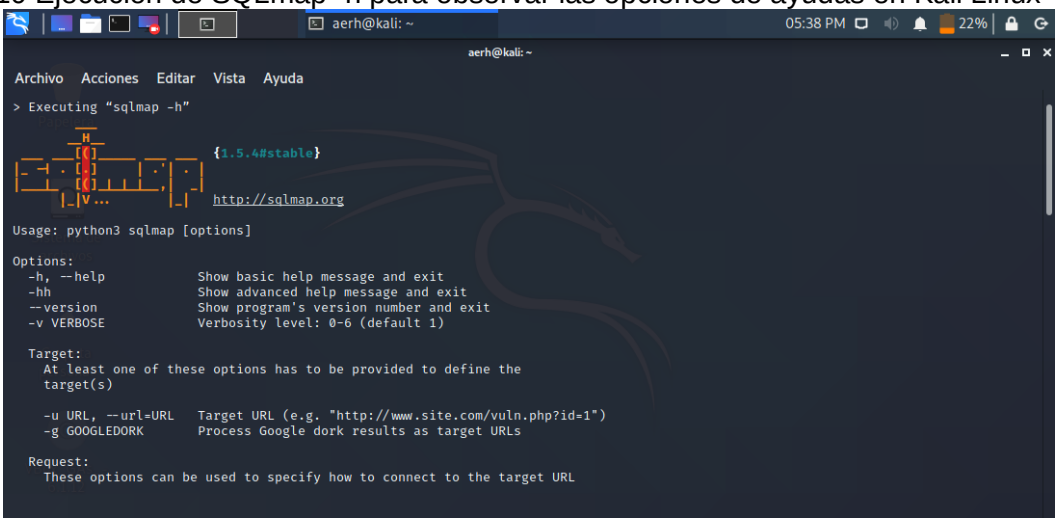
Figura 9 Ejecución de SQLmap en Kali Linux



Fuente Arturo Ruiz

En la Figura 10. Se puede visualizar la ejecución de *sqlmap-h* para observar las opciones de ayudas.

Figura 10 Ejecución de SQLmap -h para observar las opciones de ayudas en Kali Linux



Fuente Arturo Ruiz

5.4.1 Características

Soporte completo para *MySQL, Oracle, PostgreSQL, Microsoft SQL Server, Microsoft Access, IBM DB2, SQLite, Firebird, Sybase, SAP MaxDB, Informix, MariaDB, MemSQL, TiDB, CockroachDB, HSQLDB, H2, MonetDB, Apache Derby, Amazon Redshift, Vertica, Mckoi, Presto, Altibase, MimerSQL, CrateDB, Greenplum, Drizzle, Apache Ignite, Cubrid, InterSystems Cache, IRIS, eXtremeDB, FrontBase, Raima Database Manager, YugabyteDB and Virtuoso database management systems* (Ojagbule, Wimmer y Haddad, 2018).

Soporte completo para seis técnicas de inyección SQL *boolean-based blind, time-based blind, error-based, UNION query-based, stacked queries and out-of-band*. Soporte para conectarse directamente a la base de datos sin pasar a través de una inyección SQL, proporcionando credenciales DBMS, dirección IP, puerto y nombre de la base de datos. Soporte para enumerar usuarios, hashes de contraseñas, privilegios, roles, bases de datos, tablas y columnas (Ojagbule, Wimmer y Haddad, 2018).

Reconocimiento automático de formatos hash de contraseñas y soporte para descifrarlos mediante un ataque basado en diccionario. Soporte para volcar las tablas de la base de

datos por completo, un rango de entradas o columnas específicas según la elección del usuario. El usuario también puede optar por volcar solo un rango de caracteres de la entrada de cada columna. Soporte para buscar nombres de bases de datos específicos, tablas específicas en todas las bases de datos o columnas específicas en todas las tablas de las bases de datos. Esto es útil, por ejemplo, para identificar tablas que contienen credenciales de aplicaciones personalizadas donde los nombres de las columnas relevantes contienen cadenas como nombre y contraseña (Ojagbule, Wimmer y Haddad, 2018).

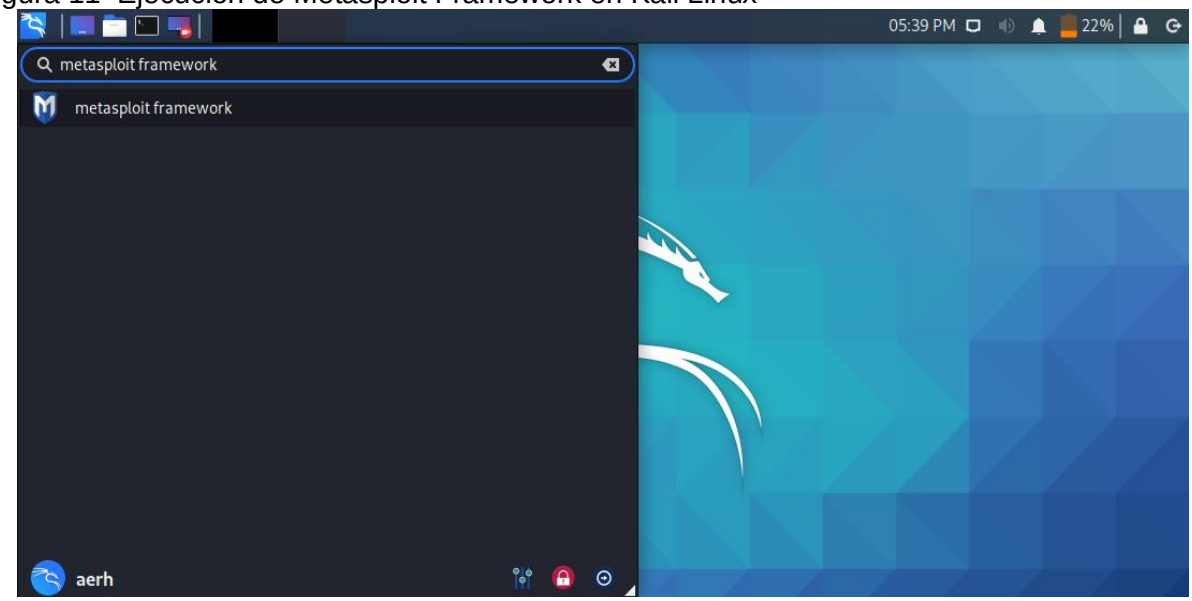
Soporte para descargar y cargar cualquier archivo desde el sistema de archivos subyacente del servidor de la base de datos cuando el software de la base de datos es MySQL, PostgreSQL o Microsoft SQL Server. Soporte para ejecutar comandos arbitrarios y recuperar su salida estándar en el sistema operativo subyacente del servidor de la base de datos cuando el software de la base de datos es MySQL, PostgreSQL o Microsoft SQL Server (Ojagbule, Wimmer y Haddad, 2018).

Soporte para establecer una conexión TCP con estado fuera de banda entre la máquina atacante y el sistema operativo subyacente del servidor de base de datos. Este canal puede ser un símbolo del sistema interactivo, una sesión de Meterpreter o una sesión de interfaz gráfica de usuario (VNC) según la elección del usuario. Soporte para la escalada de privilegios de usuario del proceso de la base de datos a través del getsystem comando Meterpreter de Metasploit (Ojagbule, Wimmer y Haddad, 2018).

5.5 METASPLOIT FRAMEWORK

En la Figura 11. Se puede visualizar la búsqueda y ejecución del programa metasploit framework.

Figura 11 Ejecución de Metasploit Framework en Kali Linux



Fuente Arturo Ruiz

5.5.1 Características

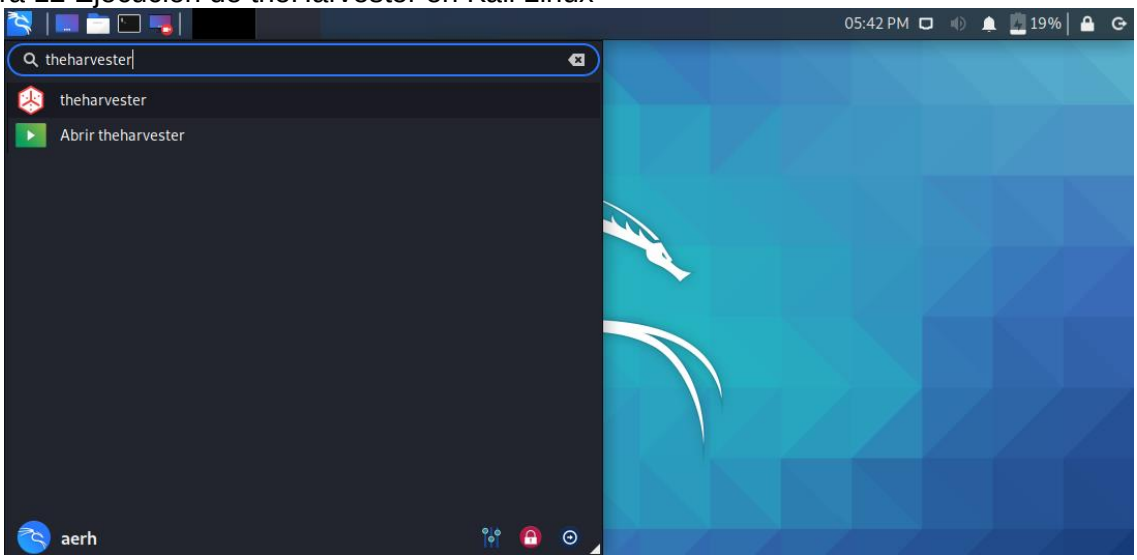
Es una herramienta muy completa que tiene muchísimos *exploits*, que son vulnerabilidades conocidas, en las cuales tienen también unos módulos, llamados *payloads*, que son los códigos que explotan estas vulnerabilidades. También dispone de otros tipos de módulos, por ejemplo, los *encoders*, que son una especie de códigos de cifrado para evasión de antivirus o sistemas de seguridad perimetral (Timalsina y Gurung, 2017).

Otra de las ventajas de este *framework* es que nos permite interactuar también con herramientas externas, como *Nmap* o *Nessus*. Además, ofrece la posibilidad de exportar nuestro malware a cualquier formato, ya sea en sistemas Unix o Windows. Destacar también que es multiplataforma y gratuita, aunque tiene una versión de pago, en la que se nos ofrecen *exploits* ya desarrollados, pero cuyo coste es bastante elevado. La versión gratuita es muy interesante porque contiene todas las vulnerabilidades públicas (Singh, 2013).

5.6 THEHARVESTER

En la Figura 12. Se puede visualizar la búsqueda y ejecución del programa theharvester.

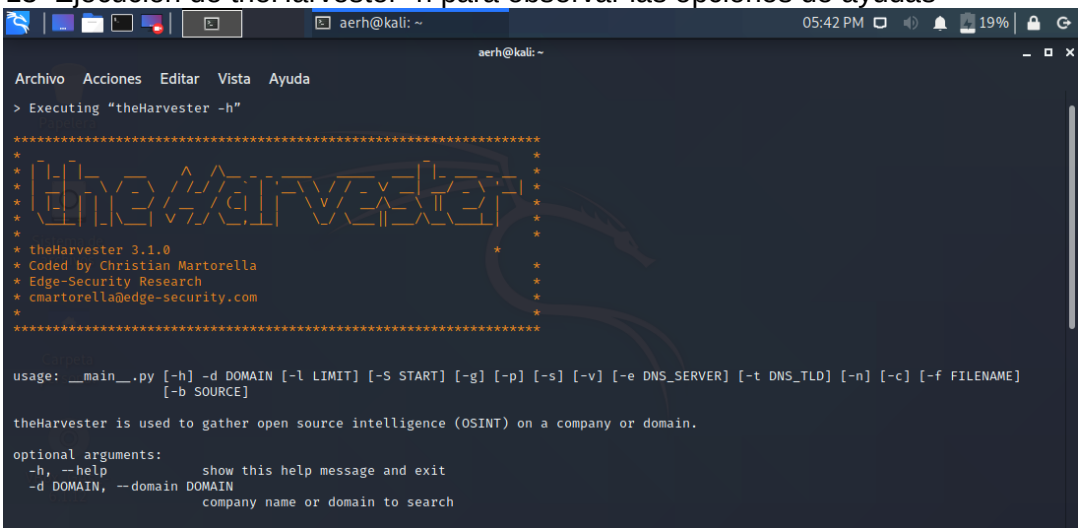
Figura 12 Ejecución de theHarvester en Kali Linux



Fuente Arturo Ruiz

En la Figura 13. Se puede visualizar la ejecución de *theharvester* -h para observar las opciones de ayudas.

Figura 13 Ejecución de theHarvester -h para observar las opciones de ayudas



Fuente Arturo Ruiz

5.6.1 Características

Herramienta de Línea de comandos (CUI).

XML y HTML como resultados de exportación.

Buscar un dominio en todas las fuentes.

Verificador de host virtual.

Shodan base de datos integrada.

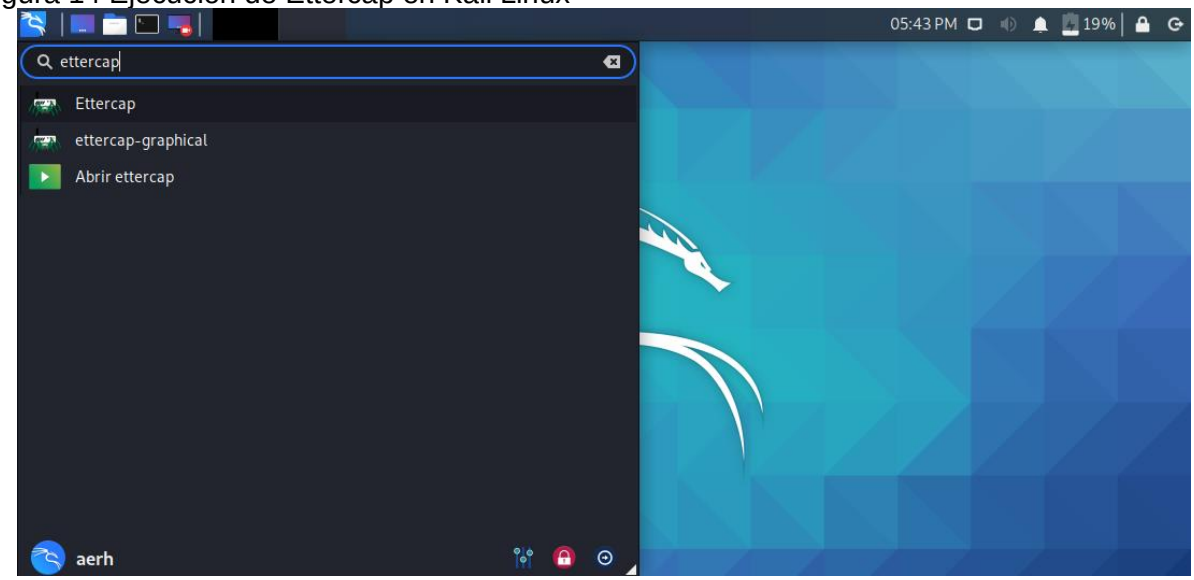
Enumeración de activos (enumeración DNS, las búsquedas de DNS inversa, DNS expansión TLD).

Resultados de las estadísticas básicas (Qian, Xu y Zuo,2018).

5.7 ETTERCAP

En la Figura 14. Se puede visualizar la búsqueda y ejecución del programa *ettercap*.

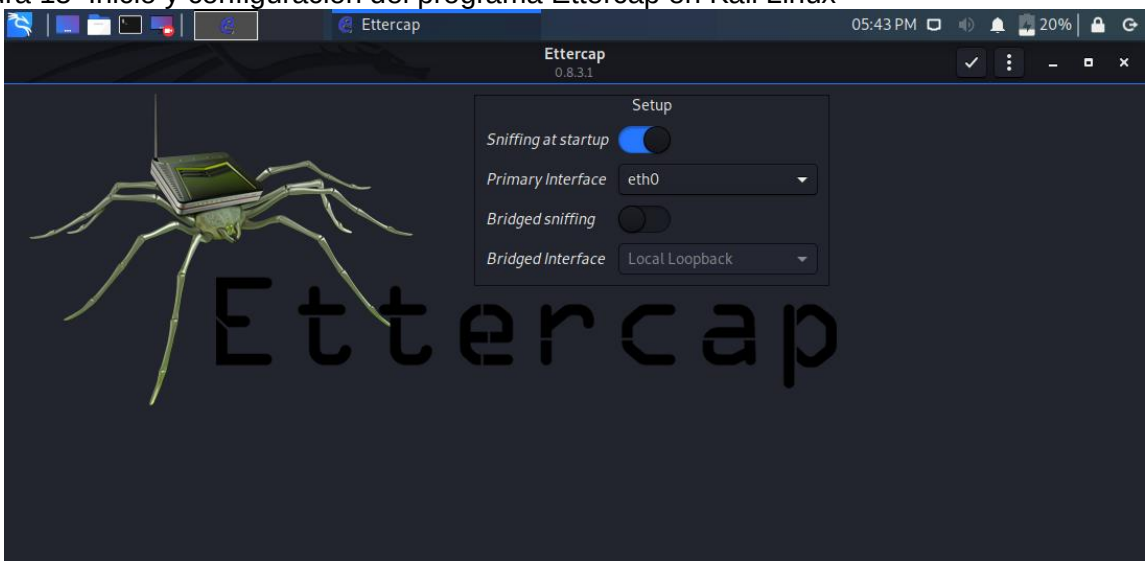
Figura 14 Ejecución de Ettercap en Kali Linux



Fuente Arturo Ruiz

En la Figura 15. Se puede visualizar el inicio y configuración del programa Ettercap.

Figura 15 Inicio y configuración del programa Ettercap en Kali Linux



Fuente Arturo Ruiz

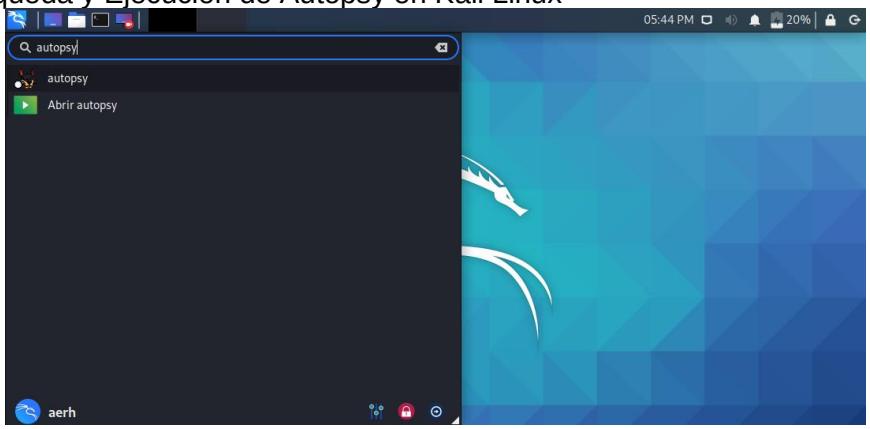
5.7.1 Características

Ettercap es una suite completa para ataques de intermediarios. Cuenta con rastreo de conexiones en vivo, filtrado de contenido sobre la marcha y muchos otros trucos interesantes. Admite la disección activa y pasiva de muchos protocolos e incluye muchas funciones para el análisis de redes y hosts (Norton, 2004).

5.8 AUTOPSY

En la Figura 16. Se puede visualizar la búsqueda y ejecución del programa autopsy.

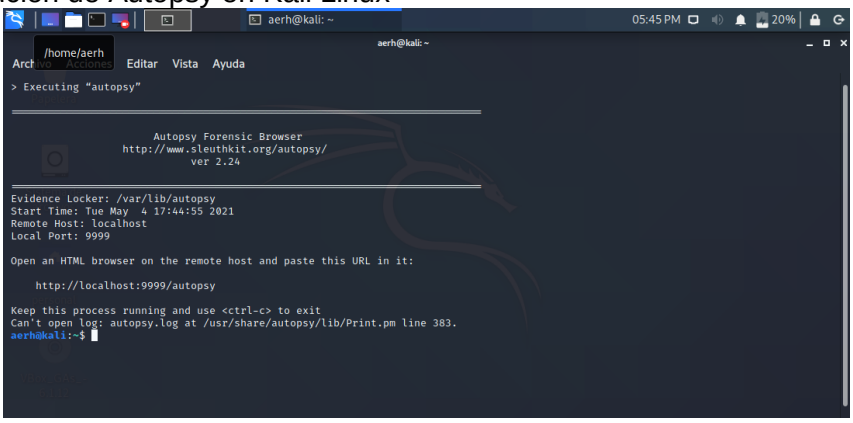
Figura 16 Búsqueda y Ejecución de Autopsy en Kali Linux



Fuente Arturo Ruiz

En la Figura 17. Se puede visualizar la ejecución de autopsy -h para observar las opciones de ayudas.

Figura 17 Ejecución de Autopsy en Kali Linux



Fuente Arturo Ruiz

5.8.1 Características

Casos multiusuario: colabore con otros examinadores en casos grandes (Lin Xiaodong, 2018).

Análisis de la línea de tiempo: muestra los eventos del sistema en una interfaz gráfica para ayudar a identificar la actividad (Lin Xiaodong, 2018).

Búsqueda de palabras clave: los módulos de búsqueda de índice y extracción de texto le permiten encontrar archivos que mencionan términos específicos y encontrar patrones de expresión regular (Lin Xiaodong, 2018).

Artefactos web: extrae la actividad web de los navegadores comunes para ayudar a identificar la actividad del usuario (Lin Xiaodong, 2018).

Análisis de registro: utiliza RegRipper para identificar documentos y dispositivos USB a los que se accedió recientemente (Lin Xiaodong, 2018).

Análisis de archivos LNK: identifica atajos y documentos a los que se accede (Lin Xiaodong, 2018).

Análisis de correo electrónico: analiza mensajes en formato MBOX, como Thunderbird (Lin Xiaodong, 2018).

EXIF: extrae la ubicación geográfica y la información de la cámara de los archivos JPEG (Lin Xiaodong, 2018).

Clasificación por tipo de archivo: agrupe los archivos por su tipo para encontrar todas las imágenes o documentos (Lin Xiaodong, 2018).

Reproducción de medios: vea videos e imágenes en la aplicación y no requiera un visor externo.

Visor de miniaturas: muestra imágenes en miniatura para ayudar a ver las imágenes rápidamente (Lin Xiaodong, 2018).

Análisis robusto del sistema de archivos: compatibilidad con sistemas de archivos comunes, incluidos NTFS, FAT12 / FAT16 / FAT32 / ExFAT, HFS +, ISO9660 (CD-ROM), Ext2 / Ext3 / Ext4, Yaffs2 y UFS de The Sleuth Kit.

Filtrado de conjuntos de hash: filtre los archivos buenos conocidos mediante NSRL y marque los archivos defectuosos conocidos mediante conjuntos de hash personalizados en los formatos HashKeeper, md5sum y EnCase (Lin Xiaodong, 2018).

Etiquetas: etiquete archivos con nombres de etiqueta arbitrarios, como "marcador" o "sospechoso", y agregue comentarios (Lin Xiaodong, 2018).

Extracción de cadenas Unicode: extrae cadenas del espacio no asignado y tipos de archivos desconocidos en muchos idiomas (árabe, chino, japonés, etc.) (Lin Xiaodong, 2018).

Detección de tipo de archivo basada en firmas y detección de discrepancias de extensión (Lin Xiaodong, 2018).

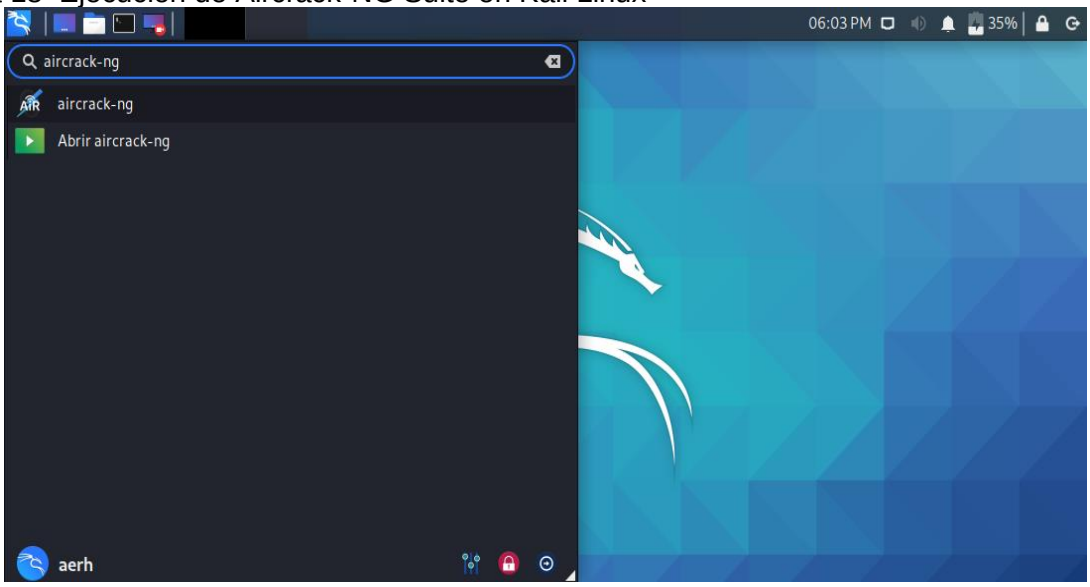
El módulo de archivos interesantes marcará archivos y carpetas según el nombre y la ruta.

Compatibilidad con Android: extrae datos de SMS, registros de llamadas, contactos, Tango, Palabras con amigos y más (Lin Xiaodong, 2018).

5.9 AIRCRACK-NG SUITE

En la Figura 18. Se puede visualizar la búsqueda y ejecución del programa aircrack -ng.

Figura 18 Ejecución de Aircrack-NG Suite en Kali Linux



Fuente Arturo Ruiz

5.9.1 Características

Aircrack- ng es un paquete completo de herramientas para evaluar la seguridad de la red Wi-Fi. Se enfoca en diferentes áreas de seguridad WiFi:

Supervisión: captura de paquetes y exportación de datos a archivos de texto para su posterior procesamiento por herramientas de terceros

Ataques: Repetir ataques, desautenticación, puntos de acceso falsos y otros mediante inyección de paquetes.

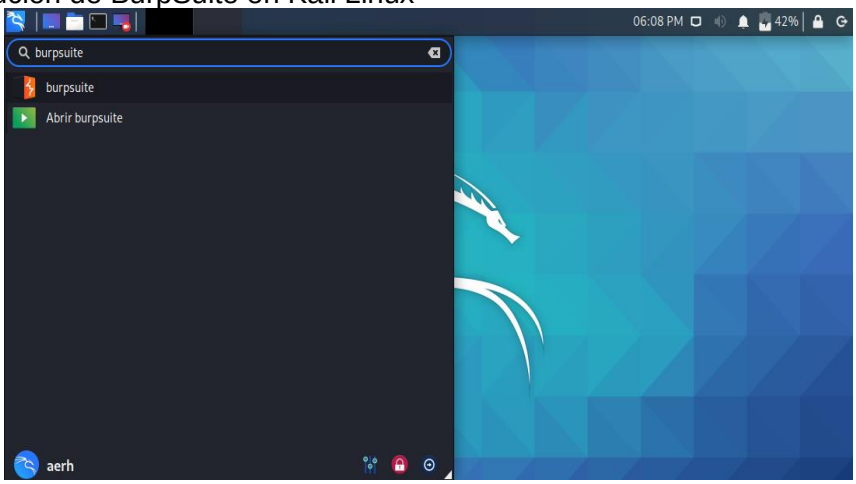
Pruebas: comprobación de las tarjetas WiFi y las capacidades del controlador (captura e inyección)

Craqueo: WEP y WPA PSK (WPA 1 y 2) (Alamanni, 2015).

5.10 BURPSUITE

En la Figura 19. Se puede visualizar la búsqueda y ejecución del programa Burpsuite.

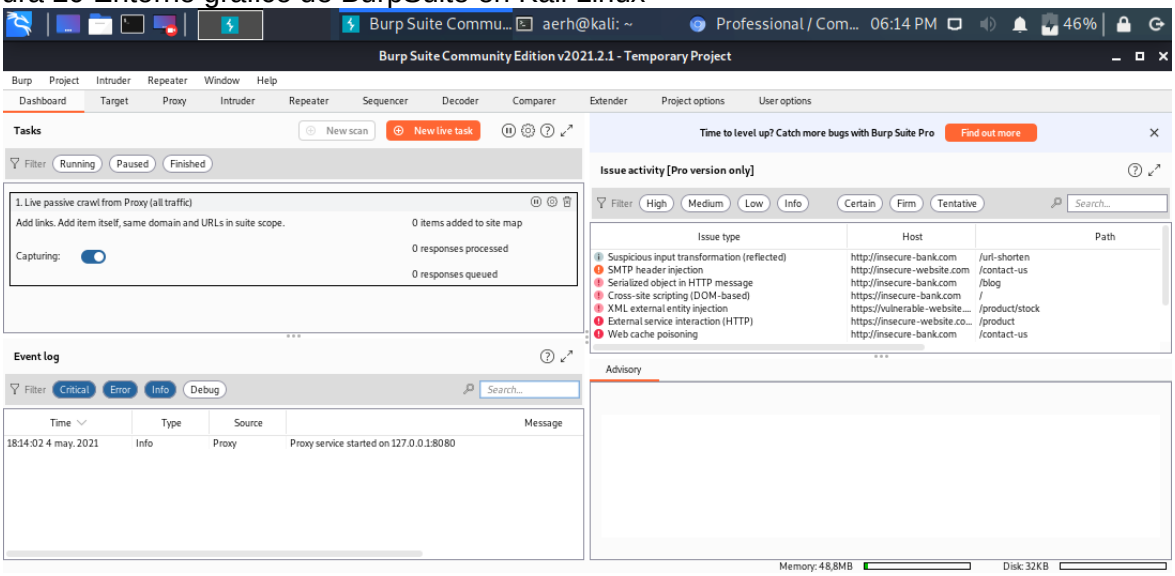
Figura 19 Ejecución de BurpSuite en Kali Linux



Fuente Arturo Ruiz

En la Figura 20. Se puede visualizar el entorno gráfico del programa Burpsuite y su menú de opciones.

Figura 20 Entorno gráfico de BurpSuite en Kali Linux



Fuente Arturo Ruiz

5.10.1 Características

Permite realizar de forma automatizada pruebas de exploración y escaneo de vulnerabilidades.

Contiene un escáner de vulnerabilidades avanzado para pruebas manuales.

Lógica de exploración de vanguardia.

Presentación clara y detallada de vulnerabilidades, con recomendaciones y los *payloads* utilizados.

Interceptar el tráfico del navegador mediante el Proxy (*man-in-the-middle*).

Ataques automatizados y personalizados usando *Burp Intruder*.

Contiene herramientas de prueba manuales avanzadas.

Brinda diferentes métodos y técnicas de conexión a las aplicaciones Web (Hutchens, 2014).

El sistema operativo Kali Linux se caracteriza por su gran componente de herramientas para realizar auditorías informáticas o test de intrusión a sistemas informáticos, gran parte de ellas son el resultado de un grupo de desarrollo y comunidad que realiza constantemente mejoras y sitúa las actualizaciones para que los *pentesters* o hacker éticos lleven a cabo sus operaciones, detectando vulnerabilidades tanto en redes como en sistemas corporativos; por otra parte el sistema operativo se extiende a otros componentes para escanear y detectar sus posibles vulnerabilidades, como son los dispositivos móviles, en estos últimos igualmente se pueden instalar herramientas que cumplen la misma funcionalidad para análisis de vulnerabilidades. Para alcanzar a conocer todos los componentes que ofrece este sistema operativo es preciso que primero se tenga una familiaridad con sistemas operativos, el entorno de las redes y ejecución de comandos básicos en Linux, este último sirve como base para iniciarse en los temas de seguridad informática, puesto que gran parte de las herramientas que se ejecutan son *Open Source* y se debe tener cierta familiaridad a la hora de llevar a cabo un escaneo y de efectuar un test de intrusión.

También, entre las herramientas más populares para realizar los respectivos análisis de vulnerabilidades y test de intrusión se puede mencionar a *nmap*, como una de las líderes o requisito indispensable que todo profesional en seguridad informática debe conocer y operar puesto que ofrece un gran número de ventajas y caracterizándose por su uso, portabilidad, potencia y además que es gratuita; ante todo, en trabajos académicos se hace referencia a esta herramienta que aporta gran valor no solo en lo académico sino en lo profesional convirtiéndose podría decirse en la abanderada para iniciarse en el mundo de la seguridad informática. Por otro lado, las estadísticas presentan que la familiaridad y uso de *nmap* para ejecutar proceso de *pentesting* están aproximadamente

en un 100% convirtiéndose en líder en la ejecución y desarrollo de los procesos de seguridad informática.

Igualmente, el sistema operativo está encaminado a ejecutarse a los procesos de seguridad informática, esto debe tener muy en cuenta el profesional que realice estas acciones bajo un concepto de ética y valores que son base fundamental para llevar a cabo las acciones pertinentes cuando se ejecutan los test de intrusión para detectar posibles vulnerabilidades a las corporaciones. De hecho, que no es el único sistema operativo que realiza acciones para la seguridad informática, existen muchos con esa similitud para acompañar y ejecutar este proceso y en cuanto a herramientas también guardan familiaridad; cabe destacar que, en el mundo del hacking ético, y más aún los profesionales que se inician o los más aventajados en este tema recomiendan el sistema operativo Kali Linux como el fundamental para ejecutar los test de intrusión o auditorías informáticas, esto por su gran desempeño a la hora de encontrar bibliografía, foros, documentación y una comunidad fuerte y talentosa que a diario se encarga de mantener actualizado el sistema operativo.

6. DOCUMENTACIÓN DE LAS PRINCIPALES HERRAMIENTAS DEL SISTEMA OPERATIVO KALI LINUX QUE PUEDEN IMPLEMENTARSE EN LOS PROCESOS DE AUDITORÍA INFORMÁTICA A NIVEL EMPRESARIAL

Para dar cumplimiento al objetivo dos se procedió a categorizar las siguientes herramientas:

Nmap: De acuerdo con la página oficial de nmap.org, esta herramienta de código abierto y gratuita es de utilidad para el descubrimiento de redes y la auditoría de seguridad, muchos administradores lo utilizan para el inventario de red y gestión de programas de actualización del servicio y la supervisión de actividad del host o servicio (Calderón, 2017).

Wireshark: Se define esta herramienta como un analizador de protocolos de red más importantes y más utilizado del mundo. Permite ver lo que está sucediendo en la red a nivel microscópico y es utilizado en muchas empresas tanto comerciales y sin fines de lucro, agencias gubernamentales e instituciones educativas (Wang, Xu y Yan, 2010).

John The Ripper: Es una herramienta de recuperación y auditoría de seguridad de contraseñas de código abierto, disponible para muchos sistemas operativos (Anurag y Kanjirappally, 2021).

SQLmap: *Sqlmap* es una herramienta de prueba de penetración de código abierto que automatiza el proceso de detección y explotación de fallas de inyección de SQL y la toma de control de los servidores de bases de datos (López, Aldana y Cuervo, 2014).

Metasploit Framework: Es una de las herramientas más utilizadas por los auditores de seguridad. Incluye una gran colección de *exploits*, aparte de proporcionarle un entorno de desarrollo para los propios *exploits*. esta herramienta también es muy utilizada por los

auditores de seguridad debido a su fácil implementación con otras herramientas como *nmap*, escaners de vulnerabilidades, etc. *Metasploit Framework* es una infraestructura que puede ser personalizada y utilizada para necesidades específicas. también hay que mencionar que *Metasploit Framework* está respaldada por una comunidad de más de 200.000 usuarios, sin contar que esta herramienta también está respaldad por una empresa, *Rapid7* (Maynor, 2011).

theHarvester: Es una herramienta de línea de comandos incluida en Kali Linux que actúa como contenedor para una variedad de motores de búsqueda y se utiliza para encontrar cuentas de correo electrónico, nombres de subdominios, hosts virtuales, puertos abiertos / banners y nombres de empleados relacionados con un dominio fuentes públicas (Gordon, 1986).

Ettercap: *Ettercap* es una suite completa para ataques de intermediarios. Cuenta con rastreo de conexiones en vivo, filtrado de contenido sobre la marcha y muchos otros trucos interesantes. Admite la disección activa y pasiva de muchos protocolos e incluye muchas funciones para el análisis de redes y *hosts* (Ghanem y Belaton, 2013).

Autopsy: Es una plataforma forense digital y una interfaz gráfica para *The Sleuth Kit*® y otras herramientas forenses digitales. Los analizadores de las fuerzas del orden público, militares y corporativos lo utilizan para investigar lo que sucedió en una computadora. Incluso puede usarlo para recuperar fotos de la tarjeta de memoria de su cámara (Mirabá Quimí, 2021).

Aircrack-NG Suite: *Aircrack-ng* es un paquete completo de herramientas para evaluar la seguridad de la red *Wi-Fi (*López Acosta, Monroy Melo y Murcia Linares, 2018).

BurpSuite: *Burp Suite* es una plataforma integrada para realizar pruebas de seguridad de aplicaciones web. Sus diversas herramientas funcionan a la perfección para respaldar todo el proceso de prueba, desde el mapeo inicial y el análisis de la superficie de ataque

de una aplicación, hasta la búsqueda y explotación de vulnerabilidades de seguridad (Mahajan, 2014).

Teniendo en cuenta que se han realizado trabajos de grado para la categorización se mencionan las conclusiones de los estudios realizados:

Kali Linux es un kit de herramientas de software para realizar pruebas de seguridad a sistemas informáticos, de fácil uso y que terceras personas podrían utilizar para adquirir información valiosa acerca de los sistemas de información de la organización a través de diferentes métodos como Ingeniería Social y *phishing*. Las pruebas de seguridad demostraron que el factor humano es pieza importante en los ataques, aumentando la posibilidad de ataques informáticos exitosos (Allen, Heriyanto y Ali, 2014).

Se determinaron metodologías de *Pen Test* y *Ethical Hacking*, teniendo en cuenta cada una de las características y funcionalidad de las mismas, además la herramienta inmersa en cada sistema operativo seleccionado para para las pruebas de penetración como lo es *Nmap* y *Kali Linux*, que contiene un paquete interno de herramientas muy seguras y robustas para el estudio analizado a las bases de datos en la Secretaría de Hacienda del Municipio de Los Patios (Allen, Heriyanto y Ali, 2014).

Después de realizado el análisis de la información obtenida se puede confirmar que ninguna aplicación web es perfectamente segura y libre de ataques, pero con el uso de técnicas o test de intrusión, *Pentesting*, como herramientas de *Hackeo* Ético, todas esas vulnerabilidades pueden ser superadas, evitando los ataques que socavan la integridad y fiabilidad de los datos que se manejan (López De Jiménez, 2017)

Kali Linux es un sistema operativo que trae instalados una gran variedad de programas relacionados con la seguridad informática donde más de 600 herramientas, siendo algunas de las más conocidas *Nmap* (escaneo de puertos), Wireshark (analizador y captura de paquetes de datos que circulan por la red), *John the Ripper* (crackeador de

contraseñas), *Metasploit* (Explotación de Vulnerabilidades) y la suite *Aircrack-ng* (*Software* para pruebas de seguridad en redes inalámbricas),donde estas son las más utilizadas en procesos de auditoría en redes y servicios corporativos (Sandoya Romero, 2021).

Teniendo en cuenta que para categorizar las principales herramientas de seguridad utilizadas en el sistema operativo *Kali Linux*, se tuvo en cuenta criterios como:

Consultas de masas documentales.
Documentación oficial en la página de kali.org.

Foros.

Como inicio en el hacking ético.

Herramientas más útiles para realizar auditorías en seguridad informática.

Páginas web con recomendaciones de su implementación y uso.

¿Cómo se realizará la clasificación de las herramientas para el sector empresarial?

Explique cada uno de los criterios:

Portabilidad. La gran parte de estas herramientas se pueden instalar en todos los sistemas operativos: *Microsoft Windows, Mac OS X* y *Linux. Kali Linux* como líder en seguridad informática permite realizar auditorías a los entornos de red empresariales y a las estaciones de usuario esto con el fin de permitir que los equipos informáticos puedan entrar a la red mundial internet de una forma segura sin el riesgo de ser vulnerados. Es por esto, que se ofrece un sinnúmero de herramientas para trabajar y contar con un sistema operativo versátil que permite a las estaciones de usuario, las redes y dispositivos

móviles entre otros enfrentarse a los peligros que a diario se encuentran. Entre otras cosas, *Kali Linux* se puede instalar como máquina virtual (por ejemplo, utilizando virtual box o vmware) o en una unidad extraíble (unidad USB o disco duro externo).

Flexibilización de uso. Al seleccionar las herramientas es preciso tener en cuenta que se encuentra documentación al día y actualizada tanto en la página oficial de Kali Linux como en foros y URL de cada una de ellas. Es por esto, que el entrenamiento es clave para adquirir destreza y domino por los menos en gran parte de ellas y según el objetivo que se requiera obtener se ofrece un sinnúmero de capacitaciones para alcanzar en lo posible a certificarse y adquirir experiencia en el manejo y dominio de ellas. Muchos profesionales utilizan esta distribución para auditar y encontrar los puntos débiles en las redes, después de esto inician sus ataques para alcanzar y evidencias las vulnerabilidades presentes e informar sobre ellas.

Economía. Gran parte o la mayoría de estas herramientas son gratuitas y de fácil descarga, aunque algunas de ellas son comerciales y ofrecen un demo por unos días, sobre todo para los sistemas operativos comerciales como *Microsoft Windows*, para *Kali Linux* se obtienen de una manera gratuita y con guías que se orientan en la instalación y configuración de ellas. Por otra parte, y debido a que las herramientas para el sistema operativo *Kali Linux* son gratuitas, las empresas deben tener claro que la inversión en infraestructura (equipos de cómputo con hardware y software, *Firewall*) debe ser más en capacitación hacia el equipo que tendrá a cargo la seguridad informática de la empresa y los usuarios finales con entrenamientos periódicos en los que se les socialice sobre los conceptos básicos y fundamentales en ciberseguridad. Durante el desarrollo de la siguiente monografía se analizarán en mayor profundidad las herramientas, se definirán su uso y funcionamiento utilizando máquinas virtuales.

Tabla 1 Características y Uso de las 10 principales herramientas de seguridad informática utilizadas en el sistema operativo Kali Linux

Herramienta	Características	Uso
Nmap (Johnson, 2021)	Herramienta gratuita de auditoría de seguridad y descubrimiento de redes. Es simple, flexible y extensible, tiene una interfaz de línea de comando donde se adicionan diferentes tipos de escaneos.	Se usa para escanear hosts individuales y grandes redes.
Wireshark (Shivanandhan, 2020)	Herramienta de análisis de redes, es un software de código abierto que le permite inspeccionar datos en tiempo real en una red en vivo.	Se utiliza este software eficiente para capturar paquetes de datos e inspeccionar las características que presentan estos en particular, lo que ayuda a identificar las debilidades en la seguridad de la red.
John the Ripper (Shivanandhan, 2020)	Es un descifrador de contraseñas súper rápido con soporte para listas de palabras personalizadas. Puede ejecutarse contra la mayoría de los tipos de métodos de cifrado como MD5 y SHA.	Los profesionales utilizan John the Ripper para probar la seguridad de las contraseñas.
Sqlmap (Unipython, 2018)	El usuario puede elegir entre diferentes opciones como enumerar usuarios, hashes de contraseñas, leer algún archivo específico del sistema de archivos, ejecutar comandos, volcar tablas y columnas del motor bases de datos, etc.	Es utilizada para detectar y explotar vulnerabilidades de inyección SQL
Metasploit framework (Mutune George, 2021)	Es un software de código abierto con el que es posible editar los exploits existentes para crear nuestros propios exploits personalizados. Estas herramientas de test de intrusión pueden examinar los diferentes sistemas de seguridad, incluidas las aplicaciones basadas en web, los servidores, las redes, etc. Metasploit puede identificar instantáneamente todas las nuevas	Se utiliza esta herramienta para lograr diversos objetivos de seguridad, como descubrir vulnerabilidades en el sistema, fortalecer la seguridad del sistema informático, tejer estrategias de defensa cibernética y mantener evaluaciones de seguridad completas.

	vulnerabilidades de seguridad tan pronto como ocurren, manteniendo así la máxima seguridad todo el tiempo.	
Theharvester (Hackeacademy, 2021).	Esta herramienta puede ser utilizada en reconocimiento pasivo y por cualquier persona que necesite saber qué puede ver un atacante sobre la organización.	El objetivo de esta herramienta es encontrar y recopilar todas las direcciones de correo electrónico, subdominios, hosts, puertos, nombres de empleados que pueden proporcionar información confidencial sobre el objetivo.
Ettercap (Salame, 2021).	Con Ettercap, se puede comprobar la seguridad de la red, qué tan susceptible es a este tipo de ataques, y también analizar el tráfico de varios equipos, e incluso modificarlo sobre la marcha.	Ettercap es una herramienta gratuita de código abierto que se puede utilizar para ataques en redes, esta herramienta sirve para verificar las vulnerabilidades de los sistemas.
Autopsy (Autopsy, 2021)	Es extensible y viene con características que incluyen búsqueda de palabras clave, coincidencia de hash, análisis de registro, análisis web y más.	Autopsy es una plataforma forense digital y una interfaz gráfica para The Sleuth Kit® y otras herramientas forenses digitales. Los examinadores de las fuerzas del orden público, militares y corporativos lo utilizan para investigar lo que sucedió en una computadora. Incluso puede usarlo para recuperar fotos de la tarjeta de memoria de su cámara.
Aircrack-NG (Autopsy, 2021)	Aircrack-ng permite a los usuarios capturar paquetes de datos conectados a través de una red para un monitoreo constante. Además, permite la captura e inyección, lo cual es vital para evaluar las tarjetas de red y el rendimiento de las tarjetas de red.	Es un software de seguridad de red completo adecuado para mejorar la seguridad general de la red. La herramienta contiene un conjunto completo de funcionalidades para analizar las debilidades de Wi-Fi.
Burpsuite (Autopsy, 2021)	Plataforma GUI profesional, útil para hallar vulnerabilidades o riesgos de seguridad en aplicaciones web de forma automática.	Es un software sólido de seguridad de redes informáticas que se utiliza para escanear redes, detectar debilidades críticas y mejorar la seguridad de la red.

7. MANUAL PARA CONFIGURACIÓN DE HERRAMIENTAS DE AUDITORÍA EN KALI LINUX

En el desarrollo del presente objetivo y a modo de realizar un manual para la configuración del sistema operativo Kali Linux es importante tener en cuenta lo siguiente: ante todo, es importante que la práctica con disciplina y constancia llevará a buen término la fidelización y entendimiento del presente manual, se deja constancia a través de este medio escrito que es un manual de tipo educativo donde no se pretende vulnerar o entrar a un sistema con las consecuencias que puede traer al penetrar a una red empresarial.

También, es necesario recalcar la importancia que ofrecen ciertos sitios web para lleva a cabo las pruebas pentest o de intrusión a una seria de máquinas que presentan vulnerabilidades, con esto se pretende abarcar que ellas se pueden instalar en forma local como máquinas virtuales lo que facilitará el desarrollo del laboratorio de seguridad informática, este entorno es donde se instalan y configuran las diferentes máquinas virtuales para llevar a cabo el proceso de adquirir las destrezas necesarias para entender los conceptos de ciberseguridad que nos ofrece la teoría y poder llevar a cabo y con éxito los laboratorios puesto que allí se entenderá y se podrá experimentar sin alterar y/o comprometer un sistema informático.

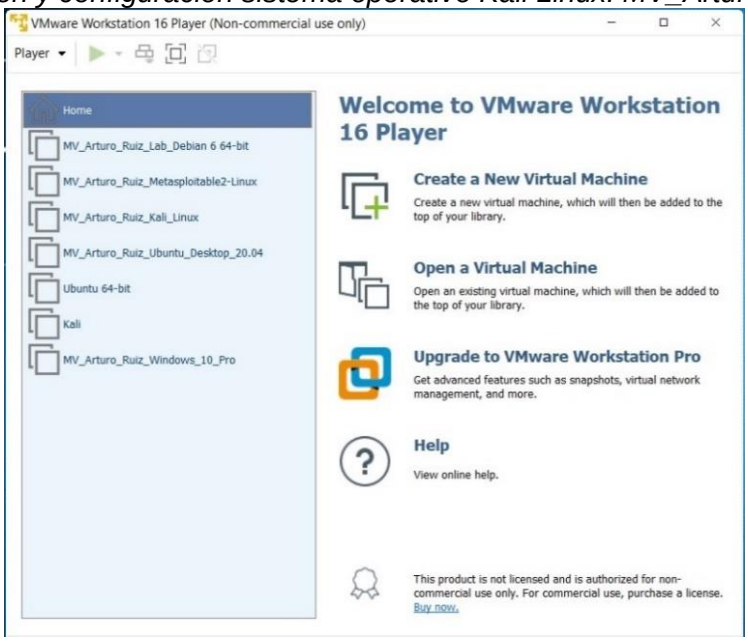
Por otra parte, y para llevar a cabo este objetivo se recurre a la instalación y configuración del *software VMware Workstation 16 Player*. En la Figura 21. Se puede visualizar la opción para descargar *vmware Workstation 16 player*.

Figura 21 Descarga *vmware Workstation 16 player*

Fuente Arturo Ruiz

Una vez descargado e instalado se procede a la configuración de las máquinas virtuales para llevar a cabo el presente manual, entre los sistemas operativos instalados y tomando como principal está *Kali Linux* el cual se ha descargado e instalado en su versión de 64 bits. En la Figura 22. Se puede visualizar la ejecución del programa *VMware Workstation 16 Player.*

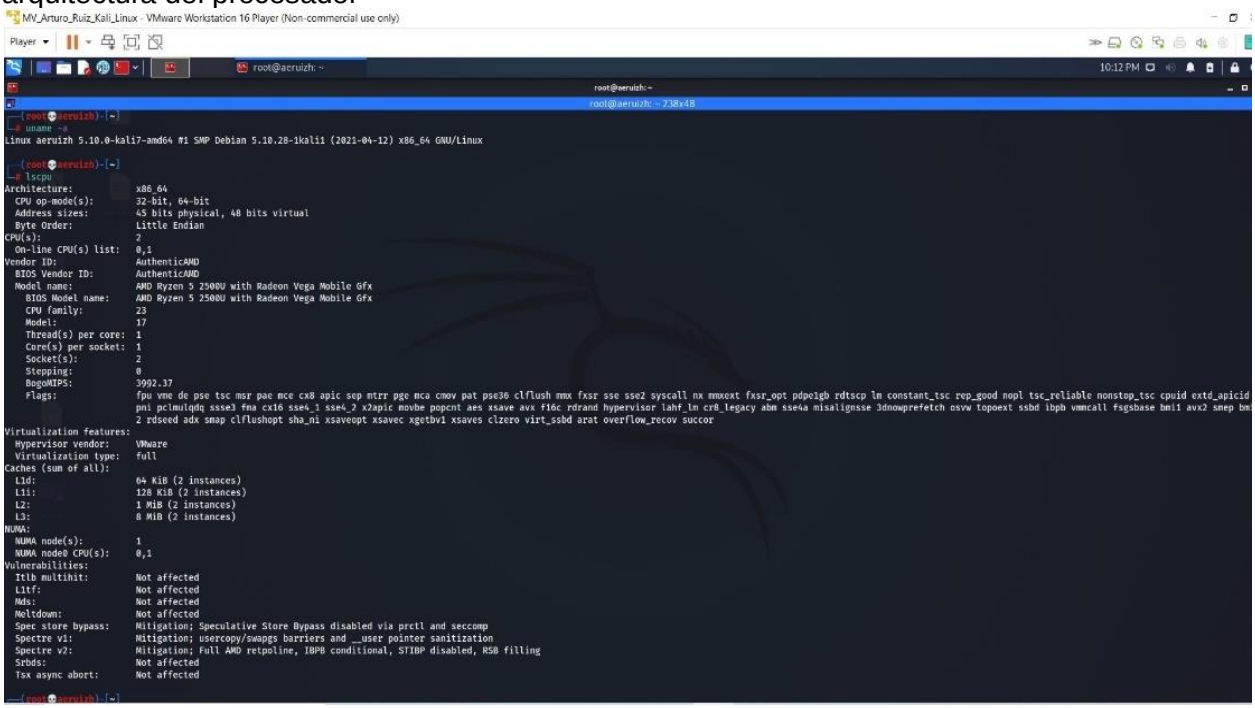
Figura 22 Instalación y configuración sistema operativo Kali Linux: MV_Arturo_Ruiz_Kali_Linux



Fuente Arturo Ruiz

En la Figura 23. Se puede visualizar la ejecución en la terminal del comando uname -h que muestra características del sistema operativo y el comando lscpu para obtener información detallada sobre de la arquitectura del procesador.

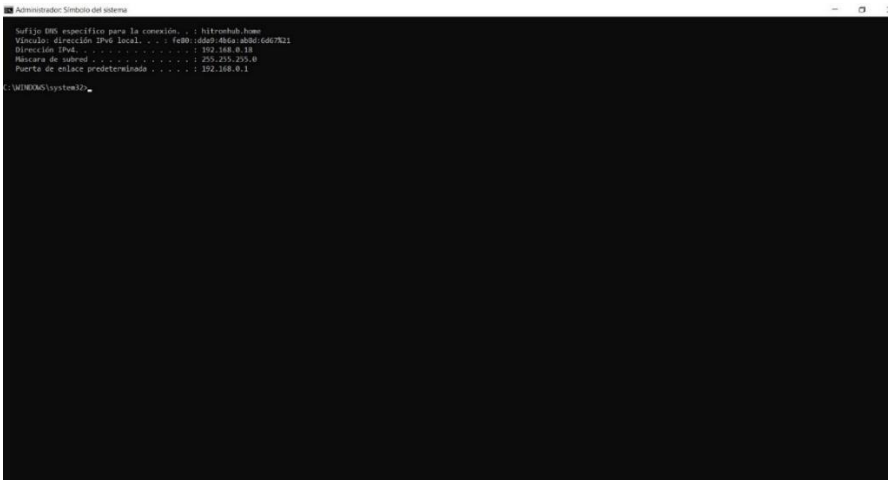
Figura 23 Comando *uname -a* para conocer características del sistema operativo *Kali Linux* instalado como máquina virtual y el comando *lscpu* obtener información detallada sobre de la arquitectura del procesador



Fuente Arturo Ruiz

A continuación, en la máquina con sistema operativo Microsoft Windows y presionando la combinación de teclas CTRL + R se abre la ventana de Ejecutar y en él se escribe CMD, y se digita el comando *ipconfig*, esto para conocer la IP de la máquina.

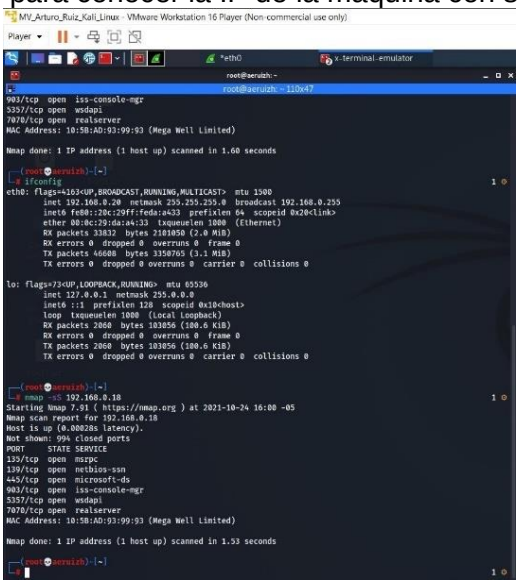
Figura 24 Comando *ipconfig* para conocer la IP de la máquina con sistema operativo *Microsoft Windows*



Fuente Arturo Ruiz

nmap. En la Figura 25. Se abre la terminal y se digita el comando *ifconfig* para conocer la IP de la máquina virtual con sistema operativo *Kali Linux*

Figura 25 Comando *ifconfig* para conocer la IP de la máquina con sistema operativo *Kali Linux*

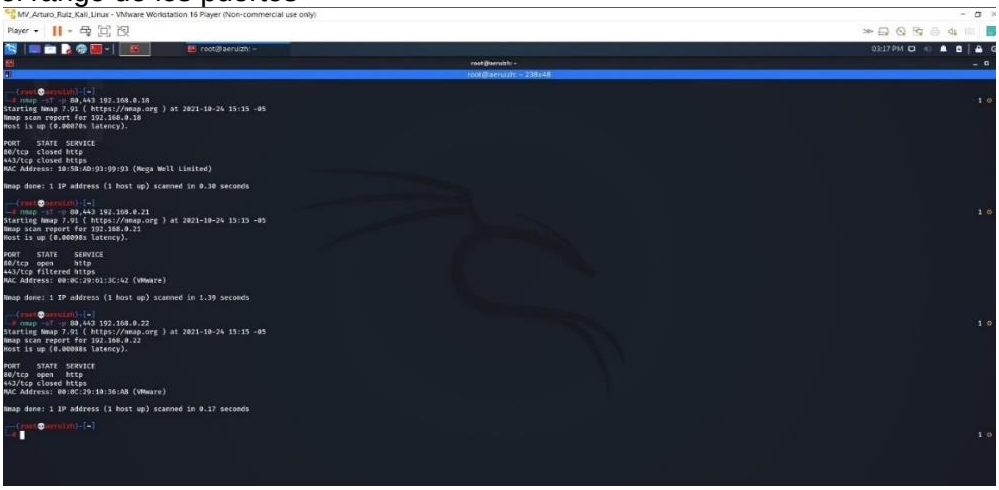


Fuente Arturo Ruiz

En la Figura 26. Una vez iniciada la sesión en el sistema operativo Kali Linux se abre una terminal y como usuario root se digita el comando nmap a tres máquinas virtuales que tienen las direcciones IP: 192.168.0.18, 192.168.021 y 192.168.0.22 se ejecuta el

comando: *nmap -sT -p 80,443 IP_máquina_virtual* para conocer la conexión TCP seguido del rango de los puertos, para el presente caso el 80 y 443:

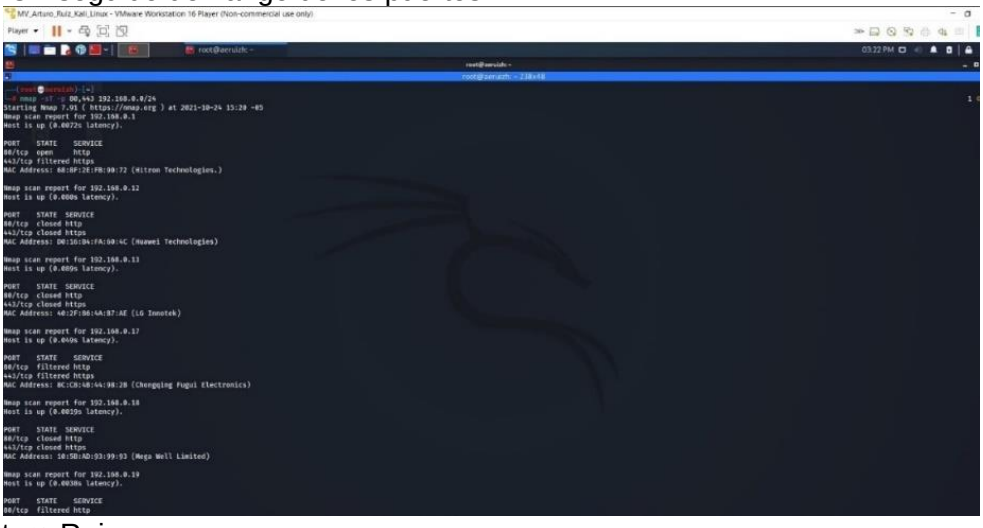
Figura 26 Comando *nmap -sT -p 80,443 IP*_máquina_virtual para conocer la conexión TCP seguido del rango de los puertos



Fuente Arturo Ruiz

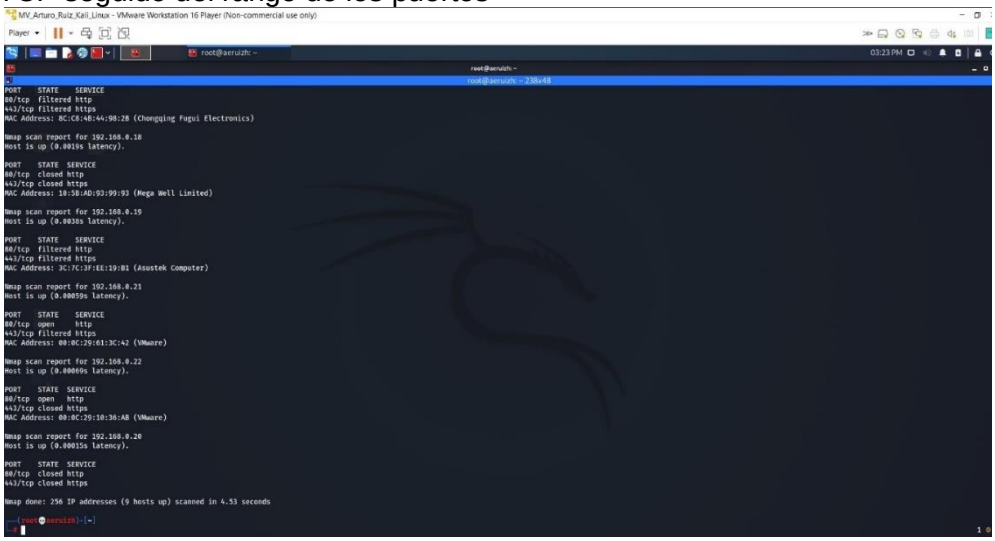
En las Figuras 27 y 28. Se observa otra variación en la ejecución del comando se puede realizar así: *nmap -sT -p 80,443 192.168.0.0/24* como se observa en las siguientes figuras:

Figura 27 Variación del comando nmap -sT -p 80,443 IP_máquina_virtual para conocer la conexión TCP seguido del rango de los puertos



Fuente Arturo Ruiz

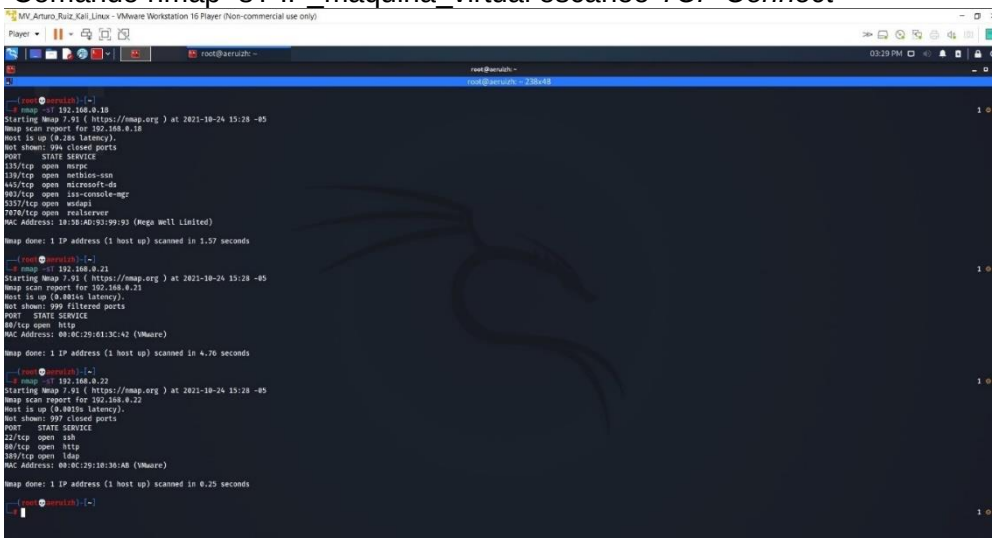
Figura 28 Variación del comando *nmap -sT -p 80,443 IP*_máquina_virtual para conocer la conexión TCP seguido del rango de los puertos



Fuente Arturo Ruiz

En la Figura 29. Se realiza la ejecución del comando nmap -sT IP_máquina_virtual, es escaneo TCP Connect

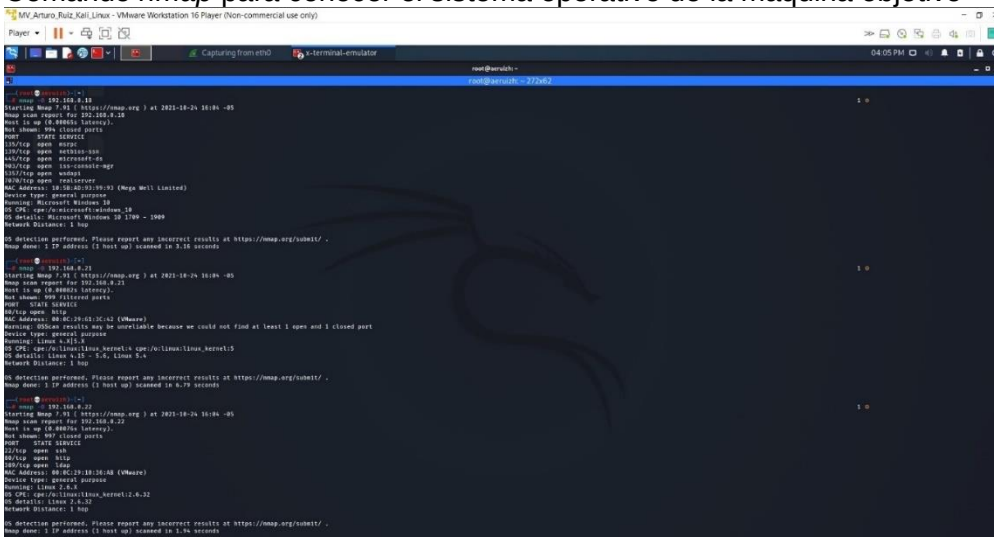
Figura 29 Comando nmap -sT IP_máquina_virtual escaneo *TCP Connect*



Fuente Arturo Ruiz

En la Figura 30. Se ejecuta el comando para conocer el sistema operativo de la máquina objetivo: *nmap -O IP_máquina_virtual*

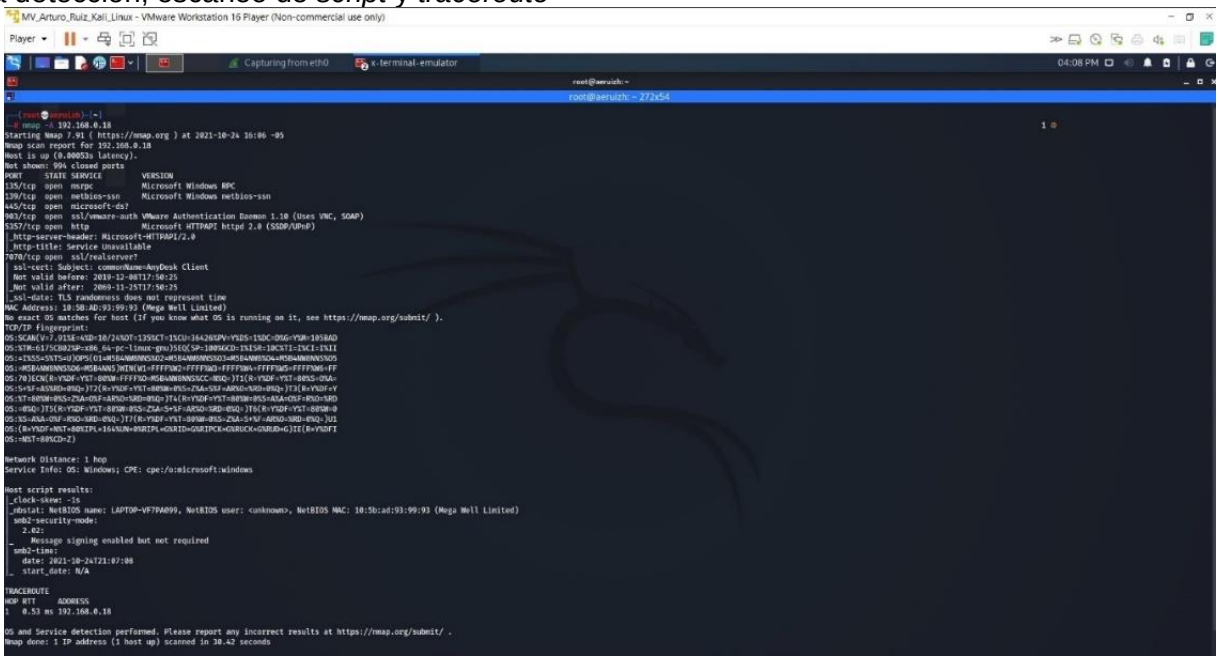
Figura 30 Comando *nmap* para conocer el sistema operativo de la máquina objetivo



Fuente Arturo Ruiz

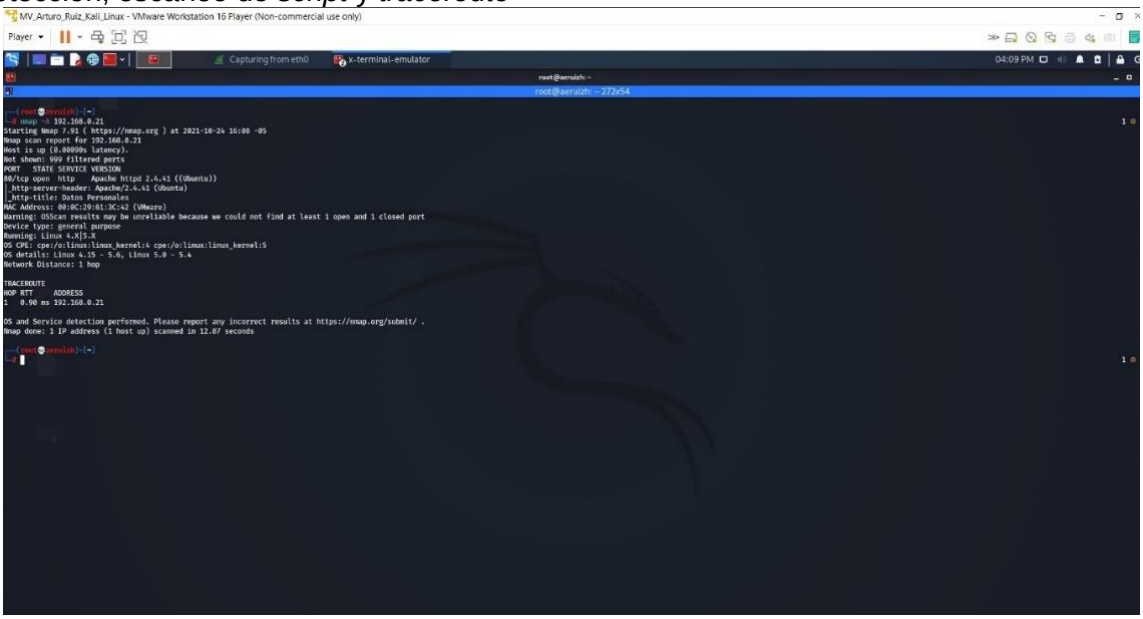
En las Figuras 31, 32 y 33. Se ejecuta el comando nmap para conocer detección de sistema operativo habilitado, versión de la detección, escaneo de script y traceroute: *nmap -A IP_máquina_virtual*

Figura 31 Comando *nmap* para conocer detección de sistema operativo habilitado, versión de la detección, escaneo de *script* y *traceroute*



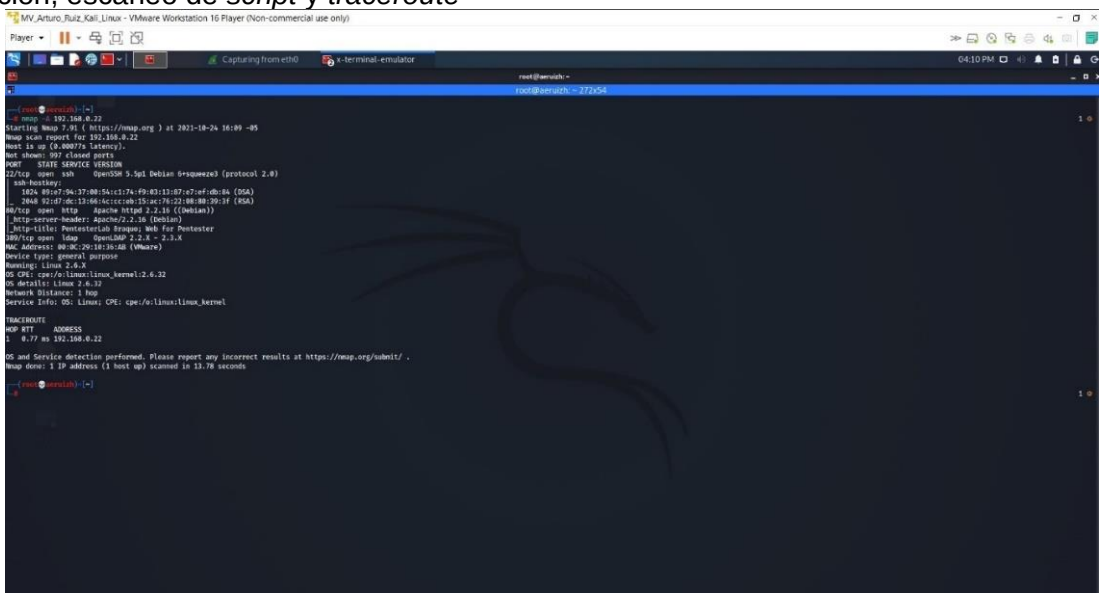
Fuente Arturo Ruiz

Figura 32 Comando *nmap* para conocer detección de sistema operativo habilitado, versión de la detección, escaneo de *script* y *traceroute*



Fuente Arturo Ruiz

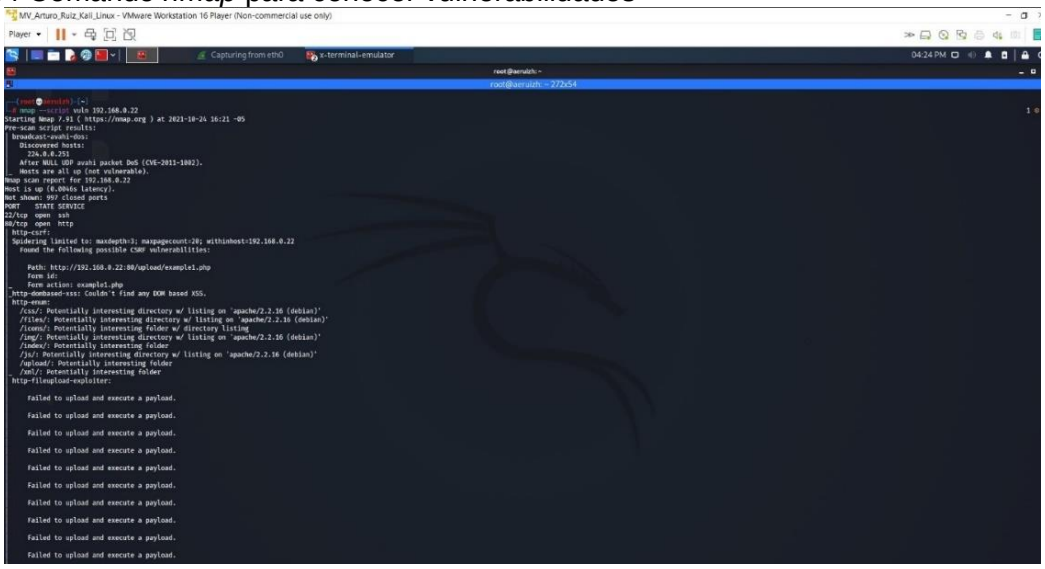
Figura 33 Comando *nmap* para conocer detección de sistema operativo habilitado, versión de la detección, escaneo de *script* y *traceroute*



Fuente Arturo Ruiz

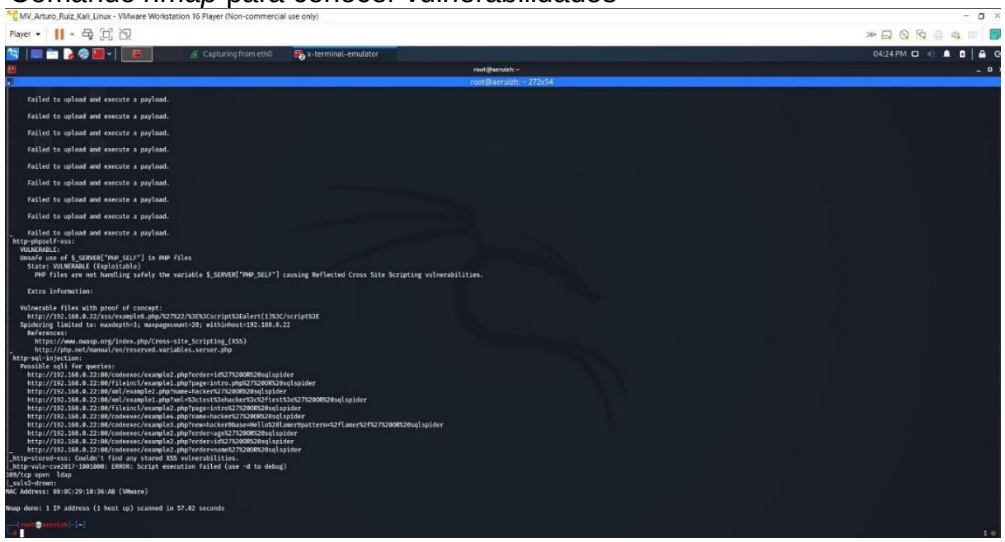
En la Figura 34 y 35. Se ejecuta el comando nmap para conocer vulnerabilidades: *nmap –script vuln IP_máquina_virtual*

Figura 34 Comando *nmap* para conocer vulnerabilidades



Fuente Arturo Ruiz

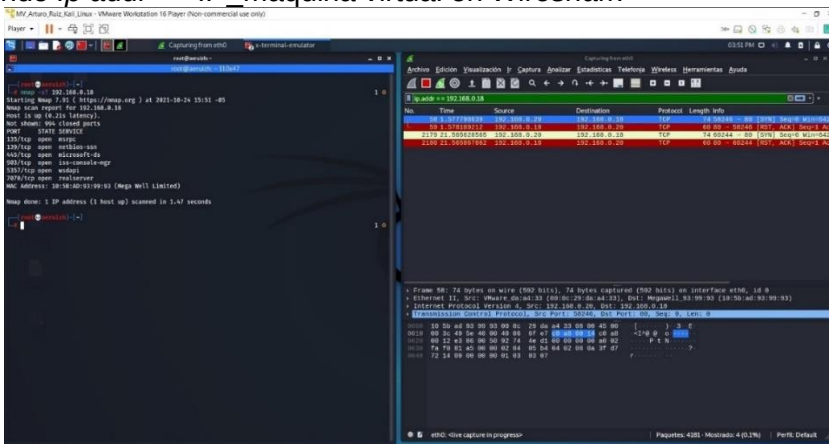
Figura 35 Comando *nmap* para conocer vulnerabilidades



Fuente Arturo Ruiz

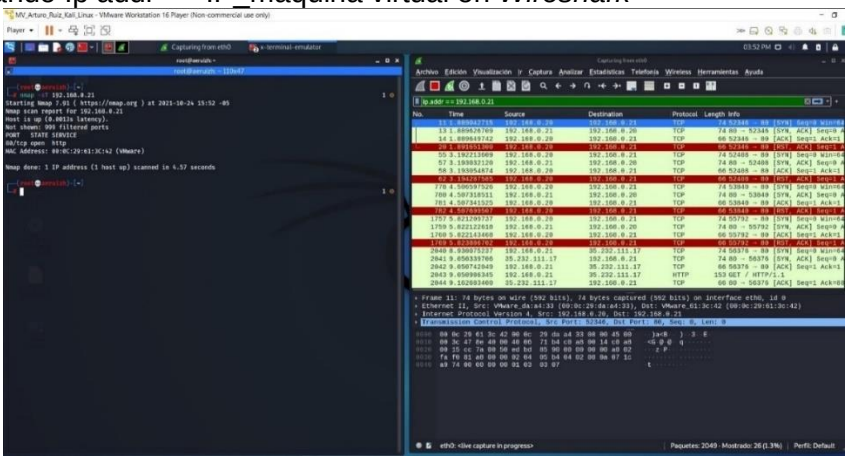
Wireshark. En las Figuras 36, 37 y 38. Una vez ejecutado el comando *nmap* se abre la herramienta *Wireshark* que nos permitirá realizar análisis sobre paquetes de red, aquí se digita en la terminal el comando *Ip addr == IP_máquina virtual*, para cada máquina virtual:

Figura 36 Comando *Ip addr == IP*_máquina virtual en *Wireshark*



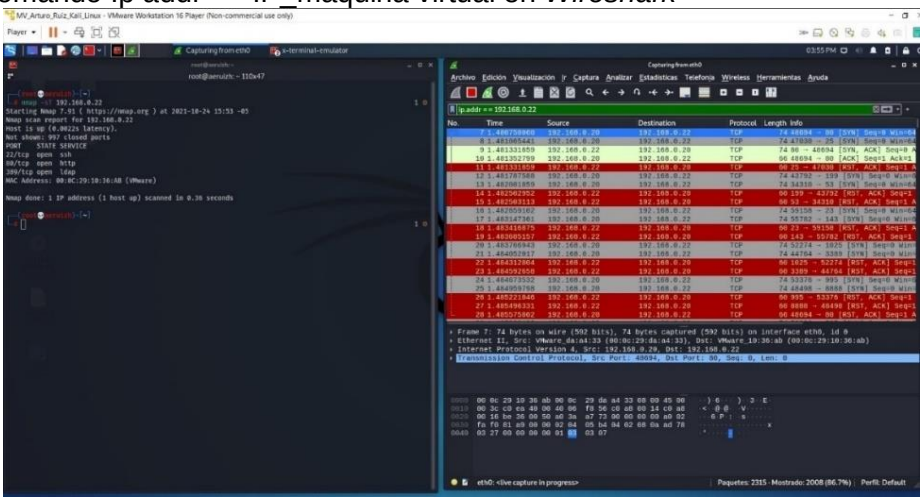
Fuente Arturo Ruiz

Figura 37 Comando Ip addr == IP_máquina virtual en *Wireshark*



Fuente Arturo Ruiz

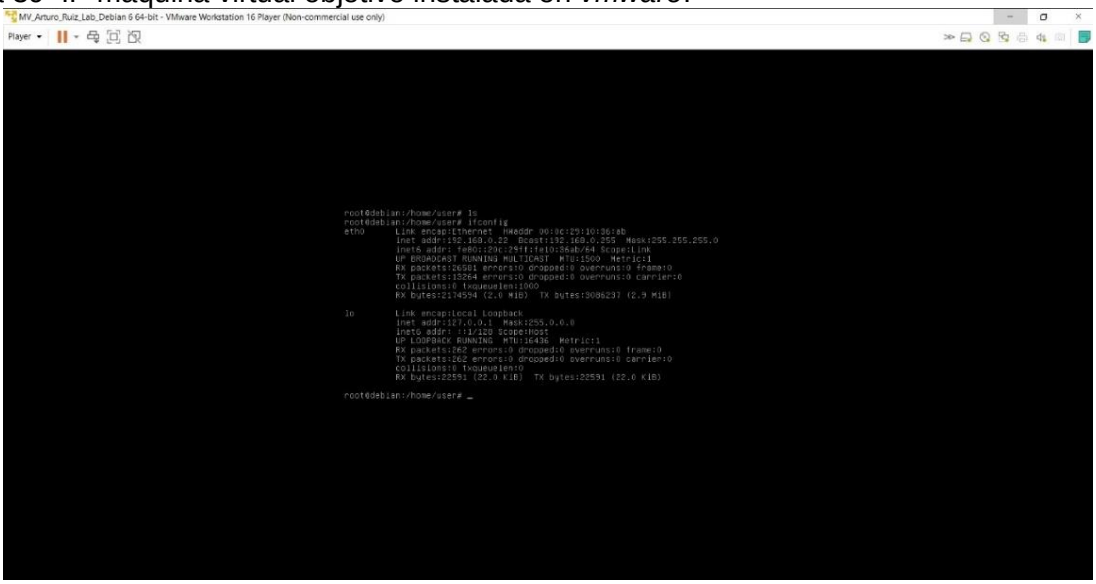
Figura 38 Comando Ip addr == IP_máquina virtual en *Wireshark*



Fuente Arturo Ruiz

SqlImap. En la Figura 39. Se observa la IP de la máquina virtual objetivo instalada en *vmware*.

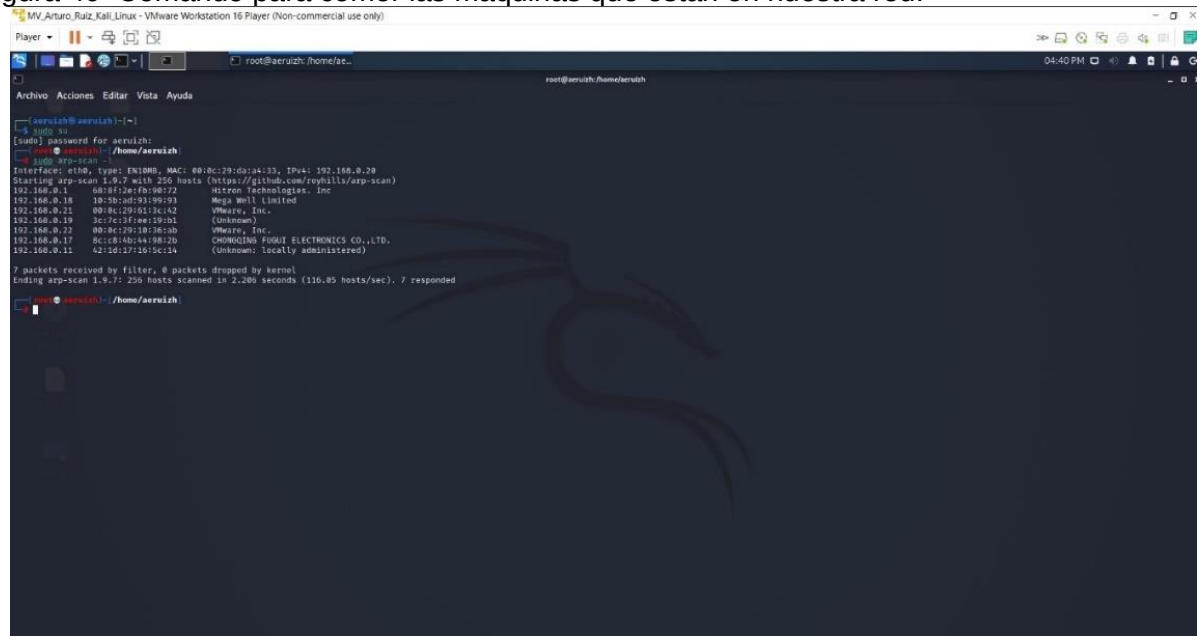
Figura 39 IP máquina virtual objetivo instalada en *vmware*.



Fuente Arturo Ruiz

En la Figura 40. Con el comando sudo *arp-scan -l* se conocen las máquinas que están dentro de nuestra red.

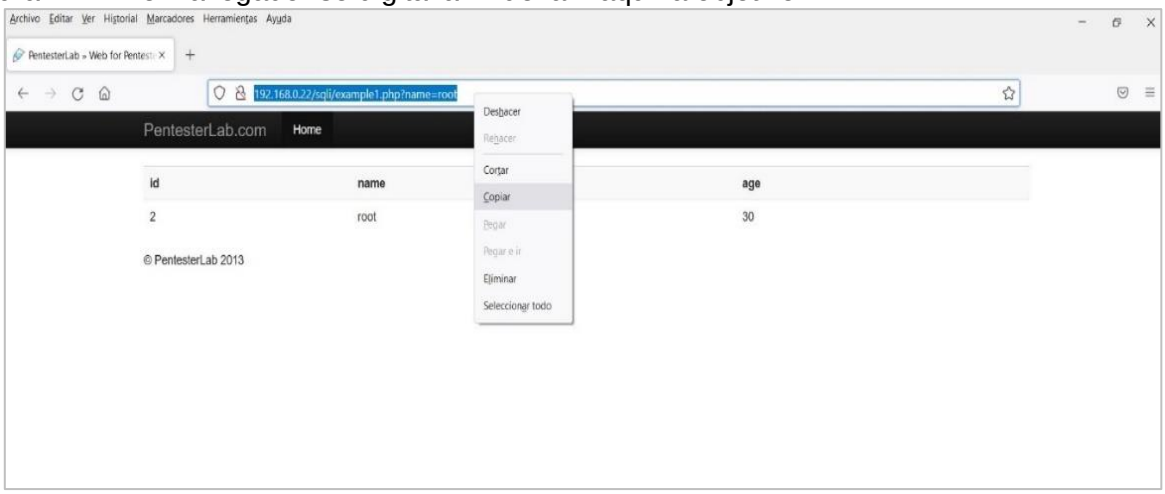
Figura 40 Comando para comer las máquinas que están en nuestra red.



Fuente Arturo Ruiz

En la Figura 41. Con la IP de la máquina virtual objetivo se digita en el navegador, esta se copia para situarla en la terminal de Kali Linux.

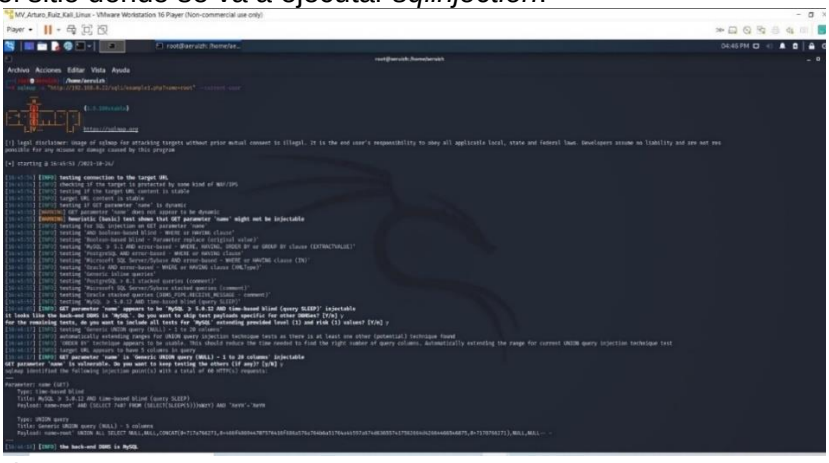
Figura 41 En el navegador se digita la IP de la máquina objetivo.



Fuente Arturo Ruiz

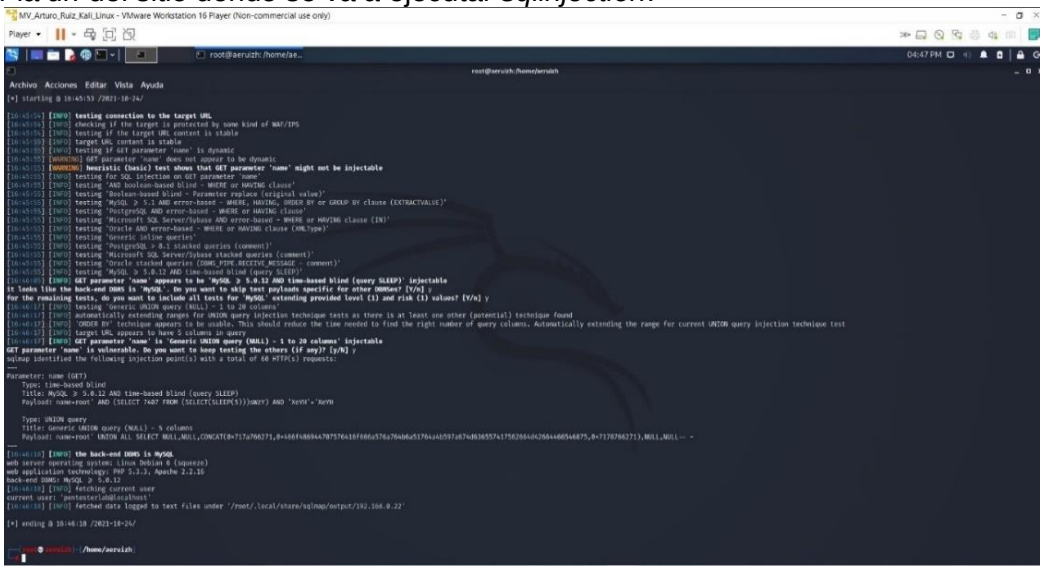
En las Figuras 42 y 43. Se observa la dirección copiada del navegador se pega en la terminal así: *sqlmap -u "IP_máquina_virtual" –current-user*, el parámetro -u sirve para conectar la *url* del sitio donde se va a ejecutar *sqlinjection*. El parámetro *–current-user* para saber cuál es el usuario actual, el que está conectado a la base de datos.

Figura 42 Comando: sqlmap -u "IP_máquina_virtual" *–current-user*, el parámetro -u sirve para conectar la *url* del sitio donde se va a ejecutar *sqlinjection*.



Fuente Arturo Ruiz

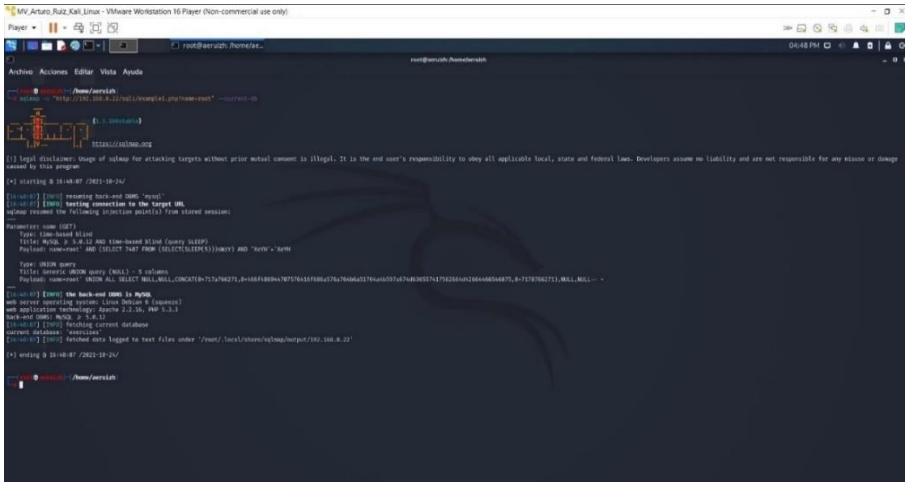
Figura 43 Comando: *sqlmap -u "IP*_máquina_virtual" *–current-user*, el parámetro -u sirve para conectar la *url* del sitio donde se va a ejecutar *sqlinjection*.



Fuente Arturo Ruiz

En la Figura 44. Se observa el comando: *sqlmap -u "IP_máquina_virtual" –current-db*, el parámetro -db sirve para saber cuál es la base de datos a la cual se está conectado:

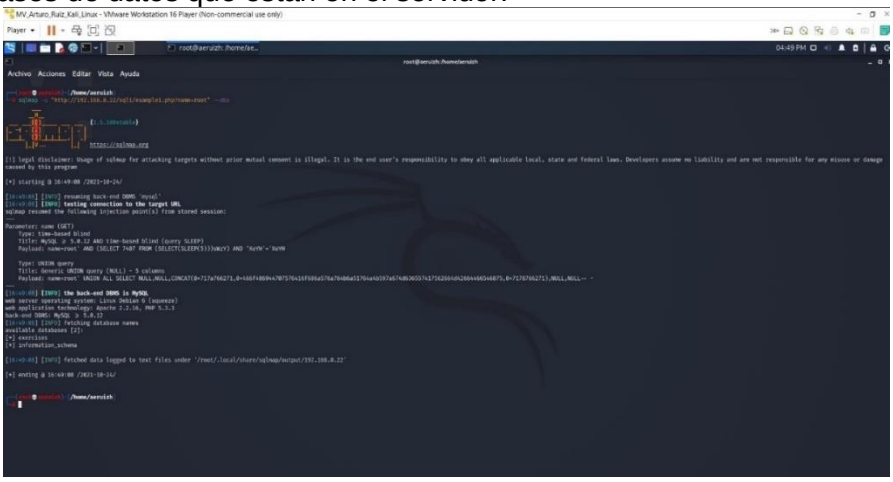
Figura 44 Comando: sqlmap -u "IP_máquina_*virtual*" *–current-db*, el parámetro -db sirve para saber cuál es la base de datos a la cual se está conectado.



Fuente Arturo Ruiz

En la Figura 45. Se observa el Comando: *sqlmap -u "IP_máquina_virtual" --dbs*: este comando sirve para que nos muestre las bases de datos que están en el servidor.

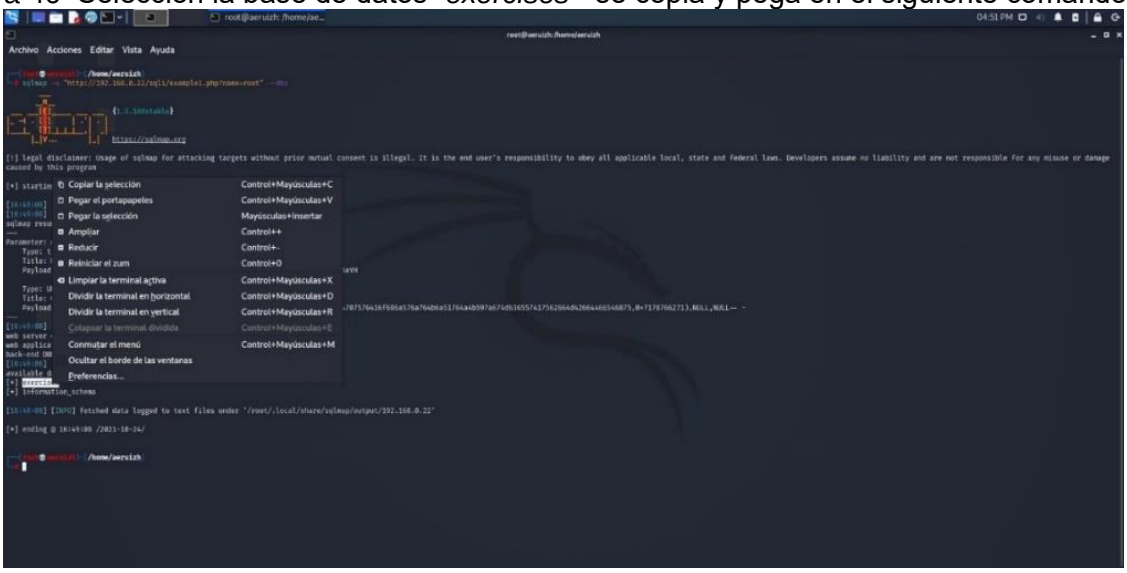
Figura 45 Comando: *sqlmap* -u “IP_máquina_virtual” --*dbs*: este comando sirve para que nos muestre las bases de datos que están en el servidor.



Fuente Arturo Ruiz

En la Figura 46. Se puede observar en esta parte que se selecciona la base de datos “exercises” se copia y pega en el siguiente comando.

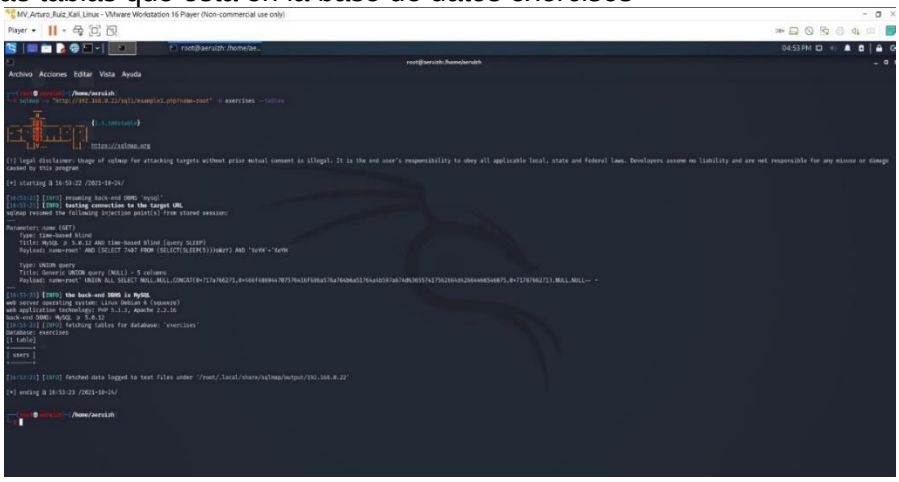
Figura 46 Selección la base de datos “*exercises*” se copia y pega en el siguiente comando.



Fuente Arturo Ruiz

En la Figura 47. Se observa el Comando: *sqlmap -u “IP_máquina_virtual” -D exercises --tables*: este comando nos muestra las tablas que está en la base de datos *exercises*.

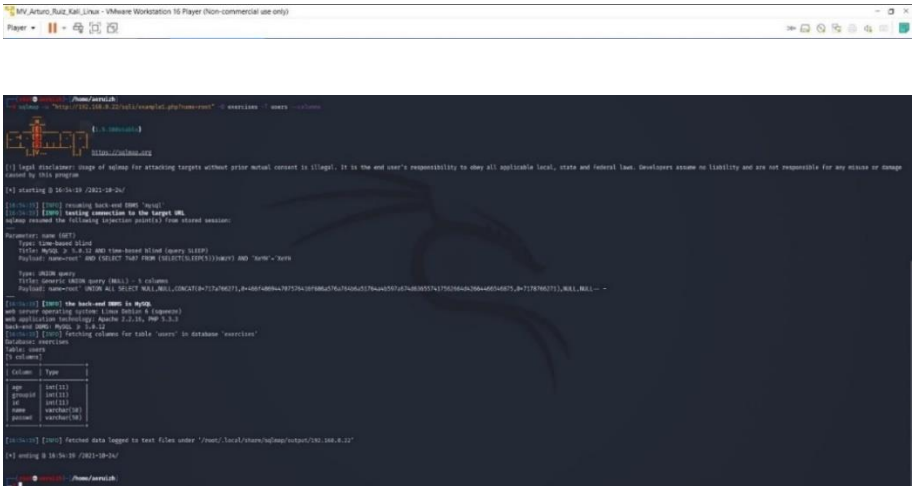
Figura 47 El Comando: *sqlmap* -u “IP_máquina_virtual” -D *exercises* --tables: este comando nos muestra las tablas que está en la base de datos *exercises*



Fuente Arturo Ruiz

En la Figura 48. Se observa el Comando: sqlmap -u “IP_máquina_virtual”-d exercises -T users –columns: para que nos muestre todas las columnas de la tabla users.

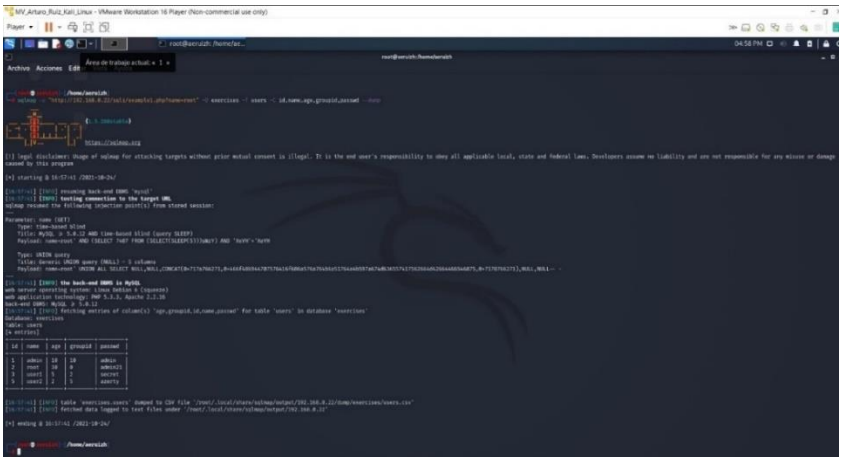
Figura 48 El Comando: *sqlmap* -u “IP_máquina_virtual” -d *exercises* -T *users –columns*: para que nos muestre todas las columnas de la tabla *users*



Fuente Arturo Ruiz

En la Figura 49. Se observa el Comando: *sqlmap -u “IP_máquina_virtual” -d exercises -T users, -C id,name,age,groupid,passwd –dump*: con el parámetro -C sirve para poder detallar el nombre de la columna y *--dump* para poder extraer todo el contenido de la columna como se muestra en la base de datos.

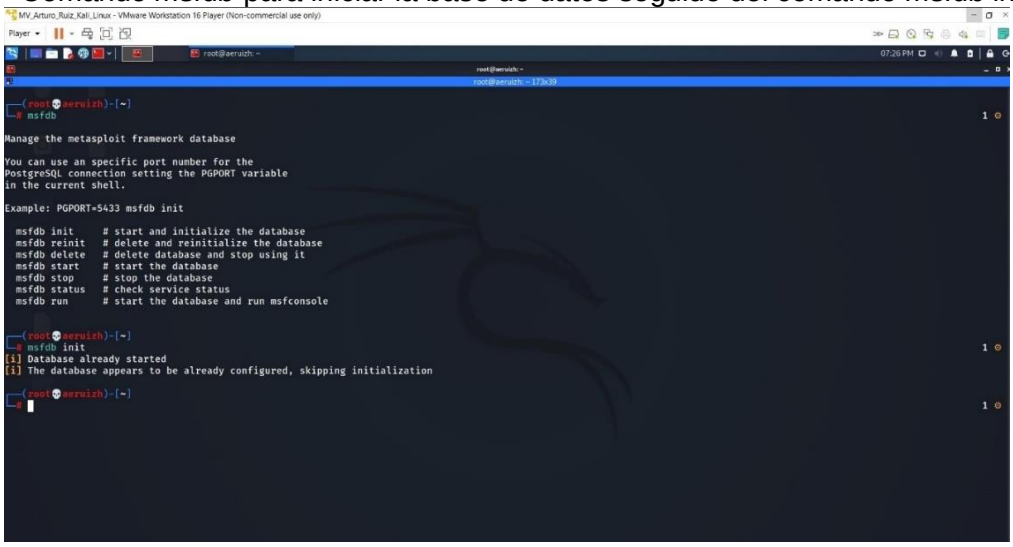
Figura 49 El Comando: sqlmap -u “IP_máquina_virtual” -d *exercises* -T *users*, -C *id,name,age,groupid,passwd*: con el parámetro -C sirve para poder detallar el nombre de la columna y --dump para poder extraer todo el contenido de la columna como se muestra en la base



Fuente Arturo Ruiz

***Metasploit Framework*.** En la Figura 50. Para iniciar la base de datos de *metasploit* se ejecuta en la terminal el comando *msfdb* y muestra todas las opciones que se tienen y se ejecuta el comando *msfdb init* y se inicia la base de datos:

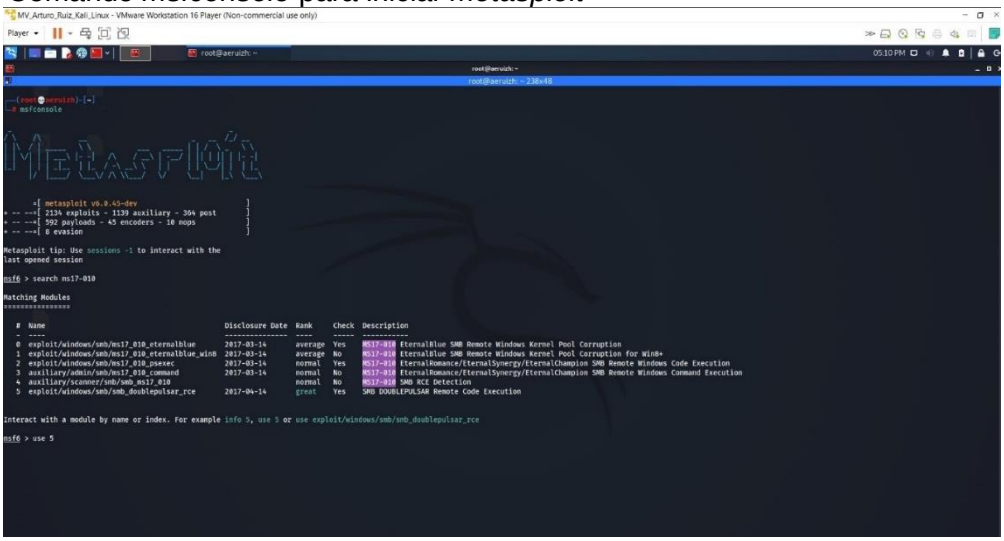
Figura 50 Comando *msfdb* para iniciar la base de datos seguido del comando *msfdb init*



Fuente Arturo Ruiz

En la Figura 51. Para iniciar *metasploit* se digita el comando *msfconsole*

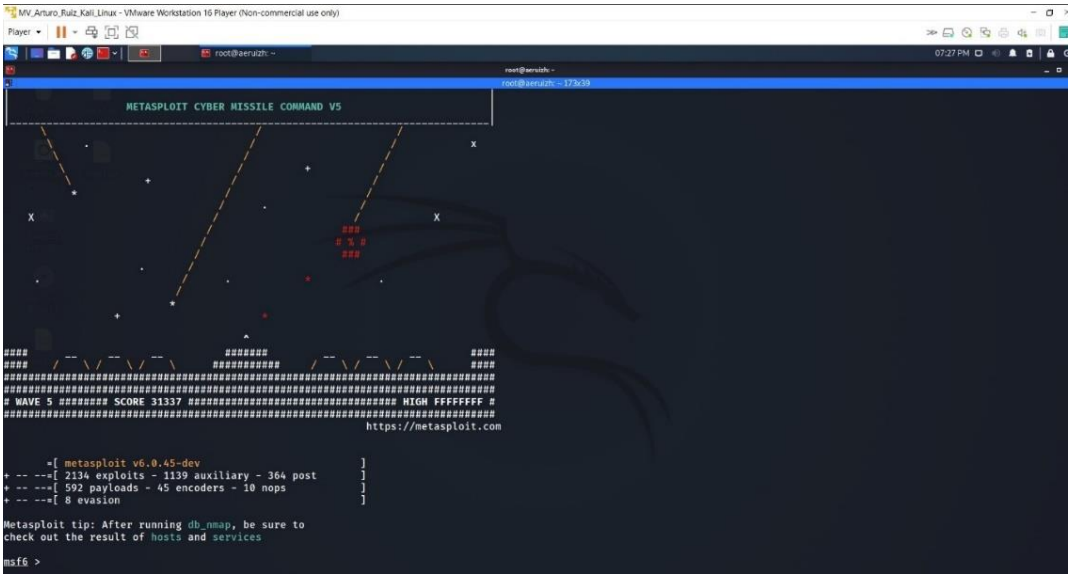
Figura 51 Comando *msfconsole* para iniciar *metasploit*



Fuente Arturo Ruiz

En la Figura 52. Se observa que cuando se inicia *metasploit* aparece un banner donde da la información del número de *exploits, payloads, encoders* y evasión.

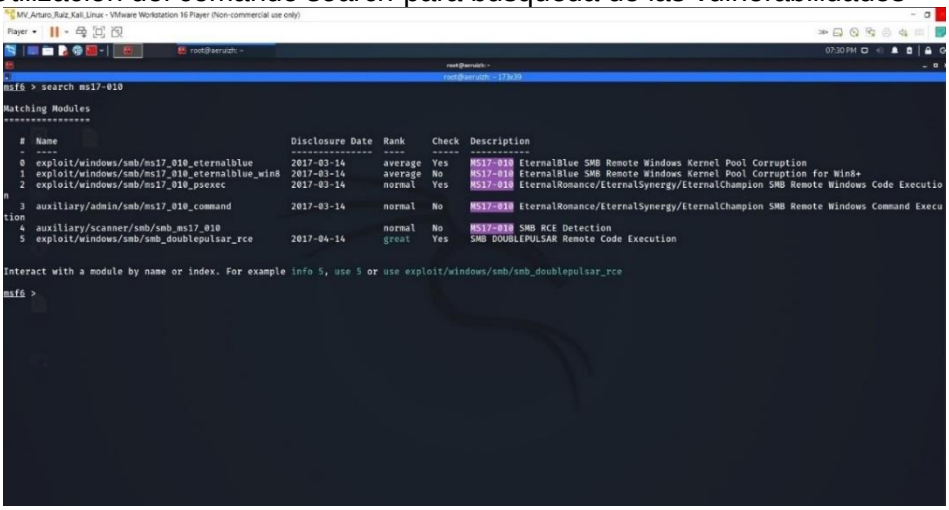
Figura 52 *Banner* de información del número de versión, *exploits, payloads, encoders* y *evasión*.



Fuente Arturo Ruiz

En la Figura 53. Se realiza la búsqueda a través del comando *search,* para tomar como ejemplo la vulnerabilidad ms17-010

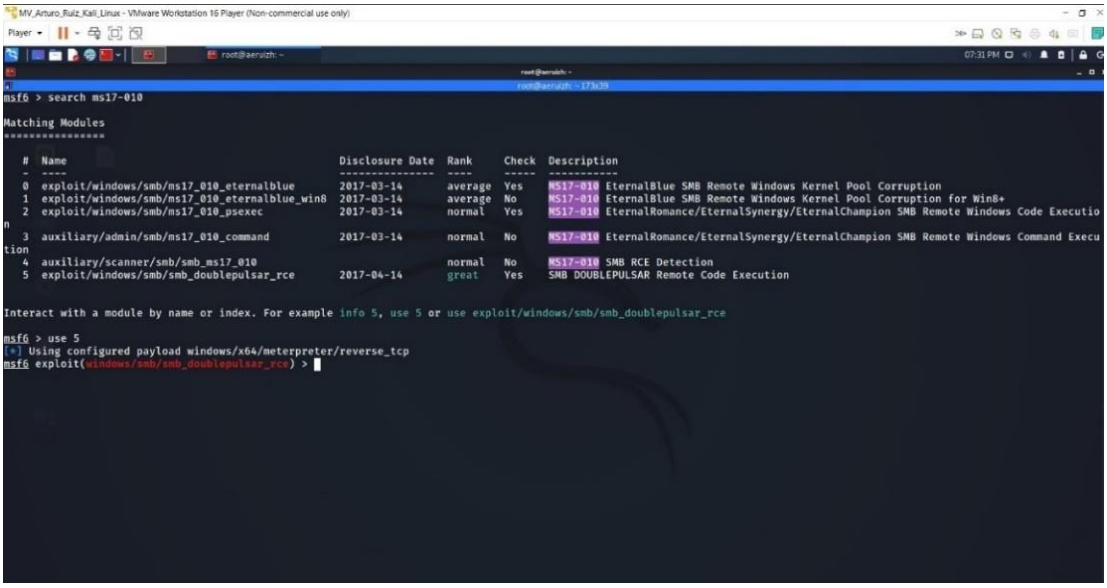
Figura 53 Utilización del comando *search* para búsqueda de las vulnerabilidades



Fuente Arturo Ruiz

En la Figura 54. Con el comando *search* se despliegan las opciones y muestra que la vulnerabilidad presente es *EternalBlue* exhibiendo varias opciones. Se digita el comando use y se sitúa el número del *exploit*, para el presente ejemplo el número 5, se presiona *enter* y aparece el módulo.

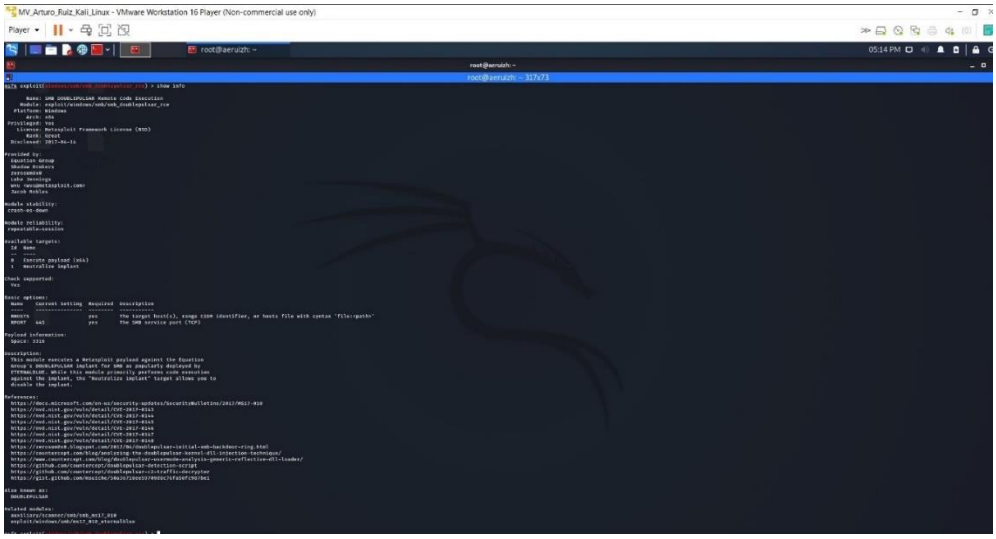
Figura 54 Opciones y descripción de la vulnerabilidad y selección del módulo usando el comando *use*.



Fuente Arturo Ruiz

En la Figura 55. Con el comando *show info* muestra documentación e información sobre el módulo

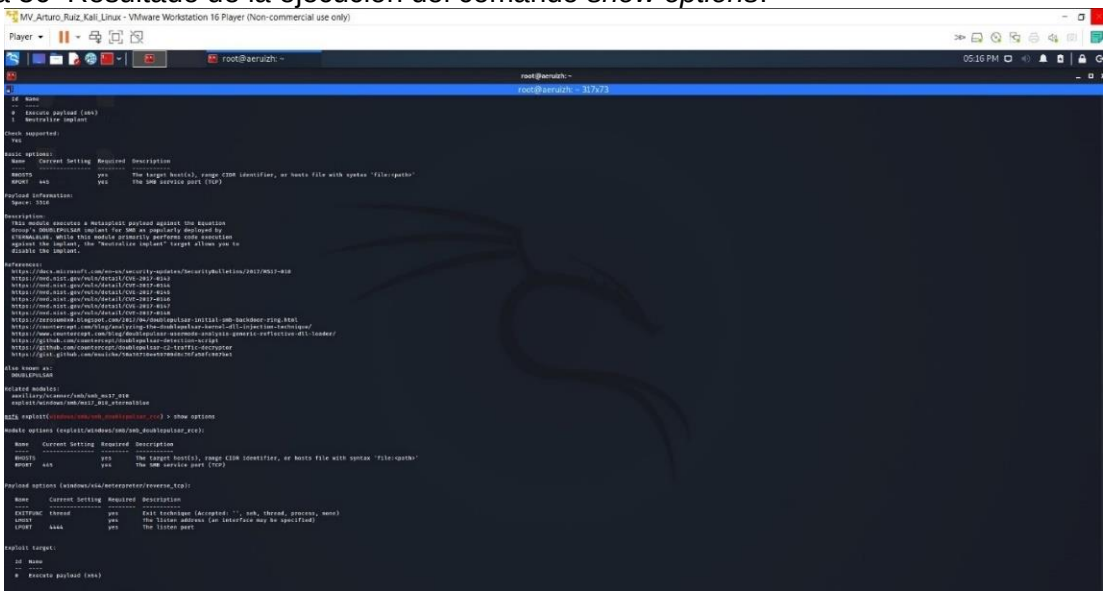
Figura 55 Comando *show info* muestra documentación e información sobre el módulo



Fuente Arturo Ruiz

En la Figura 56. Con el comando *show options* muestra la configuración que se tiene que hacer para el ataque, muestra el payload el target, el puerto.

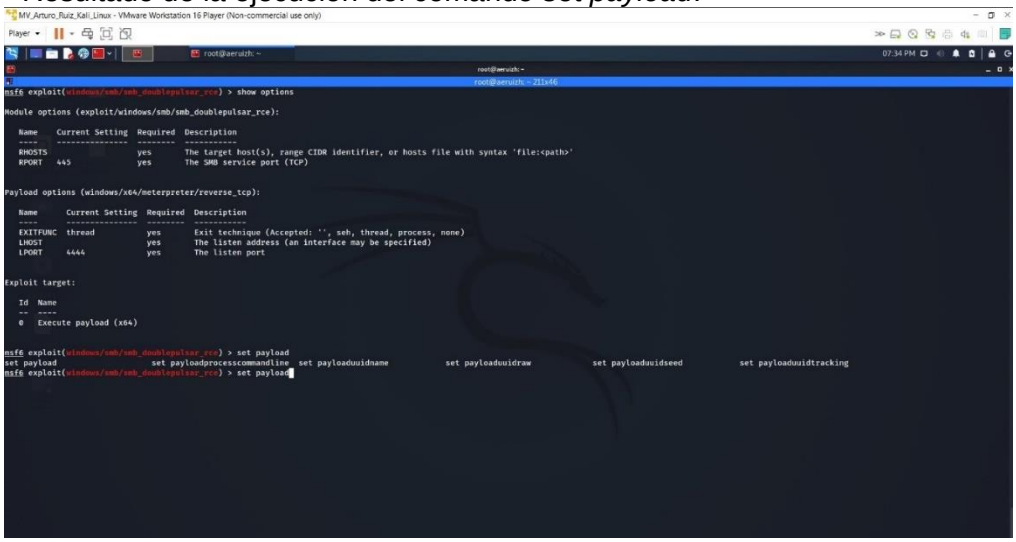
Figura 56 Resultado de la ejecución del comando *show options*.



Fuente Arturo Ruiz

En la Figura 57. Para cambiar el *payload* se digita el comando *set payload*

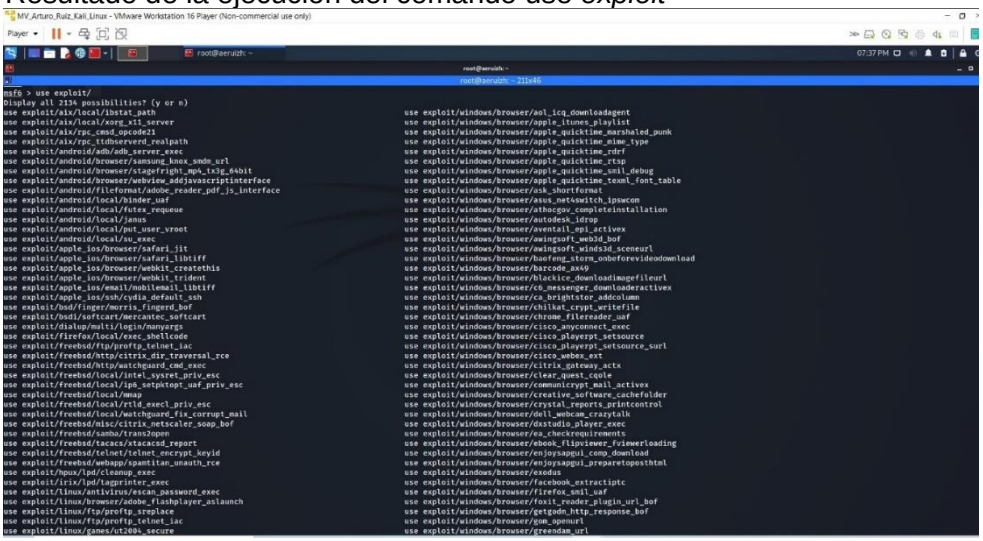
Figura 57 Resultado de la ejecución del comando set *payload*.



Fuente Arturo Ruiz

En la Figura 58. Con el comando use exploit se selecciona el módulo.

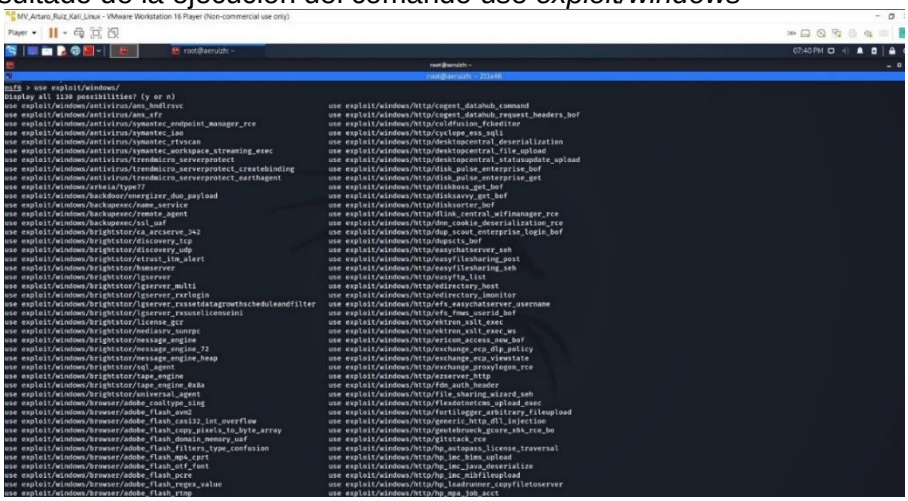
Figura 58 Resultado de la ejecución del comando use *exploit*



Fuente Arturo Ruiz

En la Figura 59. Se puede igualmente ejecutar el comando use *exploit/windows* para desplegar las opciones.

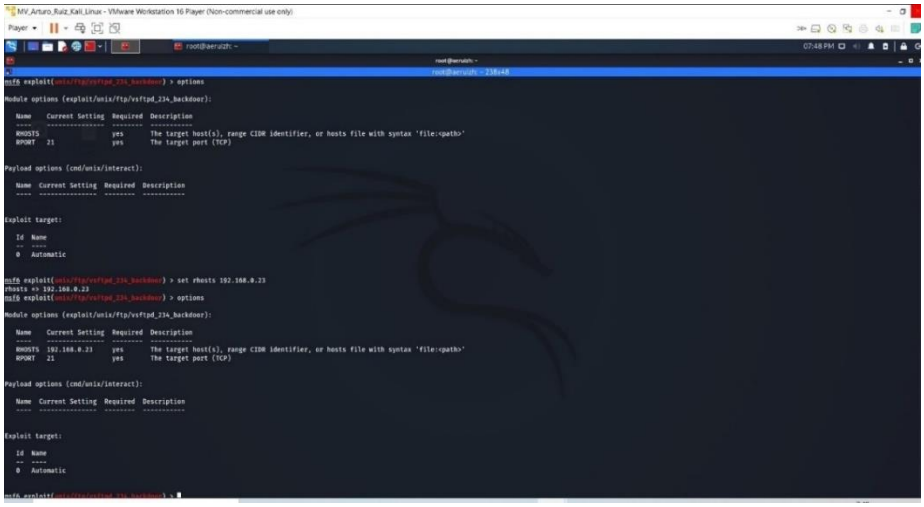
Figura 59 Resultado de la ejecución del comando use *exploit/windows*



Fuente Arturo Ruiz

En la Figura 60. Cuando se selecciona y se visualiza la vulnerabilidad se cambia el RHOST utilizando el comando ***set rhosts** “IP_máquina_virtual”*, se presiona enter y luego el comando *options.*

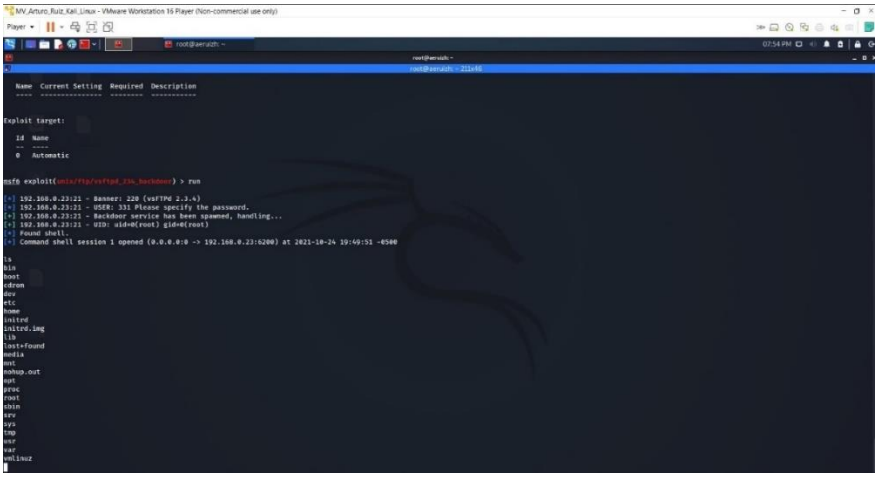
Figura 60 Ejecución del comando donde se visualiza el resultado de la IP de la máquina *metasploitable*.



Fuente Arturo Ruiz

En la Figura 61. Con la ejecución del *exploit* digitando el comando *run* donde muestra la información del banner, usuario y el inicio como usuario *root*; seguido a esto se digita el comando *ls* para conocer la entrada al directorio.

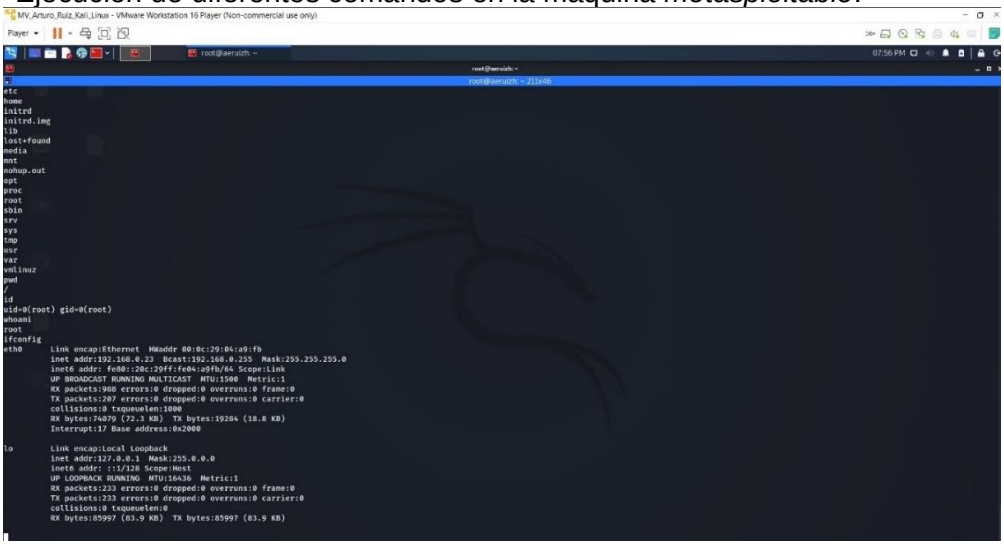
Figura 61 Resultado de la ejecución del comando *run* y *ls* donde muestra las opciones del directorio



Fuente Arturo Ruiz

En la Figura 62. Con la ejecución del comando *pwd, Id, whoami* e *ifconfig* para conocer la IP de la máquina *metasploitable*.

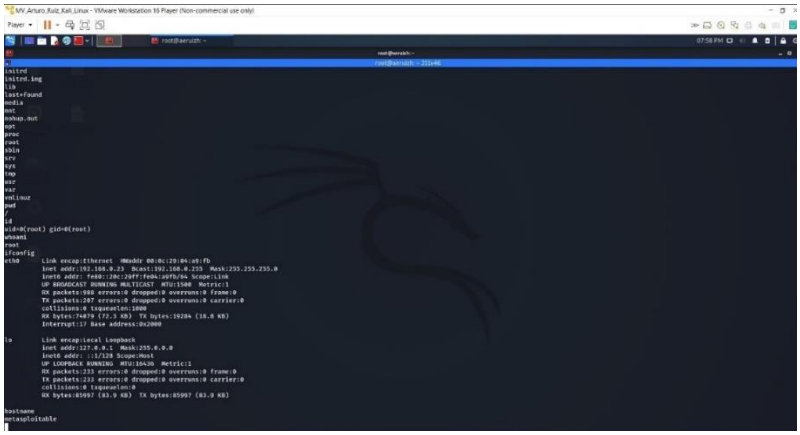
Figura 62 Ejecución de diferentes comandos en la máquina *metasploitable*.



Fuente Arturo Ruiz

En la Figura 63. Con la ejecución del comando *hostname* para conocer el nombre de la máquina; en este momento ya se tiene el control de la máquina.

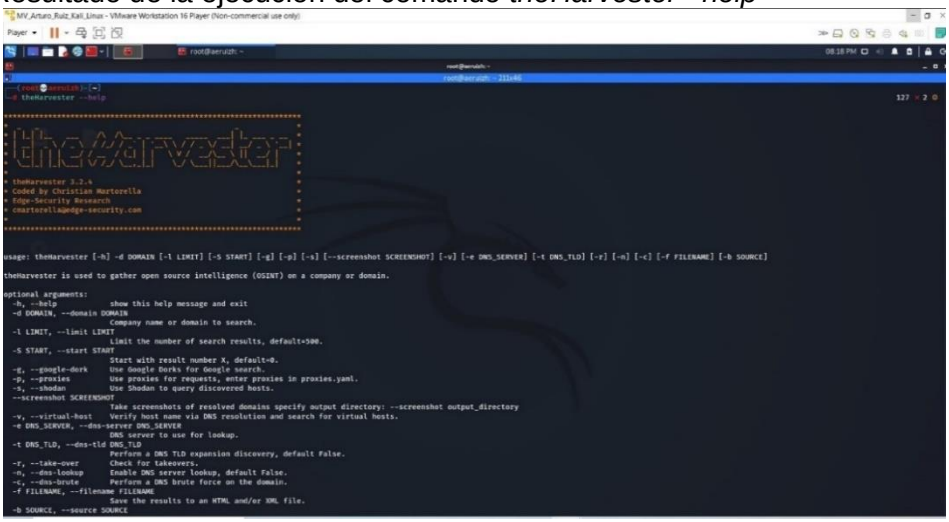
Figura 63 Resultado de la ejecución del comando *hostname* en donde se observa el nombre de la máquina



Fuente Arturo Ruiz

***theHarvester*.** Esta herramienta se usa para enumeración, en la Figura 64. Se digita el comando *theHarvester –help* para visualizar las ayudas que tiene la herramienta. Con la opción *-d*, es para iniciar la búsqueda del dominio, -l es para establecer un límite en las búsquedas, *-b* es para establecer búsquedas como *Google, Bing*, entre otros e inclusive la opción *-s* es para integrarla con *Shodan*.

Figura 64 Resultado de la ejecución del comando *theHarvester –help*

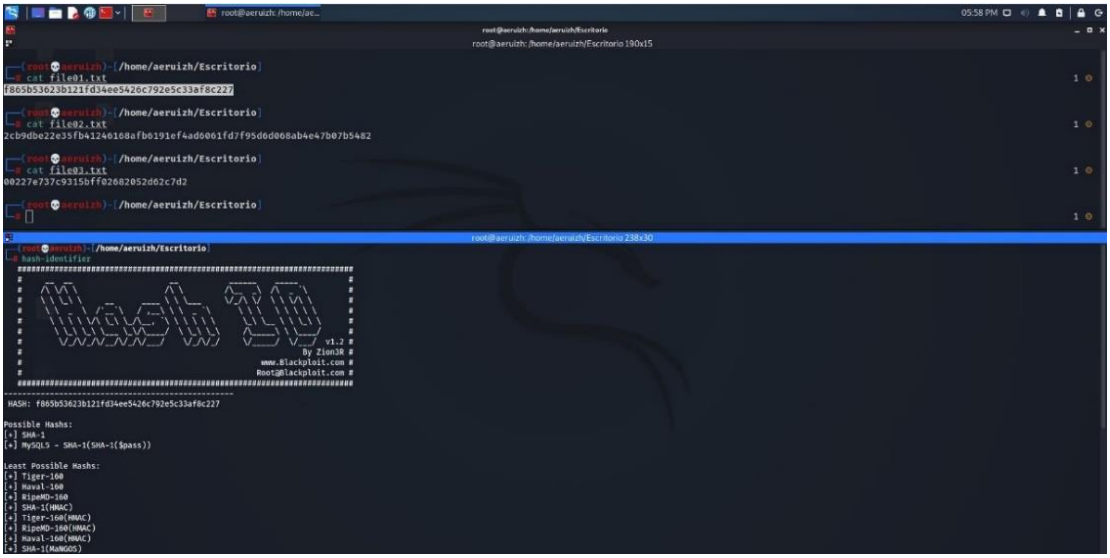


Fuente Arturo Ruiz

***John The Ripper*.** En la Figura 65. En la ejecución de esta herramienta, previamente se han configurado tres archivos: *file01.txt, file02.txt* y *file03.txt*, en la termina y con el

comando *hash-identifier*, se copia y pega el hash para identificar las posibles opciones de hash con las cuales fue configurado el archivo.

Figura 65 Ejecución del comando *hash-identifier* que nos arroja como resultado el posible *hash SHA-1*



Fuente Arturo Ruiz

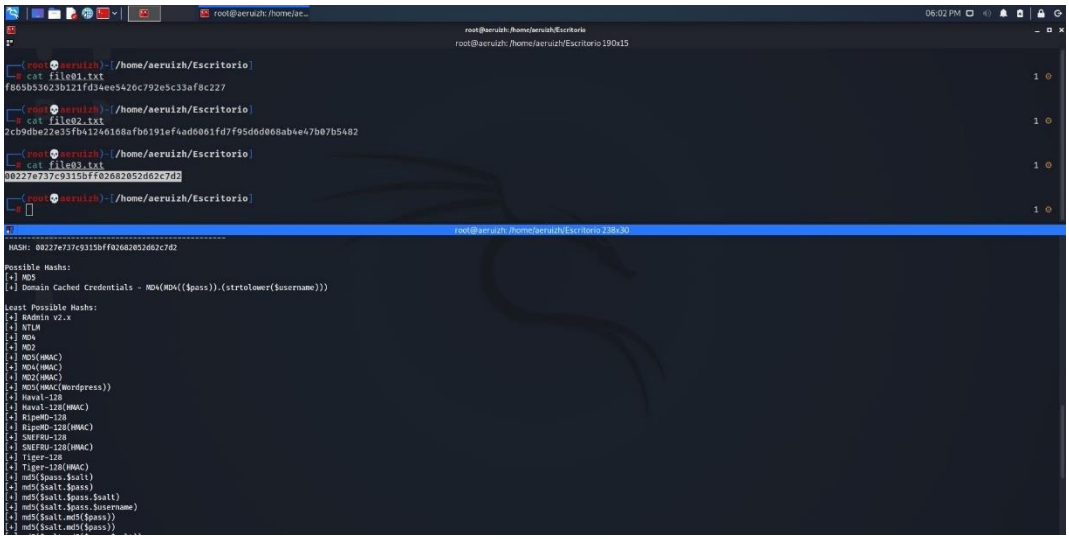
En la Figura 66. Se ejecuta el comando *hash-identifier* que nos arroja como resultado el posible *hash SHA-256*

Figura 66 Ejecución del comando *hash-identifier* que nos arroja como resultado el posible *hash SHA-256*

Fuente Arturo Ruiz

En la Figura 67. Se ejecuta el comando *hash-identifier* que nos arroja como resultado el posible *hash MD5*

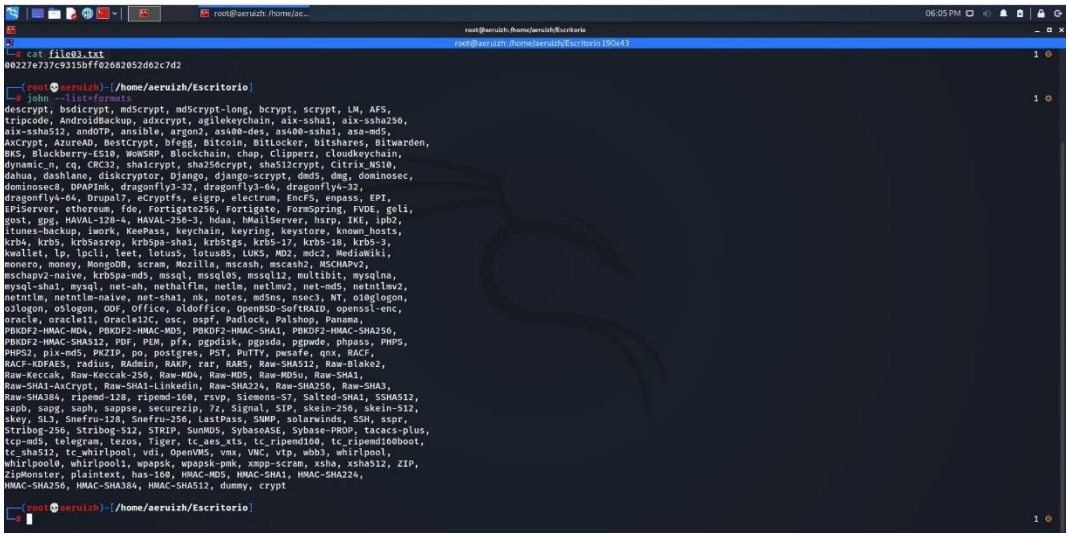
Figura 67 Ejecución del comando *hash-identifier* que nos arroja como resultado el posible *hash* MD5



Fuente Arturo Ruiz

En la Figura 68. Se ejecuta en la terminal el comando *john –list=formats* para conocer el formato del hash

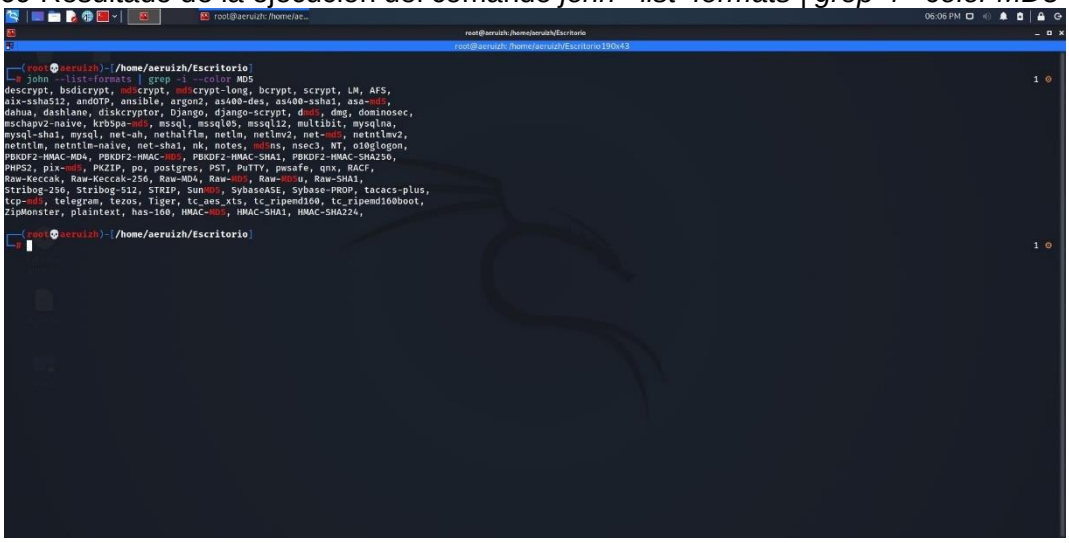
Figura 68 Resultado de la ejecución del comando *john –list=formats* que nos arroja como resultado los diferentes formatos del *hash*



Fuente Arturo Ruiz

En la Figura 69. Se ejecuta el comando *john –list=formats | grep -i --color MD5* nos da en color rojo las diferentes opciones para este tipo de *hash*.

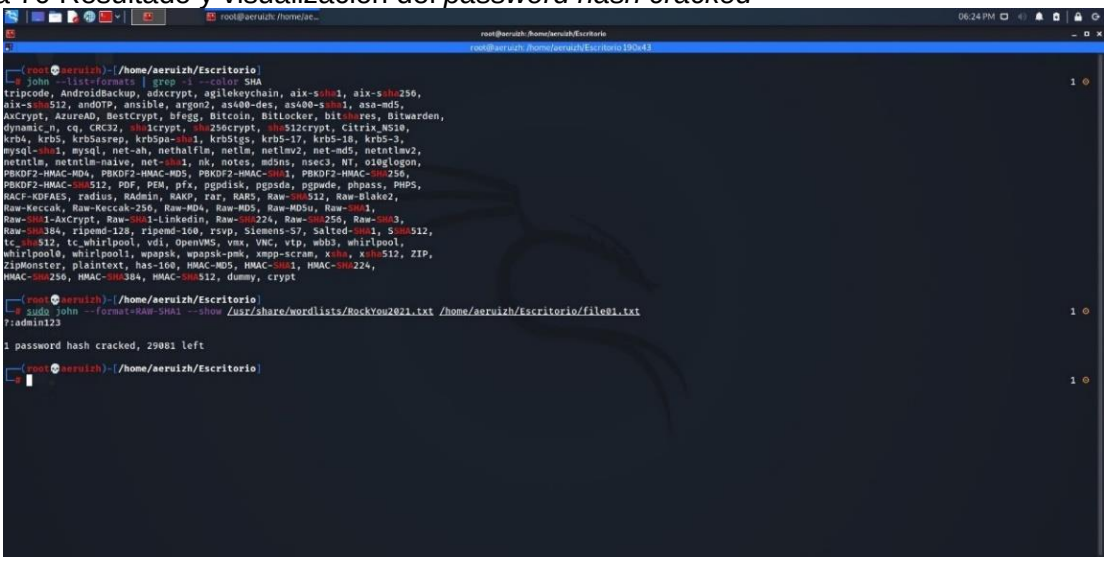
Figura 69 Resultado de la ejecución del comando *john –list=formats | grep -i --color MD5*



Fuente Arturo Ruiz

En la Figura 70. Se observa el resultado de la ejecución del comando sudo *john –format=RAW-SHA1--show/usr/share/wordlists/RockYou2021.txt /home/aeruizh/Escritorio/file01.txt*

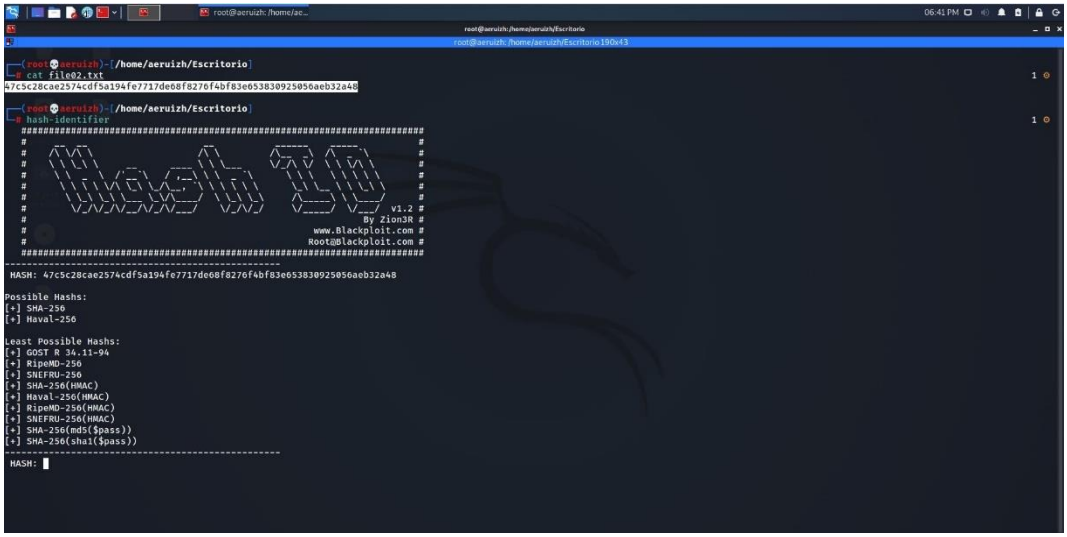
Figura 70 Resultado y visualización del *password hash cracked*



Fuente Arturo Ruiz

En la Figura 71. Se ejecuta el comando *hash-identifier* que nos arroja como resultado el posible *hash SHA-256*.

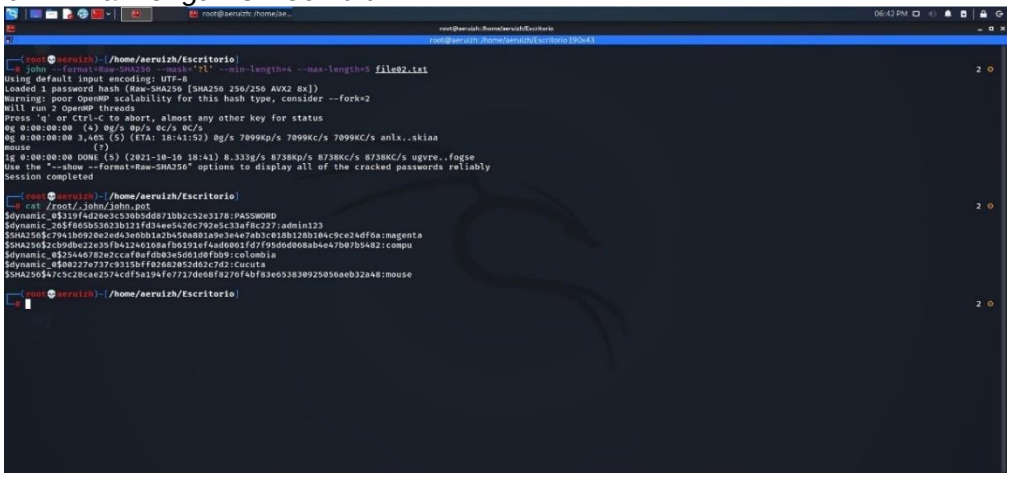
Figura 71 Ejecución del comando *hash-identifier* que nos arroja como resultado el posible *hash SHA-256*



Fuente Arturo Ruiz

En la Figura 72. Con el siguiente comando se puede visualizar la contraseña y configurando las características de este con un mínimo y máximo de longitud en el archivo file02.txt

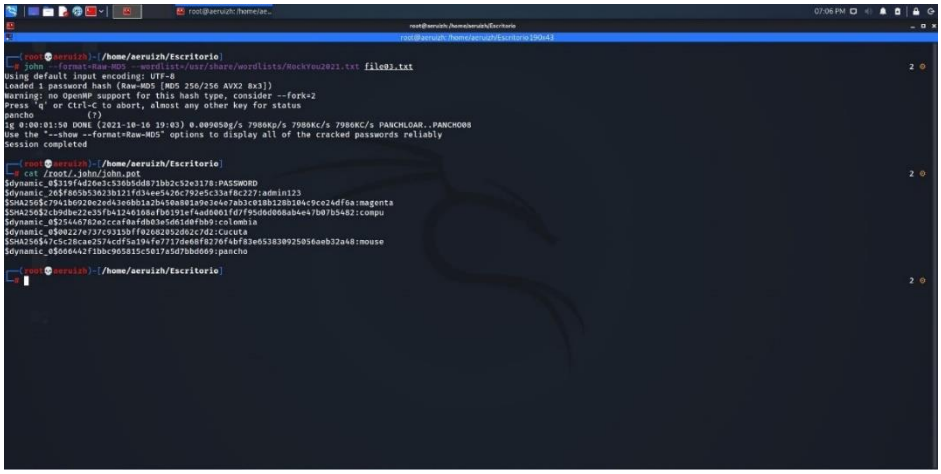
Figura 72 Resultado de la ejecución del comando *john--format=RAW-SHA256 –mask='?l' --min-lenght=4 --max-length=5 file02.txt*



Fuente Arturo Ruiz

En la Figura 73. Con el siguiente comando se recurre a identificar la contraseña del archivo file03.txt utilizando un diccionario. Utilizando el comando cat /root/./john/john.pot se pueden visualizar los password hash cracked

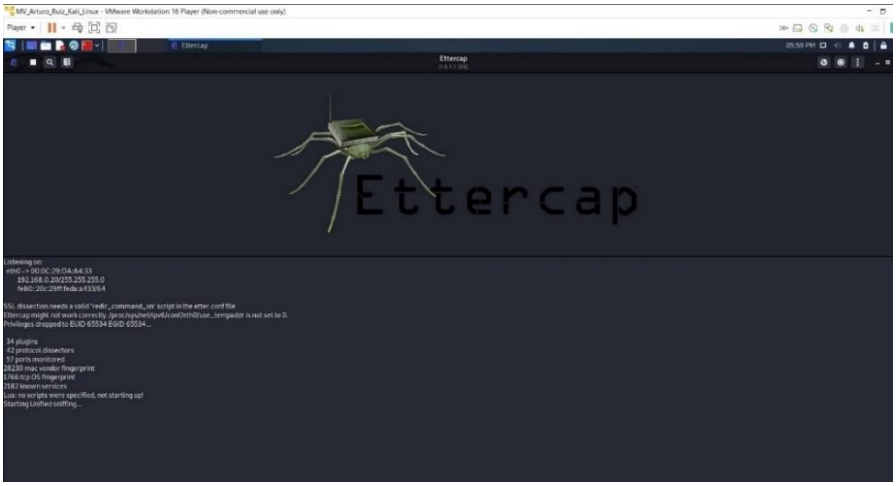
Figura 73 Resultado de la ejecución del comando *john--format=Raw-MD5 --wordlist=/usr/share/wordlists/RockYou2021.txt file03.txt*



Fuente Arturo Ruiz

***Ettercap*.** En la Figura 74. Inicio y ejecución *Ettercap* para detectar usuario y contraseña con una página que presenta vulnerabilidades

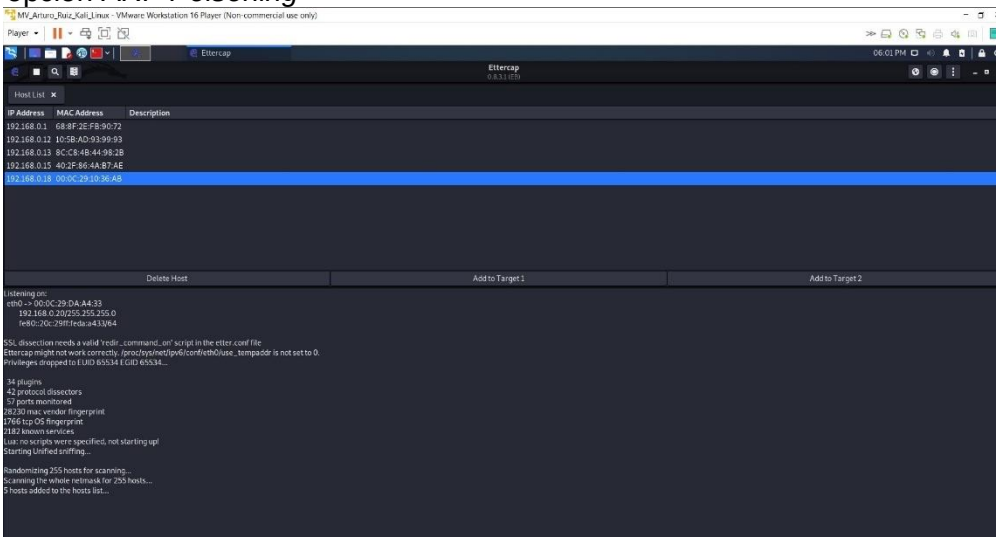
Figura 74 Inicio y ejecución del programa *Ettercap* para detectar usuario y contraseña con una página de presente vulnerabilidades



Fuente Arturo Ruiz

En la Figura 75. Se escanean y se obtiene la lista de hosts presentes en la red.

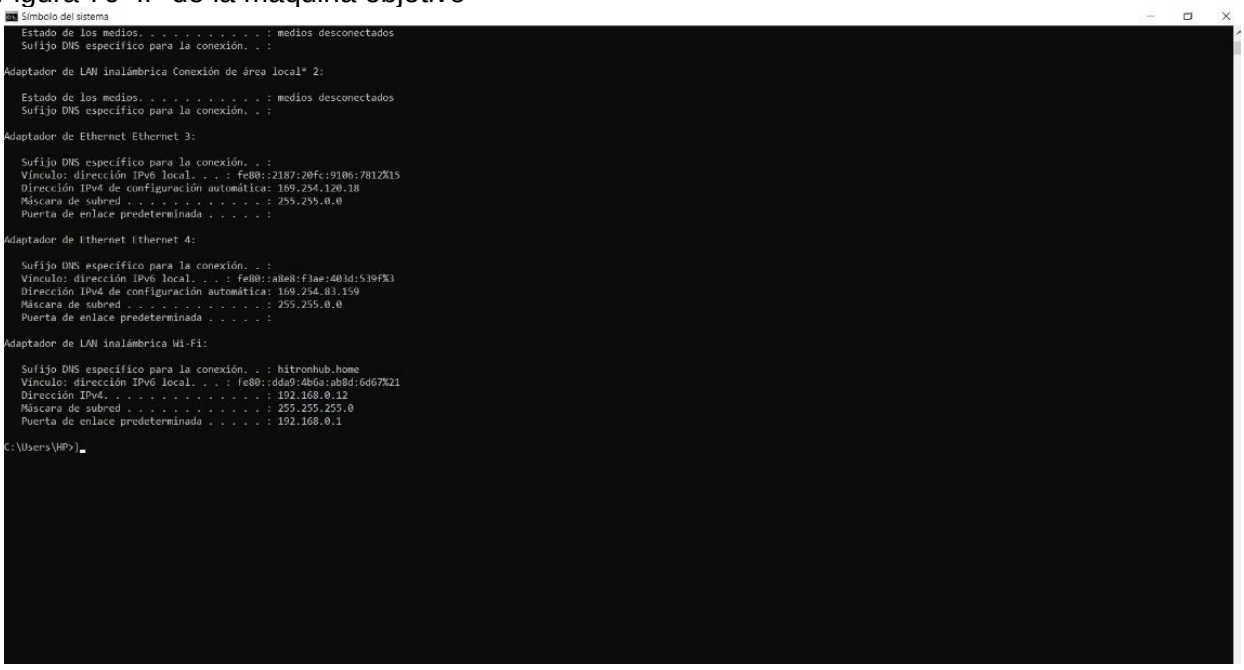
Figura 75 Se escanean y se obtiene la lista de *hosts* presentes en la red y en el menú se ejecuta la opción ARP *Poisoning*



Fuente Arturo Ruiz

En la Figura 76. Se observa la IP de la máquina objetivo.

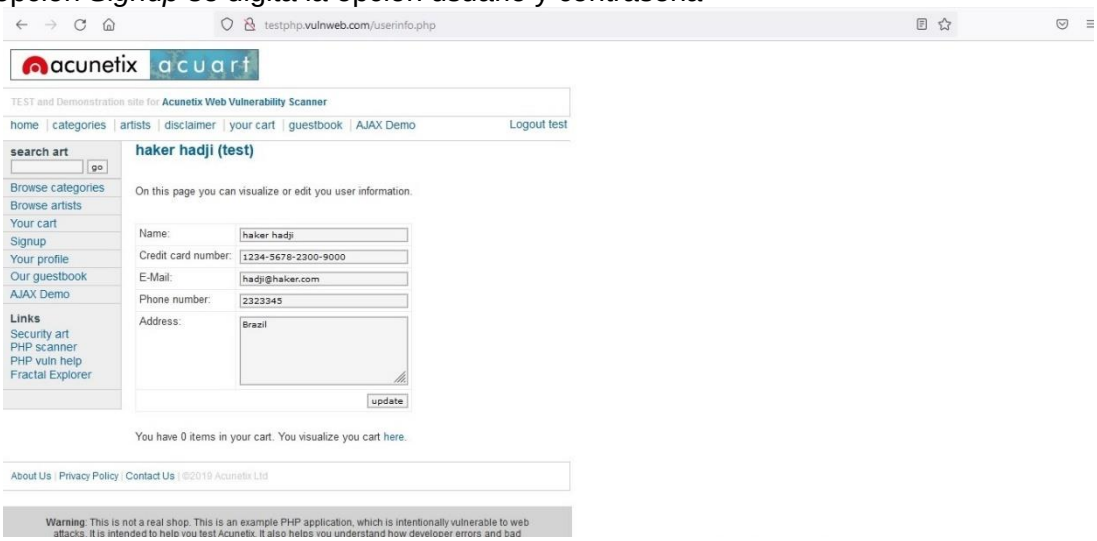
Figura 76 IP de la máquina objetivo



Fuente Arturo Ruiz

En la Figura 77. Se digita en el navegador de la máquina objetivo la URL de la máquina vulnerable.

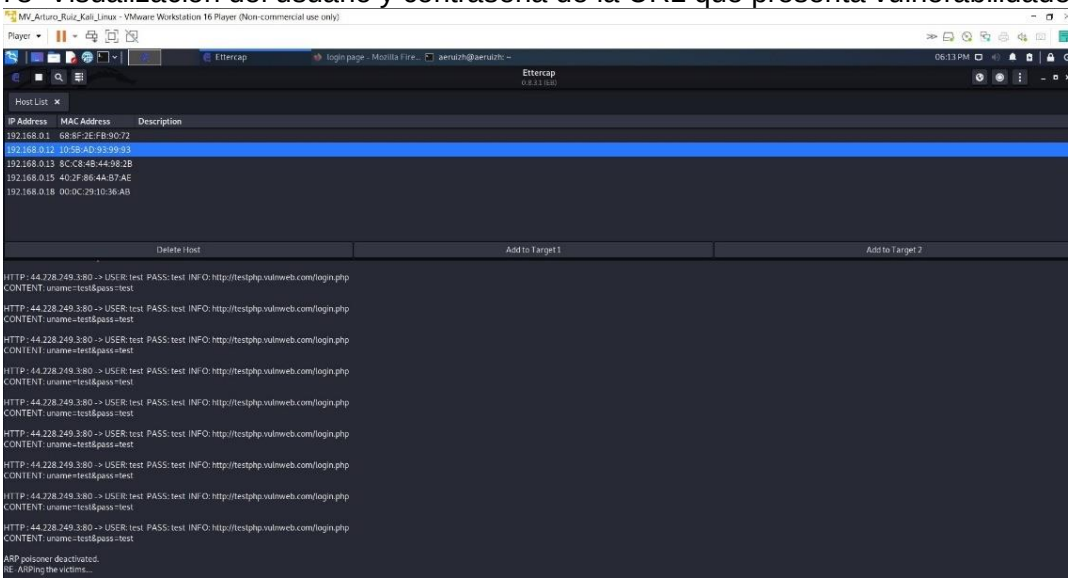
Figura 77 En el navegador de la máquina objetivo se digita la *URL* de la máquina vulnerable y en la opción *Signup* se digita la opción usuario y contraseña



Fuente Arturo Ruiz

En la Figura 78. Se visualiza el usuario y contraseña de la URL que presenta vulnerabilidades.

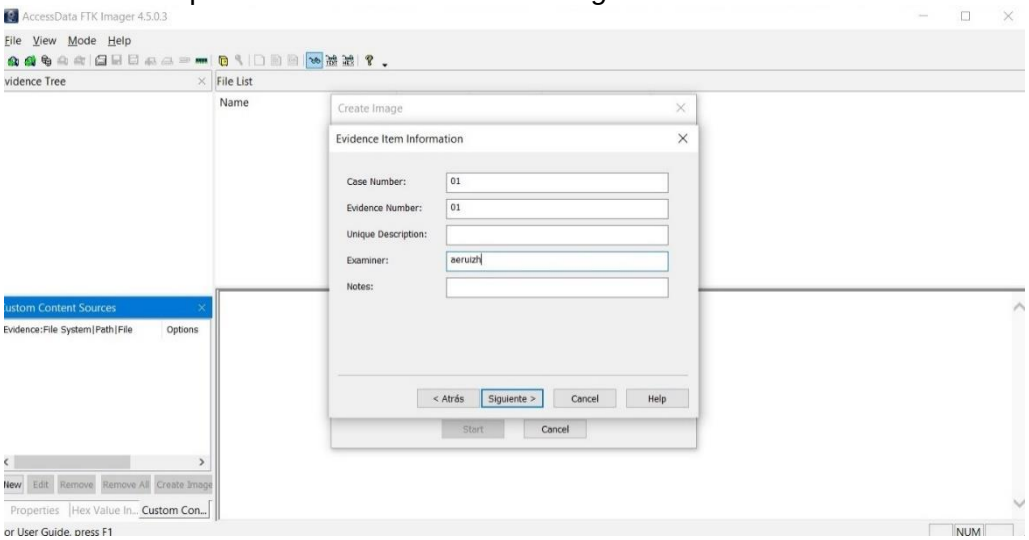
Figura 78 Visualización del usuario y contraseña de la URL que presenta vulnerabilidades



Fuente Arturo Ruiz

***Autopsy*.** En la Figura 79. Se observa el cuadro de evidencia del ítem de información

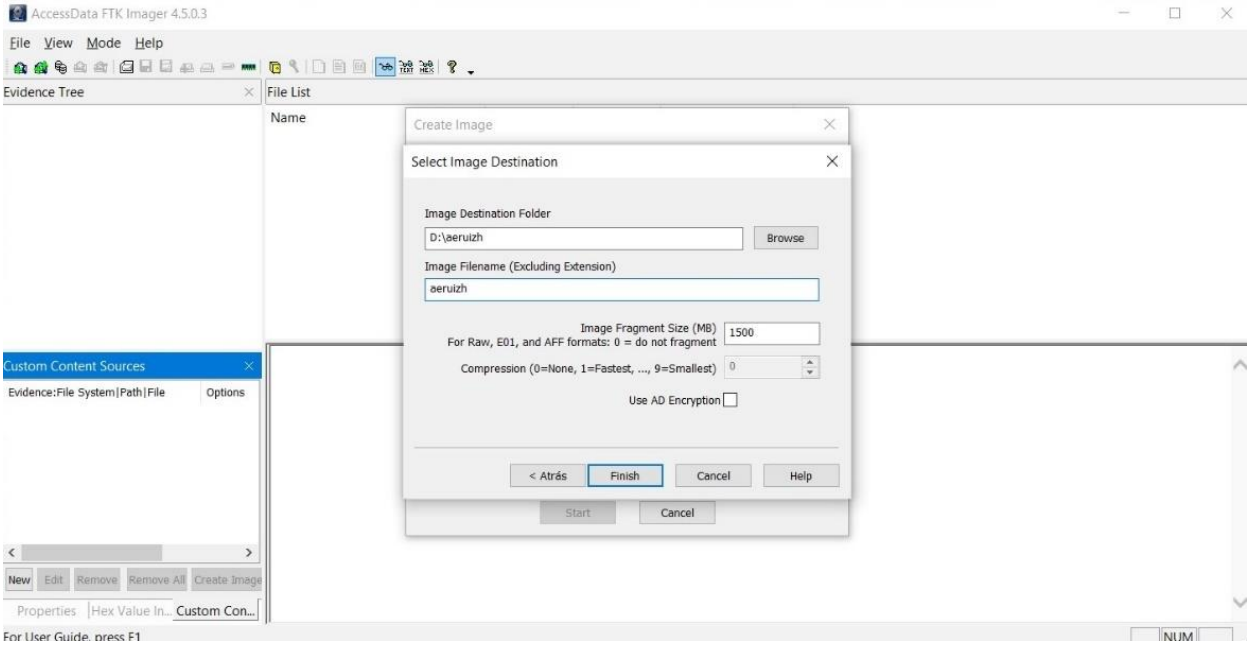
Figura 79 Información para tomar evidencia en *ftkImager*



Fuente Arturo Ruiz

En la Figura 80. Se observa el cuadro de destino de selección de la imagen.

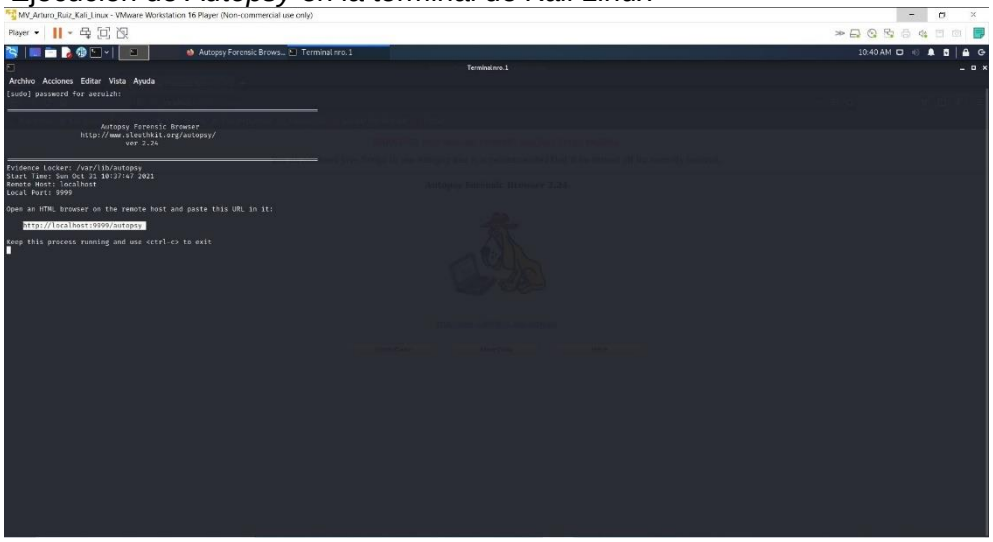
Figura 80 Descripción y destino de la imagen para ejecutar en *Autopsy*



Fuente Arturo Ruiz

En la Figura 81. En la terminal se ejecuta el programa Autopsy

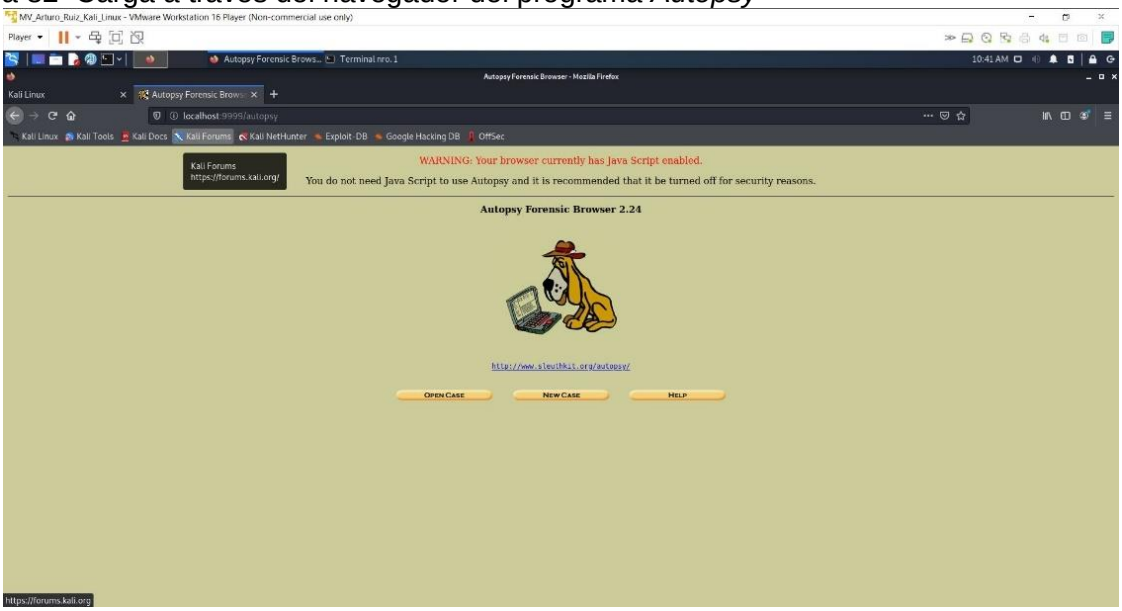
Figura 81 Ejecución de *Autopsy* en la terminal de *Kali Linux*



Fuente Arturo Ruiz

En la Figura 82. Se carga a través del navegador del programa *Autopsy*

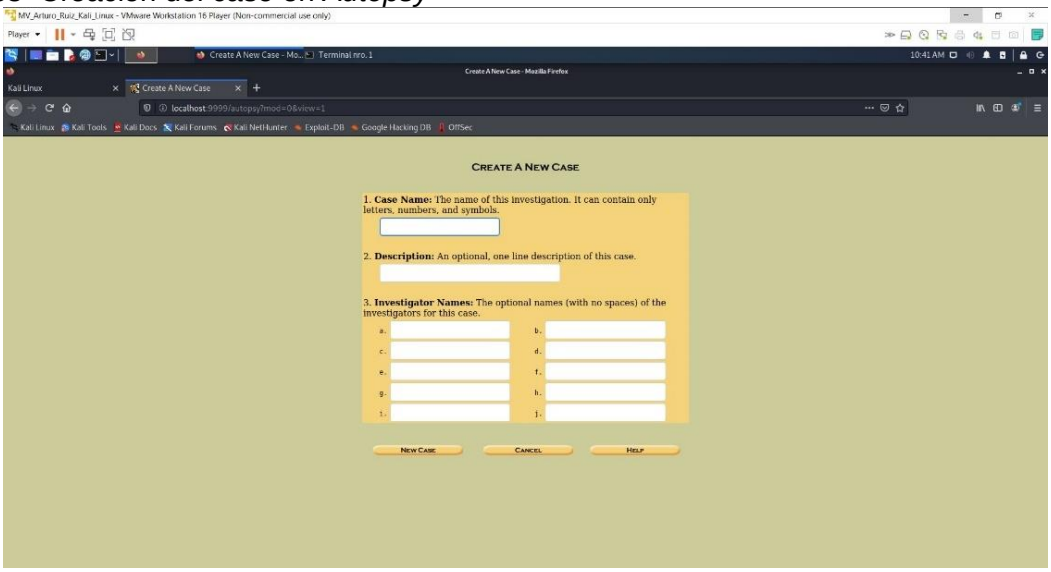
Figura 82 Carga a través del navegador del programa *Autopsy*



Fuente Arturo Ruiz

En la Figura 83. Se observa el nuevo caso de creación de *Autopsy*

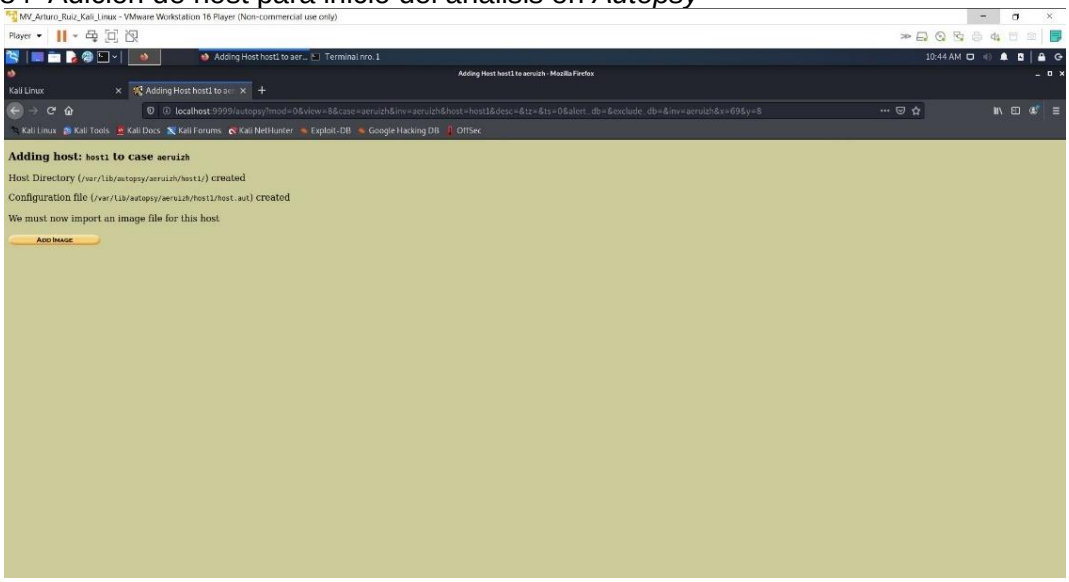
Figura 83 Creación del caso en *Autopsy*



Fuente Arturo Ruiz

En la Figura 84. Se adiciona el host para inicio del análisis en *Autopsy*

Figura 84 Adición de host para inicio del análisis en *Autopsy*

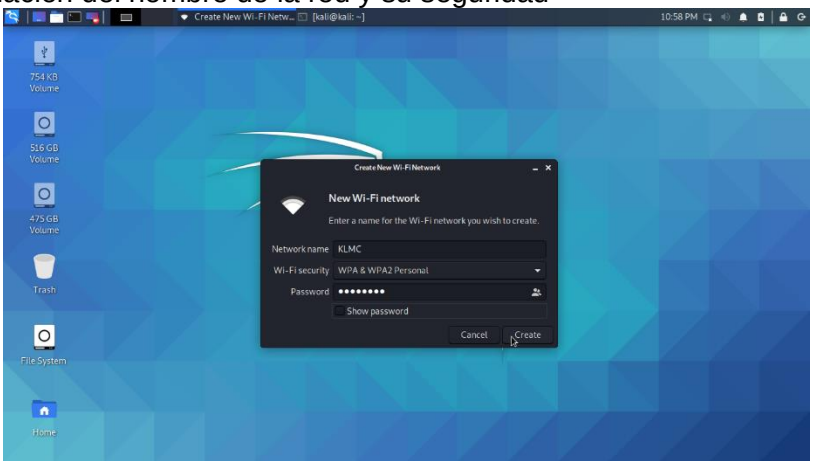


Fuente Arturo Ruiz

***Aircrack-NG Suite*.** Para la presente actividad se ejecutó en una máquina iniciando el sistema operativo *Kali Linux* versión 2020.3 en forma *live* desde USB; como no toma la red del hogar que en este caso se llama *KLMC* se configura manualmente agregando el

nombre de la red y la contraseña, la seguridad del *Wi-Fi: WPA & WPA2* Personal, se da *click* en el botón *Create*, como se observa en la Figura 85.

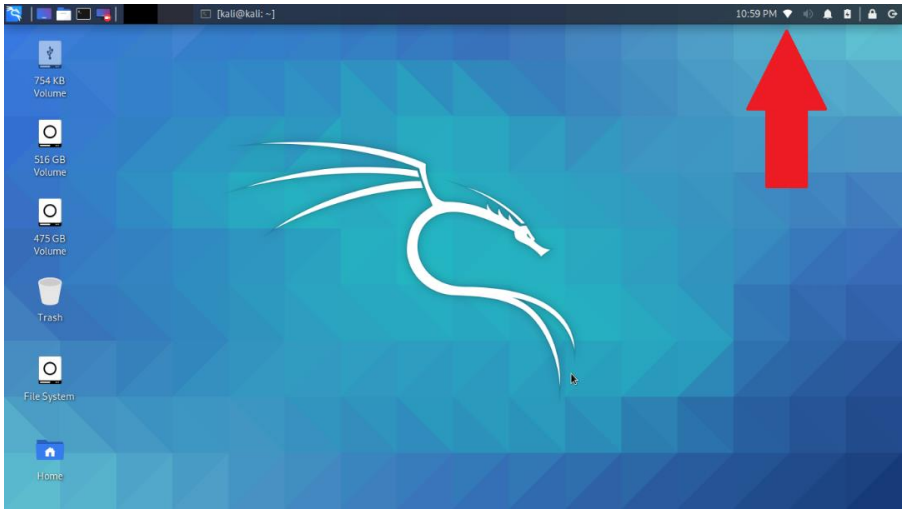
Figura 85 Información del nombre de la red y su seguridad



Fuente Arturo Ruiz

En la Figura 86. Se observa que ya existe conexión una vez digitado usuario, contraseña y configurado los parámetros de seguridad.

Figura 86 Conexión a través de red *Wi-Fi*

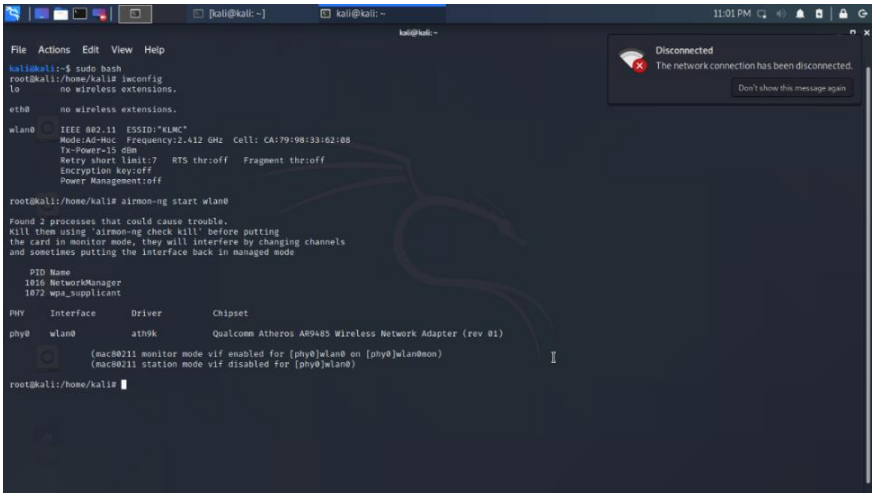


Fuente Arturo Ruiz

En la Figura 87. Se abre una terminal y se ejecutan los comandos: *sudo bash*, se presiona *enter* y luego se escribe el comando *iwconfig* que nos permite verificar las tarjetas de red

disponibles en nuestro PC para el tráfico de paquetes, luego se digita el comando *airmon-ng start wlan0* que es el nombre de la tarjeta de red.

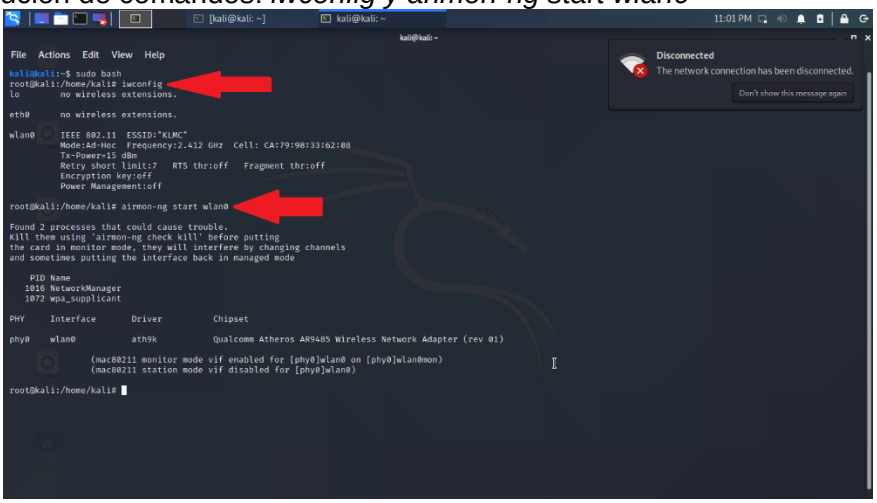
Figura 87 Desconexión física de la red



Fuente Arturo Ruiz

En la Figura 88. Se digita el comando *airdump-ng wlan0mon* permite activar el modo monitor en la tarjeta de red.

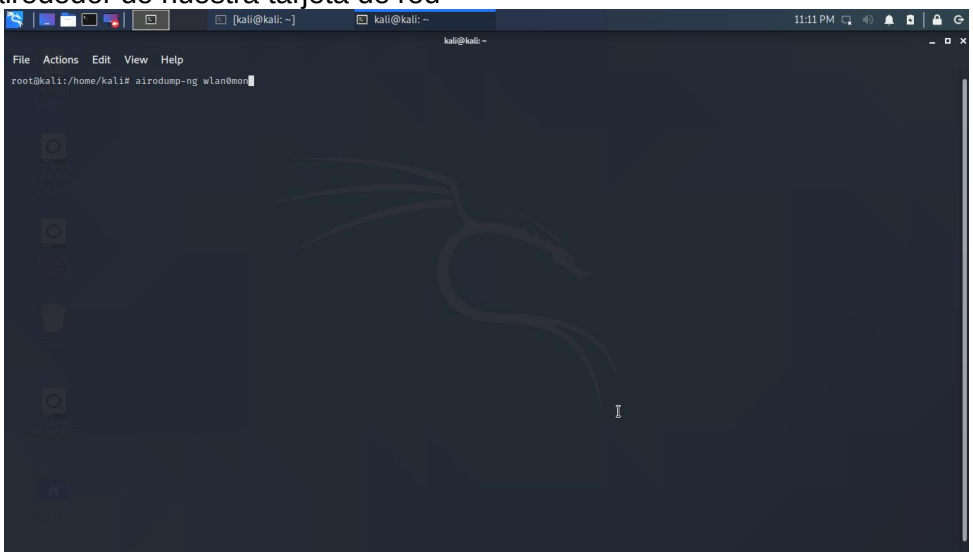
Figura 88 Ejecución de comandos: *iwconfig y arimon-ng start wlan0*



Fuente Arturo Ruiz

En la Figura 89. Con el comando: *airodump*-ng wlan0mon nos permite ver el tráfico de paquetes alrededor de nuestra tarjeta de red.

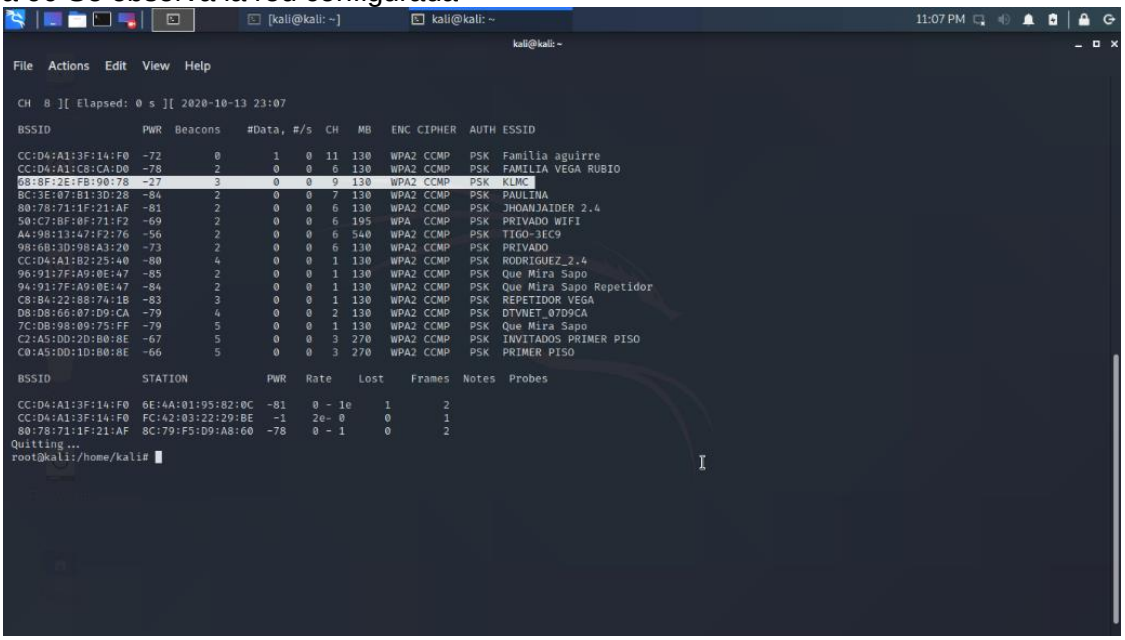
Figura 89 Ejecución del comando: *Airodump-ng wlan0mon* nos permite ver el tráfico de paquetes alrededor de nuestra tarjeta de red



Fuente Arturo Ruiz

En la Figura 90. Se detiene el tráfico de paquetes con *Ctrl + C*; aquí se va a realizar el proceso a la red *KLMC*.

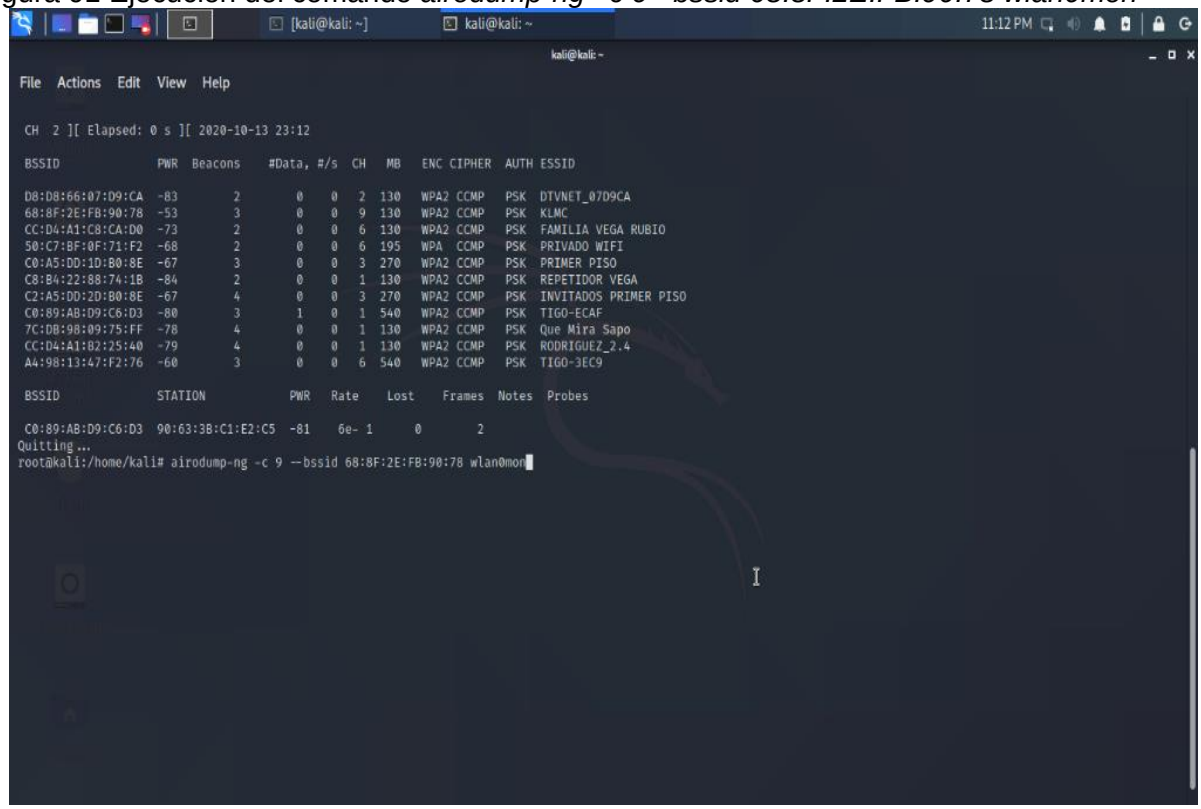
Figura 90 Se observa la red configurada



Fuente Arturo Ruiz

En la Figura 91. Se digita el comando *airodump-ng –c 9 –bssid* 68:8F:2E:FB:90:78 *wlan0mon.* Con -c <Aquí para situar el canal de la red, en este caso el número 9> --bssid<MAC> <modo de la tarjeta de red en modo monitor> wlan0mon

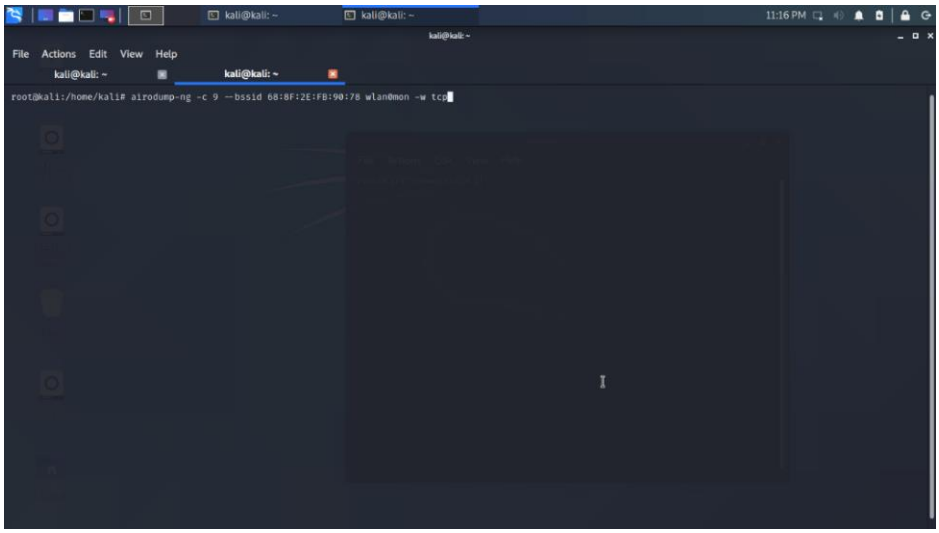
Figura 91 Ejecución del comando *airodump-ng –c 9 –bssid 68:8F:2E:FB:90:78 wlan0mon*



Fuente Arturo Ruiz

Esperar a que haya clientes conectados a esta red para sacar los datos. En la Figura 92. Se digita el comando *airodump-ng –c 9 –bssid 68:8F:2E:FB:90:78 wlan0mon –w tcp, tcp* <*Nombre* del archivo en donde va a capturar todos los datos de la red>. Se deja que el comando se ejecute y se abre otra terminal.

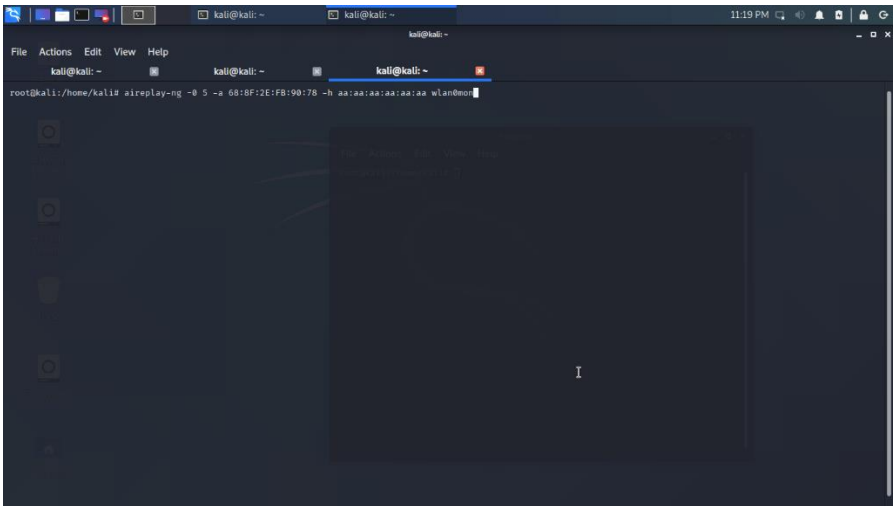
Figura 92 Ejecución del comando *airodump-ng –c 9 –bssid 68:8F:2E:FB:90:78 wlan0mon –w tcp*



Fuente Arturo Ruiz

Se digita el comando *aireplay-ng -0 5 –a 68:8F:2E:FB:90:78 –h aa: aa: aa: aa: aa: aa: wlan0mon.* En la Figura 93. Con -0 <es para desautentificar el cliente>, el número 5 es el número de mensajes de desautentificación que le va a enviar al cliente. Luego -a y la MAC del *router*, -h y una MAC cualquiera que va a simular nuestra dirección MAC, seguido de nuestra tarjeta de red en modo monitor: *wlan0mon*.

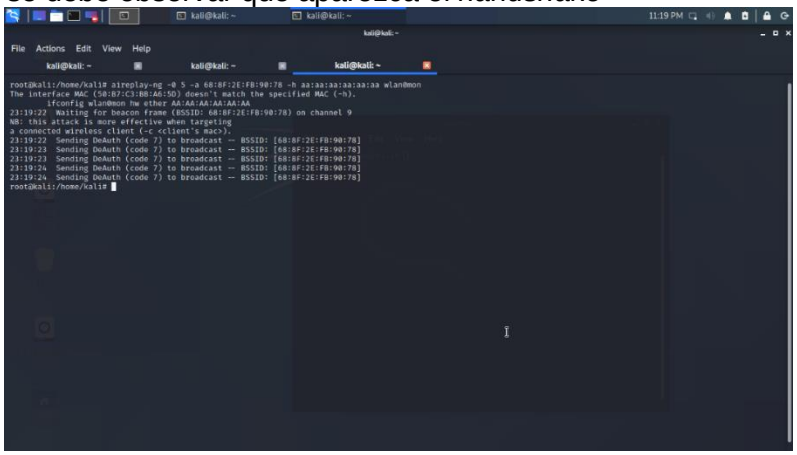
Figura 93 Ejecución del comando *aireplay-ng -0 5 –a 68:8F:2E:FB:90:78 –h aa: aa: aa: aa: aa: aa: wlan0mon*



Fuente Arturo Ruiz

En la Figura 94. Una vez digitado el comando se tiene que esperar los intentos de desautentificación.

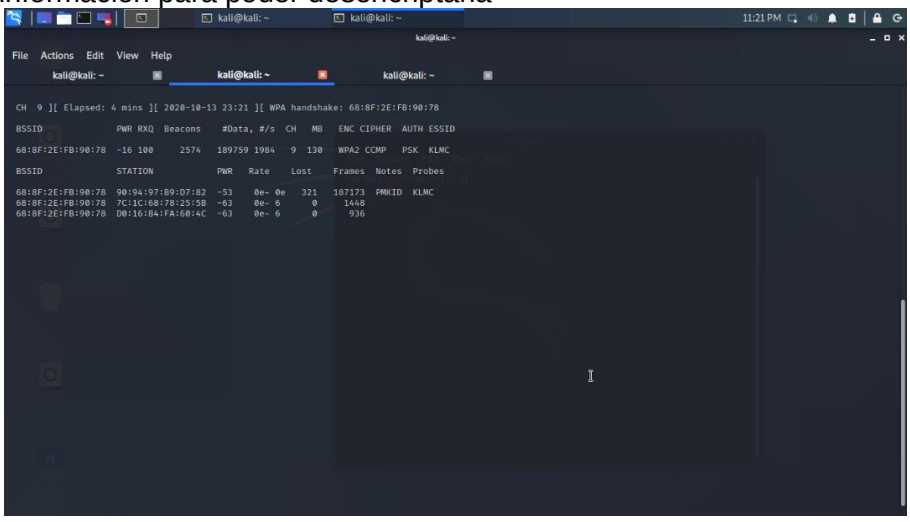
Figura 94 Una vez digitado el comando se tiene que esperar los intentos de desautentificación y en otro terminal se debe observar que aparezca el *handshake*



Fuente Arturo Ruiz

En la Figura 95. Se obtiene el *handshake* con el número de la MAC

Figura 95 Se obtiene el *handshake* con el número de la *MAC*, aquí se sabe que se ha capturado la información para poder desencriptarla

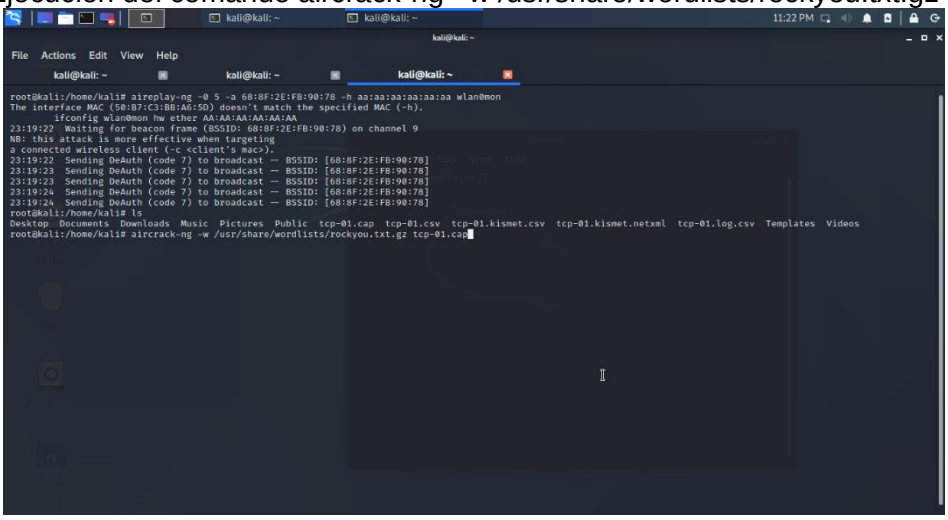


Fuente Arturo Ruiz

Se digita el comando *ls* y se observan los archivos: *tcp-01.cap, tcp-01.csv, tcp-01.kismet.csv, tcp-01.kismet.netxml, tcp-01.log.csv.* Para el presente caso se utiliza el

archivo: tcp-01.cap. En la Figura 96. Se digita el comando *aircrack-ng –w /usr/share/wordlists/rockyou.txt.gz tcp-01.cap*. En esta ruta: */usr/share/wordlists/rockyou.txt.gz* viene por defecto el diccionario de Kali Linux

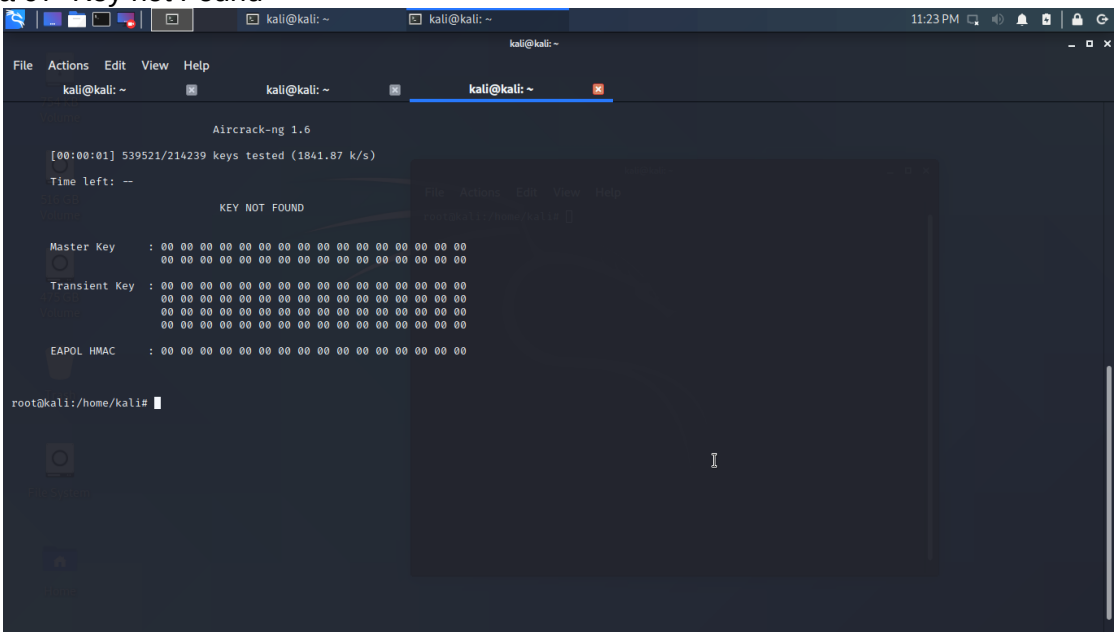
Figura 96 Ejecución del comando aircrack-ng –w /usr/share/wordlists/rockyou.txt.gz tcp-01.cap



Fuente Arturo Ruiz

En la Figura 97. Para el presente caso no se detecta la contraseña

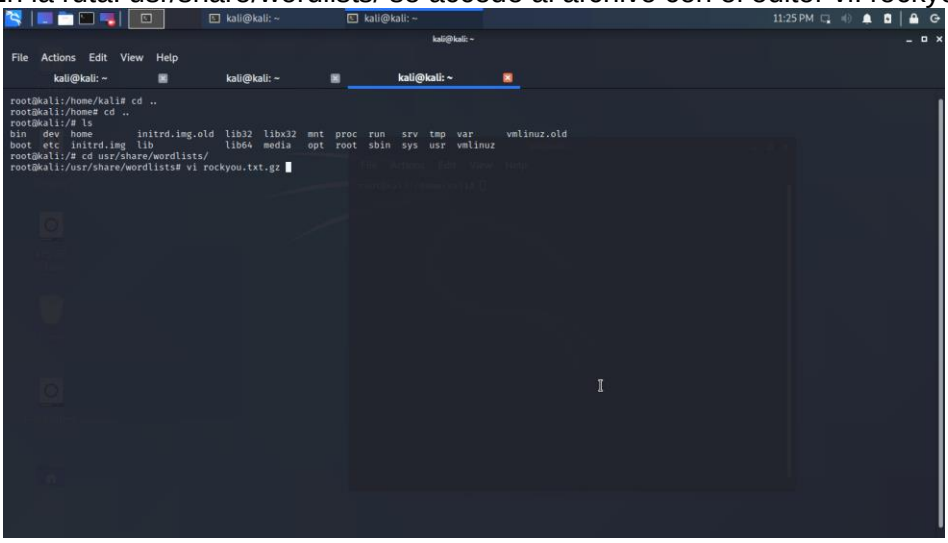
Figura 97 Key not Found



Fuente Arturo Ruiz

En la Figura 98. En la ruta: usr/share/wordlists/ se accede al archivo con el editor vi: rockyou.txt.gz

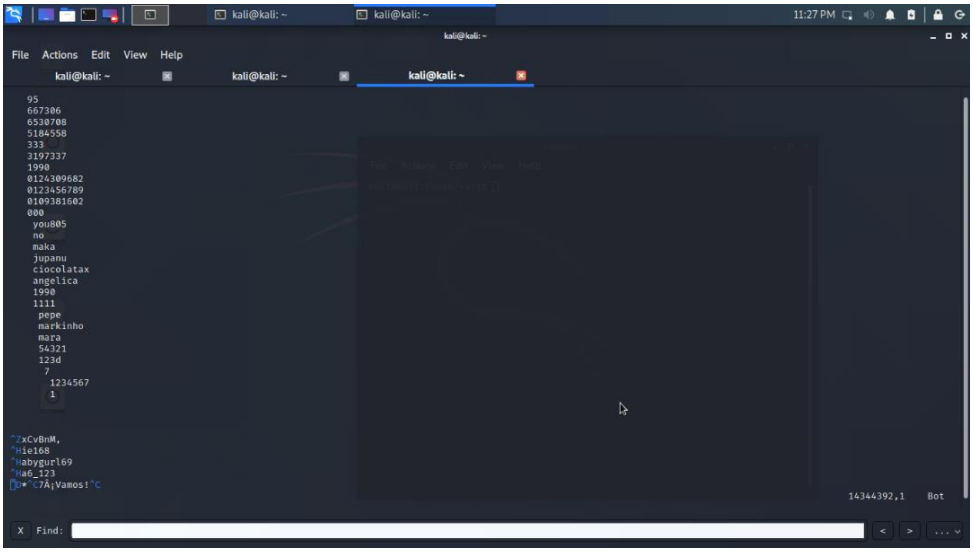
Figura 98 En la ruta: usr/share/wordlists/ se accede al archivo con el editor vi: rockyou.txt.gz



Fuente Arturo Ruiz

En la Figura 99. Se observa que la contraseña que se busca no se encuentra en el presente diccionario.

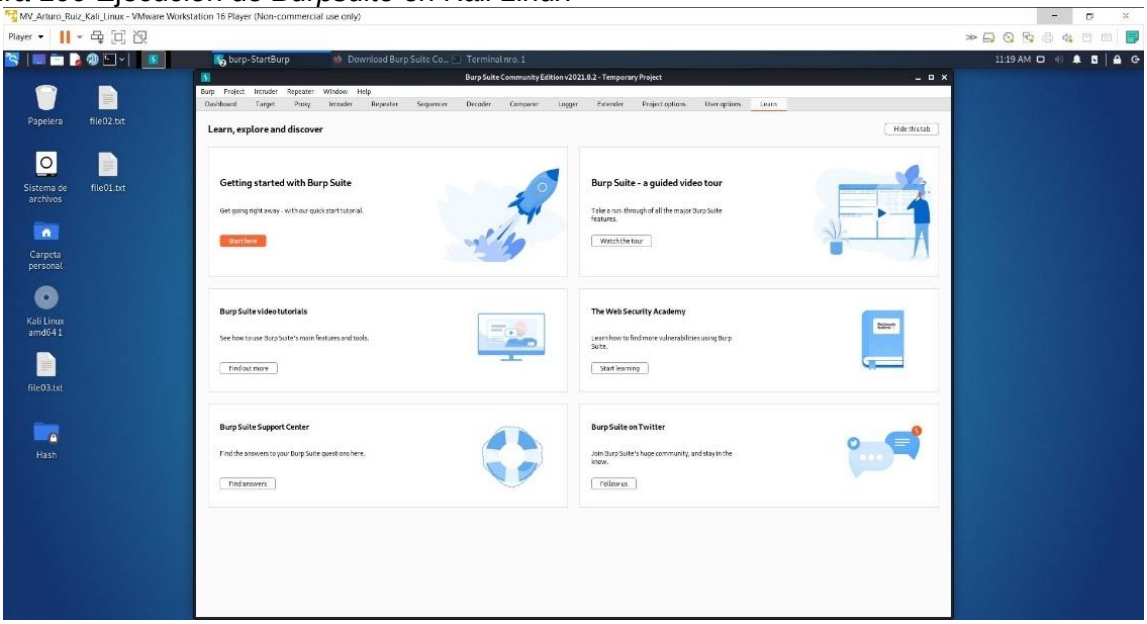
Figura 99 Se verifica en el menú Actions la opción buscar y no se encuentra la contraseña en este diccionario.



Fuente Arturo Ruiz

Burpsuite. En la Figura 100. Se observa la ejecución de *Burpsuite*

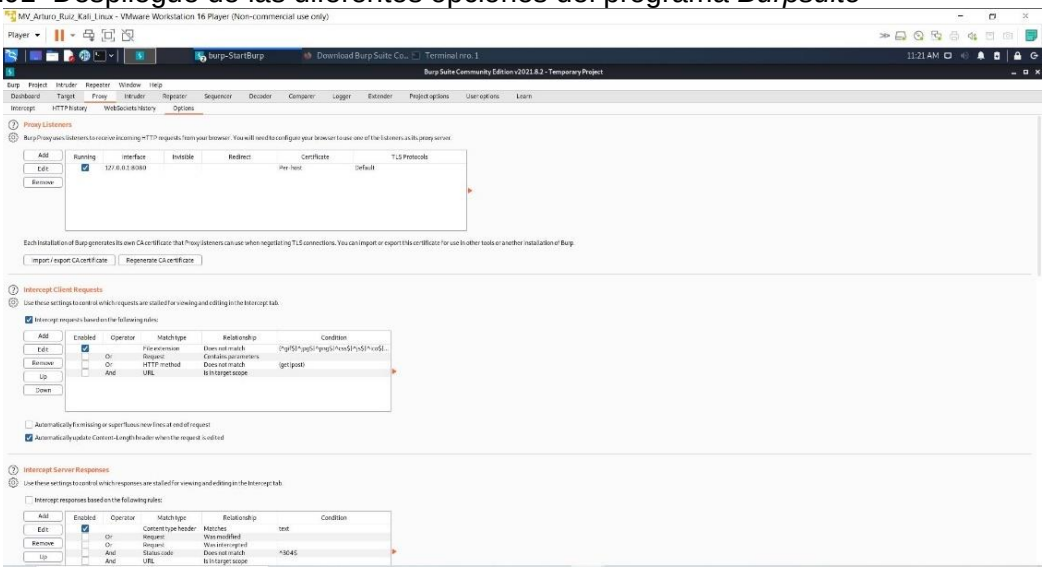
Figura 100 Ejecución de *Burpsuite en Kali Linux*



Fuente Arturo Ruiz

En la Figura 101. Se observa el despliegue de las diferentes opciones del programa *Burpsuite*

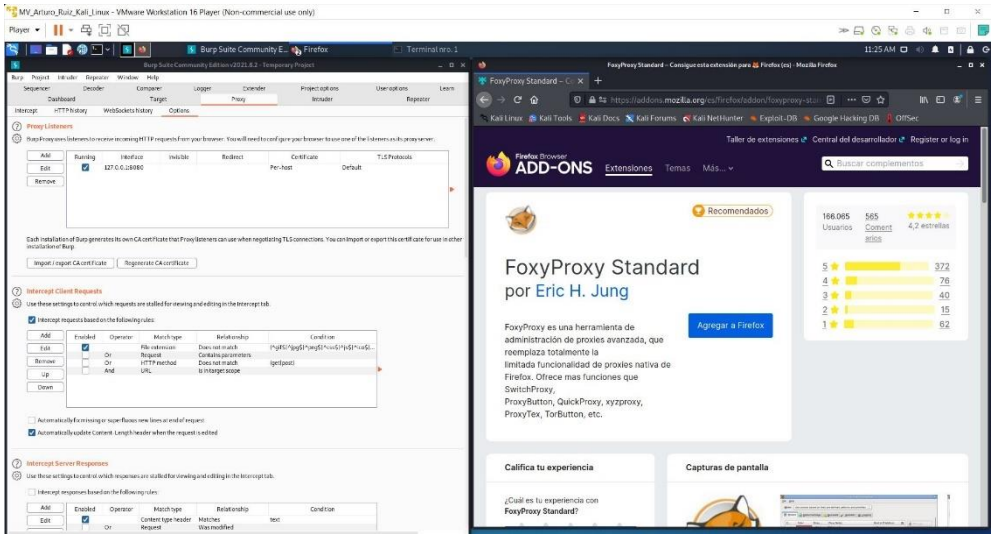
Figura 101 Despliegue de las diferentes opciones del programa *Burpsuite*



Fuente Arturo Ruiz

En la Figura 102. Se observa la apertura del navegador Mozilla Firefox para instalar el complemento *FoxyProxy Standard*

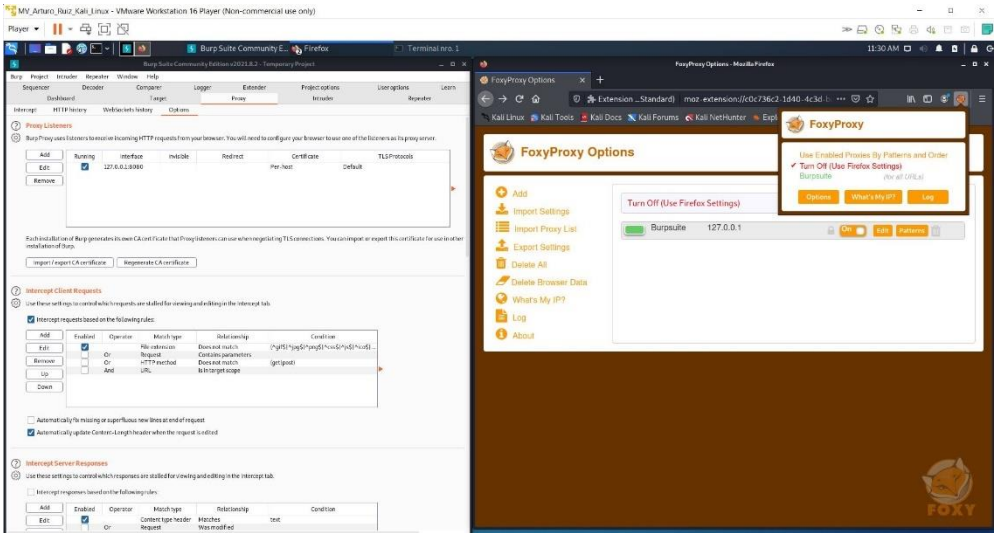
Figura 102 Apertura del navegador Mozilla Firefox para instalar el complemento *FoxyProxy Standard*



Fuente Arturo Ruiz

En la Figura 103. Se observan las Características de Burpsuite agregadas al complemento en navegador Mozilla Firefox

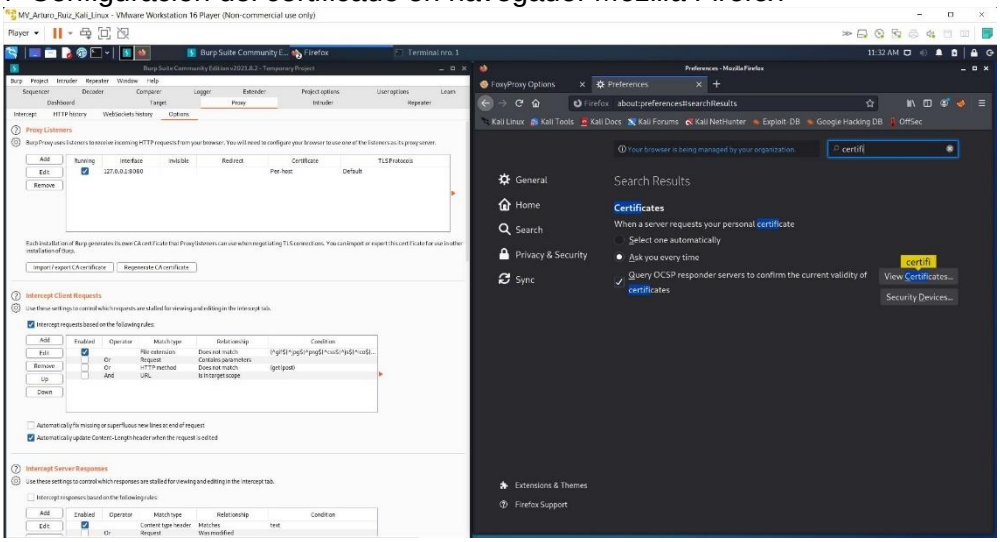
Figura 103 Características de Burpsuite agregadas al complemento en navegador Mozilla Firefox



Fuente Arturo Ruiz

En la Figura 104. Se observa la configuración del certificado en navegador Mozilla Firefox

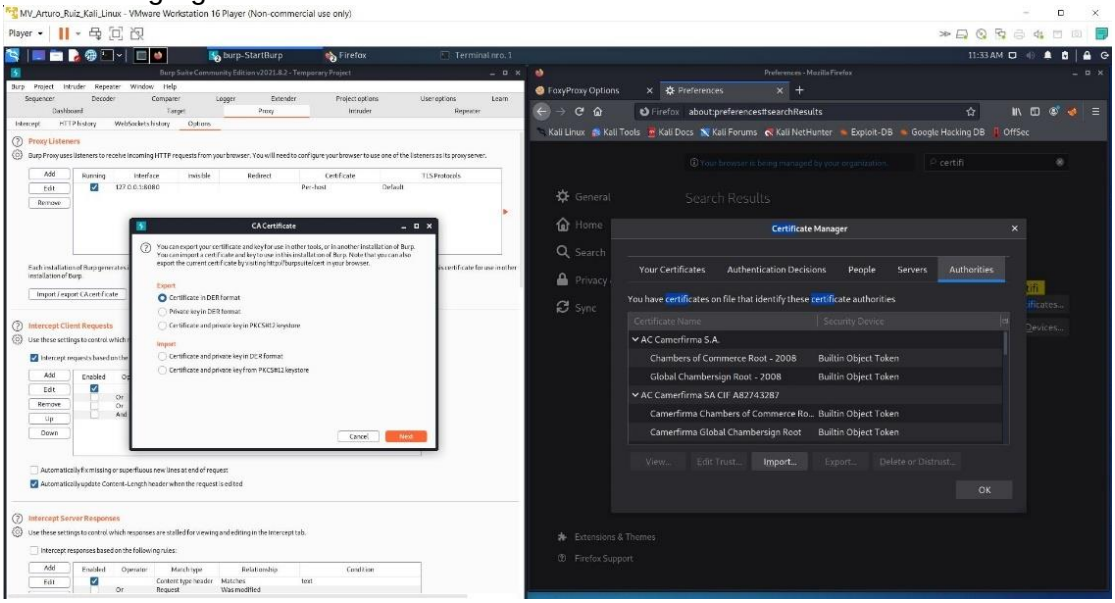
Figura 104 Configuración del certificado en navegador *Mozilla Firefox*



Fuente Arturo Ruiz

En la Figura 105. Se agrega Certificado *inDER format*

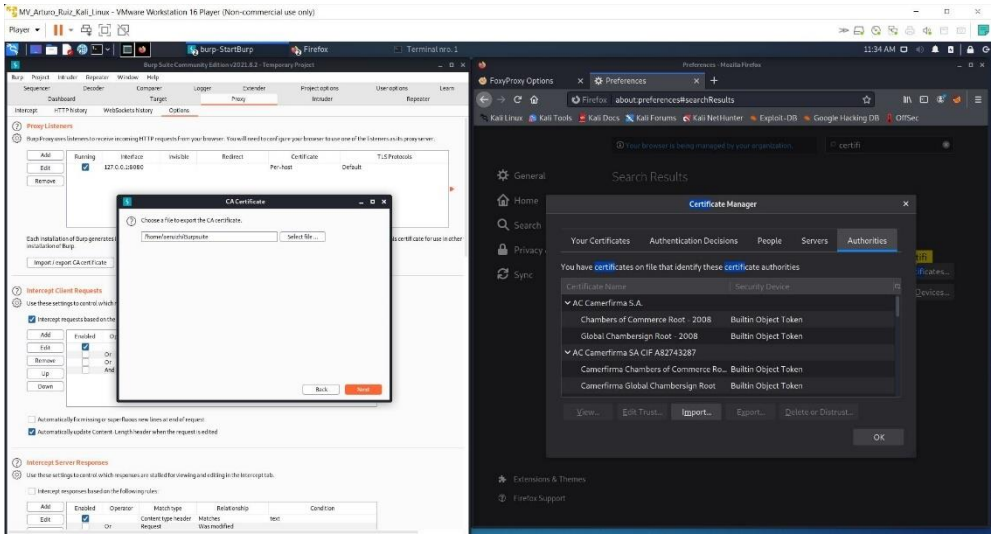
Figura 105 Se agrega Certificado *inDER format*



Fuente Arturo Ruiz

En la Figura 106. Se selecciona de la ruta del certificado

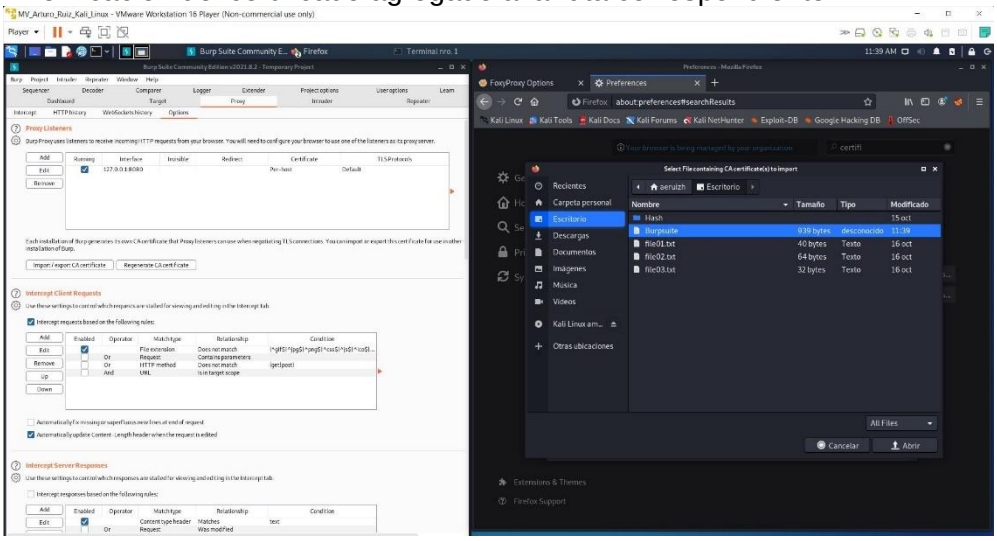
Figura 106 Selección de la ruta del certificado



Fuente Arturo Ruiz

En la Figura 107. Se verifica el certificado agregado a la ruta correspondiente.

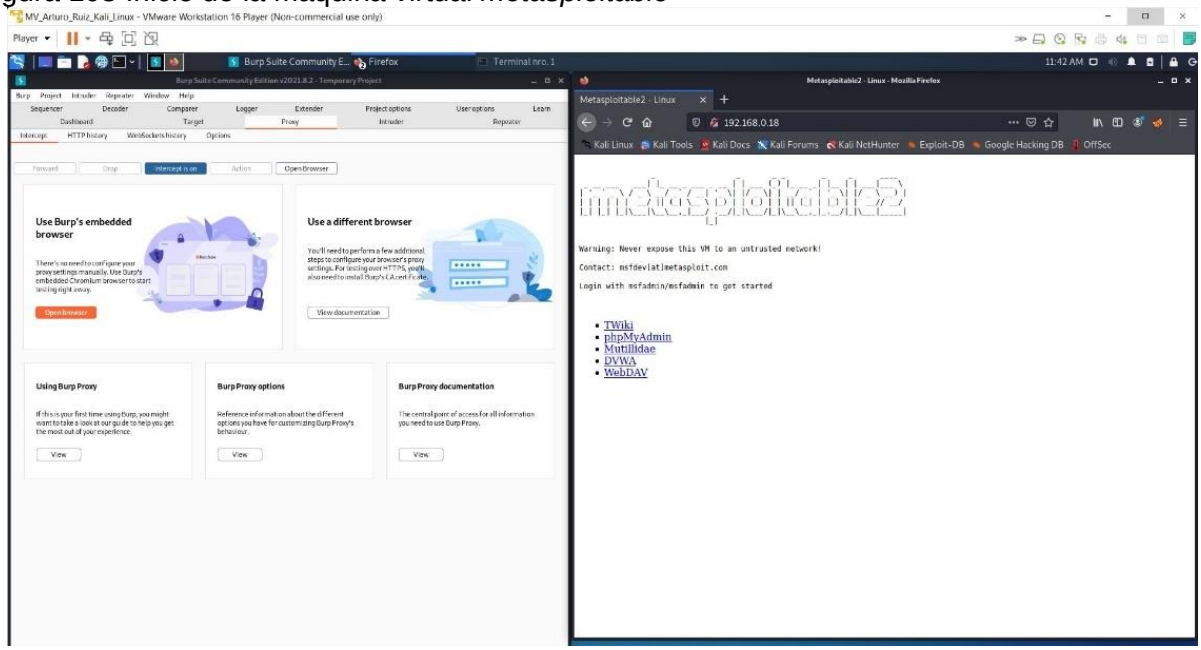
Figura 107 Verificación del certificado agregado a la ruta correspondiente



Fuente Arturo Ruiz

En la Figura 108. Se observa el inicio de la máquina virtual *Metasploitable*

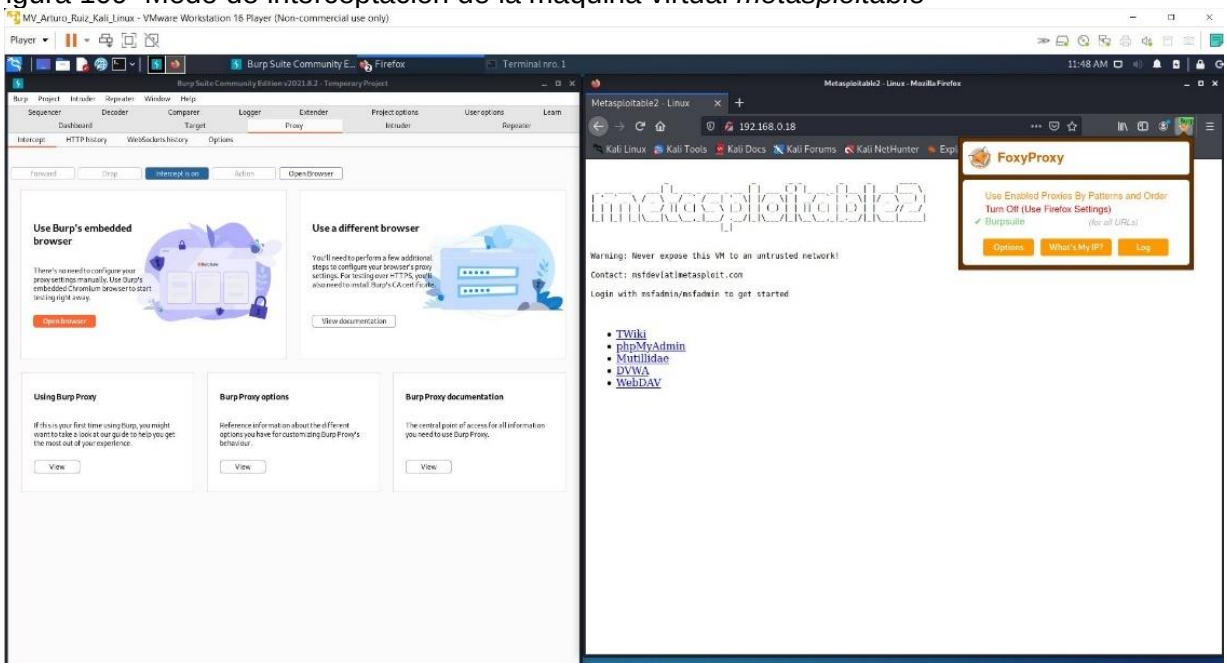
Figura 108 Inicio de la máquina virtual *metasploitable*



Fuente Arturo Ruiz

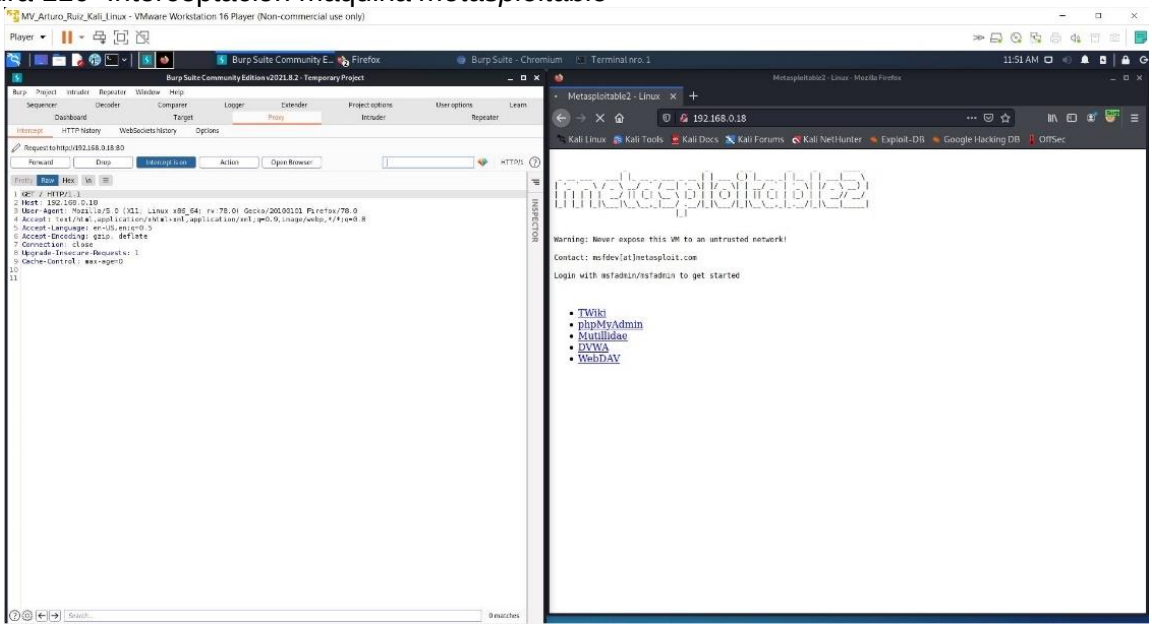
En la Figura 109 y 110. Se observa el Modo de interceptación de la máquina virtual *metasploitable*

Figura 109 Modo de interceptación de la máquina virtual *metasploitable*



Fuente Arturo Ruiz

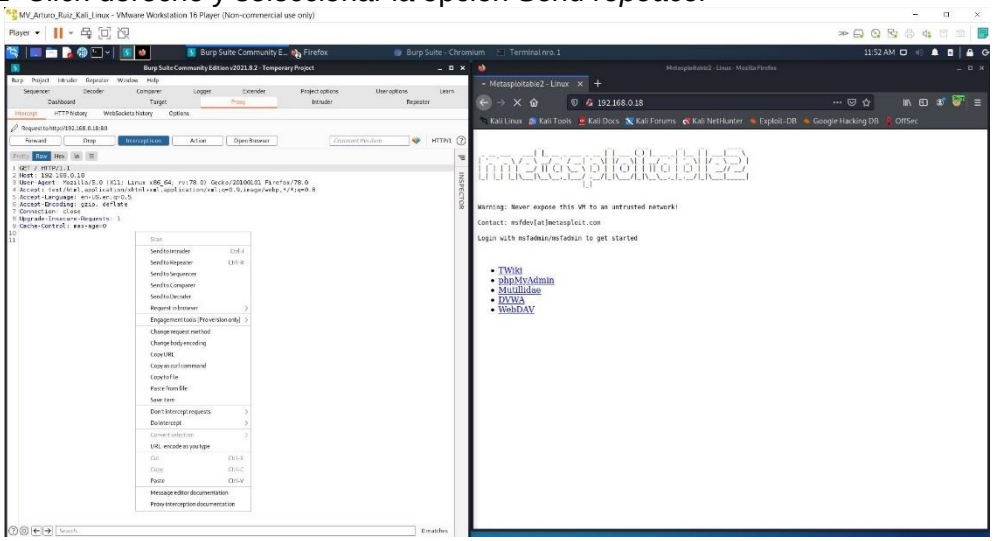
Figura 110 Interceptación máquina *metasploitable*



Fuente Arturo Ruiz

En la Figura 111. Click derecho y se selecciona la opción Send repeacer

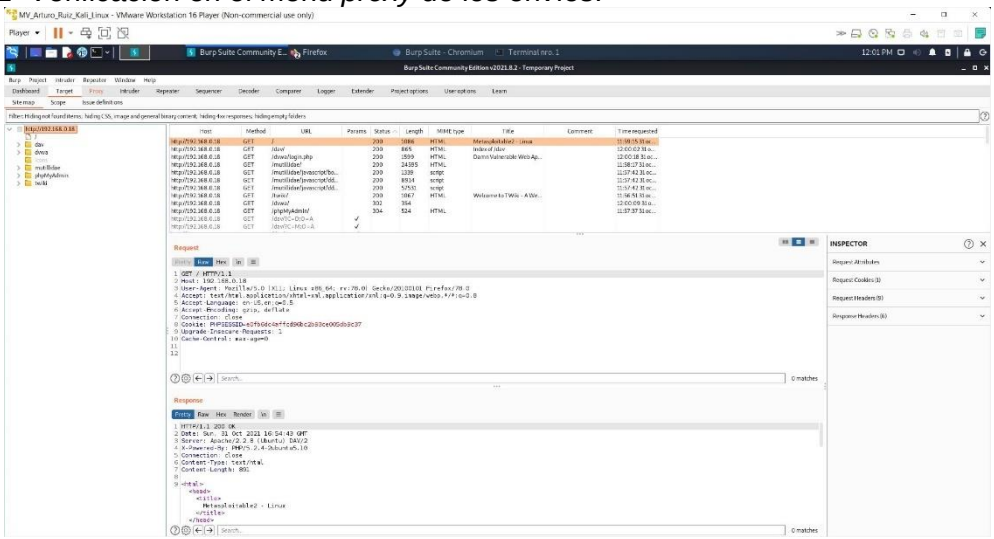
Figura 111 *Click* derecho y seleccionar la opción *Send repeacer*



Fuente Arturo Ruiz

En la Figura 112. Se verifica en el menú proxy los envíos.

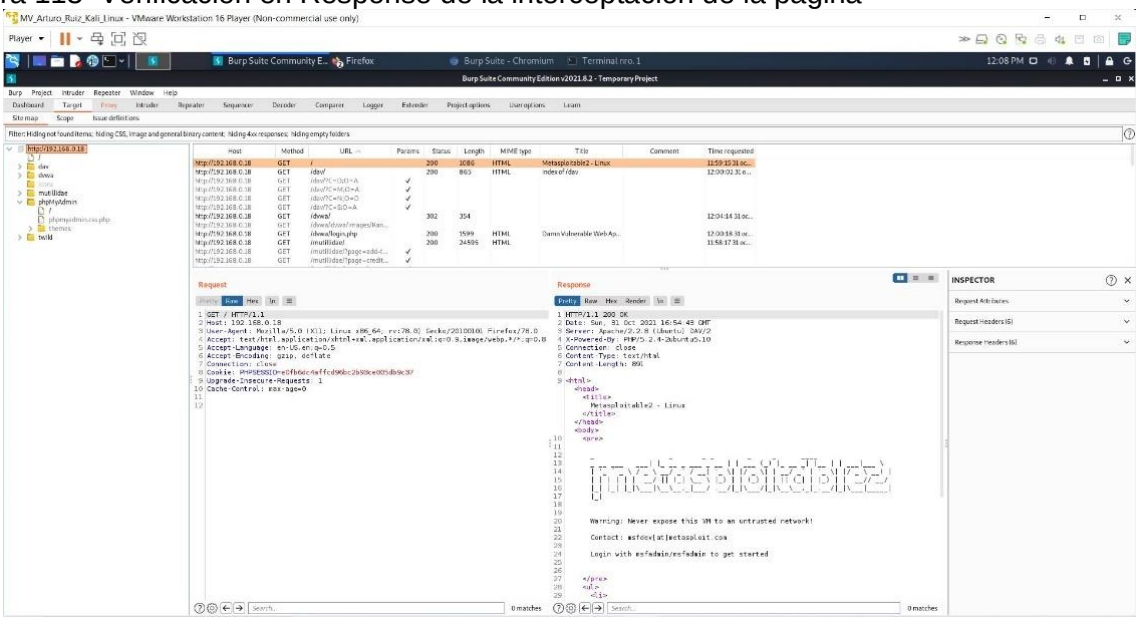
Figura 112 Verificación en el menú *proxy* de los envíos.



Fuente Arturo Ruiz

En la Figura 113. Se observa la interceptación de la página

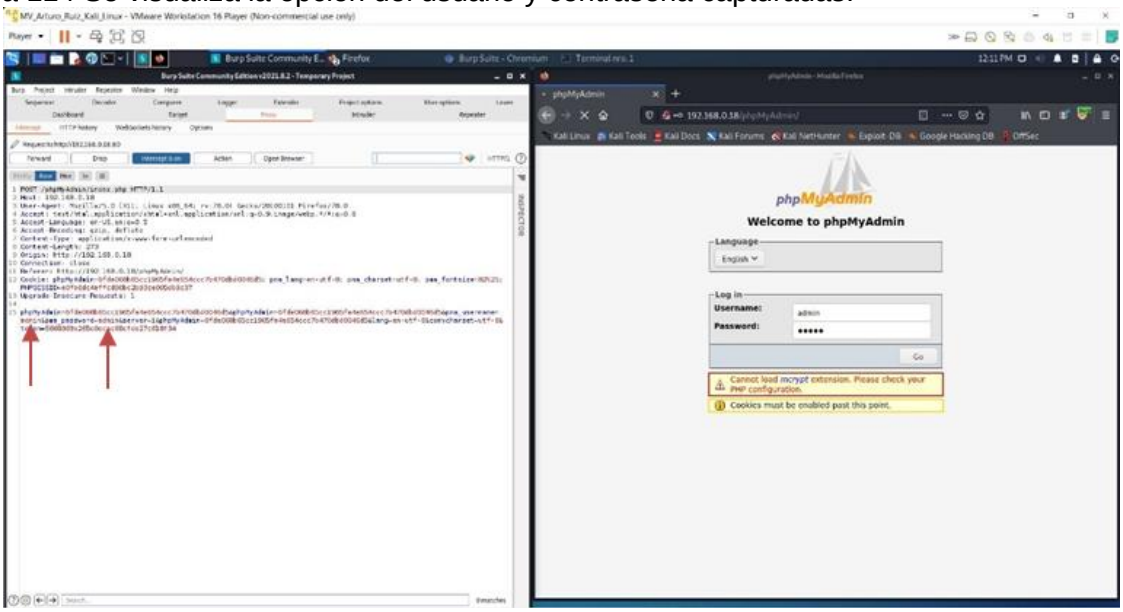
Figura 113 Verificación en Response de la interceptación de la página



Fuente Arturo Ruiz

En la Figura 114. Se visualiza la opción del usuario y contraseña capturadas.

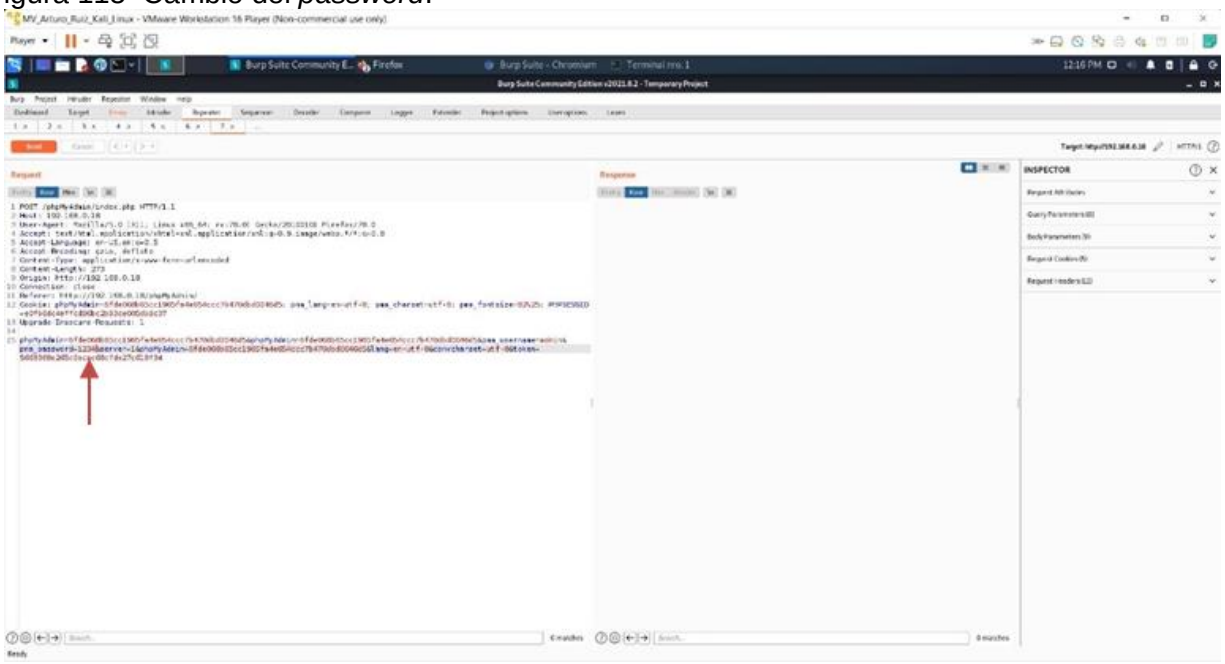
Figura 114 Se visualiza la opción del usuario y contraseña capturadas.



Fuente Arturo Ruiz

En la Figura 115. Se observa el cambio de *password*.

Figura 115 Cambio del *password*.



Fuente Arturo Ruiz

CONCLUSIONES

Según los foros, página oficial y contenidos relacionados con el sistema operativo Kali Linux, este ofrece gran variedad, uso y confiabilidad para los *pentester* y profesionales de la seguridad informática ofreciendo un gran número de herramientas que abarca documentación y tutoriales para ejecutar las pruebas de auditoría.

Desde pequeñas empresas hasta las más altas instituciones tanto privadas como de los gobiernos, la solicitud de profesionales para ejecutar pruebas de intrusión a los sistemas está siendo demandada puesto que actualmente son muy pocos los profesionales que tienen las habilidades necesarias para dar a conocer las vulnerabilidades presentes en una organización.

Se documentó a través de diversos foros, tutoriales y videos representativos del sistema operativo Kali Linux permitiendo con esto que el *pentester* pueda conocer los conceptos de seguridad informática y las técnicas junto a herramientas que ofrece el sistema operativo que abarca gran documentación en el cual una certificación avala las habilidades para ejecutar las pruebas de intrusión.

Se logró ejecutar la prueba de concepto necesaria para la instalación y configuración de laboratorios que permitieron conocer mejor el funcionamiento de cada herramienta de auditoría, en este laboratorio se aconsejó la virtualización de sistemas operativos junto a configuraciones específicas que permitieran la evaluación y uso de los diferentes comandos para cada herramienta.

Se consiguió elaborar los manuales que permiten un paso a paso en la ejecución de cada herramienta, desde la instalación hasta sus comandos principales, esto en un medio de virtualización y a modo educativo para no afectar y comprometer un sistema empresarial.

RECOMENDACIONES

Es importante que a futuro se configure otro sistema operativo relacionado con la ejecución de herramientas de seguridad informática para establecer comparaciones en el uso de estas, si son más fáciles de configurar y por sobre todo de utilizar en medios empresariales para auditorías en seguridad informáticas.

Sería importante seguir con el presente trabajo y realizar más aportes a los foros de habla hispana puestos que la gran mayoría de estas herramientas y su documentación está en el idioma inglés.

Se debe proyectar otro estudio con diferentes herramientas puesto que están en continua actualización y las mejoras son publicadas en las páginas oficiales.

Igualmente es necesario realizar proyectos de grado en las que estas herramientas se apliquen a manera de prueba piloto en el sector empresarial pues esto aumentaría la cantidad de masa documental pues la mayoría que se ejecuta es desde el punto de vista pedagógico.

BIBLIOGRAFÍA

ALAMANNI, Marco. Kali Linux wireless penetration testing essentials. [Internet] Packt Publishing Ltd, 2015. [Consultado 03 de junio 2022] Disponible en: https://books.google.es/books?hl=es&lr=&id=CrVJCgAAQBAJ&oi=fnd&pg=PP1&dq=ALAMANNI,+Marco.+Kali+Linux+wireless+penetration+testing+essentials.+Packt+Publishing+Ltd,+2015.&ots=tOPotl-C-W&sig=KKK5nhmsEJPLCbbLDaR7wwj-7hI

ALLEN LEE; Heriyanto, Tedi; ALI, Shakeel. Kali Linux–Assuring security by penetration testing. [Internet] Packt Publishing Ltd, 2014. [Consultado 03 de junio 2022] Disponible en: https://books.google.es/books?hl=es&lr=&id=QcBGAwAAQBAJ&oi=fnd&pg=PT2&dq=Kali+Linux+&ots=s73XTfTbZ8&sig=S14pIZGXf7fwoHMjjw3HYuz8H-c

ANURAG, A.; Kanjirappally, Kerala. An Implementation and Evaluation of PDF Password Cracking Using John the Ripper And Crunch. [Internet] En Proceedings of the National Conference on Emerging Computer Applications (NCECA). 2021. p. 18. [Consultado 03 de junio 2022] Disponible en: https://nceca.in/2021/4An_Implementation_and_Evaluation_of_PDF_Password_Cracking_Using_John_the_Ripper_and_Crunch.pdf

AREITIO BERTOLÍN, Javier. Seguridad de la información. Redes, informática y sistemas de información. [Internet] Editorial Paraninfo, 2008. [Consultado 21 de mayo 2022] Disponible en: https://books.google.es/books?hl=es&lr=&id=_z2GcBD3deYC&oi=fnd&pg=IA1&dq=1.%09AREITIO+BERTOL%C3%8DN,+Javier.+Seguridad+de+la+informaci%C3%B3n.+Redes,+inform%C3%A1tica+y+sistemas+de+informaci%C3%B3n.+Editorial+Paraninfo,+2008.&ots=wtlptECWTg&sig=YgvPOVFYhP3cWEPQLYtxZZLtvQ8

ARMENDÁRIZ LÓPEZ, Diana Nathaly. Modelo de gestión de los servicios de tecnología de información basado en COBIT, ITIL e ISO/IEC 27000. [Internet] Revista Tecnológica-ESPOL, 2017, vol. 30, no 1. [Consultado 30 de mayo 2022] Disponible en: http://200.10.150.204/index.php/tecnologica/article/view/581

AUTOPSY DIGITAL FORENSICS SOFTWARE. [Internet] Basistech. 2021. [Consultado 13 de junio 2022] Disponible en: https://www.basistech.com/autopsy/

BALLEN LEÓN, Diego Francisco, et al. Análisis de vulnerabilidades al servidor de pruebas del departamento de sistemas de la ESE hospital marco Felipe afanador del municipio de Tocaima Cundinamarca generando las recomendaciones para realizar un proceso de hardening. [Internet] Repositorio UNAD. 2019. [Consultado 05 de mayo 2022] Disponible en: https://repository.unad.edu.co/handle/10596/35854

BLANCO, ESQUERRA; De La Caridad, Liliana. Pruebas de penetración con la herramienta Kali Linux en la Universidad Central Marta Abreu de las Villas. 2014. [Internet] Tesis Doctoral. Universidad Central" Marta Abreu" de Las Villas. [Consultado 30 de mayo 2022] Disponible en: https://dspace.uclv.edu.cu/handle/123456789/1350

CASTRO MATURANA, Yeimar Alonso. Seguridad informática en el sistema Operativo LINUX en sus diversas distribuciones aplicadas a las tecnologías de la información. [Internet] Repositorio UNAD. 1992. [Consultado 30 de mayo 2022] Disponible en: https://repository.unad.edu.co/handle/10596/40342

CALDERÓN, Paulino. Nmap: libro de recetas de auditoría de seguridad y exploración de redes. [Internet] Packt Publishing Ltd, 2017. [Consultado 03 de junio 2022] Disponible en: https://books.google.es/books?hl=es&lr=&id=0Hc5DwAAQBAJ&oi=fnd&pg=PP1&dq=nmap&ots=bjdQv26xCv&sig=j2MJxn1Vmi29FxySjU9H_HJ48io

CONTRERAS FLÓREZ, Johan Lorenzo. Propuesta de auditoría a las aplicaciones web de la empresa C&M Consultores aplicando herramientas de software libre. [Internet] Repositorio UNAD. 2017. [Consultado 30 de mayo 2022] Disponible en: https://repository.unad.edu.co/handle/10596/14336

COLOMBIA Congreso de la República. Ley 1273 de 2009. Diario Oficial 47.223 de enero 5 de 2009. [Internet] Se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos". Bogotá, D. C. 05 de enero de 2009. [Consultado 30 de mayo 2022] Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1581 de 2012. [Internet] Diario Oficial 48587 de octubre 18 de 2012. Disposiciones generales para la protección de datos personales. Bogotá, D. C.17 de octubre de 2012. [Consultado 30 de mayo 2022] Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

CORBET, Jonathan; Rubini, Alessandro; Kroah-Hartman, Greg. Controladores de dispositivos Linux. [Internet] "O'Reilly Media, Inc.", 2005. [Consultado 25 de mayo 2022]Disponible en: https://www.iitg.ac.in/asahu/cs421/books/LDD3e.pdf

ESTRADA GARCÍA, Carlos Román. Análisis y pruebas de las herramientas de hacking ético incluidas en el sistema operativo Kali Linux, implementado en un Raspberry Pi 3, aplicadas en la empresa Fishcorp SA. [Internet] Universidad Católica de Santiago de Guayaquil. 2018. [Consultado 30 de mayo 2022] Disponible en: http://201.159.223.180/handle/3317/11338

FERNÁNDEZ, Arturo. Cámbiate a LINUX. [Internet] RC Libros, 2011. [Consultado 25 de mayo 2022] Disponible en: https://books.google.es/books?hl=es&lr=&id=OUh_NkBtWDAC&oi=fnd&pg=PR9&dq=F

ERN%C3%81NDEZ,+Arturo.+C%C3%A1mbiate+a+LINUX.+RC+Libros,+2011.&ots=EzsvrcwFCr&sig=-ZbOcw5DB402JDoxRg5dcsEICv0

FERNÁNDEZ MOYA, José Manuel. Debian GNU/Linux. [Internet] Linux Actual: la primera revista en castellano del sistema operativo Gnu/Linux, 1998, vol. 1, no 1, p. 36-38. [Consultado 25 de mayo 2022] Disponible en: http://es.tldp.org/Manuales-LuCAS/LIPP2/lipp-2.0-beta2.pdf

FERNÁNDEZ, Diego A.; ARCENTALES, Casas, CAYCEDO, Xiomara. Auditoría informática: un enfoque efectivo. [Internet] Dominio de las Ciencias, 2017, vol. 3, no 3, p. 157-173. [Consultado 30 de mayo 2022] Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=6102836

FRÜHLING Gallardo, Hugo;, Roberto. Programas de seguridad dirigidos a barrios en la experiencia chilena reciente. [Internet] Revista INVI, 2012, vol. 27, no 74, p. 149-185. [Consultado 21 de mayo 2022] Disponible en: https://scielo.conicyt.cl/scielo.php?pid=S0718-83582012000100005&script=sci_arttext

GAGO, Edgardo Aimar. El enfoque argentino sobre ciberseguridad y ciberdefensa. [Internet] Tesis Doctoral. Escuela Superior de Guerra Tte Grl Luis María Campos. 2017. [Consultado 21 de mayo 2022] Disponible en: http://cefadigital.edu.ar/bitstream/1847939/1097/1/TFL%20RRII%202017%20G1E3_214.pdf

GAMBOA SUAREZ, José Luis. Importancia de la seguridad informática y ciberseguridad en el mundo actual. [Internet] Repositorio Unipiloto. 2020. [Consultado 21 de mayo 2022] Disponible en: http://repository.unipiloto.edu.co/handle/20.500.12277/8668

GHANEM, WAHEED Ali Hm; BELATON, Bahari. Mejora de la precisión de la toma de huellas dactilares de aplicaciones en redes locales utilizando NMAP-AMAP-ETTERCAP

como marco híbrido. [Internet] En 2013 Conferencia internacional IEEE sobre sistemas de control, computación e ingeniería. IEEE, 2013. pág. 403-407. [Consultado 03 de junio 2022] Disponible en: https://ieeexplore.ieee.org/abstract/document/6719998/

GÓMEZ VIEITES, Álvaro. Seguridad Informática Básico. Sterbook. [Internet] ECOE EDICIONES. Primera edición: Bogotá DC, 2011. [Consultado 30 de mayo 2022] Disponible en: https://www.ecoeediciones.com/wp-content/uploads/2015/08/seguridad-informatica-basico.pdf

GORDON, Deborah M. The dynamics of the daily round of the harvester ant colony (Pogonomyrmex barbatus). [Internet] Animal Behaviour, 1986, vol. 34, no 5, p. 1402-1419. [Consultado 03 de junio 2022] Disponible en: https://www.sciencedirect.com/science/article/pii/S0003347286802111

GORDON FYODOR Lyon. Nmap network scanning: The official Nmap project guide to network discovery and security scanning. Insecure. [Internet] Com LLC (US), 2008. [Consultado 30 de mayo 2022] Disponible en: http://repository.ntt.edu.vn/jspui/handle/298300331/3157

HACKEACADEMY. How to use the harvester tool for Information Gathering. [Internet] Hackeracademy. 2021. [Consultado 13 de junio 2022] Disponible en: https://www.hackeracademy.org/how-to-use-the-harvester-tool-for-information-gathering/

HERTZOG, Raphaël; O'GORMAN, Jim; AHARONI, Mati. Kali Linux Revealed. [Internet] Cornelius, NC: Offensive Security, 2017. [Consultado 29 de mayo 2022] Disponible en: https://jom.fti.budiluhur.ac.id/index.php/IDEALIS/article/view/118

HUTCHENS, Justin. Kali Linux network scanning cookbook. [Internet] Packt Publishing Ltd, 2014. [Consultado 03 de junio 2022] Disponible en: https://books.google.es/books?hl=es&lr=&id=9R1VBAAAQBAJ&oi=fnd&pg=PT18&dq=H

UTCHENS,+Justin.+Kali+Linux+network+scanning+cookbook.+Packt+Publishing+Ltd,+2014.&ots=qBWSyRowpi&sig=rp2nCmCOa3zD0oQYhGNj3ijU8TI

INCIBE – Instituto Nacional de Ciberseguridad. Glosario de términos de ciberseguridad. [Internet] INCIBE. 2017. [Consultado 05 de mayo 2022] Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf

JOHNSON Josh. 17 free cybersecurity tools you should know about. Cybersecurity products can get pricy but there are many excellent open-source tools to help secure your systems and data. Here's a list of some of the most popular with cyber pros. [Internet] TechTarget. 2021. [Consultado 05 de junio 2022] Disponible en: https://whatis.techtarget.com/feature/17-free-cybersecurity-tools-you-should-know-about

KASPERSKY, Eugene; FURNELL, Steven. A security education Q&A. Information Management & Computer Security. [Internet] Emerald Group Publishing Limited. 2014. [Consultado 30 de mayo 2022] Disponible en: https://www.emerald.com/insight/content/doi/10.1108/IMCS-01-2014-0006/full/html

KIRCH OLAF; Dawson Terry. Guía de Administración de Redes con Linux. [Internet] Varsovia: OReilly, 2000. [Consultado 25 de mayo 2022] Disponible en: http://ganimides.ucm.cl/haraya/doc/GuiaLinux.pdf

LAMPING, ULF; Warnicke, Ed. Wireshark user's guide. [Internet] Interface, 2004, vol. 4, no 6, p. 1. [Consultado 30 de mayo 2022] Disponible en: https://deim.urv.cat/~carlos.molina/Recursos/WireShark/wireshark_user_guide.pdf

LIN, Xiaodong. Building a Forensics Workstation. En Introductory Computer Forensics. [Internet] Springer, Cham, 2018. p. 53-89. [Consultado 03 de junio 2022] Disponible en: https://link.springer.com/chapter/10.1007/978-3-030-00581-8_3

LÓPEZ BARINAS, Alexander; ALDANA, Andrea Catherine; ALARCÓN, Cuervo, CALLEJAS, Mauro. Vulnerabilidad de Ambientes Virtuales de Aprendizaje utilizando SQLMap, RIPS, W3AF y Nessus [Vulnerability in Virtual Learning Environments using SQLMap, RIPS, W3AF and Nessus]. [Internet] Ventana Informática, 2014, no 30. [Consultado 03 de junio 2022] Disponible en: http://revistasum.umanizales.edu.co/ojs/index.php/ventanainformatica/article/view/276

LÓPEZ DE JIMÉNEZ, Rina Elizabeth. Pruebas de penetración en aplicaciones Web usando hackeo ético. [Internet] En: Revista tecnológica (2017). p 13. [Consultado 03 de junio 2022] Disponible en: http://www.redicces.org.sv/jspui/handle/10972/3018

LÓPEZ ACOSTA, Alberto; Monroy, Elver Yesid; MELO, Murcia, Pablo; LINARES, Andrés. Evaluation of the WPA2-PSK wireless network security protocol using the Linset and Aircrack-ng tools. [Internet] Facultad de Ingeniería, 2018, vol. 27, no 47, p. 71-78. [Consultado 03 de junio 2022] Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=6359518

MAYNOR, David. Metasploit toolkit for penetration testing, exploit development, and vulnerability research. [Internet] Elsevier, 2011. [Consultado 03 de junio 2022] Disponible en: https://books.google.es/books?hl=es&lr=&id=JWgNVFtbWJ4C&oi=fnd&pg=PP1&dq=Metasploit+Framework&ots=N94wReUUOZ&sig=7NwAJSKb96T0XhOnBQjUwJ98nGE

MAHAJAN, Akash. Elementos básicos de Burp Suite. [Internet] Packt Publishing Ltd, 2014. [Consultado 03 de junio 2022] Disponible en:https://books.google.es/books?hl=es&lr=&id=LsWiBQAAQBAJ&oi=fnd&pg=PT7&dq=Burp+Suite&ots=AwgEHVrdcS&sig=ZAcCYRzwj1MYP5BM8MydTZ_ZSJ4

MASON, ANDREW G.; Newcomb, Mark J. Cisco secure Internet security solutions. [Internet] Cisco press, 2001. [Consultado 21 de mayo 2022] Disponible en:

https://books.google.es/books?hl=es&lr=&id=8D90NjKvmBAC&oi=fnd&pg=PR18&dq=1.%09MASON,+Andrew+G.%3B+NEWCOMB,+Mark+J.+Cisco+secure+Internet+security+solutions.+Cisco+press,+2001.&ots=EVQ4qbLmM8&sig=dAEOm_XyTEXIb2p18FApAD6qjos

MELLER, Yosef; LIBERZON, Alex. Particle data management software for 3dparticle tracking velocimetry and related applications–the flowtracks package. [Internet] Journal of Open Research Software, 2016, vol. 4, no 1. [Consultado 29 de mayo 2022] Disponible en: https://openresearchsoftware.metajnl.com/articles/10.5334/jors.101/

MIRABÁ QUIMÍ, Freddy José. Diseño de una guía metodológica para el análisis forense digital tomando como base equipos con el sistema operativo Windows 8.1. 2021. Tesis de Licenciatura. [Internet] La Libertad: Universidad Estatal Península de Santa Elena, 2021. [Consultado 03 de junio 2022] Disponible en: https://repositorio.upse.edu.ec/handle/46000/6491

MUTUNE George. 27 Top Cybersecurity Tools for 2021. [Internet] Cyberexperts. 2021. [Consultado 13 de junio 2022] Disponible en: https://cyberexperts.com/cybersecurity-tools/

NORTON, DUANE. An ettercap primer. [Internet] SANS Institute InfoSec Reading Room, 2004, vol. 5. [Consultado 03 de junio 2022] Disponible en: https://www.sans.org/white-papers/1488

OCHOA GUEVARA, Frey Marín. Estudio de seguridad en las bases de datos, mediante metodologías de Pen Test, Ethical Hacking en la secretaria de Hacienda Municipal de Los Patios. [Internet] Repositorio UNAD. 2018. [Consultado 05 de mayo 2022] Disponible en: https://repository.unad.edu.co/handle/10596/21194

OSORIO CARRERO, John Edward. Análisis y valoración de vulnerabilidades de la Empresa NOSTRADAMUS SA. [Internet] Repositorio UNAD. 2020. [Consultado 05 de mayo 2022] Disponible en: https://repository.unad.edu.co/handle/10596/37434

OJAGBULE, OLAJIDE; Wimmer, Hayden; Haddad, Rami J. Vulnerability Analysis of Content Management Systems to SQL Injection Using SQLMAP. [Internet] 2018. IEEE, 2018. p. 1-7. [Consultado 30 de mayo 2022] Disponible en: https://ieeexplore.ieee.org/abstract/document/8479130/

PASCUALE Darío, SOFÍA,. Linux: Hacia una revolución silenciosa de la sociedad de la información. [Internet] Revista de Ciencias Sociales (Ve), 2004, vol. 10, no 2, p. 207-223. [Consultado 21 de mayo 2022] Disponible en: https://www.redalyc.org/pdf/280/28010202.pdf

PASTRANA FRANCO, Adrián; Marmolejo Serrano, Javier. Pruebas de penetración a la infraestructura tecnológica de la Empresa Taller Industrial ALKAN SAS de la ciudad Guadalajara de Buga, Valle para identificar vulnerabilidades. [Internet] Repositorio UNAD. 2018. [Consultado 05 de mayo 2022] Disponible en: https://repository.unad.edu.co/handle/10596/20724

QIAN FENG; Xu, TIAN-BING; Zuo, Lei. Design, optimization, modeling and testing of a piezoelectric footwear energy harvester. [Internet] Energy conversion and management, 2018, vol. 171, p. 1352-1364. [Consultado 03 de junio 2022] Disponible en: https://www.sciencedirect.com/science/article/pii/S0196890418306782

RAMADHAN, Akhmad; FAJAR, Putra; BIMA, Cahya. Rancang bangun sistem informasi penjualan dan pembelian secara tunai alat-alat kesehatan berbasis object oriented pada toko ichsan médica. [Internet] Idealis: InDonEsiA journaL Information System, 2018, vol. 1, no 1, p. 65-72. [Consultado 29 de mayo 2022] Disponible en: https://jom.fti.budiluhur.ac.id/index.php/IDEALIS/article/view/118

REVISTA SEMANA. Ciberseguridad. Diez datos sobre el estado de la ciberseguridad tras la pandemia [Internet] Semana. 2020. [Consultado 30 de mayo 2022] Disponible en: https://www.semana.com/tecnologia/articulo/cifras-sobre-el-estado-de-la-ciberseguridad-en-america-latina-en-2020/311346/

RODRÍGUEZ LLERENA, Alain Eduardo. Herramientas fundamentales para el hacking ético. [Internet] Revista Cubana de Informática Médica, 2020, vol. 12, no 1, p. 116-131. [Consultado 25 de mayo 2022] Disponible en: https://www.medigraphic.com/cgi-bin/new/resumen.cgi?IDARTICULO=94154

SALAME Walid. How to use Ettercap. [Internet] Kalitut. 2021. [Consultado 13 de junio 2022] Disponible en: https://kalitut.com/how-to-use-ettercap/

SANTO ORCERO, David. Kali linux. [Internet] Grupo Editorial RA-MA, 2018. [Consultado 30 de mayo 2022] Disponible en: https://www.ra-ma.es/libro/kali-linux_83260/

SANDOYA ROMERO, Álvaro William. Aplicación de herramientas de hacking ético y análisis forense para la explotación de vulnerabilidades en servidores basados en linux mediante exploits, detección de ransomware en ordenadores con sistemas Windows, recolección de evidencias digitales y la ejecución de sandbox para la identificación de software malicioso. Caso de estudio: hospital león becerra. [Internet] 2021, 138p. Trabajo de grado (obtener el título de Ingeniero en Networking y Teleomunicaciones). Universidad de Guayaquil. [Consultado 03 de junio 2022] Disponible en:http://repositorio.ug.edu.ec/handle/redug/52299

SINGH, Abhinav. Instant Kali Linux. [Internet] Packt Publishing Ltd, 2013. [Consultado 03 de junio 2022] Disponible en: https://www.researchgate.net/profile/Abhinav-Singh-31/publication/313821091_Instant_Kali_Linux/links/58a750f6a6fdcc0e078aed50/Instant-Kali-Linux.pdf

SHIVANANDHAN Manish. 10 Tools you should know as a cybersecurity engineer. [Internet] FreeCodeCamp. 2020. [Consultado 05 de junio 2022] Disponible en: https://www.freecodecamp.org/news/10-tools-you-should-know-as-a-cybersecurity-engineer/

TIBAQUIRA CORTES, Yesid Alberto. Metodología de gestión de incidentes de seguridad de la información y gestión de riesgos para la plataforma SIEM de una entidad financiera basada en la Norma ISO/IEC 27035 e ISO/IEC 27005. [Internet] Repositorio UNAD. 2015. [Consultado 21 de mayo 2022] Disponible en: https://repository.unad.edu.co/handle/10596/3634

TIMALSINA, Umesh; GURUNG, Kiran. Metasploit framework with kali linux. [Internet] Department of Electronics and Computer Engineering, IOE, Thapathali Campus, Thapathali, Kathmandu March, 2017, vol. 10 [Consultado 03 de junio 2022] Disponible en: https://www.researchgate.net/profile/Umesh-Timalsina/publication/316874535_Use_of_Metasploit_Framework_in_Kali_Linux/links/59150ff4aca27200fe4ea286/Use-of-Metasploit-Framework-in-Kali-Linux.pdf

UNIPYTHON. Los mejores 20 programas de seguridad informática. [Internet] UNIPYTHON. 2021. [Consultado 05 de junio 2022] Disponible en: https://unipython.com/las-mejores-20-programas-de-seguridad-informatica/

WANG, SHAOQIANG; XU, Dongsheng; YAN, Shiliang. Análisis y aplicación de Wireshark en la enseñanza del protocolo TCP/IP. [Internet] En 2010 Conferencia Internacional sobre Ecosistemas y Tecnologías Digitales en Redes de E-Salud (EDT). IEEE, 2010. pág. 269-272. [Consultado 03 de junio 2022] Disponible en: https://ieeexplore.ieee.org/abstract/document/5496372/

WOLF, GUNNAR. Fundamentos de sistemas operativos. [Internet] Lulu.com, 2015. [Consultado 25 de mayo 2022]Disponible en:

https://books.google.es/books?hl=es&lr=&id=836YCgAAQBAJ&oi=fnd&pg=PA11&dq=1.%09WOLF,+Gunnar.+Fundamentos+de+sistemas+operativos.+Lulu.+com,+2015.&ots=OTZ10y3K1r&sig=ZDKFOTU9zPCJKpjS4iPVTUgZ08M