Benemérita Universidad Autónoma de Puebla

Facultad de Ciencias de la Computación

CÓMPUTO FORENSE BAJO LINUX.

TESIS

PARA OBTENER EL TÍTULO DE:

LIC. EN INGENIERÍA EN CIENCIAS DE LA COMPUTACIÓN

PRESENTA: GIOVANNY VARGAS GUTIÉRREZ

DIRECTOR DE TESIS:

M.C. YEINY ROMERO HERNÁNDEZ

ASESOR DE TESIS:

M.C. MA. DEL CARMEN SANTIAGO DÍAZ

Puebla, Pue., México. 26 de Noviembre de 2021

Agradecimientos

Quiero dar gracias a Dios por darme la oportunidad de concluir mis estudios a nivel profesional y dedicar este trabajo a mi mamá Vanessa Gutiérrez Arcos por su muestra de cariño en momentos difíciles dentro de ésta, el apoyo, esfuerzo, consejos, junto con la motivación que me dio desde el primer día que ingresé a la máxima casa de estudios BUAP donde conocí gratas amistades y mi estancia fue más que amena; A su vez a mi papá el Ing. J. Adolfo Vargas Labastida por darme la oportunidad de estudiar y el aprendizaje profesional que me ha brindado dentro del área de las TIC como la motivación que día a día me da para seguir creciendo como persona moral y profesional. Y como olvidar a mi abuelita Ma. R. Dolores Arcos Casco por los apapachos, consejos, regaños y momentos inolvidables que me sirvieron para poder sentirme animoso para llegar hasta el final. También agradezco la enseñanza y métodos de estudio que me impartieron los profesores con los cuales cursé mis materias del plan de estudios dentro de la facultad de Ciencias de la Computación que me dejaron más que satisfecho y complacido de que al egresar de esta importante institución podré desempeñarme de una manera exitosa en los campos que involucran ésta. Mi agradecimiento también va dirigido a J. Mariana Horta Thomé por haber caminado de la mano durante todo este transcurso de preparación profesional, como haberme brindado agradables momentos y experiencias que siempre llevaré presentes de esta etapa de mi vida. Y para finalizar quiero dar gracias infinitas y reconocer la experiencia profesional, académica, laboral y personal, al mismo tiempo la oportunidad que me dieron para trabajar y concluir con este trabajo a mis asesoras de tesis: M.C. Yeiny Romero Hernández y M.C. Ma. del Carmen Santiago Díaz.

Introducción

Hoy en día el uso de los medios digitales ha tomado una gran relevancia, existen millones de dispositivos conectados a la red por minuto, lo que hace que fluyan millones de datos en cuestión de segundos, por lo que es de suma importancia la protección de todos los dispositivos que se encuentran conectados a la red, dado que debemos cuidar la información que fluye a través de ella, es decir, hay que librarla de ataques u otros fines maliciosos, aquí es donde damos cabida a la ciberseguridad. La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, acciones tecnológicas que pueden utilizarse para proteger nuestros equipos en la red de usuarios maliciosos o posibles ataques a nuestros datos. El número de incidentes de seguridad informática está creciendo exponencialmente y la capacidad de responder a este tipo de problemas se ve limitada por la falta de ingenieros profesionales capacitados.

Dentro de la ciberseguridad existen varias ramas que protegen diferentes sectores en la red con el fin de librar los equipos de algún ataque. Entre los más destacados tenemos el Hacking Ético, las auditorías de sistemas y el Cómputo Forense. El campo de la informática forense es prácticamente nuevo y se va actualizando hasta la fecha, podemos describir esta disciplina como la solución y desarrollo a los problemas críticos asociados con delitos informáticos de ciberseguridad o casos especiales que se dieron en un lugar en específico donde se indaga qué pasó con la información, como surgió el ataque, que dispositivos y herramientas se ocuparon para llevarlos a cabo y determinar qué fue lo que sucedió con la información. Estas ramas en particular nos sirven de apoyo para la prevención, dado que una vez estudiado el delito se pueden proponer reglas y estrategias que apoyen al sistema a evitar nuevos ataques.

En esta investigación se va a crear una mesa de trabajo donde propondremos el desarrollo de un laboratorio forense y la implementación de una metodología de apoyo que junto con las técnicas basadas en ciberseguridad y herramientas de Linux (Kali). Demostraremos la eficiencia de cada una de estas, buscando implementar dentro de la materia de seguridad en redes de la Facultad de Ciencias

|de la Computación de la Benemérita Universidad Autónoma de Puebla. Se abarcará desde el punto de vista teórico la importancia de la ciberseguridad. Consideraremos las ramas de la ciberseguridad experimentando en un caso en específico dando una aportación académica sobre este tipo de técnicas de ciberseguridad para el nivel de educación superior. El uso de un laboratorio de cómputo forense puede ayudar a solucionar diferentes problemas, los cuales pueden ser fiscales, investigativos, como diferentes ataques maliciosos a diferentes individuos, es por ello que surgen nuevas implementaciones de tecnologías que facilitan el proceso informático investigativo dentro de una investigación forense, la cual se resuelve por un análisis digital, donde se lleva a cabo una metodología que aplicando sus técnicas y las distintas herramientas existentes de cómputo forense resaltan diferentes hallazgos de evidencia digital. Los beneficios de la implementación de un laboratorio de cómputo forense en diferentes organizaciones facilita actuar dentro de una mesa de trabajo de la manera más adecuada, donde existen diferentes herramientas de entorno confiable las cuales analizan los datos de forma segura y se encarga de proteger los datos recuperados y analizarlos desde diferentes dispositivos, tratando de proporcionar un reporte final como expediente, donde un juez o encargado de una investigación de casos en específico interviene de una manera más adecuada.

Objetivo General

El objetivo de esta investigación es crear una metodología junto con la aplicación de técnicas y medidas de ciberseguridad que utilizan herramientas del sistema operativo Linux basadas en el “cómputo forense” para prevenir delitos cibernéticos. Cabe mencionar que para cumplir el objetivo general se necesita revisar la teoría de la ciberseguridad y sus ramas dentro del cómputo forense para realizar un análisis comparativo de la eficiencia de herramientas, donde se probarán tres herramientas seleccionadas que se ocupan dentro de un laboratorio de cómputo forense con un caso específico y así podamos realizar la adecuada preservación, identificación, extracción y documentación de los casos específicos a investigar, donde se puedan interpretar y deducir las evidencias digitales recolectadas, estableciendo una metodología donde se incorporen estas técnicas basadas en la teoría del “cómputo forense” y demostrar su funcionamiento en una computadora.

Objetivos Específicos

- Revisar la teoría de ciberseguridad y sus ramas del cómputo forense.
- Realizar un análisis y comparativa de la eficiencia de herramientas para llevar a cabo el Cómputo Forense.
- Establecer una metodología donde se incorporen técnicas basadas en la teoría del “cómputo forense” y demostrar su funcionamiento en una computadora.

El documento de tesis se encuentra organizado en tres capítulos, en el primero abordamos el marco teórico, en el segundo capítulo plateamos la metodología y en el tercer capítulo presentamos los resultados. Finalmente presentamos las conclusiones del trabajo, así como las referencias bibliográficas y tres apéndices.

ÍNDICE

ÍNDICE DE FIGURAS

CAPÍTULO 1

1.MARCO TEÓRICO

1.1 ¿Qué es la seguridad en la red?

En la actualidad, el uso de la tecnología ha aumentado exponencialmente y la protección de los datos que contienen los dispositivos pone al descubierto la vulnerabilidad de la información. Actualmente es complicado asegurar nuestra privacidad en un navegador web ya que hay diferentes tipos de ataques malintencionados como: phishing, ransomware, spyware, robo de identidad, apoderamiento de dispositivos, fraudes cibernéticos, extorsión, etc. Por ello los especialistas en seguridad informática desarrollan nuevas herramientas para que diferentes usuarios puedan ocuparlas para no estar expuestos en la red. La seguridad de la red es el uso de políticas, servicios y prácticas que previenen y supervisan acciones que se realizan en la red como: el acceso no autorizado, la modificación o la denegación de servicios o recursos, intercambio de información etc. En cambio, la ciberseguridad es la práctica de defender las computadoras, los servidores y los diferentes dispositivos que se conecten a las redes manteniéndolos al margen de cualquier ataque malicioso.

Originalmente, el internet era una red transparente y de libre acceso al conocimiento, no era necesario registrarse y abrir cuentas con claves para poder acceder a la información o servicios que éste brindaba. La privacidad y seguridad no eran temas de relevancia hasta que se inició la comercialización en el internet, y los datos personales se expandieron por toda la red. Debido a ese crecimiento tan espontáneo surgió la arquitectura de red determinada como una organización funcional que usa aplicaciones de red junto con distintos protocolos que sirven para poder comunicarnos, generalmente el desarrollador de una red se enfoca en el trayecto, seguridad y vulnerabilidades, escaneando el tráfico de la red que fue diseñada, para poder observar lo que sucede con el intercambio de información. Parte de la seguridad de red es la encriptación de los datos lo que ayuda a protegerlos en su paso por la red. La “criptografía” se encarga del cifrado de la información, está garantiza que el texto plano sufra modificaciones al momento que

se envía y no pueda ser legible a simple vista. El mensaje va identificado por una cadena hash, la cual si llega a tener una alteración cambiará por completo su contenido. Por lo tanto, las personas encargadas de la seguridad de una red deben contemplar diferentes aspectos de seguridad en las aplicaciones que usan Internet, aplicando pruebas de penetración de la red para garantizar que la información que transfieren llegue segura a su destino. [1]

La ciberseguridad permite a diferentes organizaciones proteger sus recursos financieros, sistemas de información, datos personales de diferentes ataques. Existen softwares dedicados a la protección de la información sensible que permite evaluar el nivel óptimo de seguridad que deben tener las diferentes organizaciones, considerando los aspectos relacionados con la reducción de riesgos. Sin embargo, con el aumento en el uso de dispositivos y sus actualizaciones se generan vulnerabilidades que tienen como consecuencia la inseguridad, por lo cual, al generarse ataques a dichos dispositivos es necesario guardar antecedentes para en un futuro resolver algún otro de similares características, es aquí donde entra la informática forense la cual nos sirve para identificar los posibles delitos informáticos, pero aplicando métodos y técnicas de investigación de cómputo forense que permiten reconstruir y seguir los pasos de los eventos que tuvieron lugar en uno o varios equipos donde se alteró información. La efectividad de estos métodos se basa en las herramientas de software que ocupan para solucionar problemas de alteración en la información. Se pueden emplear dos tipos de sistemas de detección de intrusos, (Host-IDS) permite la detección de la ubicación del equipo de cómputo además de las actividades que se están llevando a cabo en este. (Network IDS) se utiliza para detectar segmentos de red donde están haciendo uso de la red que ocupa el equipo de cómputo o los intrusos que quieren tener acceso a esta, arrojando el rastro de procedencia de estos intrusos, capturando el tráfico de procedencia de la red. Con lo anterior podemos comentar que, si las diferentes organizaciones no cuentan con una estrategia óptima para la protección de su información, no podrán protegerse de diferentes ataques cibernéticos. [2][3]

Por otro lado, otro recurso que nos puede ayudar a mejorar la seguridad dentro de cualquier organización es la implementación y conocimientos de diferentes dispositivos, como un firewall el cual es una solución de ciberseguridad que utiliza mecanismos de defensa que ayudan a la protección de la información que va de un punto a otro, este ayuda a minimizar los riesgos de incrustación o modificación de la información de nuestros equipos enlazados a la red. Existen diferentes dispositivos con diferentes soluciones de seguridad informática que pueden utilizar diferentes organizaciones permitiéndoles identificar y afrontar con precisión los riesgos de seguridad en la transmisión de datos de una red, permitiéndoles tener una protección integral y completa. Dada las necesidades de las diferentes organizaciones surgen nuevas cuestiones de seguridad y con fines de reducir los riesgos se pueden implementar servidores firewall Linux. Esto nos resultaría muy efectivo de acuerdo con las exigencias de las políticas de seguridad que se ocupan hoy en día, minimizando riesgos, costos y ataques malintencionados. [4]

Desde otro punto de vista el surgimiento de las redes de comunicación, en particular de Internet, han abierto nuevas posibilidades para el intercambio de información. Al mismo tiempo, se han hecho más vulnerables, amenazando la seguridad e información que se transmite. Por eso, es necesario crear diferentes mecanismos de protección, dirigidos a la confidencialidad y autenticidad de los documentos electrónicos, todo esto es parte de una tecnología denominada criptografía. Debido a la necesidad de resguardar, compartir y ocultar información confidencial nació la “criptografía”, a lo largo de la historia existen y existieron algunas situaciones en las cuales se debía compartir información con personas específicas, esta información se cifraba y se enviaba a una persona en específico, la cual podía recuperar la información que venía oculta en el mensaje, se hacía de esta manera para evitar que supieran información confidencial, si un mensaje llegaba a ser interceptado por enemigos o atacantes de esta forma no podían saber el tipo de información que contenía el mensaje. La criptografía tiene como objetivo intercambiar información entre dos o más individuos de manera segura y confidencial mediante un canal de transmisión. Para llevar a cabo este proceso de encriptamiento, el mensaje original

conocido como “texto plano” se transforma en una clave con la ayuda de métodos como: transposición, sustitución o cifrado, el texto se cifra con un conjunto de claves y reglas que solo los conocían los usuarios (personas) autorizadas. Los métodos de criptografía se han utilizado a lo largo de los años, desde la época griega hasta finales del siglo XIX, para ocultar información a sus adversarios o personas no autorizadas que no podían tener acceso a cierta información clasificada, donde se buscaba solo transmitir dicha información con personas que tenían conocimiento de estos mensajes. Una de las principales formas de encriptamiento clásico que mantenía resguardada la información en general, fueron los mensajes con contenido militar su objetivo era comunicarse con su ejército de manera rápida y segura de esta forma si el mensajero era capturado el enemigo nunca conocería la información ya que esta iba cifrada. Este tipo de método criptográfico fue documentado como “escítala lacedemonia”, utilizada por el ejército de espartanos en Grecia, fue el primer sistema criptográfico militar de la historia del siglo V a.c utilizado por Alejandro Magno en el año 356-323 a.c. Como iban pasando los años surgieron nuevos métodos criptográficos algunos de ellos (Atbash, Cifrado de Julio César, Cifrado de Polibio,etc). Como consecuencia, en la segunda guerra mundial nacen las “máquinas criptográficas” eran cifradores de rotación mediante discos de cifrado considerados como las primeras herramientas de cifrado avanzado, estas se usaron para crear sistemas de cifrado complejo donde sus operaciones dentro de los criptogramas usaban bases matemáticas considerando sus operaciones exigentes para cifrar un mensaje. Las primeras máquinas que podían hacer criptogramas fueron desarrolladas por Boris Caesar Wilhem Hagelin (1892-1983) desde ese entonces la criptografía utilizada a partir de la segunda guerra mundial fue creciendo y actualizándose constantemente, hasta llegar al uso extendido de ordenadores personales (Pc´s), su desarrollo como las aplicaciones han tenido un gran impacto desde los años setenta del siglo XX hasta ahora. Hoy en día existen diferentes algoritmos de criptografía de clave simétrica y asimétrica los cuales fueron diseñados para proteger mensajes privados entre usuarios, instituciones, organizaciones, etc. En deducción es importante implementar como medio de seguridad un algoritmo de cifrado en la información delicada que compartimos

dentro de la red, en absoluto podemos considerar esto una técnica de seguridad donde nuestra información será transmitida de modo seguro y así se pueda evitar ciertos problemas de inseguridad que pueden surgir cuando navegamos en la red.
Por lo anterior la “criptografía” se ocupa para el cifrado o codificado de mensajes que contienen información confidencial, intercambiando mensajes de un usuario a otro con el fin de hacerlos intangibles a receptores no autorizados. La seguridad informática en específico ocupa diversas variantes criptográficas estas cuentan con algunos esquemas de manejo de llaves privadas y públicas: RSA y PGP que se han convertido en estándares para sistemas eficientes que intercambian información. En conclusión, se pueden ocupar diferentes mecanismos de defensa de archivos para reducir ciberataques, tratando las limitaciones y soluciones que ofrecen contra cualquier forma de intromisión que exista. [5][6]

1.2 ¿Qué es la ciberseguridad?

Hoy en día la información digital se ha convertido en una parte esencial de nuestras vidas cotidianas. Diferentes tipos de organizaciones, como instituciones médicas, financieras y académicas utilizan una red donde transmiten información de manera eficaz, la cual utilizan para recopilar, procesar, almacenar y compartir cantidades exhaustivas de información digital. En vista de que se recopila y comparte esta información surge la importancia de la protección de la información la cual se encarga de proteger nuestra identidad, seguridad nacional y estabilidad en nuestra vida económica y cotidiana.
La ciberseguridad tiene la tarea de encargarse constantemente de proteger sistemas de red y todos los datos digitales contra el uso no autorizado o los daños a nivel personal, donde se encarga de proteger nuestra identidad, datos y todos los dispositivos digitales que utilizamos. A nivel corporativo, tiene la responsabilidad de proteger la reputación de los datos personales de sus usuarios y clientes buscando siempre su bienestar e intereses como también de las diferentes organizaciones que estén relacionadas.

La confidencialidad, integridad y disponibilidad, llamadas la tríada CID véalo en figura 1. Son una guía para la seguridad informática que pueden utilizar diferentes organizaciones.

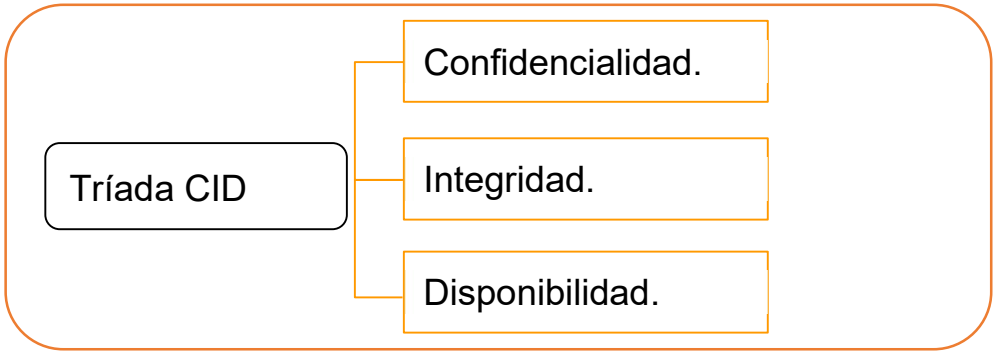


Figura 1. Tríada "CID".

Confidencialidad garantiza la privacidad de los datos digitales mediante la restricción de la información de las personas que no tienen derecho a tener acceso a esta, mediante un cifrado de datos que sirve de manera de autenticación.

La integridad asegura la información de que sea confiable y precisa durante una transferencia de datos donde estos permanecerán inalterados, teniendo una consistencia y cifrado adecuados para no tener daños en la información digital garantizando accesos no autorizados a la información de diferentes usuarios.

La disponibilidad garantiza que toda la información digital esté disponible en cualquier momento que la soliciten las diferentes personas autorizadas. [7]

Dando cabida a lo anterior, en la ciberseguridad se pueden llevar a cabo diferentes acciones para prevenir ciberataques, realizando diferentes procesos para solucionar los efectos de un ataque y poder actuar de la mejor manera para dar solución al ataque y determinar quién lo realizó. Es por ello que, existen distintas ramas de la ciberseguridad como: peritaje informático, seguridad de las redes informáticas, protección de base de datos, cómputo forense, hacking ético, big data en entornos seguros, entre otras; que se encargan de los distintos delitos y ataques informáticos que hoy en día van creciendo de manera espontánea. [8]

1.3 Ramas de la ciberseguridad.

Debido al crecimiento de la tecnología puede hacerse complicado conocer a fondo la existencia de todos los ataques informáticos diferentes que existen y que pueden dañar a un usuario a través de un dispositivo, es por ello que existen las ramas de la ciberseguridad mencionadas anteriormente, que ayudan a prevenir ese tipo de ataques, donde se investigan y buscan nuevos procesos como metodologías para solucionar los efectos que hubo durante un ataque informático, las que más resaltan en su investigación debido a los problemas que han ocasionado con conductas inseguras, dañinas e inadecuadas para diferentes usuarios son: Peritaje informático, Seguridad en las redes informáticas, Protección de la base de datos, Cómputo forense, Hacking ético, Big data en entornos seguros, etc. Por lo que, cada vez que surge un ataque estas ramas de la ciberseguridad junto con sus técnicas se van actualizando constantemente para crear nuevas normas de seguridad y especializarse en cada rama para contrarrestar los sucesos que ocurrieron en diferentes tipos de ataques. [9]

Peritaje informático: Hoy en día diferentes motivos del uso excesivo del internet y de los diferentes dispositivos que tienen acceso a este, tienen ciertas leyes civiles como penales dentro de cada país, es por ello que se debe hacer conciencia de las consecuencias que genera hacer mal uso de estos dispositivos y aplicaciones que dan uso dentro de estos, ya que las conductas inadecuadas o intencionales como: acoso, robos de identidad, agresión verbal, sexual, psicológica, accesos no autorizados a la red, robo de información confidencial, etc. Pueden ser investigadas por un perito informático donde buscará las pruebas necesarias para determinar qué pasó con la información afectada, la persona que fue a atacada, ubicación de la red donde se hizo el ataque, como los dispositivos y posibles herramientas que se ocuparon y proceder a un juicio penal donde se investigan los casos específicos que se realizaron dentro de estos dispositivos informáticos y dar con el posible responsable. [10]

Seguridad en las redes informáticas: Es una barrera de defensa que contiene varios niveles de protección en una red, cada uno de estos niveles de seguridad tiene políticas y controles de seguridad los cuales autorizan a diferentes usuarios

los recursos que pueden utilizar en la red, por otra parte, bloquea a los usuarios no autorizados (atacantes) evitando que ataquen vulnerabilidades y amenacen la seguridad de la red como los usuarios que pertenecen a esta. [11]

Protección de la base de datos: La protección de los datos es esencial para cualquier tipo de empresas, asociaciones e instituciones que almacenan grandes cantidades de datos, por lo que, existen sistemas de almacenamiento que son utilizados para guardar, administrar y gestionar información confidencial que es administrada por un profesionista o experto en bases de datos estructuradas. Este tipo de sistemas empleados en diferentes organizaciones se les conoce como sistemas de planificación (ERP, Enterprise Resource Planning); estos sistemas crean y mantienen archivadores electrónicos donde tienen la tarea de garantizar la seguridad de los datos, esto representa un gran reto para los diferentes sistemas que existen, de tal manera que existen procedimientos de seguridad en los datos como: las copias de seguridad, supervisión de las modificaciones automáticas en aplicaciones, cifrado de datos y la implementación de hardware que ayude a reducir los riesgos de ataque a la base de datos como a los archivos locales que se encuentren dentro de una red estructurada, sabemos que en muchas ocasiones son susceptibles a fallos, vulnerabilidades y ataques externos, por eso debemos familiarizarnos con los componentes involucrados para la protección de los datos como: servidores, aplicaciones, antivirus, firewalls, sistemas de gestión de base de datos y las diferentes normas de seguridad que existen para prevenir diferentes tipos de ataques, los más conocidos en esta rama son las "inyecciones SQL" que se hacen comúnmente a las bases de datos. Una inyección SQL se le define a la explotación de una vulnerabilidad dentro de los sistemas de bases de datos existentes, donde un atacante accede a los datos de manera intrusiva (ilegal) por medio del lenguaje SQL, donde busca aprovechar los fallos de seguridad en la superficie de la base de datos modificando los datos que no han sido enmascarados correctamente, agregando nuevos metacaracteres como: guión doble, comillas, el punto y coma, en los datos. Estos caracteres especiales representan diferentes funciones para el lenguaje SQL y permiten la influencia externa sobre las instrucciones ejecutadas. Este tipo de inyecciones SQL son comunes que se

realicen con la ayuda de programas PGP y ASP que dependen de interfaces antiguas de estos sistemas de bases de datos haciendo un blanco perfecto para poder ser atacados.[12]

Cómputo forense: Se encarga de preservar, identificar, recolectar, examinar y exponer los datos digitales encontrados para un proceso legal o bien para alguna prueba de seguridad dentro de diferentes organizaciones con el fin de evitar este tipo de delitos y ataques malintencionados en diferentes sistemas de software y equipos de hardware como: USB, discos duros, servidores, PC´s, laptops, tablets, entre otro tipo de dispositivos. La información que contienen estos equipos de diferente estructura tecnológica son tratados por expertos para analizar la información que contienen y determinar que fue con lo que se hizo con la información, sabiendo de qué manera se actuó con ellos donde se aplica una serie de técnicas, metodologías y un análisis científico profundo a la información recopilada, con la ayuda de herramientas de software y hardware que se encargan de determinar y reconstruir las pruebas informáticas dentro de los dispositivos electrónicos, presentando los análisis de esta información y concluir que hizo la persona que ocupó estos dispositivos o sistemas.[13]

Hacking ético: Se refiere a la acción de realizar pruebas de intrusión en una red, controladas por un responsable donde estas son efectuadas dentro de los sistemas informáticos de una empresa o diferentes instituciones, es decir el consultor llamado “pentester” actuará como un atacante malintencionado conocidos como hackers, pirata informático, cracker. Donde buscará tratar de encontrar vulnerabilidades en los equipos que audite y explotará diferentes recursos, usando como medio la red, donde tratará de obtener accesos a los sistemas y determinará cuáles podrían ser afectados, este tipo de ataques están siendo supervisados por la organización que paga por los servicios de un pentester. Este tipo de servicios busca garantizar la reducción de riesgos en la operatividad de sus servicios informáticos dentro de una organización, evitando poner en riesgo su información. Cabe mencionar que un auditor en seguridad informática “pentester” debe poseer conocimientos concretos en tecnologías basadas en cómputo forense y diferentes que ayudan a efectuar este tipo de técnicas de hacking ético. También se aplican diferentes metodologías para

llevar a cabo este tipo de auditoría, donde se llevan a cabo un orden del trabajo que se realizó para optimizar el tiempo en las fases del hacking.[14]

Big data en entornos seguros: Para poder comprender lo que significa “big data” podemos citar lo que dijo Gartner, por el año 2001 que continúa siendo la definición de referencia: Big data son los datos que contienen una mayor variedad y se presentan en volúmenes crecientes a una velocidad superior conocida como “las tres V”. Citado lo anterior podemos decir que un big data está conformado por un conjunto de datos de volumen complejo procedente de una fuente de datos. Este conjunto de datos es demasiado grande para ser procesado por un software de procesamiento convencional, por lo cual una computadora común no podrá procesarlos ni administrarlos. Sin embargo, estos datos de gran volumen pueden utilizarse para solucionar problemas de ciberseguridad en diferentes organizaciones. Un big data en un entorno seguro se centra en la seguridad como en el almacenamiento y transmisión de datos, donde estos son administrados por profesionales que cimientan bases teóricas firmes de big data, business intelligence y seguridad, estos colaboran con empresas u organizaciones de primer orden en el tratamiento y análisis de grandes volúmenes de datos. Hoy en día un big data se caracteriza por tener organizados, analizados y seguros su gran tamaño de datos, es por ello que ocupan la ciberseguridad optando por usar las nuevas tecnologías que se van desarrollando para el análisis y almacenamiento de datos, ya que un volumen de datos duplica su tamaño cada dos años aproximadamente. Por lo cual las organizaciones continúan esmerándose por mantener seguros los datos con los que trabajan, haciendo ese crecimiento de datos confiable y con una garantía de resguardo, por ello siempre las organizaciones tratarán de encontrar nuevas formas para almacenarlos de una manera eficiente y segura. [15]

1.4 Cómputo forense.

Es la rama de la ciberseguridad que se encarga de determinar el origen de los datos dañados, robados o modificados que se hicieron en uno o varios dispositivos que almacenan información, esta ciencia busca adquirir, preservar y presentar las pruebas obtenidas mediante una investigación y análisis a fondo de qué fue lo que ocurrió a la información durante el ataque en diferentes dispositivos. El cómputo forense no tiene exactamente como objetivo prevenir los delitos informáticos, pero sí se encarga de preservar la información exacta de lo que sucede durante un ataque malintencionado, determinando lo que le ocurrió a la información almacenada en diferentes dispositivos.

Esta rama tiene como objetivo:

- Comprensión de daños causados por ciberatacantes.
- Persecución y procesamiento judicial de los ciberatacantes o personas que cometen delitos de otra índole que ocuparon dispositivos para realizar estos.
- Aplicación de métodos y técnicas, que reducen y previenen ataques informáticos.

Estos objetivos se pueden lograr con la ayuda de distintas herramientas de software y hardware que se ocupan en el “cómputo forense”, estas se ocupan según sea el caso, donde lo primordial es la recopilación de información o evidencia dentro de los dispositivos que fueron recolectados de una investigación en especial. Las herramientas que se ocupan dentro del “cómputo forense” pueden analizar un disco duro, servidores, dispositivos móviles, memorias USB, BIOS, archivos, carpetas, direcciones MAC, logs de seguridad IP, redes, software, hardware, credenciales de autenticación, agendas electrónicas (correos), dispositivos GPS, impresoras, cámaras IP, etc. En la actualidad existen diferentes herramientas que facilitan este tipo de investigaciones en análisis forense, las cuales nos pueden ayudar a saber que paso con la información que fue afectada y prevenir cómo contrarrestar diferentes ataques de ciberseguridad.[16]

1.4.1 Ramas del cómputo forense.

Un área de la ciberseguridad que está adquiriendo bastante interés es el cómputo forense, debido al crecimiento exponencial de la información en diferentes dispositivos como discos duros, memorias usb, tabletas, smartphones, etc. Ha crecido el robo de información. A su vez, el internet es indispensable para realizar parte de nuestras actividades cotidianas como: el pago de servicios, envío de información, comunicación con otras personas, transacciones bancarias, lo que pone en vulnerabilidad la información almacenada en estas aplicaciones o dispositivos donde pueden surgir ciberataques con un propósito específico, en esta parte entra el "cómputo forense" que consiste en tratar la información que fue expuesta o tomada de forma indebida de un dispositivo, este busca saber desde donde se realizó el ataque y que paso con esa información como también fomentar las pruebas de pentesting con diferentes herramientas de ciberseguridad para evitar los ciberataques. [8]

La informática forense preserva cualquier evidencia de información digital en su forma original, recopilando, identificando información digital y protegiéndose de ataques malintencionados con el propósito de proteger y reconstruir archivos que pudieron ser dañados en un ataque cibernético. Cabe mencionar que la informática forense ocupa subramas principales como: análisis forense de móviles, análisis forense de la red, análisis forense de los datos, análisis forense en base de datos, donde estas se pueden poner en práctica en dispositivos móviles, laptops, Pc's, tabletas, etc.; donde estas pueden usar diferentes herramientas tecnológicas para recuperar datos. A la vez estas herramientas de cómputo forense son muy usadas para combatir los delitos informáticos, investigando escenas de crimen donde buscan saber qué pasó con la información almacenada en una computadora personal o de diferentes dispositivos. El pentesting es muy significativo y aporta una gran solución para problemas de pérdida de información, robo o modificación, utilizando hardware y software específico de ciberseguridad, este método cubre las necesidades para la protección de una red que podemos implementar para reducir los diferentes tipos de vulnerabilidades. [17]

Análisis forense de dispositivos móviles: la información que contiene un dispositivo móvil cambia o varía con facilidad y de forma poco predecible, ya que no solo usa el espacio en memoria interna si no también ocupa espacio en la nube y comparte con otras aplicaciones dentro del dispositivo, lo que hace que la información que contiene tenga cierta movilidad convirtiéndola en susceptible y fácil de perderse o ser tomada en algún sitio que recopile información personal. Por muy efectiva que sea una herramienta de análisis forense en sus funcionalidades las cuales identifican y recuperan información de datos eliminados o robados las posibilidades de éxito de recuperar estos datos son inversamente proporcionales al tiempo de uso del dispositivo o el estado en el que se encuentre. Por consiguiente, si queremos evitar o recuperar la pérdida de información (de forma intencionada o accidental) se tiene que anticipar y planificar la forma y el momento adecuado para acceder al dispositivo. Por otro lado, debemos identificar todo lo relativo a sus características como el estado del dispositivo y qué uso se le dio. A su vez, investigar el contenido y características del dispositivo. y por otro, planificar las herramientas con las que se va a tratar el dispositivo, eligiendo las más eficientes para el caso específico que se está tratando, de forma que se pueda garantizar una custodia adecuada y un análisis controlado de la información.[18]

Análisis forense de la red: Se le conoce como el proceso del monitoreo de paquetes donde se analiza el tipo de tráfico de la red para detectar ataques como: el escaneo de puertos, intrusiones, barridos de ping, incrustación de malware dentro de la red, entre otros. Esto conlleva identificar los problemas que surjan dentro de una red, recopilando y revisando los datos que se intercambian entre un cliente y servidor, para resolver esto se debe elegir las mejores estrategias de defensa para darle solución a los diferentes tipos de problemas que surjan e implementar normas adecuadas de seguridad. Esta rama del cómputo forense se encarga de estudiar las comunicaciones y redes, con el objetivo de descubrir el origen de un incidente o ataque, para ser utilizado como evidencia digital de lo que pasó en la red donde se transmitieron datos en tiempo real identificando los protocolos inseguros o comportamiento anormal dentro de la red.[19]

Análisis forense de los datos: Consiste en organizar una estación de trabajo para contrarrestar los incidentes que surgen en una red, dispositivos, aplicaciones, entre otro tipo de software y hardware. Este tipo de análisis con lleva a un proceso de métodos que permiten identificar, recuperar, reconstruir y determinar lo que ocurrió con las evidencias obtenidas por una organización que tiene la necesidad de saber que paso con la información asignada para comenzar una investigación ya sea de tipo criminal (distribución de pornografía infantil, fraudes, robos de identidad, extorsión, acoso cibernético, etc.) o de pruebas de penetración (intrusiones, phishing y hacking), con la ayuda de las herramientas de ciencias forenses que cubren diferentes necesidades como diferentes técnicas que aportan principios necesarios para poder deducir la información que se adquirió y se analizó dónde estás buscan conservar la documentación y análisis adecuado para presentar evidencias digitales y después se pueda aceptar legalmente ante un proceso judicial o de la organización que la solicite.[20]

Análisis forense en base de datos: Es el proceso donde se verifica, demuestra, monitorea, registra y analiza los accesos que tuvieron diferentes usuarios a la información almacenada en una base de datos para poder determinar: quien accedió a los datos, cuando se accedió a los datos, desde qué tipo de dispositivo o aplicación se tuvo acceso, ubicación de la red donde se realizó el ataque, comandos SQL o de otro tipo ejecutados dentro de la base de datos, cuál fue el daño y los efectos secundarios que dejó en los datos. Esta rama como los procesos que se llevan a cabo son demasiado importantes ya que determina lo que le paso a la información que fue atacada demostrando la integridad que tienen los datos afectados durante un ataque. Existen diferentes servicios de “auditorías de base de datos” los cuales consisten en realizar un análisis exhaustivo y personalizado a la información determinando nuevas políticas de seguridad para conservar la integridad de los datos.[21]

1.5 Herramientas del cómputo forense.

En la actualidad existen diversas aplicaciones (herramientas) que se utilizan para realizar la labor de un pentester (auditor de ciberseguridad), que ayudan a los expertos en esta rama a solucionar los problemas que surgen de diferentes casos, donde buscan dentro de los diferentes dispositivos asignados por caso, identificar la información afectada como el uso que se le dio, estas facilitan la manera de encontrar las pruebas suficientes de lo que se hizo con la información y con los diferentes dispositivos electrónicos y así poder exponer estas pruebas ante una organización. Estas herramientas de ciberseguridad son muy significativas ya que aportan una gran solución para los problemas de cómputo forense que son la pérdida información, robo o modificación; como el mal uso que le pueden dar distintos usuarios con diferentes intenciones, cabe mencionar que estas pueden utilizar hardware y software con licenciamiento o de uso libre, las diferentes organizaciones pueden elegir en qué tipo de software y hardware pueden ocupar para así satisfacer sus necesidades para realizar el análisis de la información que surja en cada caso. Por esa razón diferentes profesionales en ciberseguridad emplean una estrategia óptima para la protección de la información que tratan, pero hay casos en los que una organización o profesional deben invertir en aplicativos de software de seguridad para alcanzar los niveles de seguridad adecuados para protegerse de diferentes ataques cibernéticos o reestructurar la información que se vio afectada dentro de un ataque.

EnCase Enterprise es un software para uso del análisis forense, este tipo de herramienta se utiliza dentro de un laboratorio de cómputo forense donde se realizan investigaciones digitales, cuenta con un entorno gráfico que es interactivo con el usuario, este tipo de programa lo ocupan investigadores como profesionales en seguridad informática. Este tipo de solución permite a los analistas analizar una gran cantidad de datos y anexarlas a sus pruebas digitales, como también la recuperación de ficheros eliminados o alterados; a su vez pueden tratar zonas de paginación como diferentes clusters de datos. Este programa se ejecuta dentro de un servidor que normalmente se encuentra dentro de un laboratorio forense, contiene diversas herramientas y funciones de recuperación de datos, análisis y la

generación de reportes de los datos tratados. Una vez que el usuario que ocupa el software culmina la investigación de los datos, este genera un esquema que despliega los datos analizados y completa las secciones solicitadas, también se pueden agregar comentarios, instrucciones, explicaciones, etc. Para poder finalizar la investigación de los datos. Este tipo de herramienta sirve como apoyo para el desarrollo profesional como estudiantil en el área de auditoría y seguridad informática donde se minoriza el trabajo de diversas investigaciones. [22]

Autopsy fue desarrollado para el uso de profesionales en computo forense donde tratan incidentes de ciberseguridad como: intrusiones, escenas de crimen cibernético y de uso militar, también tiene una sub-herramienta llamada “Cyber Triage” software de respuesta para incidentes que sucedieron en un tiempo determinado y debe darse solución instantánea a estos, donde encuentra los puntos finales y comprometidos de la investigación que se está llevando a cabo. Dicho lo anterior esta plataforma digital de código abierto cuenta con las principales características de herramientas de cómputo forense, donde arroja los procesos de cómputo forense digital desde la base de datos de la autopsia digital, búsqueda de palabras clave, etiquetado de funciones y la generación de un reporte general de los resultados finales, donde permite desarrollar nuevas soluciones para el análisis forense digital, esta es una solución eficiente y rápida para el análisis de discos duros y esta herramienta se va actualizando con el tiempo para las diferentes necesidades que surgen en hoy en día. [23]

CAINE (Computer Aided Investigative Environment) es una herramienta de código abierto, distribución de GNU/LINUX basada en ubuntu creada en Italia, como un proyecto de “digital forensics” el creador de este proyecto fué Nanni Bassetti, esta ofrece una mesa de trabajo completa, que cuenta con múltiples módulos de herramientas forenses que se visualizan mediante una interfaz gráfica, los objetivos principales de esta es garantizar una interoperabilidad dentro de una investigación digital cumpliendo con las políticas del software establecidas, este sistema está diseñado para ayudarnos en prácticas de cómputo forense profesionales o académicas que abarca desde la preservación de los datos, recolección de la información hasta el análisis de datos exhaustivo en un dispositivo electrónico. [24]

NetworkMiner es una herramienta que se usa para el análisis forense de datos, esta se puede utilizar en sistemas operativos Windows, Linux, Mac OS y FreeBSD. Esta se caracteriza por el análisis de paquetes de diferentes servidores (host) es decir captura el tráfico de la red que deseemos para poder proceder con la investigación de los datos y recolectar las pruebas necesarias para poder tratar cada caso en específico y actuar de la manera más adecuada. Este tipo de herramienta es muy útil para el análisis de tráfico de malware, como también la recuperación de usuarios y contraseñas extraídos de un dispositivo electrónico proporcionando al usuario la posibilidad de encontrar los datos requeridos o solicitados.[25]

Snort software libre de código abierto que se utiliza en el análisis forense y tiene una aplicabilidad en la investigación de delitos informáticos, este previene y detecta las intrusiones dentro de una red. Analizando el tráfico de datos en tiempo real obteniendo un registro de paquetes generado por el protocolo IP, lo cual deja un reporte en forma de archivo para realizar el análisis profundo de la red. Se puede configurar en tres modos:

- **Rastreador:** realiza un registro de paquetes de red y detecta las posibles intrusiones dentro de esta.
- **Sniffer:** interpretar el intercambio de los paquetes dentro la red, mostrándolos en consola y los registra en el disco.
- **Detector de intrusos:** se rastrea el tráfico de la red y es analizado por un conjunto de reglas definidas por el usuario, de acuerdo a la recolección de datos se iniciará una investigación para determinar mejores reglas para el intercambio de datos.[4]

Forensic Toolkit (FTK) debido al crecimiento de los datos almacenados en diferentes dispositivos electrónicos se ha vuelto una tarea compleja recopilar evidencia digital de manera adecuada y eficiente es por ello que surgió esta solución para brindarle a diferentes usuarios que estudian, trabajan y analizan el cómputo forense a reducir la complejidad de trabajo con las cantidades masivas de datos que investigan, esta es reconocida por la velocidad de análisis de datos como correo electrónico, vista de datos personalizables, bloqueador de escritura, procesamiento de datos y facilidad de uso. Dicho lo anterior esta herramienta también puede

realizar réplicas y visualización previa de grandes cantidades de datos para no afectar los datos originales dentro de una averiguación forense, la evaluación de esta herramienta en los diferentes tipos de datos garantiza un análisis complejo.[26]
NMAP (Network Mapper) es un software de código abierto que se ocupa tanto para el análisis de tráfico en la red como también facilitar las auditorías de seguridad en los servidores de una red, donde podemos escanear puertos, protocolos y un mapeo completo de diferentes redes. Es multiplataforma para Linux y Windows cuenta con diferentes versiones que se pueden ocupar dependiendo sea el caso de investigación y las características que se necesiten para cumplir con las tareas a realizar y el monitoreo sea útil y eficiente. [27]

1.6 Distribuciones de Linux que manejan cómputo forense.

Hoy en día existen diversos incidentes en ciberseguridad es por ello que se debe encarar cada caso con diferentes herramientas para amenizar este tipo de incidentes informáticos, en cuestión un informático forense, analista de seguridad, estudiante u otra persona que quiera comenzar a prepararse para este tipo peritaje informático debe conocer una gran variedad de herramientas y comenzar a gestionar cada una de ellas para dar el uso adecuado para posteriormente montar una mesa de trabajo la que podemos llamar “laboratorio de cómputo forense” el cual será destinado para llevar a cabo las pericias correspondientes para uno o más casos en particular. Como ya lo hemos dicho anteriormente un análisis forense tiene como objetivo dar respuesta a saber que paso con la información en diferentes dispositivos electrónicos, abarcando desde que fue lo que ocurrió hasta el origen del ataque, las víctimas y como se fue afectado y comprometido, para deducir lo que exactamente ocurrió y dar seguimiento a una investigación clara y justa. Por ello un profesionista en seguridad busca elegir un conjunto de técnicas analíticas, herramientas y metodologías para poder identificar, preservar, analizar y presentar pruebas válidas dentro de una investigación lo cual lo ayudará a resolver el incidente de manera global y de manera satisfactoria. Dicho lo anterior vamos a describir algunas distribuciones de software libre de Linux las cuales se usan para resolver

la mayoría de los escenarios posibles cuando surgen estos incidentes de ciberseguridad.

DEFT (Digital Evidence and Forensic Toolkit) es un sistema GNU/LINUX dedicado a la ciencia forense digital y actividades de inteligencia militar, la primera versión de esta distribución se introdujo en el año 2005, en la actualidad existen diversas versiones utilizadas para impartir cursos educativos sobre ciencias forenses digitales, análisis de seguridad, etc. También se ocupan en el ámbito profesional para las investigaciones estatales jurídicas y diversos departamentos especializados en ciberseguridad, este S.O posee diversas herramientas que facilitan el análisis de información digital.

SIFT (SANS Investigative Forensic Toolkit) un conjunto internacional de expertos forenses junto con el apoyo del SANS, desarrollaron este sistema de trabajo basado en una distribución de código abierto de GNU/LINUX (Ubuntu) para dar respuesta a los incidentes de ciberseguridad y análisis forense digital. Este cuenta con un kit de herramientas forenses y guías rápidas de usuario como: comandos, operaciones entre otras que ayudan al usuario a entender el sistema y comprender cómo se desenvuelve la ciencia forense con las herramientas que tiene este sistema, las más ocupadas dentro de este son sleuthkit y autopsy. Hay diversas investigaciones desarrolladas por estudiantes que en base al uso de este sistema se crean foros que los hacen muy activos para diferente tipo de público y ayudan a explorar e investigar más de lo que se puede realizar dentro de las ciencias forenses. Una ventaja de esta distribución es que se puede utilizar una distribución ya instalada de Ubuntu y convertir el sistema ya instalado en un kit de herramientas forenses para comenzar a poner en práctica estas.

CAINE 7 (Computer Aide Investigation Environment) distribución de código abierto GNU/LINUX basada en Ubuntu 14.04.1 desarrollada por un italiano, liberada en noviembre del año 2015, esta cuenta con diferentes versiones, una de las funciones más llamativas es que permite bloquear dispositivos como: discos duros, unidades de almacenamiento y la implementación de solo lectura. Esta distribución cuenta con una interfaz gráfica ergonómica para el analista forense y esto hace que facilite las fases de la investigación que debe realizar desde la adquisición de pruebas

hasta el reporte de las pruebas obtenidas. Muchos profesionales de análisis forense les parece muy útil este sistema ya que cuenta con una aplicación llamada “Systemback” la cual permite volver atrás desde un punto de restauración en las copias de los dispositivos que se están investigando y así no contaminar la información o intervenga con el avance de su investigación forense, como también se vuelva inestable el sistema por alguna actualización o se inserte una mala instrucción.

KALI LINUX es una distribución basada en Debian GNU/LINUX diseñada para la auditoría y seguridad informática en general. Fue desarrollada y mantenida por Offensive Security Ltd por Mati Aharoni y Devon Kearns, desarrollando esta distribución a partir de la reescritura de “Backtrack” distribución antecesora de Kali Linux, este S.O puede utilizarse como sistema principal de arranque o por un live-CD o USB. Esta distribución es muy utilizada para hacer pruebas de penetración, diversas auditorías de seguridad, investigación de seguridad, cómputo forense e ingeniería inversa; ocupando las herramientas de software libre más populares en las ciencias forenses y cuenta con diversos manuales para utilizarlas de manera eficaz y sencilla. Muchos profesionales eligen esta herramienta ya que cuenta con herramientas que explotan muchas partes de la investigación forense y facilita los resultados de la evidencia digital de los datos a su vez existe diversa información en internet y cada vez se vuelve más popular para llevar a cabo las ciencias forenses.

Muchos profesionistas de seguridad, investigadores, estudiantes o personas que estudian las ciencias forenses cuentan con conocimientos de hacking ético, lo cual resulta en comprender un poco mejor qué tipo de herramientas se pueden ocupar con mayor facilidad y pueden ocupar para resolver incidentes ocurridos en la vida real o para realizar prácticas que mejoren sus habilidades con herramientas forenses. Por lo que, cada analista forense crea y elige su entorno predilecto y el mismo se sienta cómodo para desarrollar una investigación forense cumpliendo con diferentes estándares, técnicas y metodologías que generan un resultado satisfactorio arrojando un excelente resultado de evidencia digital. [28][29]

1.7 Herramientas en Linux en una distribución Kali.

Dicho lo anterior dentro de la seguridad informática existen demasiadas herramientas sofisticadas que nos pueden ayudar a realizar e implementar las técnicas de cómputo forense para investigar la información de un caso en específico. Aunque estas nos ayudan a disminuir la cantidad de tiempo para poder obtener resultados favorables, no siempre es fácil escoger cuales ocupar y el por qué, ya que diferentes profesionistas escogen su mesa de trabajo y ocupan los aplicativos con los cuales están más familiarizados y se les facilita implementarlos en una investigación que lleva a cabo el cómputo forense y hace una investigación a fondo de la información. También debemos conocer la mayoría de los fallos o las funciones más importantes de cada herramienta para así aprovechar lo máximo posible de lo que nos brindan, para realizar un análisis de la información exhaustivo generando un resultado convincente.

Kali Linux es una distribución que se ocupa para la auditoría de seguridad de sistemas y el análisis de la información en diferentes dispositivos electrónicos, es muy ocupada en el campo laboral, investigativo y estudiantil. Ya que cuenta con trescientas herramientas que pueden realizar análisis de penetración, ethical hacking entre otras actividades. Es por ello que describiremos brevemente una lista de herramientas las cuales se consideran las mejores para poder implementar una mesa de trabajo de cómputo forense la que podemos llamar “laboratorio forense”.

NESSUS esta aplicación ayuda a la identificación de vulnerabilidades en diferentes servicios dentro de nuestro sistema operativo como: escaneo amplio de la red, hasta una base de datos y las aplicaciones con las que cuenta el sistema, esta herramienta muestra al usuario un informe completo de estado de los escaneos que se realizaron e informa los problemas de seguridad, posteriormente es recomendable dar una solución a las amenazas que se encuentran normalmente son malware, virus, puertas traseras, servidores que se comunican entre sí y están infectados con botnets. Esta herramienta puede ser programada desde la consola del sistema operativo para hacer escaneos programados donde ejecutará los procesos que deben ser ejecutados y la hora en específico en que deben hacerlo.

METASPLOIT es un framework que sirve para explotar vulnerabilidades presentes dentro de un sistema, surgió como un subproyecto de seguridad de la información en el año 2003 con el objetivo principal de ayudar a las pruebas de intrusión (pentesting) que se llevan a cabo dentro de la disciplina de hacking ético, en esta herramienta podemos implementar barridos de ping, identificación de IP y nos permite tomar contramedidas contra las posibles amenazas que encuentren gracias a los módulos llamados "payloads" que son los que se encargan de explotar las vulnerabilidades, una de las ventajas de esta es que permite interactuar con otras herramientas como NMAP y NESSUS.[30]

NMAP es una de las herramientas de código abierto más utilizadas hoy en día en las redes y auditorias de seguridad, esta nos sirve para escanear los puertos de un servidor, computadora, permitiéndonos saber cuáles están abiertos y que vulnerabilidades presentan; Diversos administradores de sistemas y redes lo clasifican de mayor utilidad para administrar las tareas de una red y la gestión de los programas que se ocupan dentro de la institución donde trabajan, los principales sistemas operativos de computadoras cuentan con esta aplicación. Además, incluye una sub-herramienta (Zenmap) que depura, redirecciona y transfiere datos comparando los resultados de cada escaneo dando un mejor análisis de respuesta a los paquetes que están en uso.[31]

WIRESHARK sirve para comprender el tráfico de la red dentro de una institución, analiza diversos protocolos capturando el tráfico en tiempo real e informa que es lo que sucede a detalle con cada paquete que se está transfiriendo en una red; Es muy utilizado para controlar conexiones TCP/IP donde posteriormente se analizaran las amenazas que surgieron en una red de tal manera los administradores de seguridad deberán comenzar a actuar de forma rápida garantizando la transferencia de información como seguridad de la red. Es multiplataforma ejecutándose en diversos sistemas operativos, a su vez puede analizar sistemas de VoIP, lee y escribe formatos diferentes de archivos de captura haciendo una herramienta de bastante utilidad para el análisis profundo de una red.[32]

OWASP ZAP (zed attack proxy) escáner de seguridad web, esta aplicación de seguridad es ocupada para pruebas de penetración y análisis de datos, enfocada a

la mejora y seguridad de diferentes softwares para darles un mejor uso. Se puede ocupar como servidor proxy permitiendo manipular el tráfico de la red administrando los paquetes que pasan a través de este junto con sus protocolos. Es una herramienta multiplataforma que cuenta con diferentes complementos que son muy ocupados por profesionales de seguridad los más destacados son: lenguajes de scripting, websocket, navegación forzada, escáner automatizado y rastreadores web.[33][34]

MAGNET FORENSICS diseñada para la captura de la memoria física de una computadora donde se llevaron a cabo los hechos; esta le permite al usuario durante la investigación recuperar, analizar e implementar un reporte de los datos recopilados que se encontraron en el dispositivo. También permite exportar los datos capturados en un archivo de formato “raw” para poder analizarlos fácilmente en otras herramientas de análisis forense.

MAGNET WEB PAGE SERVER Y FAW esta herramienta es una alternativa a la anterior ya que cuenta con algunas mejoras de mejor capacidad para la captura de los datos de la web, se ocupa especialmente para ver que contiene un sitio web cuando no hay conexión a internet con solo tener la URL podemos introducirla en la herramienta ya sea manualmente o desde un fichero de texto CVS. Faw (Forensic Acquisition of Websites) nos ayuda a descargar páginas web completas para su posterior análisis forense, para ocupar esta los requisitos son mínimos por lo que se podrá ejecutar desde cualquier sistema operativo, obteniendo evidencias del sitio web fácil y rápido, además de que podemos analizar qué área de la página web que deseemos capturando imágenes, código fuente, incluso podemos analizar los paquetes de la mano de la herramienta de wireshark.

VOLATILITY existen diferentes ataques de intrusión, actividades ilícitas que no dejan rastro en el disco duro es por ello que esta aplicación forense de código abierto nos ayuda a dar respuesta a incidentes de seguridad para el análisis de malware u otro tipo de actividades malintencionadas, permitiéndoles a los profesionales en seguridad informática analizar en tiempo real la ejecución de un dispositivo electrónico mediante la lectura de la memoria RAM identificando qué

procesos se estuvieron ejecutando y de donde se derivó la información de los diferentes ataques que se llevaron a cabo en uno o más dispositivos electrónicos.

FTK IMAGER herramienta forense que nos permite obtener una vista previa de los datos recuperados en un disco duro de cualquier tipo, creando copias perfectas llamadas "imágenes forenses de disco" donde se pueden analizar los datos y manipular la información de manera que no se contamine el disco original, creando pruebas y un reporte completo de lo que se hizo dentro de ese dispositivo para deducir qué movimientos se realizaron con qué intención se compartieron, robaron o modificaron los datos.

BULK-EXTRACTOR nos da la posibilidad de escanear la imagen de un disco duro, un archivo específico o varios directorios de archivos. Los resultados que obtiene esta herramienta dentro de las diferentes carpetas del disco es que pueden inspeccionarse y analizarse de manera automatizada destacando la rapidez con la que lo hace a diferencia de otras herramientas, de esta manera recolecta datos de procesos dump, extracción de demonios, números de teléfono, emails, URL´S, etc. Informando en un archivo los desplazamientos de la información que se llevaron a cabo.[35]

1.8 Laboratorios de cómputo forense.

Cada día la informática forense va cambiando, viéndose en la necesidad de ocupar nuevas herramientas, técnicas y metodologías; Para satisfacer de manera adecuada las mesas de trabajo de esta disciplina, facilitando la investigación del cómputo forense y creando nuevas herramientas de entornos confiables y seguros para realizar diferentes actividades. Existen diferentes organizaciones que se encargan de cumplir con la ley y protección de los datos, éstas establecen constantemente laboratorios forenses digitales, algunas tienen diferentes alcances ya que tienen la posibilidad de facilitar una gran inversión en herramientas con licenciamiento para realizar trabajos a diferentes instituciones, otras optan por la investigación donde ocupan herramientas forenses de libre acceso. Un **laboratorio forense** tiene la tarea de realizar una investigación inicial a los individuos que realizaron actividades ilícitas con diferentes dispositivos, donde se establece una

incautación de dispositivos electrónicos para llevar a cabo un análisis del tipo de delitos que se cometieron con estos, esta recopilación de información puede ser algo tardada todo dependerá del tamaño de la información y desde cuando se comenzó a realizar diferentes actividades ilícitas, este debe proporcionar un expediente justo y eficaz para que un juez o encargado de la investigación intervenga de la manera más adecuada.[36]

CAPÍTULO 2

2.METODOLOGÍA

2.1. Cómputo forense

Se encarga de determinar el origen de la información que pudo ser dañada, robada o modificada en diferentes dispositivos que almacenan datos. Trabajaremos con esta rama porque nos ayuda a identificar la evidencia digital (actividades maliciosas) de manera segura y confiable, teniendo un impacto potencial donde sabremos que hizo el atacante a la víctima. Podremos realizar un informe completo sobre un caso específico, validando la adquisición, preservación y presentación de las pruebas obtenidas mediante herramientas, técnicas y nuestra metodología basada en diferentes investigaciones que llevan a un análisis profundo concluyendo que fue lo que ocurrió con la información digital de distintos dispositivos electrónicos que almacenan información. A su vez, compararemos las herramientas elegidas de software libre elegidas para realizar la examinación de datos digitales y deducir el potencial de cada una de estas.

2.2. Herramientas para el cómputo forense

Seleccionamos el conjunto de herramientas vistas en la **sección 1.7** las cuales por su desempeño y eficiencia seleccionamos tres:

- NMAP: herramienta de código abierto utilizada para la inspección de red y auditorías de seguridad, escaneo de puertos, servidores y diferentes redes.
- OWASP ZAP: escáner de seguridad web que detecta fallos en diferentes softwares y sus aplicaciones, utilizado para pruebas de penetración en diferentes hosts, análisis de datos de sitios web, tráfico y los servicios que utilizan.
- BULK-EXTRACTOR: herramienta diseñada para recabar información de la memoria física de una computadora, que permite al usuario recuperar, analizar e implementar un reporte de los datos que se utilizaron.

2.3. Selección de distribución Linux para el uso de las herramientas

Se considera que KALI LINUX es una distribución de software libre con la cual podemos realizar pruebas de penetración, diversas investigaciones de seguridad, cómputo forense e ingeniería inversa. Ya que este sistema operativo ofrece un entorno donde podemos desenvolver prácticas de seguridad informática y hacking ético. Además, de que es usado por diferente tipo de profesionales para realizar investigaciones y pruebas de ciberseguridad.

2.4. Metodología aplicada en un caso específico de ciberseguridad

Revisando diferentes bibliografías observamos que las metodologías basadas en el cómputo forense ocupan técnicas de ciberseguridad y tratamos de apegarnos a las diferentes investigaciones, proponiendo la siguiente metodología con base a lo observado. El diseño metodológico se visualiza en la figura 2.

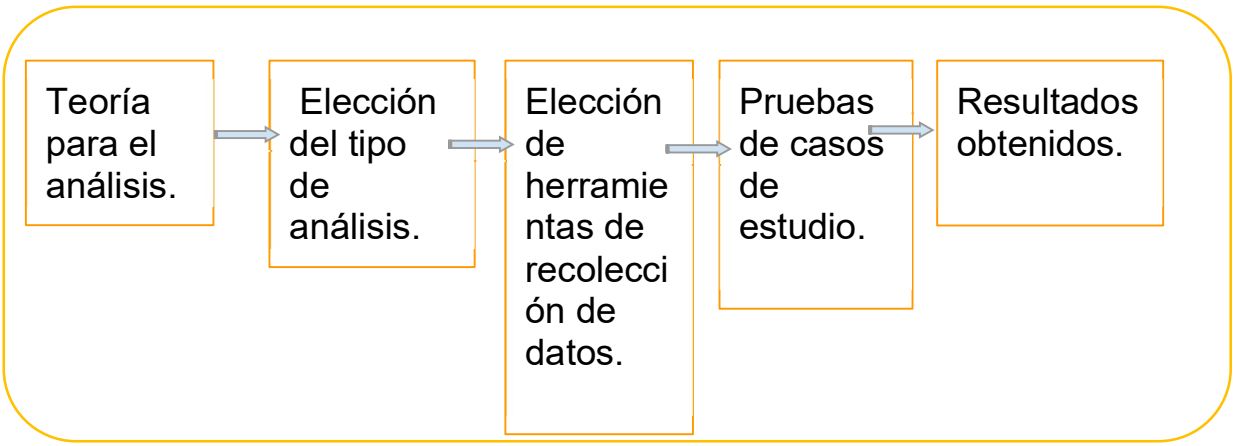


Figura 2. Metodología basada para el análisis de información con herramientas de cómputo forense.

Para el análisis de las herramientas seleccionadas encontramos diferentes resultados y beneficios los cuales son muy útiles para aplicarlos en campo, estas se realizan dentro de un laboratorio de cómputo forense y nos ayudan a resolver diferentes escenarios que surgen hoy en día.

Ocupamos **NMAP** como herramienta de reconocimiento activo dónde existe cierta interacción directa con los objetivos, detección de servicios, descubrimiento de puertos, versiones de aplicaciones, detección de host y las posibles problemáticas

de ataques que se pueden realizar a diferentes usuarios y dispositivos. Las diferentes utilidades se muestran en la tabla 1.

Tabla 1. Beneficios de la herramienta NMAP

Parámetros herramienta	Herramienta	Capacidad-ALTA	Capacidad-MEDIA	Capacidad-BAJA	Observaciones
Barridos de ping exhaustivos	**NMAP**				Se determinan los equipos públicos o privados que se encuentran dentro de ciertos rangos de una red.
Conexión de puertos y aplicaciones	**NMAP**				Sabremos los puertos y aplicaciones que están ligadas a la red, verificando lo que pasa en cada transmisión y comunicación de datos desde las versiones de diferentes aplicaciones ejecutadas en los ordenadores conectados a la red, sistemas operativos, puertos, servidores, tarjetas de red, etc.

Ingeniería inversa o social	**NMAP**				Sabiendo qué datos se ocupan y transmiten dentro de una red, podemos obtener información de diferentes usuarios, lo cual nos permite explotar distintos tipos de información confidencial la cual se puede utilizar para atacar organizaciones o personas en específico para obtener un beneficio ya sea contraproducente o para una mejora en seguridad.
Mapeo de red	**NMAP**				Podemos determinar la existencia de firewalls, routers u otros dispositivos que se encuentren en el borde de una red, esto nos permitirá saber de qué manera atacar o defendernos de

					diferentes amenazas que circulan dentro de una red.
Facilidad de uso	**NMAP**	✓			
Requerimientos de sistema (Windows, Linux)	**NMAP**			✓	
Facilidad de instalación	**NMAP**	✓			
Interfaz ergonómica	**NMAP**	✓			
Complejidad de uso de la herramienta	**NMAP**		✓		
Eficiencia para detectar y contrarrestar vulnerabilidades	**NMAP**	✓			
Legibilidad y veracidad del reporte final de la herramienta	**NMAP**	✓			
Eficiencia final del reporte	**NAMP**	✓			

Vea figura 3, 4, 5, 6, 7, 8, 9 ,10,11,12,13,14. algunos de los mejores beneficios que nos ofrece la herramienta NMAP. Para más información vea el apéndice A.

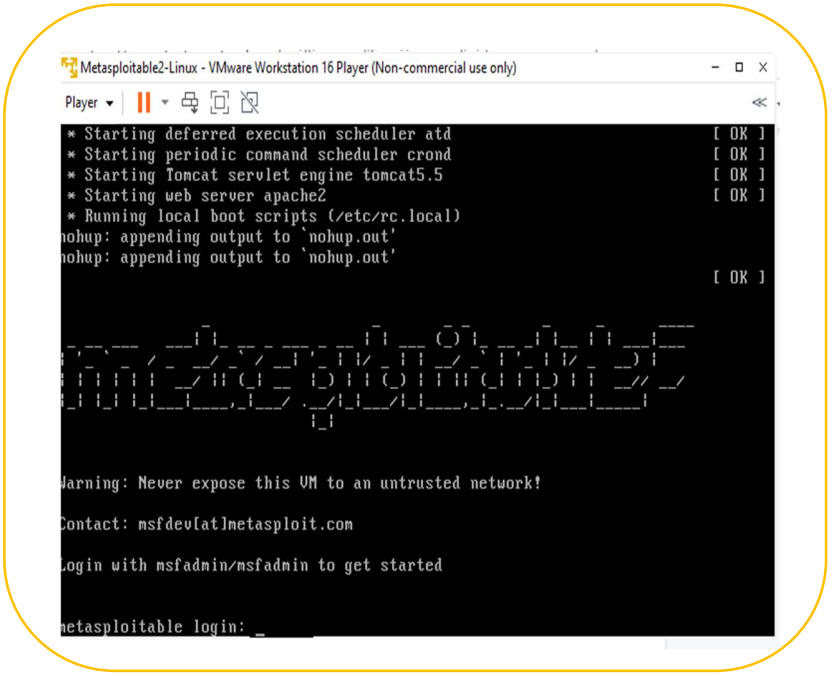


Figura 3. Máquina Linux, utilizada como víctima para el uso de la herramienta NMAP.

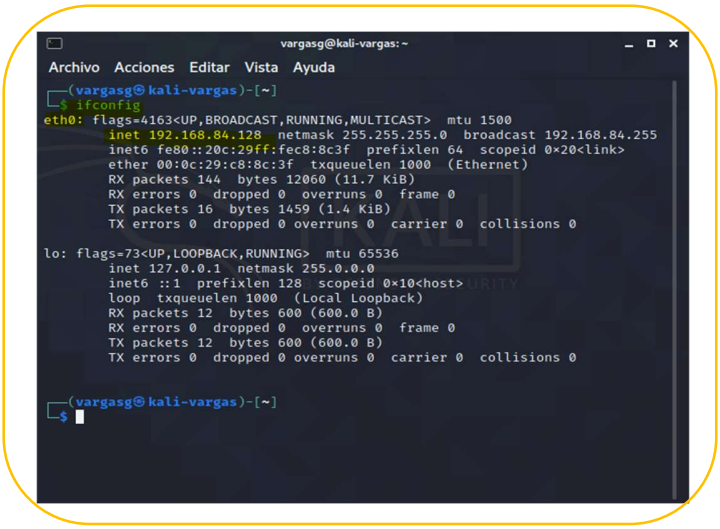


Figura 4. Comando **ifconfig** permite observar la dirección IP una máquina virtual de Kali Linux e identifica otros hosts conectados a una red.

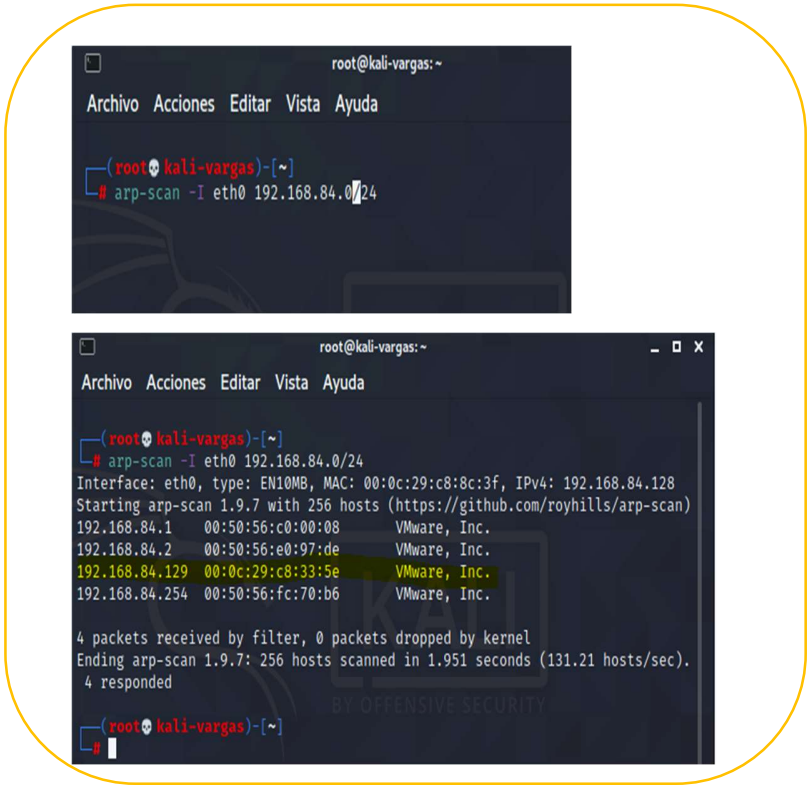


Figura 5. Comando **arp-scan** brinda la interfaz y el rango de direcciones de la red.

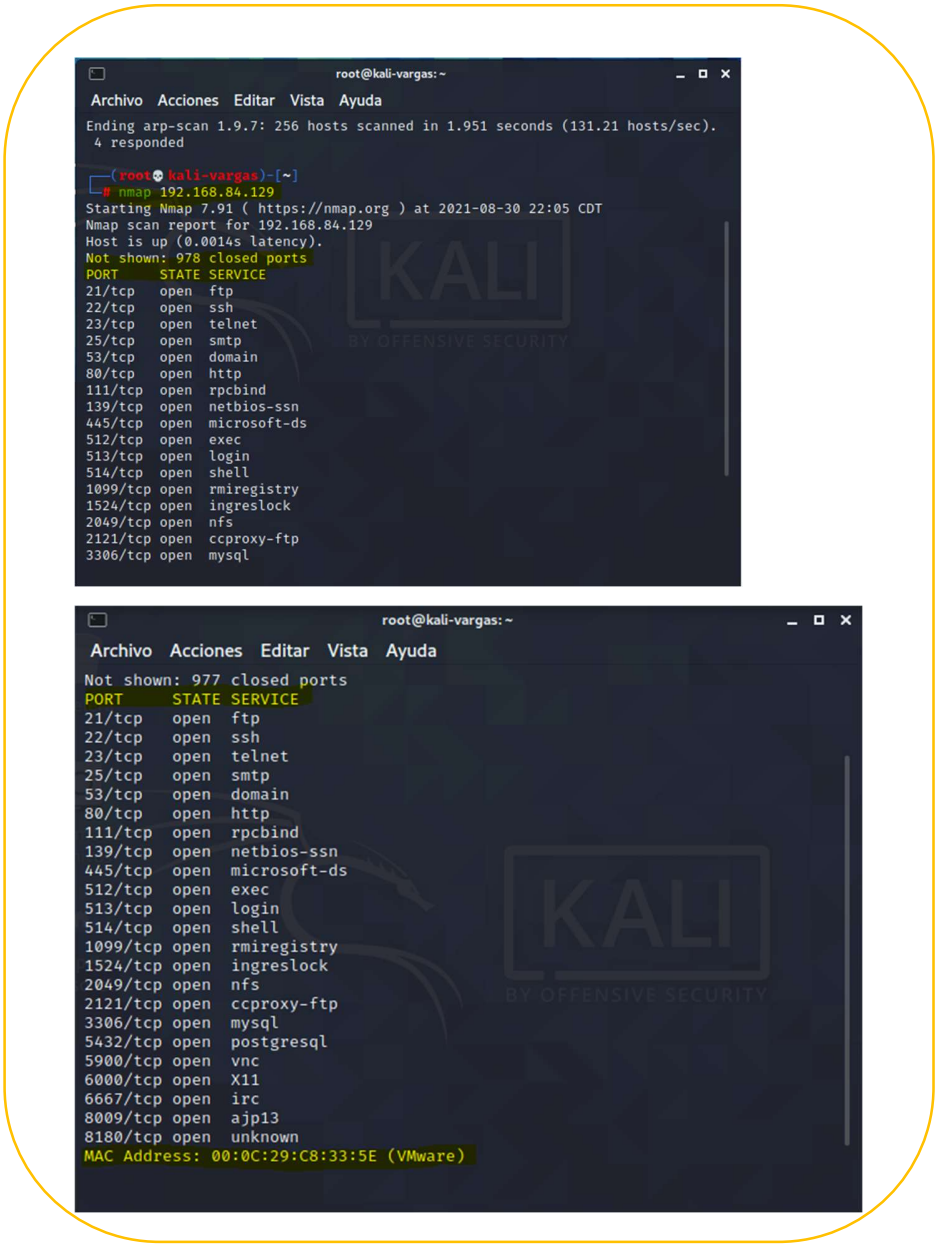


Figura 6. Escáner a máquinas virtuales víctimas, arrojando los parámetros más importantes como sus puertos, direcciones MAC, estado del puerto y el tipo de servicio que ofrece.

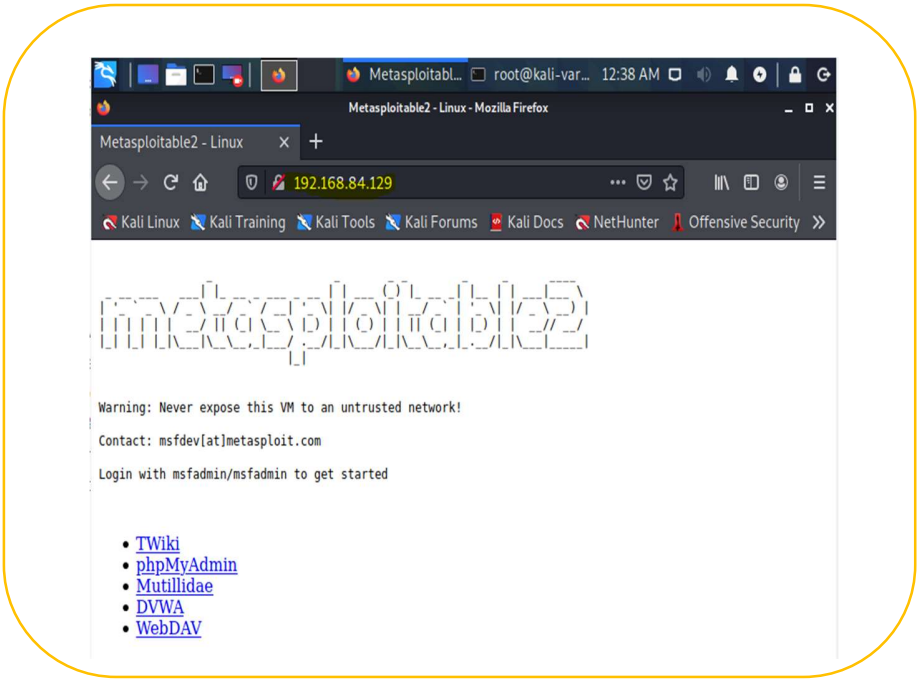


Figura 7. Acceso a máquina virtual víctima por medio de su dirección IP encontrando versiones de cada servicio que utiliza.

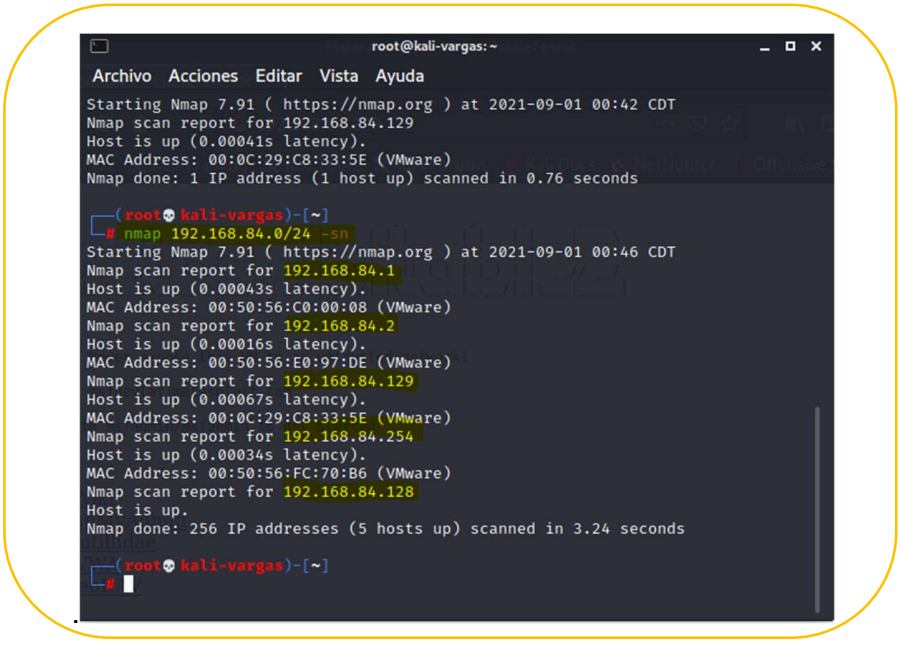


Figura 8. Escaneo de dispositivos conectados a la red mostrando rangos de direcciones, número de host, direcciones IP y MAC address.

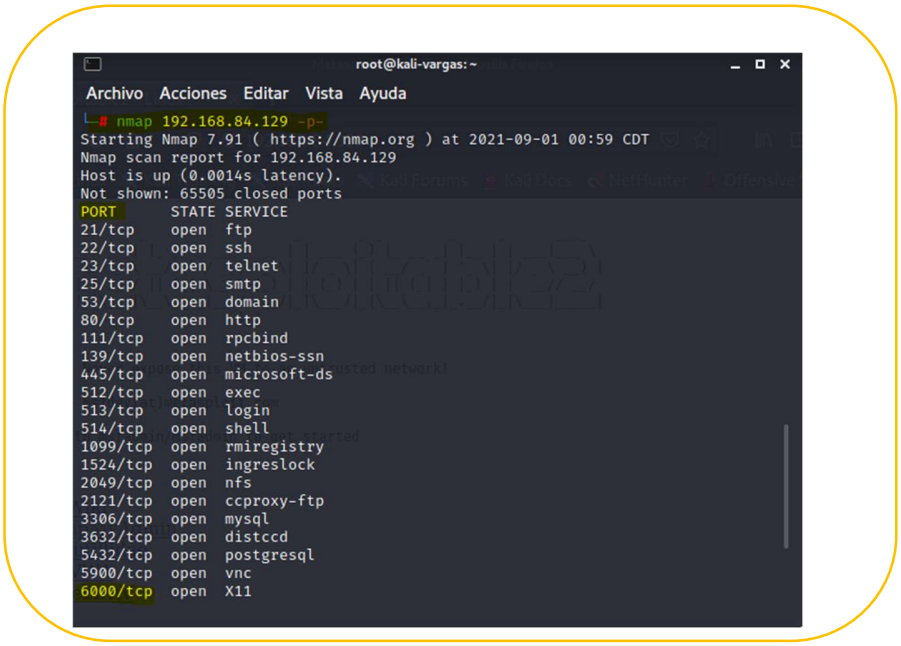


Figura 9. Análisis de los puertos abiertos en una máquina víctima.

Figura 10. Escáner de puertos determinados por el usuario.

De otra forma ésta también nos ayuda a averiguar los scripts que están dentro de un puerto determinado, con el comando **nmap 192.168.84.129 -p 21 -sC** véalo en figura 12 nos permitirá visualizar contraseñas, versiones de transferencia de archivos, como el estado del puerto si se encuentra abierto o cerrado, averiguando si hay alguna posible conexión, permitiéndonos saber de qué manera podríamos

entrar y modificar los archivos que contiene la máquina que está siendo atacada por algún puerto en específico.

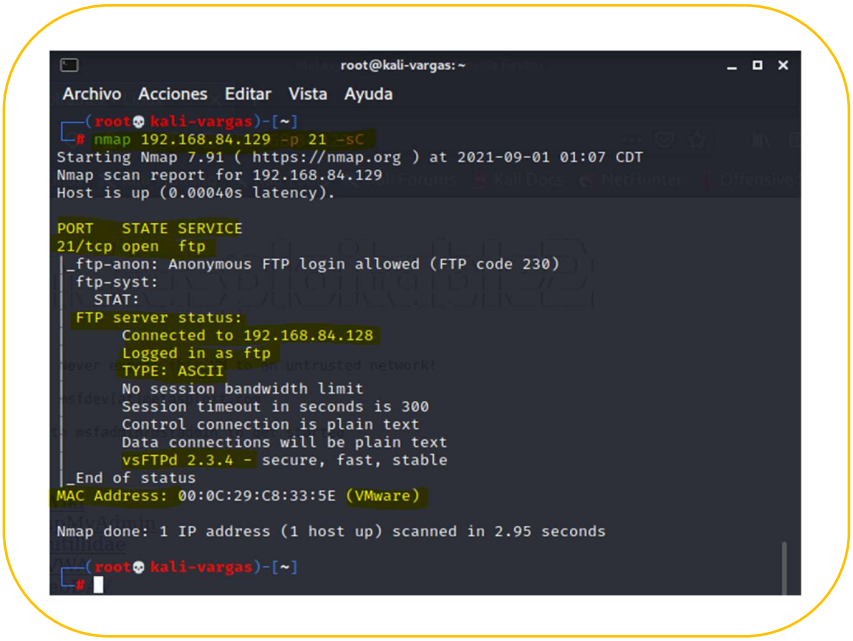


Figura 11. Identificación de información por puerto.

NMAP averigua vulnerabilidades, como versiones específicas de cada puerto, para ese beneficio utilizamos el comando **nmap 192.168.84.129 -p 20-30 -sV**, el cual nos mostrará información más a detalle de cada puerto y ver de qué manera podríamos explotar el acceso de cada uno de estos. Véalo en la figura 13.

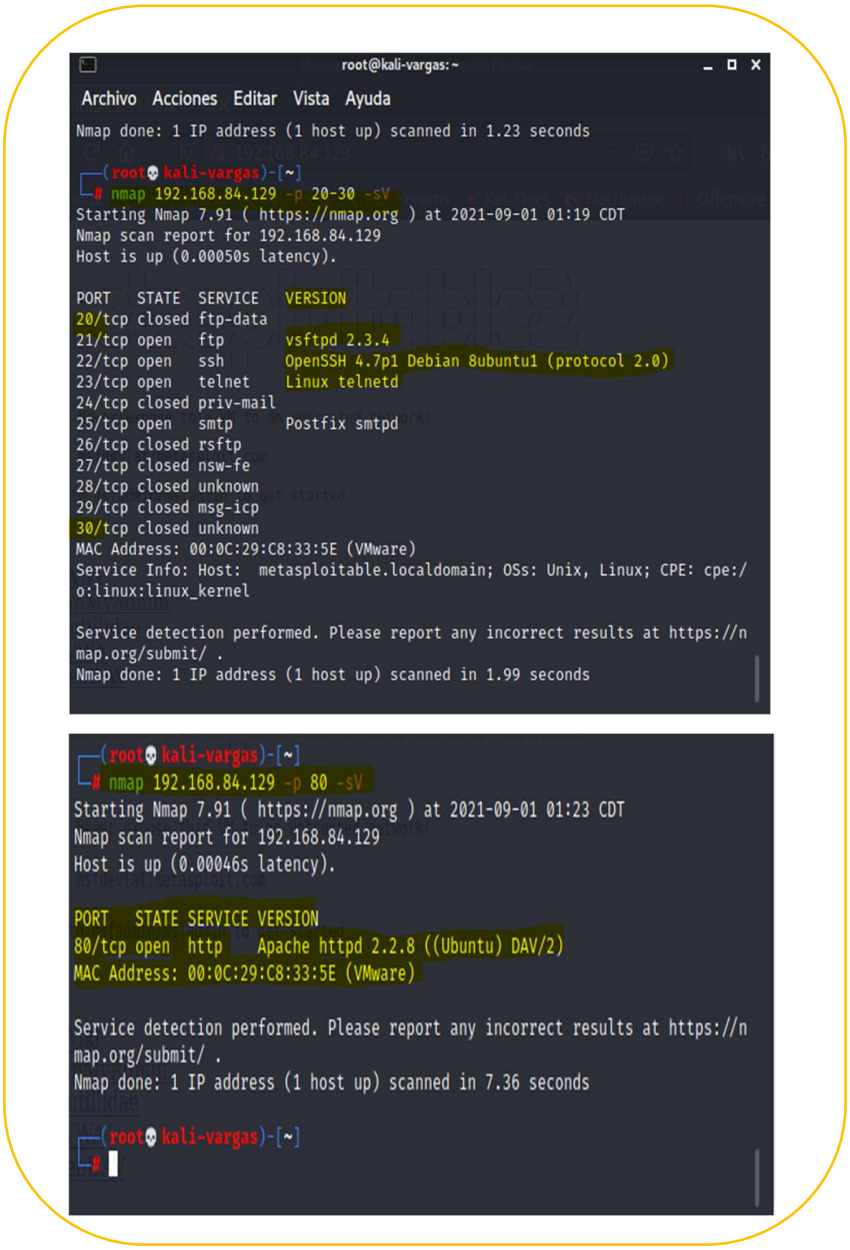


Figura 12. Vulnerabilidad de puertos específicos.

De igual manera podemos averiguar que S.O están utilizando los dispositivos conectados a una red, en este caso veremos cuál es el de una máquina víctima. Con el comando **nmap 192.168.84.129 -O** véalo en la figura 14.

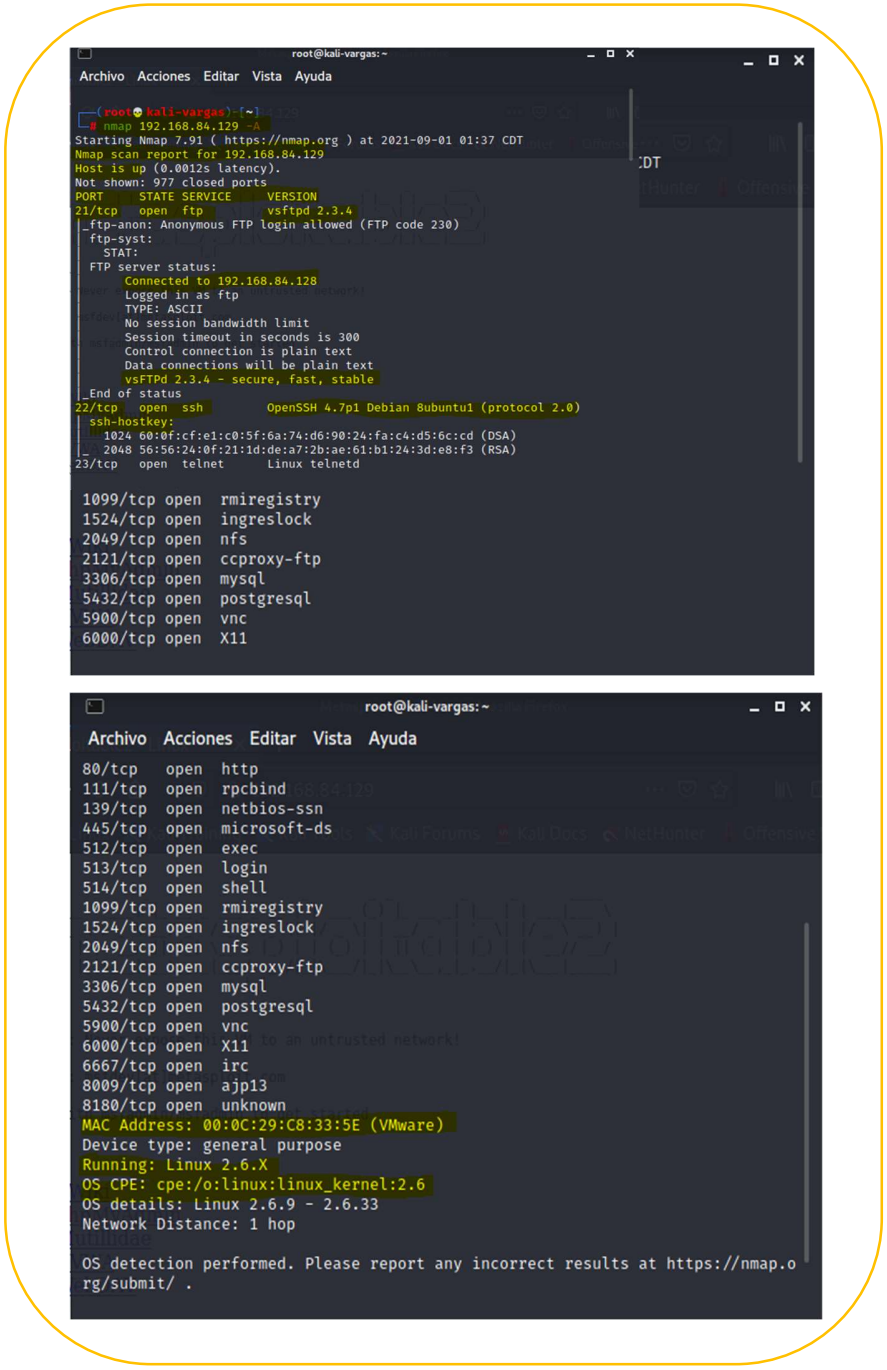


Figura 13. Identificación de sistema operativo.

Por otra parte, podemos resumir los anteriores ejemplos de escaneo (-sC, - sV, -O) con el comando **nmap 192.168.84.129 -A** vea en figura 15 el cual incluye todas las opciones de escaneo incluyendo el análisis de host para reconocer los dispositivos conectados a una red.

Figura 14. Identificación y recolección de datos.

Owasp es una herramienta que nos sirve para diagnosticar y resolver problemas de seguridad a profesionales, investigadores como a diferentes usuarios, está generalmente se ocupa dentro de un laboratorio de cómputo forense donde podremos comprender el por qué, cuándo y dónde se originó una brecha de ataques a sitios web, aplicaciones y sistemas que comparten cualquier tipo de información.

Esta nos ofrece demasiados beneficios satisfactorios que podemos utilizar para aplicar pruebas de seguridad dentro de una empresa, institución o centros educativos las que hoy en día realiza un pentester. Por ello tener la experiencia de esta herramienta nos ayuda a brindar una solución significativa a problemas de ciberseguridad global, teniendo una iniciativa y responsabilidad de proteger cualquier tipo de información digital de las diferentes tecnologías que podamos ocupar en la actualidad. Además de mantenernos actualizados con esta herramienta de ciberseguridad, OWASP nos ofrece artículos, metodologías, documentación, herramientas y tecnologías que se liberan y pueden ser usadas gratuitamente por cualquier usuario para mejorar la calidad de seguridad informática de cualquier sitio que maneje información, la cual podemos utilizar para mantener libre de amenazas los diferentes sitios web, aplicaciones, sistemas web, etc. Actuando de manera rápida y eficiente. Utilizando diferentes tipos de escaneos los más utilizados son activo, pasivo, automáticos etc. Véase en figuras 15, 16, 17, 18, 19, 20. Para más información vea el apéndice B. Los beneficios y utilidades que nos brinda esta herramienta se muestran en la tabla 2.

Tabla 2. Beneficios de la herramienta OWASP

Parámetros herramienta	Herramienta	Capacidad-ALTA	Capacidad-MEDIA	Capacidad-BAJA	Observaciones
Modo de ataque activo	**OWASP**				El modo activo simplemente nos sirve para auditar una dirección web deseada, obteniendo las vulnerabilidades de esta.
Modo de ataque pasivo	**OWASP**				Su funcionamiento consiste en la configuración de un proxy dónde nos permite establecer los puertos (http, https), la dirección IP (X.X.X.X), destacando la seguridad de protocolos.
Automatic scan	**OWASP**				Realiza un escaneo automatizado a la URL deseada buscando vulnerabilidades dentro de una dirección IP o dominio.

Ataques a servidores web NAS QNAP	**OWASP**				Podremos ver las peticiones GET y POST de los propios servicios HTTP/HTTPS. Como todas las alertas de seguridad y ver qué tipo de vulnerabilidades y errores hemos localizado en un sitio web.
Visualización de código, archivos ocultos, modificados, eliminados y existentes en diferentes servidores	**OWASP**				Con la ayuda de su herramienta "spider" encontraremos toda la información necesaria para evaluar la seguridad de un sitio web como aplicaciones web, donde observaremos vulnerabilidades de acceso a diferentes partes del sitio.
Facilidad de uso	**OWASP**				
Requerimientos de sistema (Windows, Linux)	**OWASP**				

Facilidad de instalación	**OWASP**	✓			
Interfaz ergonómica	**OWASP**	✓			
Complejidad de uso de la herramienta	**OWASP**		✓		
Eficiencia para detectar y contrarrestar vulnerabilidades	**OWASP**	✓			
Legibilidad y veracidad del reporte final de la herramienta	**OWASP**	✓			
Eficiencia final del reporte	**OWASP**	✓			

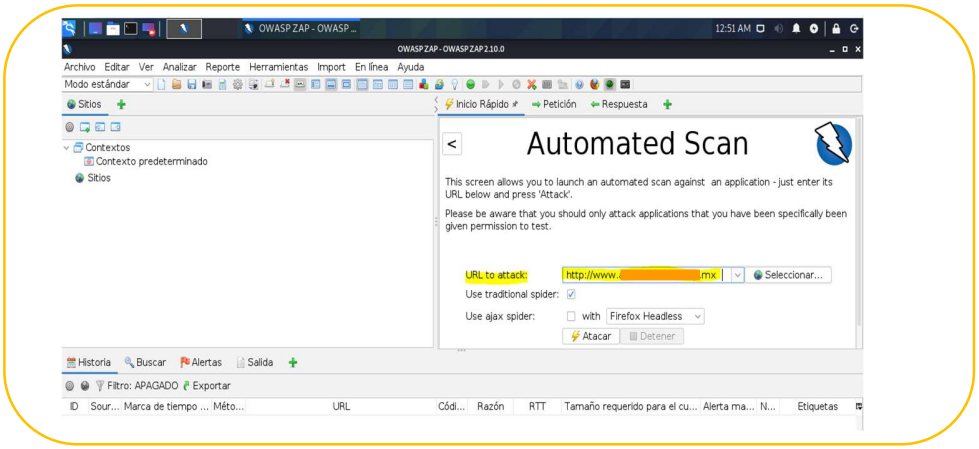


Figura 15. Modo de ataque activo a un sitio web “http.mx”.

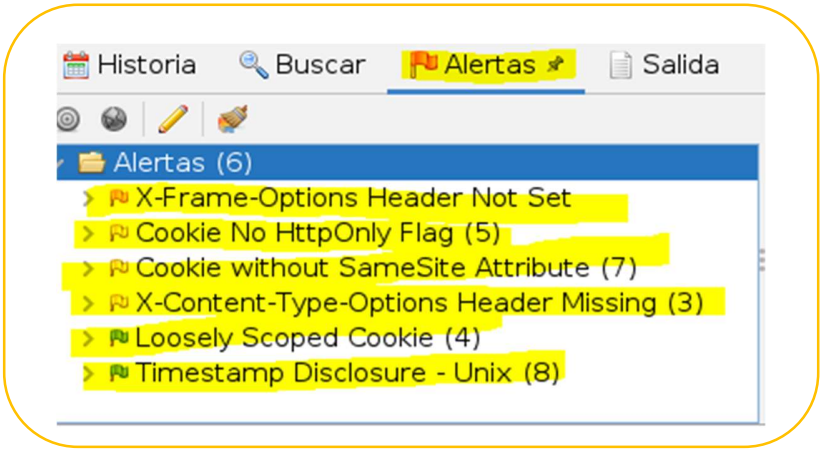


Figura 16. Vulnerabilidades encontradas en un sitio web “http.mx”.

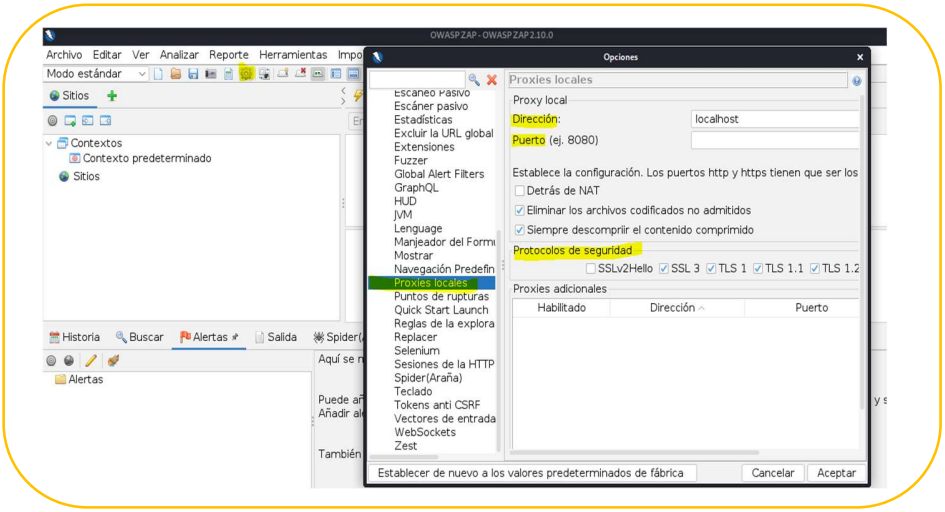


Figura 17. Ataque pasivo a un sitio web determinado servidor y puertos específicos.

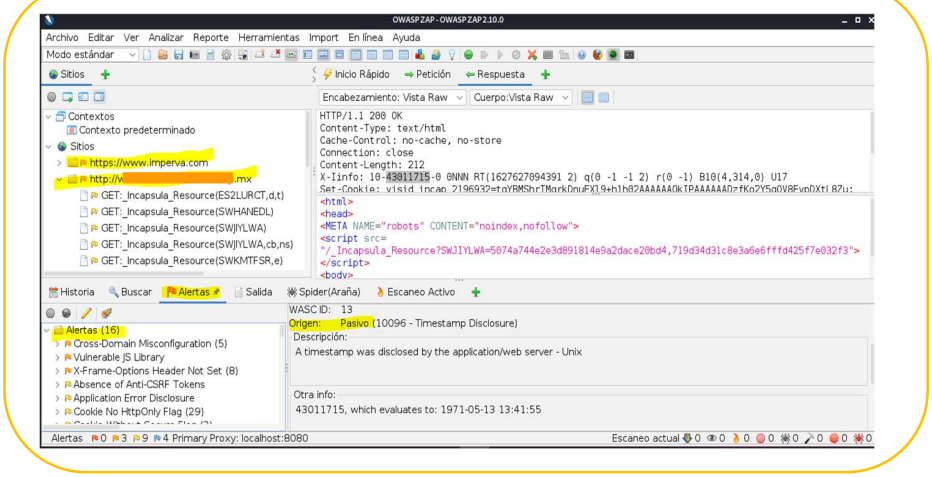


Figura 18. Archivos vulnerables de una página web “http.mx” atacada y su código fuente que conforma.

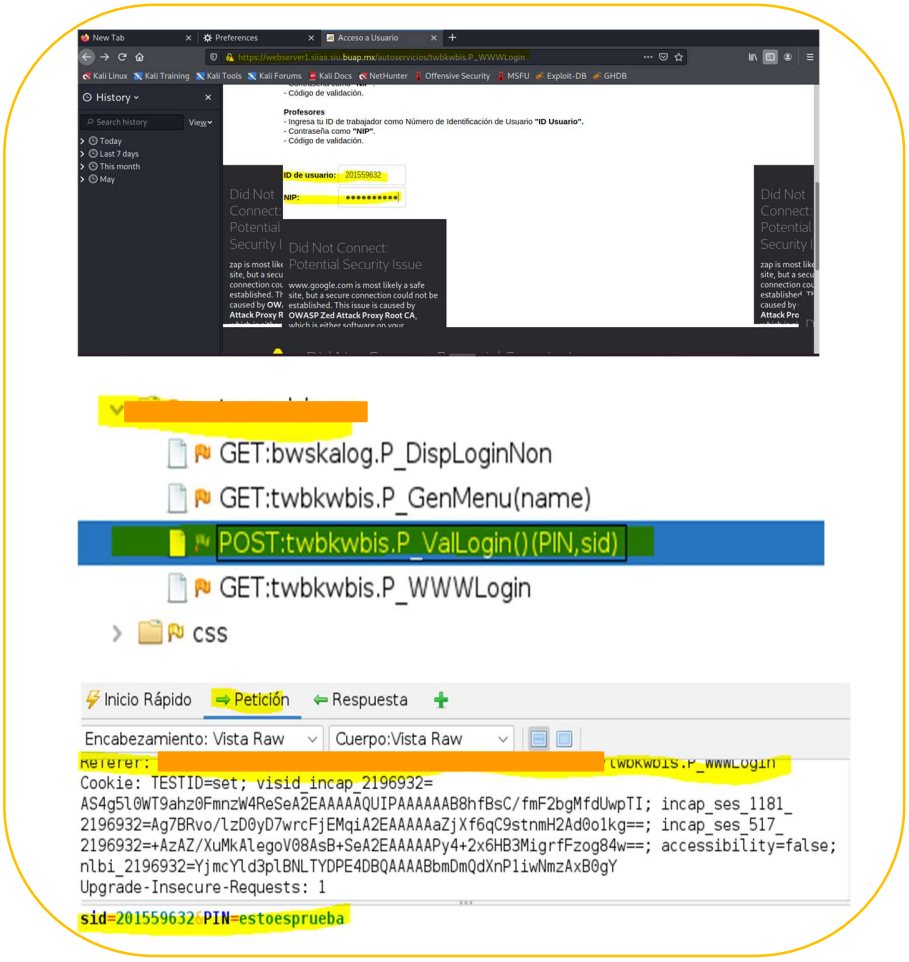


Figura 19. Auto scan petición y respuesta de servidores.

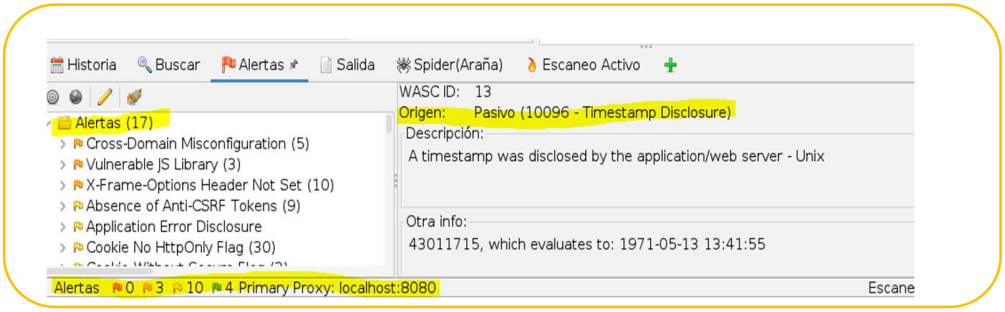


Figura 20. Vulnerabilidades encontradas en el sitio web arrojando todas las carpetas que utiliza.

Bulk-Extractor es una herramienta que nos sirve para recuperar (indagar) información de una memoria RAM, estos elementos pueden ser: correos electrónicos, números de teléfono, direcciones IP, tarjetas de crédito, archivos de texto de diferentes extensiones, procesamiento de datos, recuperación de datos, URL´S u otros archivos de evidencia digital. Ésta se utiliza durante una investigación de cómputo forense, siendo muy útil para investigaciones de implantación de malware y ataques de intrusión.

En nuestra prueba de estudio pudimos realizar la captura de la memoria RAM de la computadora física véase en la figura 21,22 en la cual se realizaron las pruebas con las anteriores herramientas, obteniendo un excelente resultado de recolección de diferente información de lo que se ha realizado con esa computadora, está la podríamos ocupar dentro de una investigación de cómputo forense para saber qué información se utilizó, sitios web, direcciones IP, números telefónicos almacenados, tarjetas de crédito utilizadas y que otros archivos ocupó este dispositivo para posteriormente analizar la diferente información digital almacenada en la memoria RAM. Véase en las figuras 23, 24, 25, 26, 27 Si estuviéramos en un caso donde se haya cometido un ciberataque podríamos ocupar esta información digital para llegar a una deducción verídica y con fundamentos, concluyendo si se cometió algún delito o está relacionado con actividades sospechosas que lo vinculen a un ciberataque a uno o diferentes usuarios.

Podemos decir que **"BULK-EXTRACTOR"** es una excelente herramienta para realizar la recolección de información digital dentro de un o distintos casos de cómputo forense, aportando un **90%** de efectividad para indagar diferentes datos digitales. Cabe mencionar otro de sus beneficios es que puede realizar análisis de imágenes de memoria (RAM) incompletos, dañados o reconstruidos, por ello es mucho mejor herramienta que otras herramientas de cómputo forense como: VOLATILITY, FTK IMAGER Y MAGNET RAM CAPTURE, ya que esta no necesita un archivo de imagen de volcado de memoria completo pues esta puede sin ninguna dificultad analizar archivos de diferentes extensiones ya sea que estén incompletos o dañados, permitiéndonos investigar a fondo la información recabada en los

archivos que deseemos analizar, agregando que podemos generar un reporte final de la información obtenida y este puede ser utilizado por otras herramientas de cómputo forense, haciendo que la información recolectada pueda ser analizada en diferentes frameworks que se utilicen en el cómputo forense. Para más información vea el apéndice C. Las utilidades con las que cuenta ésta se muestran en la tabla 3.

Tabla 3. Beneficios de la herramienta BULK-EXTRACTOR

Parámetros herramienta	Herramienta	Capacidad - ALTA	Capacidad-MEDIA	Capacidad-BAJA	Observaciones
Extracción de claves AES	**BULK-EXTRACTOR**				Extracción de los datos que se encuentran dentro del archivo de volcado de memoria, contraseñas e información sensible, donde serán almacenados en archivos .txt
Extracción de direcciones de correo electrónico	**BULK-EXTRACTOR**				Mediante el proceso de recolección de datos podremos encontrar los correos electrónicos almacenados en el archivo de volcado de memoria RAM.

Extracción de direcciones de dominio	**BULK-EXTRACTOR**				Localización de peticiones a diferentes servidores que pudo haber realizado un usuario en su computadora.
Extracción de direcciones MAC	**BULK-EXTRACTOR**				Extracción de información digital de un archivo de volcado de memoria RAM, que contiene la dirección MAC de una computadora física o virtual.
Análisis de imágenes exif y segmentos de videos	**BULK-EXTRACTOR**				Realiza un escaneo al archivo de volcado de memoria para obtener las páginas web visitadas.
Extracción de direcciones IP (packet carving)	**BULK-EXTRACTOR**				Mediante el escaneo al archivo de volcado de memoria RAM, arroja las direcciones IP que se ocuparon dentro de una computadora.

Extracción de contraseñas almacenadas	**BULK-EXTRACTOR**				Disposición de credenciales almacenas en el archivo de volcado de memoria.
Extracción de URLS, caché de navegación, correos y archivos ejecutables	**BULK-EXTRACTOR**				Acceso a información digital, acerca de sitios web, cache y datos de navegación dentro del archivo de volcado de memoria.
Extracción de números telefónicos almacenados en la memoria RAM	**BULK-EXTRACTOR**				Visualización de números telefónicos almacenados en el archivo de volcado de memoria RAM.
Extracción de número de tarjetas bancarias utilizadas en una computadora	**BULK-EXTRACTOR**				Extracción de números de tarjetas bancarias que se ocuparon en una computadora y se almacenaron en el archivo de volcado de memoria RAM.
Extracción de información de archivos .zip	**BULK-EXTRACTOR**				Extracción de información de los archivos .ZIP almacenado en el archivo de

					volcado de memoria. (fecha, tamaño, nombre)
Facilidad de uso	**BULK-EXTRACTOR**	✓			Herramienta intuitiva con el usuario.
Requerimientos de sistema (Windows, Linux)	**BULK-EXTRACTOR**			✓	Compatibilidad para usar en diferentes sistemas operativos.
Facilidad de instalación	**BULK-EXTRACTOR**	✓			
Interfaz ergonómica	**BULK-EXTRACTOR**	✓			
Complejidad de uso de la herramienta	**BULK-EXTRACTOR**		✓		
Eficiencia para detectar y contrarrestar vulnerabilidades	**BULK-EXTRACTOR**	✓			
Legibilidad y veracidad del reporte final de la herramienta	**BULK-EXTRACTOR**	✓			
Eficiencia final del reporte	**BULK-EXTRACTOR**	✓			

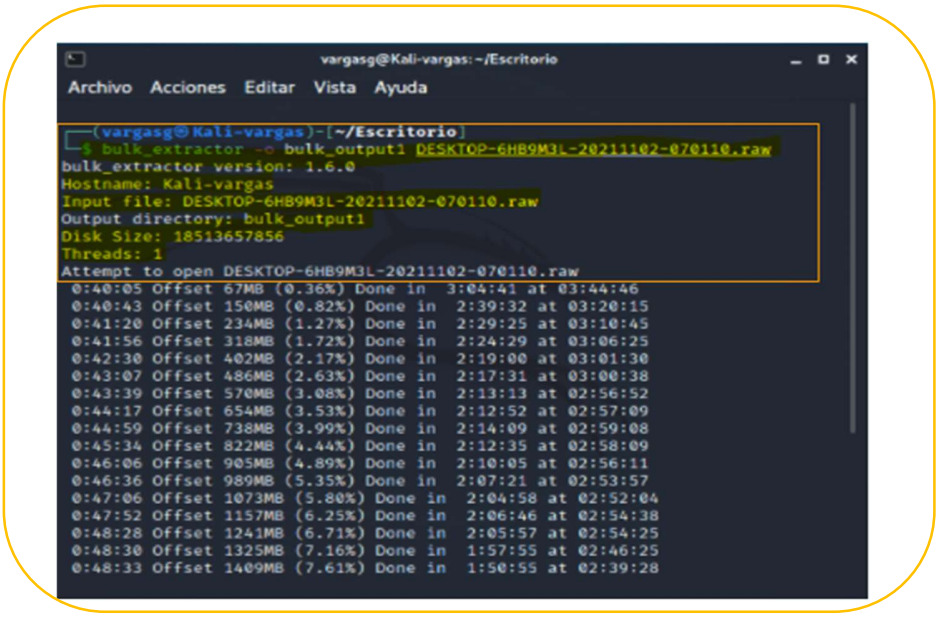


Figura 21. Extracción de información del archivo de volcado de memoria.

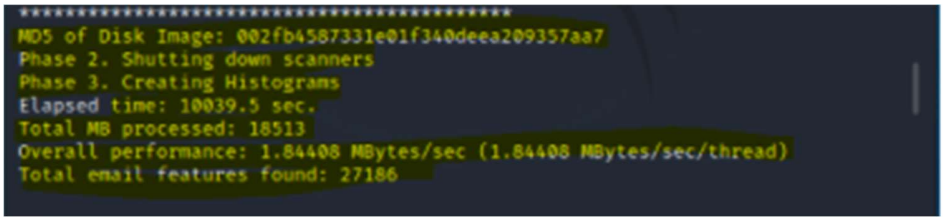


Figura 22. Recolección de la información del archivo de volcado de memoria.

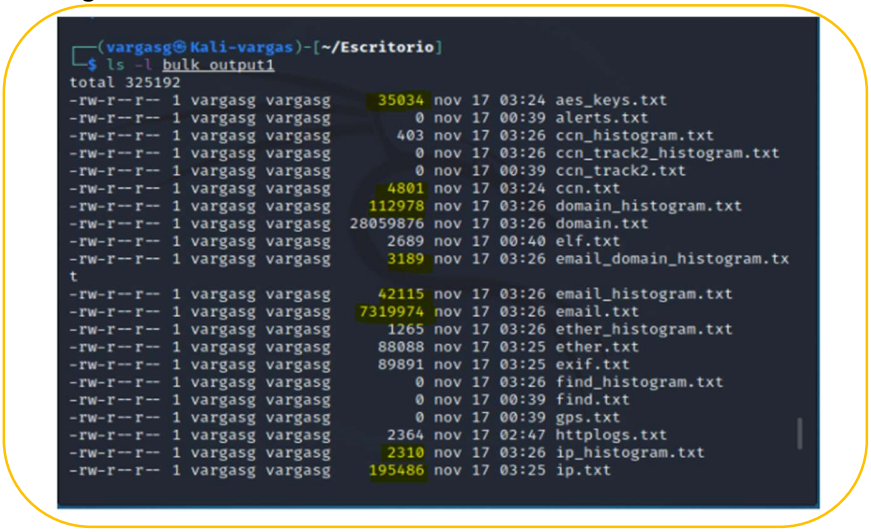


Figura 23. Datos recolectados en forma de archivos .txt.

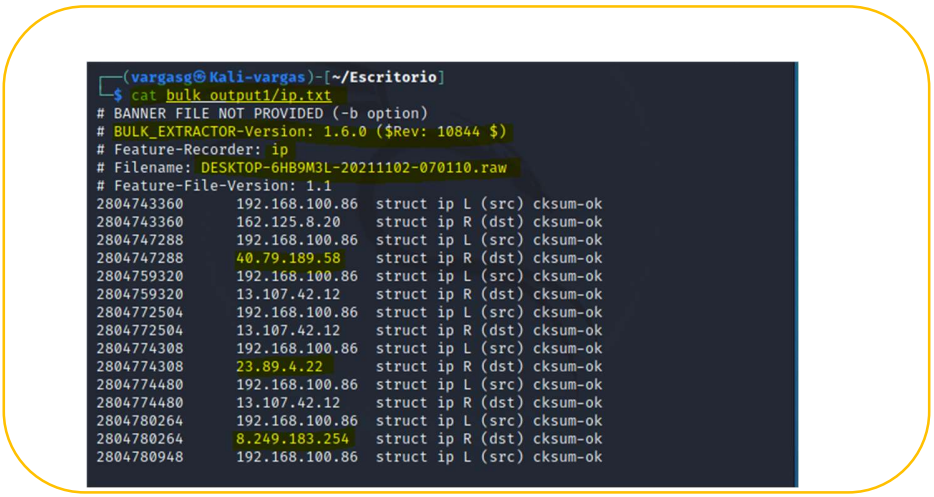


Figura 24. Direcciones IP que se ocuparon en una máquina física.

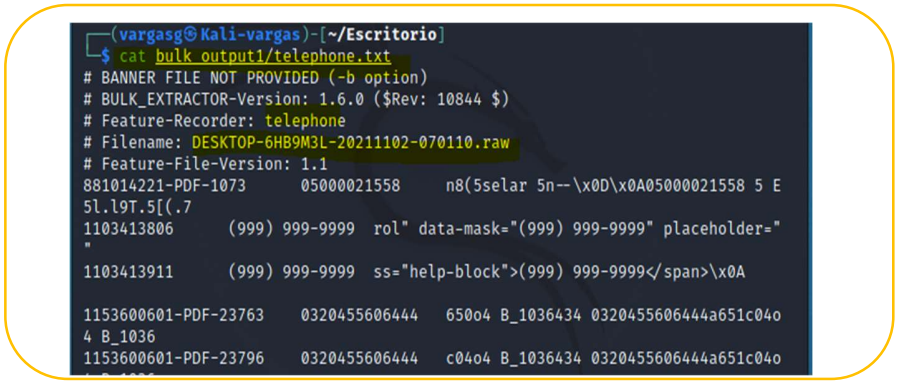


Figura 25. Teléfonos encontrados y almacenados en el archivo de volcado de memoria.

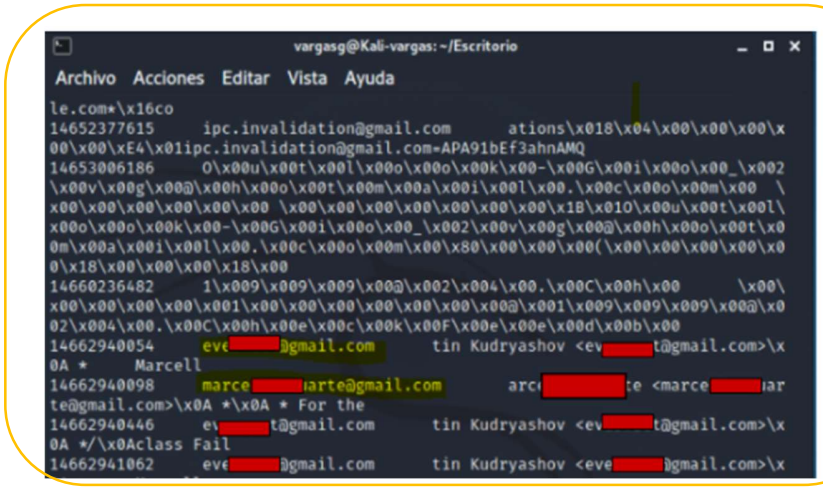


Figura 26. Emails almacenados en el archivo de volcado de memoria.

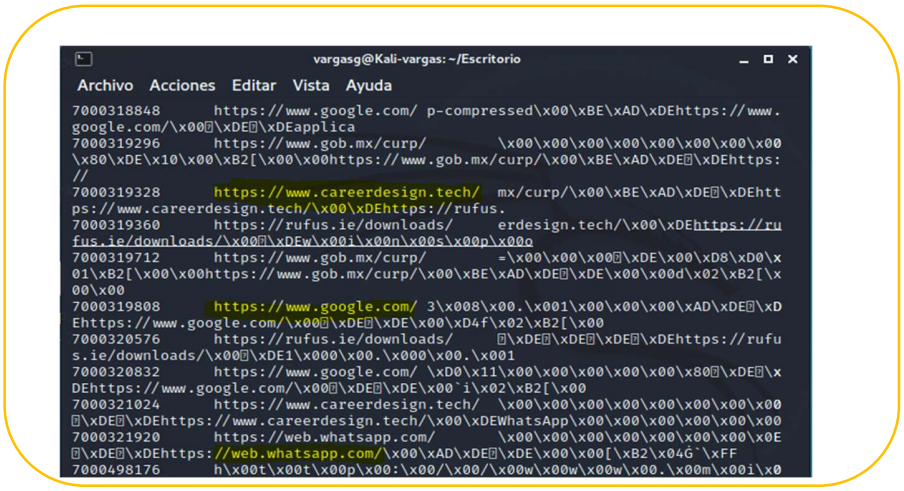


Figura 27. Peticiones a diferentes servidores almacenados en el archivo de volcado de memoria.

2.5. Propuesta de laboratorio de prácticas de un “laboratorio forense”

La infraestructura, hardware y software de un laboratorio de cómputo forense inicial, la cual podríamos llamar “laboratorio de cómputo forense básico” puede comenzar teniendo desde un espacio pequeño donde tengamos acceso a la red en una o más computadoras dónde podamos instalar las herramientas de cómputo forense para comenzar a realizar diferentes pruebas, tratando de analizar diferentes casos de estudio como también tener diferentes equipos de trabajo como: discos duros, memorias RAM, memorias externas (USB), servidores, impresoras, ups, módems, cables para diferentes dispositivos, dispositivos móviles, etc. Los cuales nos puedan ayudar a realizar diferentes pruebas

Ventajas de la implementación de un laboratorio de cómputo forense.

Anteriormente podemos notar los aspectos más relevantes como las soluciones que ofrece y puede realizar un laboratorio de cómputo forense, cierta implementación podría ser muy útil para diferentes organizaciones para resolver y dar un valor importante a las investigaciones que se realicen dentro de este. Las soluciones que nos puede ofrecer este son:

Litigación civil: recolecta y analiza la evidencia incriminatoria, la cual pudo haber sido usada para diferentes tipos de crímenes cibernéticos contra una organización o persona. Esta solución nos puede ayudar a resolver casos que tratan con fraudes, discriminación, acoso, divorcios, etc. Casos que con el cómputo forense podemos resolver.

Investigación: La evidencia encontrada dentro de las computadoras de una organización o persona pueden ayudar a disminuir el riesgo de incriminación en casos donde haya habido un incidente informático donde trataron de usurpar una identidad y quisieron tener una compensación dentro de los ataques a otros usuarios u organizaciones. Por lo que, con la ayuda de las herramientas instaladas dentro de las computadoras de un laboratorio de cómputo forense podemos realizar un análisis de diferentes dispositivos electrónicos donde se llega a una conclusión de lo que se manipuló dentro de estos y saber quién fue el responsable de dichos actos.

Elementos: Son la evidencia digital recolectada de los diferentes escenarios que puede resolver el computo forense como: acoso sexual, robo de dispositivos, mal uso de información confidencial o propietaria, espionaje, suplantación de personas o de diferentes organizaciones, etc.

¿Cómo funciona un laboratorio básico de cómputo forense?

Podemos encontrar diferentes escenarios de incidentes informáticos estos pueden ser o no ser un delito. Cualquier problema dentro de la informática como la fuga de datos, extorsión, mal uso de información, robo intencionado de información, o un sin fin de ataques que existen hoy en día, tienen cierta evidencia que podemos averiguar dentro de un laboratorio de cómputo forense para saber que paso y quien lo hizo. Simplemente podemos realizar diferentes tipos de investigaciones que arrojaron evidencia digital, donde se ocupan técnicas y metodologías para la extracción de la diferente información que podamos encontrar en diferentes dispositivos electrónicos, sitios web u otra evidencia física recolectada.

¿Cómo se hace este análisis? Por medio de **cuatro pasos** que se llevan a cabo dentro de cualquier investigación de cómputo forense que arroja una evidencia digital y posteriormente despliega un reporte para una deducción final.

IDENTIFICACIÓN: Utilizando **NMAP y OWASP** herramientas de cómputo forense que nos brindan el beneficio de saber cómo averiguar y ayudar a conocer los antecedentes de un escenario y la situación actual en la que se encuentran, así como los procesos a seguir para decidir qué estrategia, técnicas y metodologías tomar dentro de la investigación.

Para proceder a la identificación de la información con estas herramientas en la mayoría de los casos primero deben realizarse los siguientes pasos:

- Identificación del bien informático a analizar.
- Su uso que se le dio y en qué redes se ocupó.
- Inicio de custodia (proceso que verifica la procedencia e integridad del dispositivo para el manejo adecuado y extracción de información.)
- Revisión del entorno legal (se analiza cómo se obtuvo el bien y qué función se le dio.)

PRESERVACIÓN: En este paso podemos ocupar la herramienta **bulk-extractor** donde se realiza la revisión y generación de las imágenes forenses de diferentes dispositivos, lo cual permite generar evidencias digitales y el análisis de la información que contienen los diferentes dispositivos electrónicos que se van a investigar. Este proceso se realiza para no contaminar la información de los dispositivos confiscados, haciendo una copia fiel de "bit a bit" de un disco duro, memoria u otro dispositivo. Lo cual nos permitirá recuperar toda la información que contiene o se borró de los dispositivos, dicha duplicación se realiza utilizando herramientas de cómputo forense que podemos encontrar en diferentes S.O de Linux y Windows esta tecnología puede ser de software libre o con costo, lo cual cada analista puede decidir que herramientas prefiere utilizar.

ANÁLISIS: En este punto de la investigación se aplican las técnicas científicas, metodológicas y analíticas que podemos agilizar con la ayuda de las diferentes herramientas (NMAP, OWASP, BULK EXTRACTOR) de cómputo forense que mencionamos anteriormente en los capítulos anteriores. En este proceso podemos encontrar pruebas y conductas del usuario sabiendo que hizo, tecnología que utilizó y el uso que les dio a los diferentes dispositivos recolectados. Como resultado de evidencia digital podemos saber:

- Uso de USB (marca, modelo, velocidad, tipo de archivos e información.)
- Búsqueda de archivos específicos.
- Inspección de sitios web (passwords, usuarios, explotación de vulnerabilidades, servidores, puertos, etc.)
- Análisis de memoria RAM.
- Recuperación e identificación de correos, números telefónicos, tarjetas de crédito, contactos, historial web, etc.
- Inspección de puertos, tráfico de paquetes, identificación de IP´s.
- Recuperación de últimos sitios y aplicaciones utilizadas.
- Identificación de servidores utilizados.
- Análisis de discos duros.
- Ataques de ingeniería inversa, entre otros.

PRESENTACIÓN: En esta fase dentro de una investigación que involucra al cómputo forense se hace la recopilación de todas pruebas que se obtuvieron a partir del análisis de la información con las diferentes herramientas las cuales pueden resolver infinidad de casos sobre seguridad informática, obteniendo estos resultados se realiza un reporte y presentación de pruebas a las autoridades o personas calificadas que darán y generarán una decisión final justa. [38]

En la figura 28 se presenta nuestra propuesta de la implementación del laboratorio de cómputo forense básico donde podemos observar un croquis con la organización distribución de accesos, mobiliario, conectividad, mesas de trabajo, módulo de atención y la posible distribución de espacio para que se pueda utilizar cómodamente, aprovechando todos sus beneficios.

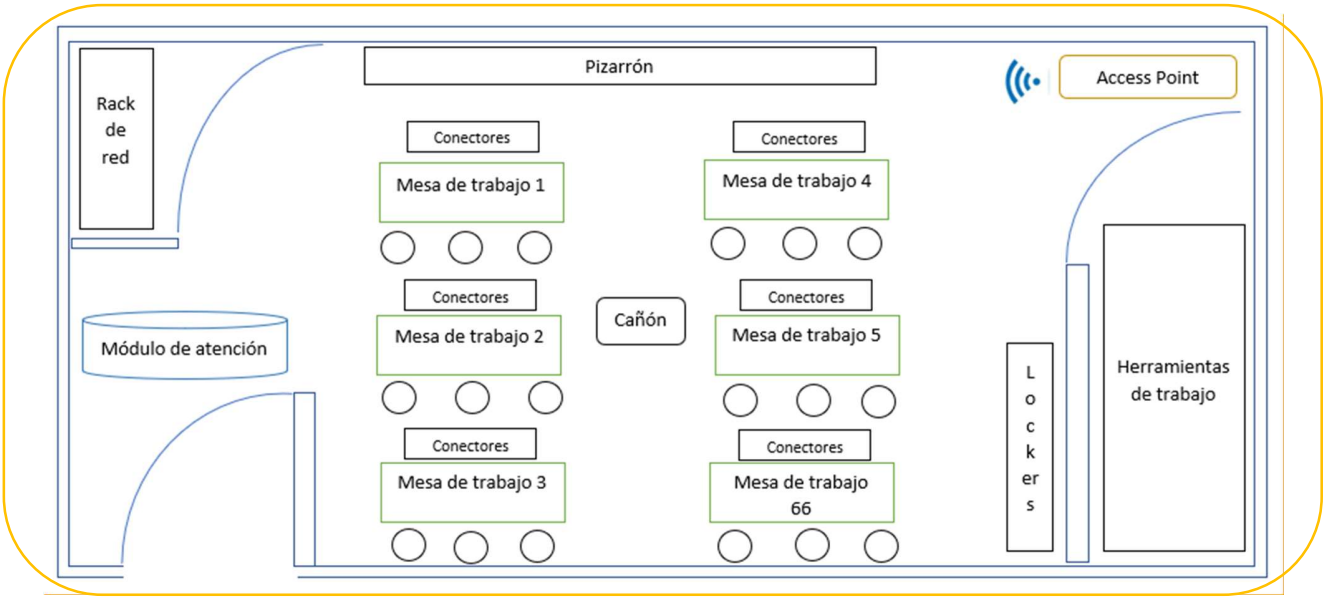


Figura 28. Croquis de la posible infraestructura del laboratorio de cómputo forense.

CAPÍTULO 3

3.RESULTADOS

Las vulnerabilidades informáticas son la causa principal de ciberataques por ello fue necesario estimar un caso de estudio para cada herramienta, se eligieron tres de ellas mencionadas en el capítulo anterior. Éstas se eligieron por la facilidad de manejo, procesamiento, interfaz amigable, curva de aprendizaje, costos, recursos y la facilidad de integración dentro de un S.O. A su vez, en diferentes artículos y trabajos de investigación han arrojado excelentes resultados para resolver problemas de ciberseguridad y del cómputo forense. Una vez utilizadas las herramientas de cómputo forense detallamos lo más importante de las pruebas realizadas que nos ayudaron y aprendimos a identificar y minimizar distintos riesgos.

OWASP y NMAP son herramientas que se complementan ya que en nuestras pruebas nos brindan un escaneo de vulnerabilidades, mediante este desarrollo descubrimos e identificamos vulnerabilidades en una red, sitios web y aplicaciones que se utilizan hoy en día. En este proceso se inspecciona una gran cantidad de tráfico de información que conecta con demasiados servidores, pudiendo también inducir a tomar decisiones de seguridad informática como condiciones de protección de servicios en los dispositivos que ocupemos dentro de una red. Estas herramientas son capaces de realizar un escaneo de vulnerabilidades mediante sus poderosas y flexibles características que nos brindan, las cuales permiten a los usuarios analizar, experimentar y compartir conocimientos de ciberseguridad para automatizar una amplia diversidad de tareas de una red que sirven para administrar una institución, empresa, laboratorio, etc.

Bulk-extractor es un software de código abierto que puede encontrar datos examinando una imagen de la memoria RAM de una computadora, el beneficio de ocupar esta herramienta de open source es que siempre está en constante actualización por ello la podemos considerarla una herramienta de cómputo forense moderna. Esta la podemos utilizar dentro de una estación de trabajo (laboratorio de cómputo forense) para recabar información de archivos y directorios de un disco duro en específico. Obteniendo esta información podemos saber qué información está dentro de una computadora en específico y donde se utilizó. Los resultados de

nuestro análisis de recolección de información fueron encontrar los datos almacenados en forma de archivos los cuales pueden contener correo electrónico, número de tarjetas de crédito, URLS de sitios web y otro tipo archivos digitales que sirven como evidencia digital. Por consiguiente, podemos decir que esta herramienta complementa a las anteriores herramientas de cómputo forense mencionadas, ya que ésta nos ayuda a buscar rastros de los daños que se provocaron con una computadora donde podemos identificar, preservar y analizar la información encontrada dentro de los diferentes escenarios que puedan surgir dentro de una investigación de cómputo forense.

3.1 Desarrollo de los experimentos

Basándonos en nuestra metodología podemos definir numerosos factores que nos ayudan a contrarrestar y calcular el riesgo de una vulnerabilidad identificada.

3.1.2 Resultados herramienta NMAP

Las pruebas se realizaron con diversos casos de uso por ejemplo **NMAP** se probó para la identificación de host donde obtuvimos resultados muy satisfactorios sabiendo quienes están conectados a nuestra red e identificar los posibles ataques que puedan surgir en ésta. Con esta herramienta podemos saber e identificar qué puertos son vulnerables con un filtrado de puertos de cada host, sistemas operativos de máquinas virtuales y físicas con sus respectivas direcciones MAC, también pudimos realizar barridos de ping exhaustivos obteniendo versiones de los servicios que ocupa una máquina (física o virtual), también distinguir los gateways internos de las máquinas que ocupan diferentes usuarios conectados a una red lo cual nos sirve para escanear (reunir) información de una red y de quienes la utilizan, percibiendo lo mencionado podemos utilizar esta información que nos brinda esta herramienta para explotar las diferentes vulnerabilidades que existan en una red y podamos protegernos de un ataque de hacking vea figuras 29, 30, 31, 32, 33 o simplemente para aprender a contrarrestar las diferentes situaciones de inseguridad informática que existen hoy en día. A su vez, ésta nos puede servir para recabar información dentro de un caso de cómputo forense sabiendo que puede reunir toda

esta información podremos determinar y averiguar quién fue el causante de un delito o intrusión en los diferentes dispositivos conectados a una red. Colocando un reporte final de toda la información que recabamos dentro de un archivo que puede utilizarse en otras herramientas de C.F.

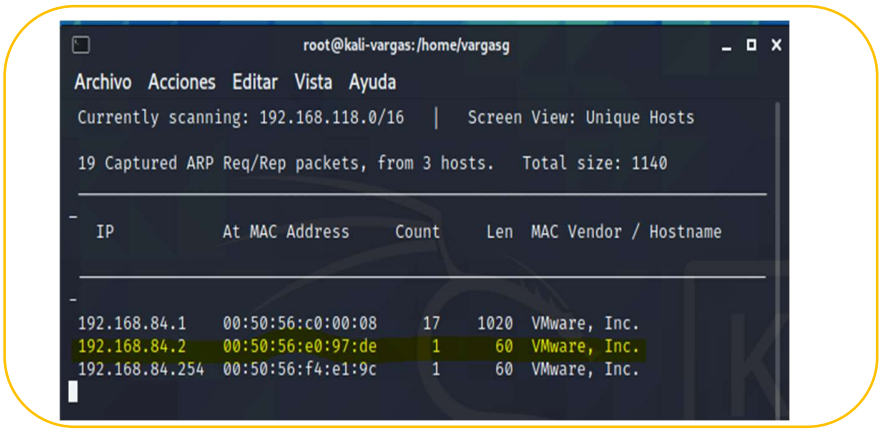


Figura 29. Identificación de dispositivos conectados a una red, host y Gateway.

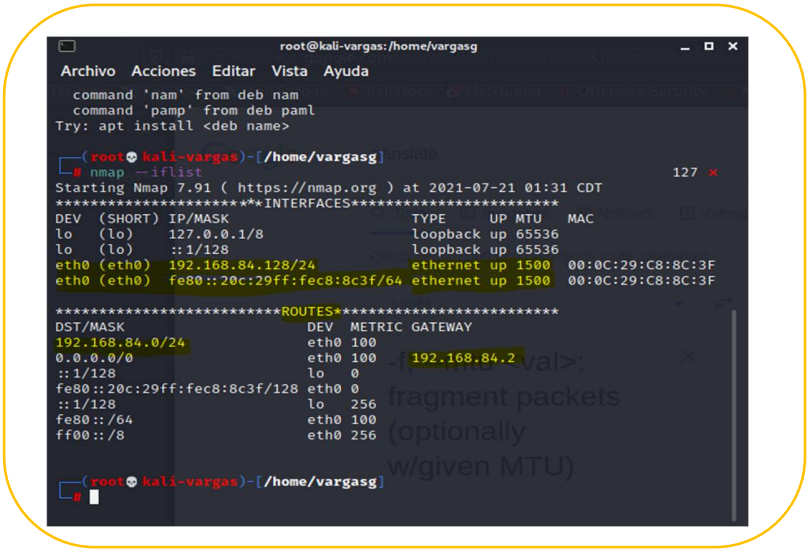


Figura 30. Identificación de red IP X.X.X.X en forma de tabla arrojando nombre de la tarjeta de red.

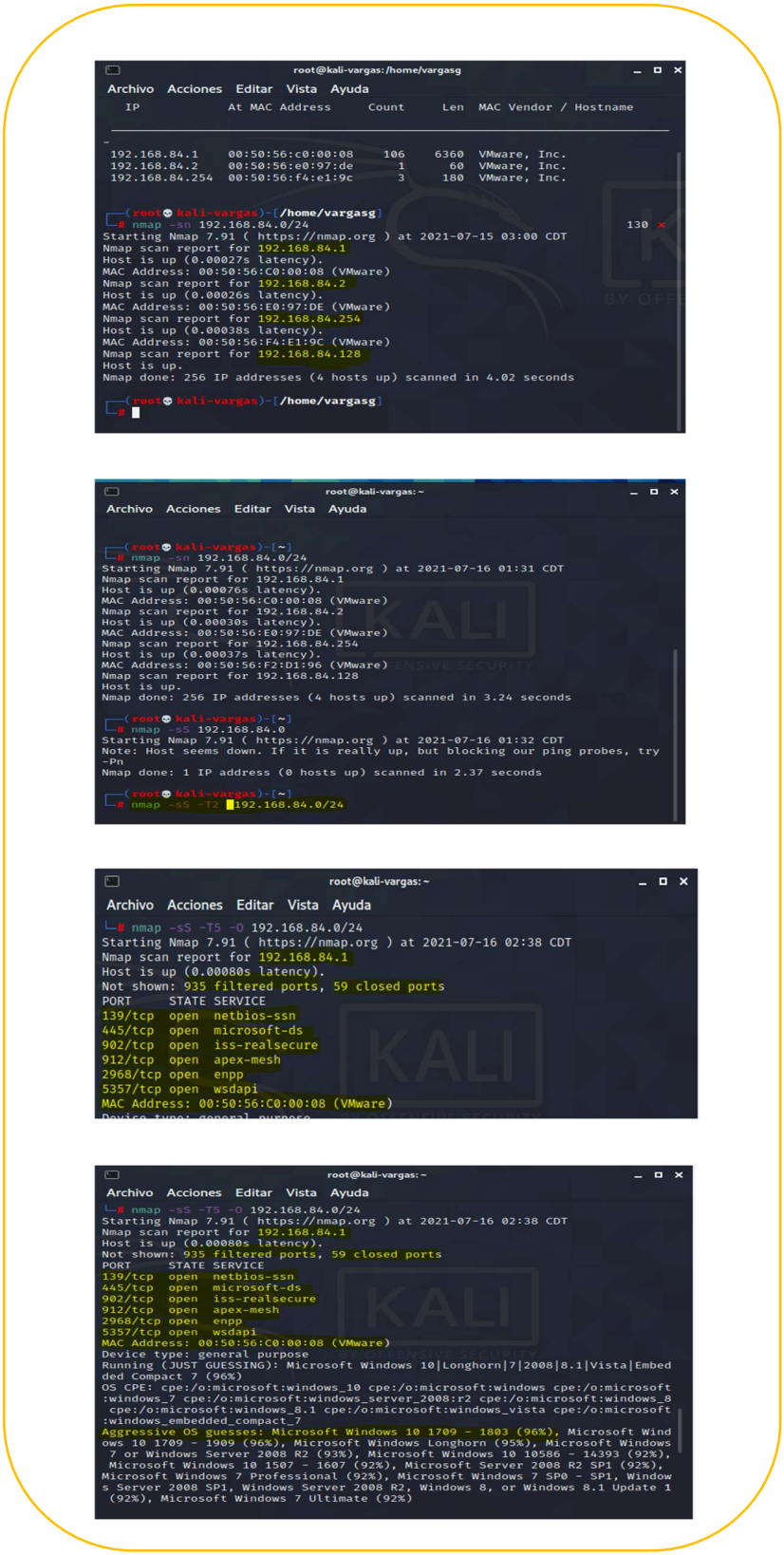


Figura 31. Identificación de puertos, host, direcciones MAC, sistema operativo de máquina física y virtual conectados a una red.

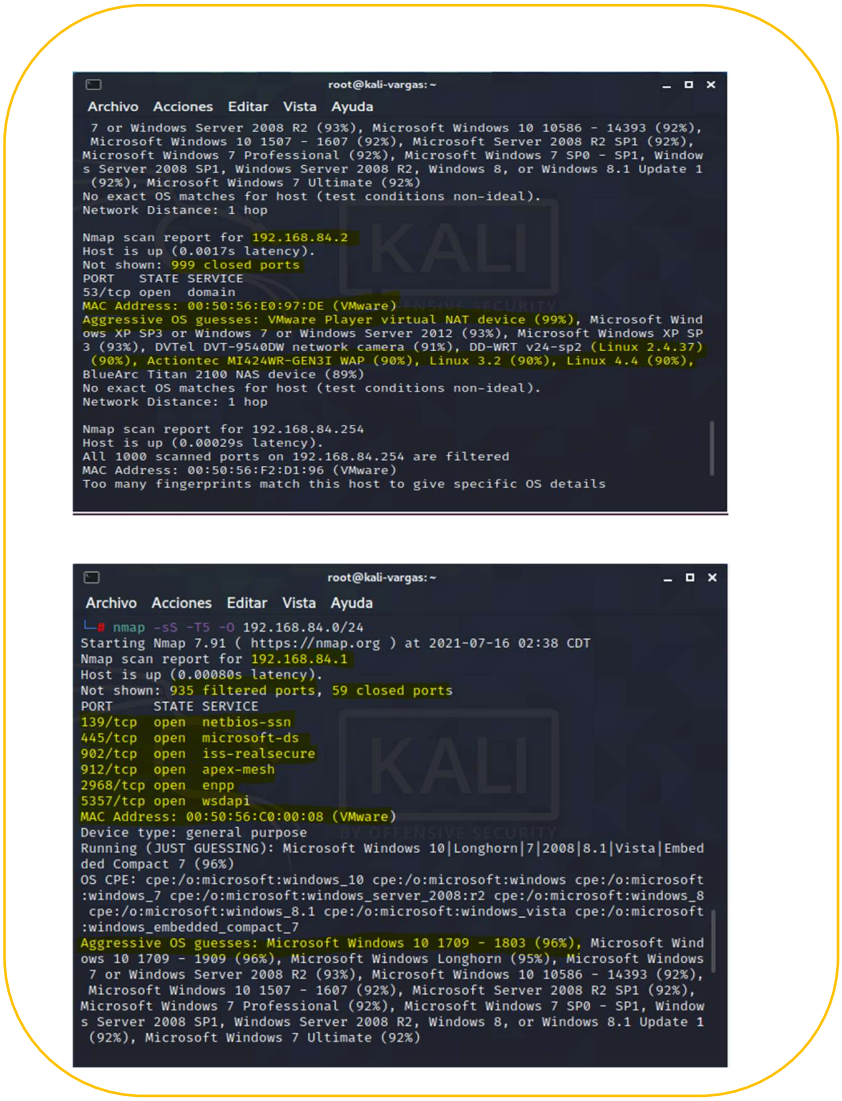


Figura 32. Identificación de S.O de una máquina física y virtual.

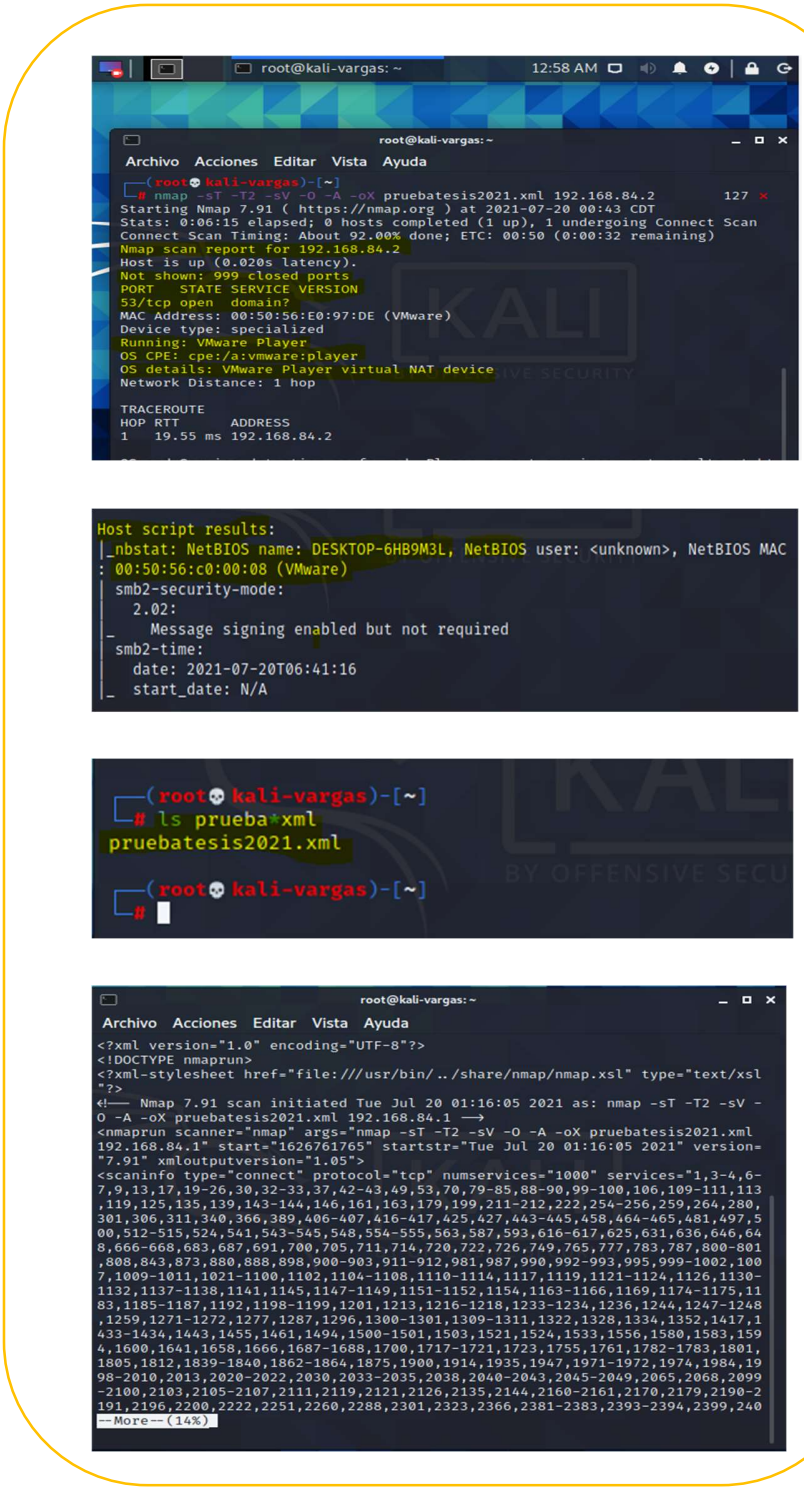


Figura 33. Creación de reporte final en formato archivo para poder utilizarlo en otras herramientas.

3.1.3 Resultado herramienta OWASP

Owasp es una herramienta utilizada en el cómputo forense, además de ser muy completa para diferentes investigaciones ayuda a los profesionales como a diferentes usuarios a comprender los fallos de seguridad (vulnerabilidades) que existen dentro un sitio web, aplicación o sistemas de infraestructura que ocupan las diferentes organizaciones hoy presente, arrojando todas las pruebas suficientes para determinar una mejora y solución específica para cada sistema, página web o aplicación que utilicemos. Utilizamos esta herramienta mayormente para evaluar la seguridad de un sitio web identificando cada vulnerabilidad en este y poder minimizar un ataque malicioso, preservando la información de lo que contenga este, el cual puede contener información digital importante. Esta herramienta la podemos utilizar como prueba de penetración en investigaciones de cómputo forense, como también en los servicios que ocupemos dentro de una institución, empresa u organización evitando que exploten los accesos de riesgo de las posibles herramientas de trabajo que podamos utilizar en la actualidad.

En nuestras pruebas ocupamos un sitio web como prueba “http://------.mx” en el cual realizamos un análisis de vulnerabilidades, los motores de búsqueda de esta herramienta nos otorgan información detallada del sitio web inspeccionado, podemos ocupar un **modo de búsqueda activo y pasivo,** en el modo activo simplemente colocamos el sitio web, IP o dominio en la interfaz de la herramienta y esta hará peticiones al servidor donde se encuentra localizado este sitio web, mostrándonos diferente información que contiene cada carpetas y directorios, en esta información podremos descubrir y visualizar los formularios, información confidencial, servidor que ocupa y lenguaje de programación del sitio, todo dependerá del certificado de seguridad de transferencia de información del sitio web, entre más seguro sea correrá menos riesgos de ataques (vulnerabilidades) como la confidencialidad de lo que contenga.

En el modo pasivo determinamos un servidor proxy el cual establecimos los puertos del sitio web analizado y su dirección IP (X.X.X.X). Este modo de reconocimiento de vulnerabilidades nos permitió visualizar los archivos del sitio como código fuente

con el que cuenta, de igual manera percibimos las modificaciones en este desde imágenes y texto (información que actualizan dentro del sitio).

En estas pruebas encontramos 17 vulnerabilidades dentro del sitio web vea figuras 34, 35, 36, 37 que lo hacen susceptible a ataques de ingeniería inversa o simplemente cuando un atacante encuentre estas tratara de encontrar la manera de delinquir con él o sacar un beneficio para el mismo, afectando la reputación de las organizaciones, instituciones u empresa que lo ocupen.

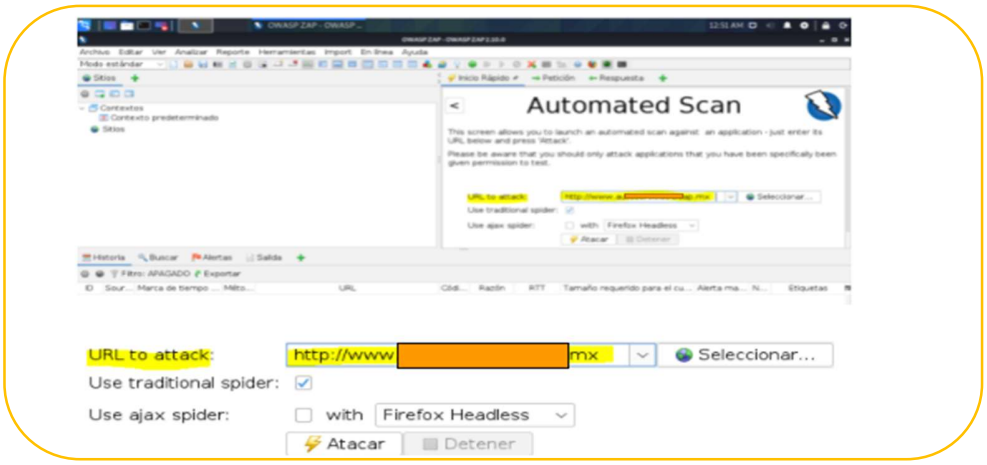


Figura 34. Ataque activo a un sitio web con protocolo de seguridad de transferencia “http” específico.

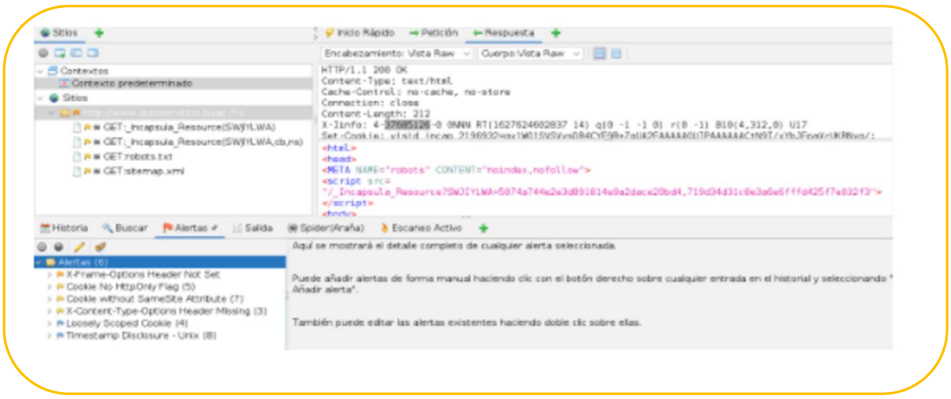


Figura 35. Identificación de vulnerabilidades del sitio web.

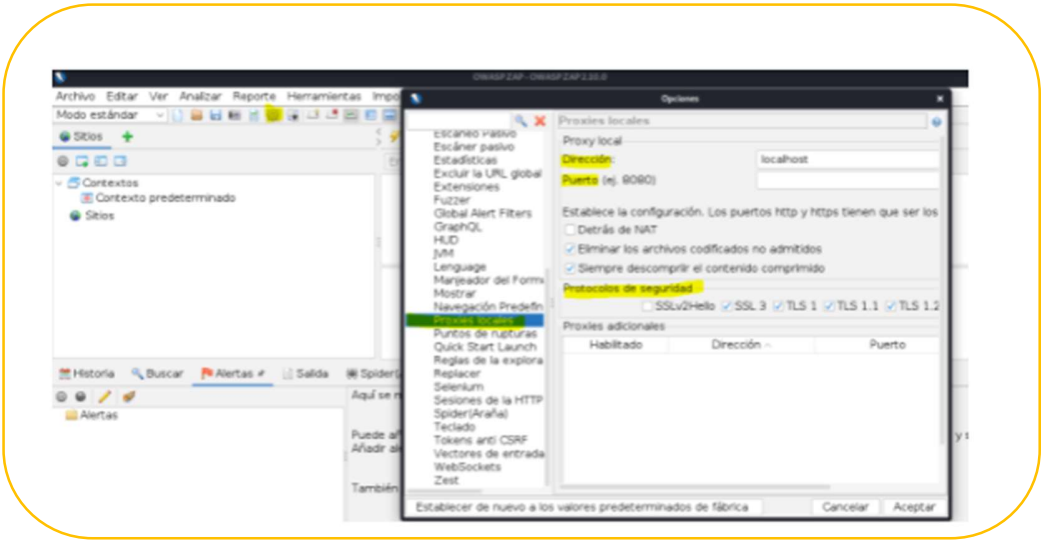


Figura 36. Ataque pasivo ocupando servidor proxy para determinar dominio y puertos específicos de un sitio web “http.mx”.

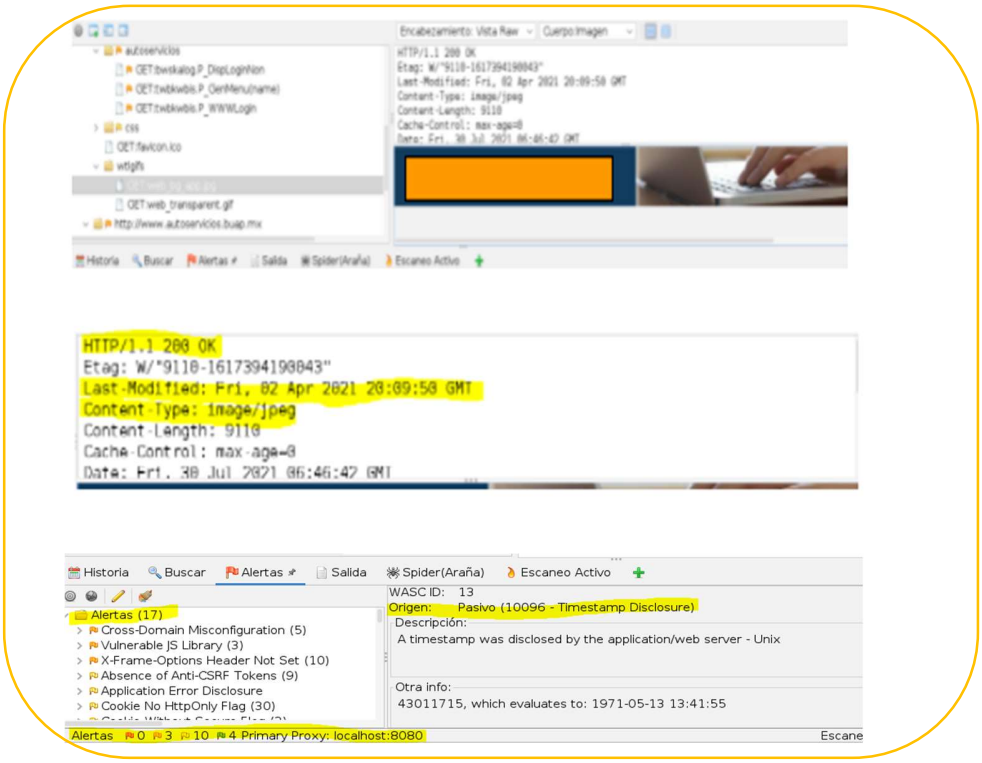


Figura 37. Vulnerabilidades encontradas en un sitio web, con todo el contenido de carpetas de información importante y las modificaciones que se realizan en el servidor.

3.1.4 Resultado herramienta BULK-EXTRACTOR

El beneficio de ocupar esta herramienta de open source (software libre) es que siempre se mantendrá actualizada, considerándola como una “herramienta moderna de cómputo forense” la cual podemos utilizar en diferentes escenarios de trabajo que involucren incidentes de ciberseguridad. Ayudando a amenizar con un **95%** de efectividad investigaciones complejas de cómputo forense, dentro de nuestra estación de trabajo nos dimos cuenta que esta herramienta es demasiado eficiente para la recolección de información, la cual realizamos en nuestro archivo de volcado de memoria de nuestra máquina física, vea in figuras 38, 39, 40, 41, 42, 43. A su vez, también realizamos pruebas con otro archivo de volcado de memoria donde analizamos diferente información digital y nos dimos cuenta que esta herramienta forense de análisis de memoria es mucho mejor que VOLATILITY, FTK-IMAGER, MAGNET FORENSICS, ya que ésta nos ayuda realiza un análisis minucioso (escaneo) de todos los archivos que se encuentran lo suficientemente ocultos dentro de la memoria RAM. Contribuyendo a una recolección completa y satisfactoria para ayudarnos a investigar la diferente información que podemos encontrar dentro de diferentes dispositivos sin dejar datos analizados. También con esta herramienta podemos analizar una imagen de disco duro completa de igual manera podríamos obtener diferentes elementos como: registros, direcciones de correo electrónico, números de tarjetas de crédito, extracción de claves AES, credenciales de usuario, URLs, direcciones IP, etc. En pocas palabras “BULK-EXTRACTOR” es una excelente herramienta para realizar investigaciones de cómputo forense ya que las tareas que nos ayuda a realizar también pueden tener índole en: investigaciones de incrustación de malware, intrusiones, ciberataques, recolección de datos comprimidos, datos dañados parcialmente o incompletos, reconstrucción de archivos, reconstrucción de imágenes JPG, GIF, PNG, TFF y diferentes datos digitales. Muy útil para generar histogramas de toda la información que se recopiló y analizó almacenando en un archivo final que es compatible con diferentes herramientas open source que se ocupan para realizar análisis de cómputo forense. Podemos decir que NMAP, OWASP Y BULK-EXTRACTOR nos ayudan a mejorar las técnicas destinadas a la extracción, preservación y análisis de

la información digital obtenida de los diferentes dispositivos que existen para almacenar información. Estas nos permitieron deducir que cumplen con todas las características para implementarlas dentro de un laboratorio forense y poder llevar a cabo un caso de análisis de información digital dentro de un caso de cómputo forense.

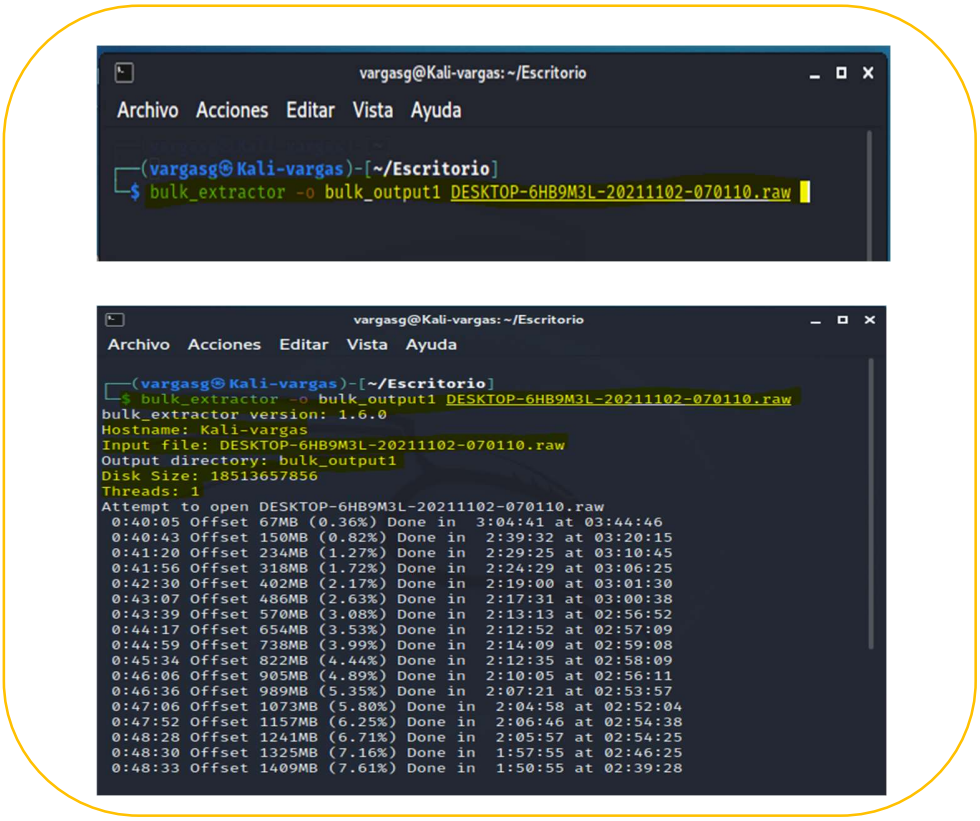


Figura 38. Análisis del archivo de volcado de memoria.

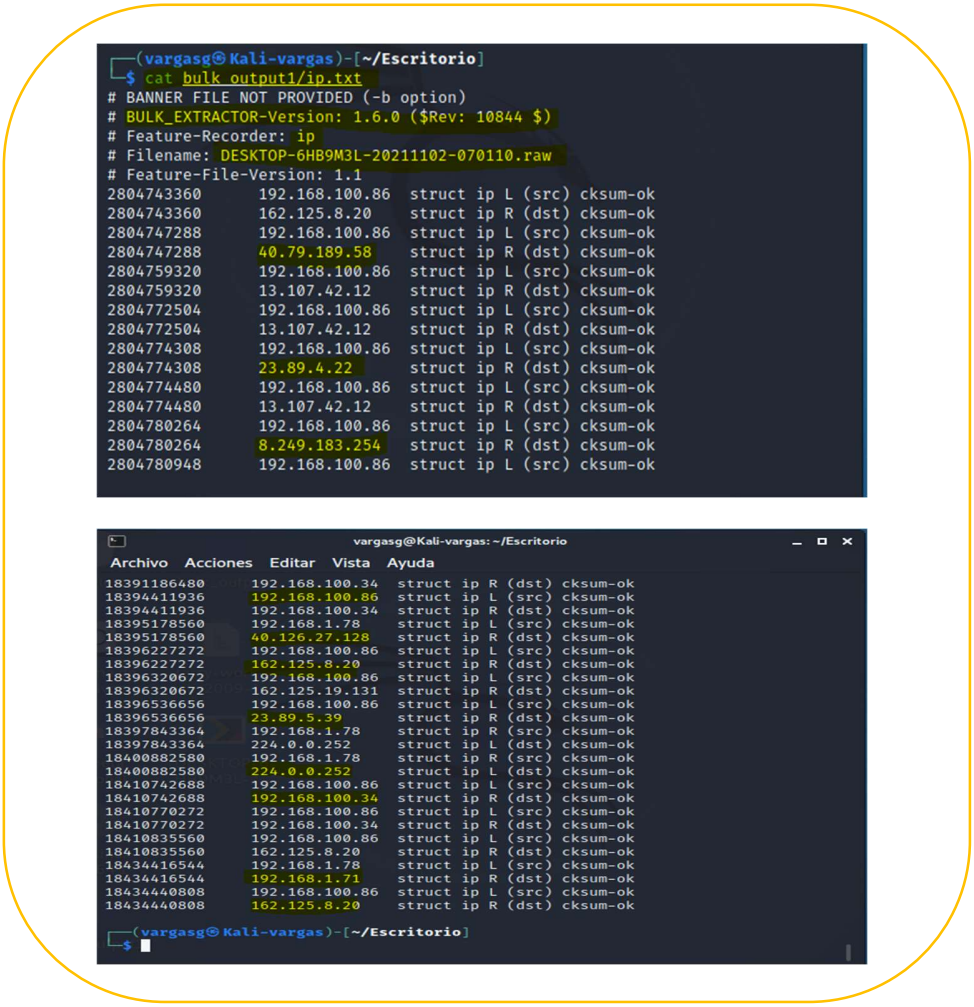


Figura 39. Inspección de IP´s almacenadas en la memoria RAM.

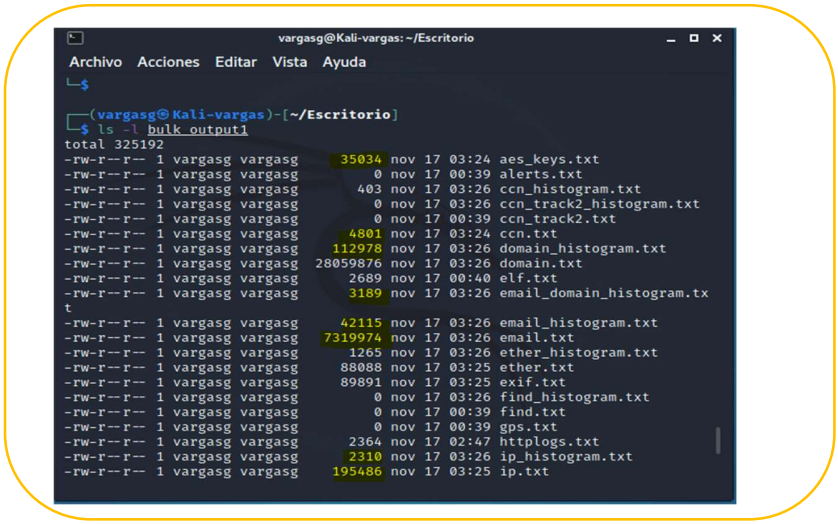


Figura 40. Histograma de extracción y recolección de archivos del archivo de volcado de memoria.

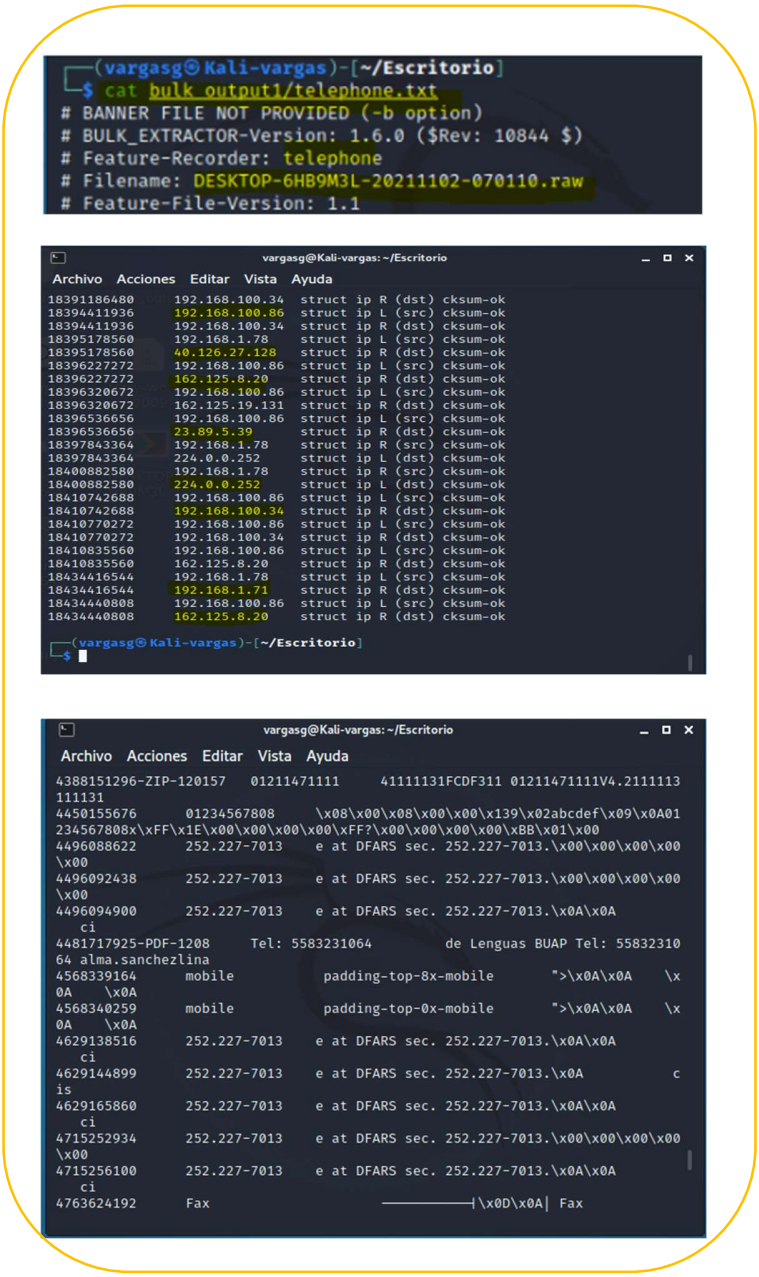


Figura 41. Extracción de números telefónicos del archivo de volcado de memoria RAM.

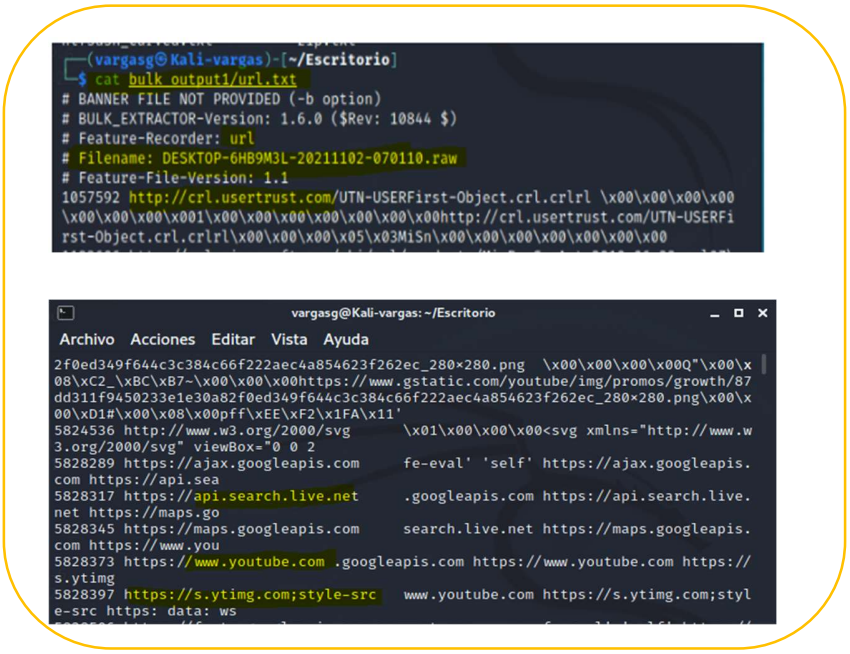


Figura 42. Emails encontrados en el archivo de volcado de memoria.

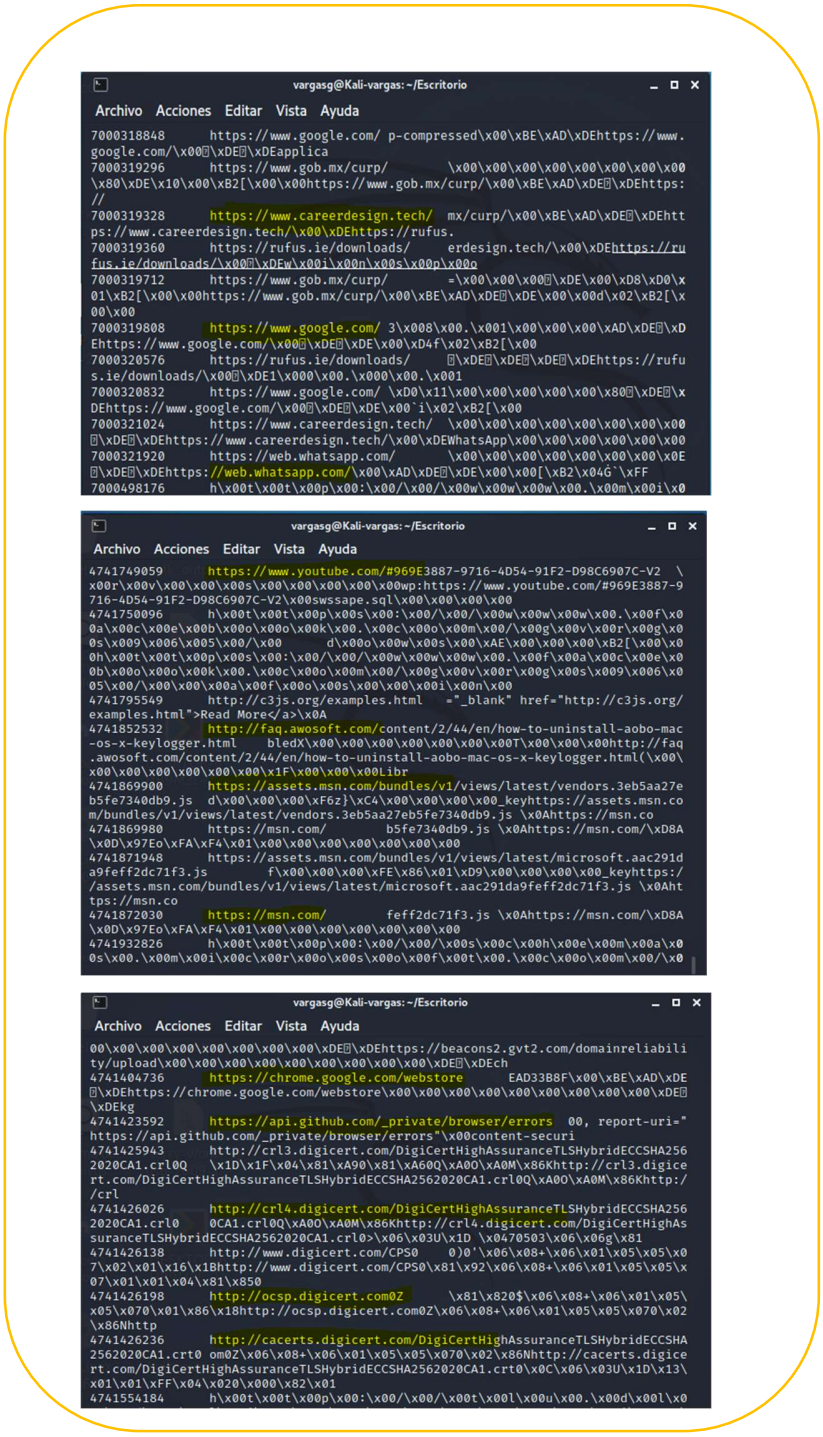


Figura 43. Direcciones URL´S visitadas en la máquina física, encontradas dentro del archivo de volcado de memoria RAM.

3.1.5 Análisis de resultados

Con las herramientas utilizadas obtuvimos un reporte forense final, con esta recolección de información (evidencia digital) cumplimos con los objetivos del cómputo forense, éste es descubrir la causa del incidente, desde donde se originó y cómo prevenir estas reincidencias, agregando toda esta información a un reporte final, éste se puede ocupar en diferentes herramientas que se usan para resolver problemas del cómputo forense. Por ello decretamos que podemos cubrir un **85%** de una investigación de cómputo forense, ya que a pesar de la velocidad y minuciosidad de la recolección de datos digitales con las diferentes herramientas, aún hay otras que se distinguen por sus técnicas y procesos de recolección y análisis de distintos datos que pueden contener diversos dispositivos, pero algunas de ellas son herramientas de software de paga donde pueden existir otras pruebas que serían muy significativas y útiles para una resolver una investigación que conlleve al cómputo forense. Así mismo, estas herramientas de cómputo forense utilizadas fueron muy eficientes las cuales nos pueden ayudar a determinar de manera justa la sentencia de un delito cometido mediante diferentes dispositivos electrónicos. Con estas tres herramientas de software libre pudimos identificar, preservar y analizar distinta información encontrada dentro de los diferentes escenarios estudiados, también podremos resolver investigaciones que puedan surgir en diferentes casos de cómputo forense, Considerando el espacio adecuado propuesto en nuestra metodología junto con los equipos de cómputo donde pueden ser instaladas estas herramientas y teniendo acceso a una red, podemos ayudar a reducir y comprender este tipo de incidentes aportando una mejora en la seguridad y privacidad de las personas que ocupen diferentes dispositivos, como también difundir la importancia de la ciberseguridad. En consecuencia podríamos culminar con nuestra propuesta de integrar un laboratorio de cómputo forense dentro de las instalaciones de nuestra facultad de ciencias de la computación para poder reducir diferentes tipos de incidentes que puedan ocurrir, vinculados a la protección de la información, vulnerabilidades en dispositivos, sistemas operativos, sitios web, aplicaciones, redes e inspección y recolección de información como la preservación

de evidencias digitales; Tomando las medidas adecuadas para que se puedan ocupar estas técnicas de manera independiente en la vida laboral o estudiantil.

CONCLUSIONES Y TRABAJOS FUTUROS

Conclusiones y trabajos futuros

Existen demasiadas generalidades que tienen cabida en vulnerabilidades específicas en una red como en los sitios web, sistemas operativos, aplicaciones y APIS reales que se utilizan en la actualidad. En consecuencia, nunca podremos ser tan precisos para calcular los riesgos de las diferentes tecnologías que se utilizan por distintas organizaciones. Pero el encargado o administrador de un departamento de tecnología dentro de una organización de TI estará familiarizado con estas herramientas y estará capacitado para juzgar la importancia de las vulnerabilidades que existen en una red, aplicaciones, dominios, sitios web y datos digitales que administra dentro diferentes sistemas, sabiendo cómo defenderse y de qué manera actuar, además de que podrá identificar las amenazas que pueden surgir para contrarrestarlas.

La experiencia que nos brindó el cómputo forense fue que nos ayuda a comprender y analizar la evidencia de delitos cibernéticos, por ello se necesita un conocimiento complejo en la teoría de la ciberseguridad como el manejo de herramientas especializadas para esta, cuyo objetivo es la revisión de la información recolectada por estas herramientas mediante las técnicas que utilizamos, conociendo estos componentes tecnológicos de software podremos analizar diferentes casos de estudio que puedan surgir en la actualidad, dando una solución científica que puede ser evaluada por un experto o investigador, con las herramientas que expusimos podemos decir que aplicándolas dentro de una computadora conectada a una red podremos obtener muy buenos resultados cerca del **85%**, sobre diferentes dispositivos electrónicos que podríamos analizar, adicionalmente la metodología propuesta está basada en modelos de recolección de evidencias digitales forenses por autores que realizan pentesting, lo cual significa que las evidencias digitales analizadas tienen un fin forense informático el cual es analizar información de manera segura y correcta, brindándonos confiabilidad en la información que resultó, esta información se puede adjuntar en un archivo final para que pueda ser utilizada en diferentes herramientas de cómputo forense; la labor que hacen estas herramientas de identificación, preservación y análisis de información es que

pueden ser utilizadas para que se analicen dispositivos recolectados por un área legal y se juzguen los delitos cometidos por una o más personas. Sabiendo esto si utilizáramos más herramientas dentro del laboratorio de cómputo forense propuesto y adjuntando más componentes (dispositivos de software y hardware) a éste, podríamos realizar investigaciones más complejas, reflejando la importancia de la ciberseguridad dentro de los dispositivos que ocupamos, como mejorar las técnicas de cómputo forense que nos ayudan a recolectar información utilizando más herramientas que nos sirvan para detectar nuevas vulnerabilidades y minimizar los riesgos de ciberataques.

REFERENCIAS BIBLIOGRÁFICAS

REFERENCIAS

[1] Sánchez Cano, Gabriel. SEGURIDAD CIBERNÉTICA, Hackeo ético y programación defensiva. (PP 268). Alfaomega; 1era Edición (2018).

[2] Gil Vera VD, Gil Vera JC. Seguridad informática organizacional: un modelo de simulación basado en dinámica de sistemas. Scientia et Technica. 2017;22(2):193-197. doi:10.22517/23447214.11371. Recuperado de: https://web-a-ebscohost-com.proxydgb.buap.mx/ehost/pdfviewer/pdfviewer?vid=5&sid=d44920b6-e80b-49a4-8a70-0a4bb35e64d8%40sessionmgr4007

[3] Arnedo Blanco, Pedro. García Rosado, David. (Marzo 11, 2014). Herramientas de análisis forense y su aplicabilidad en la investigación de delitos informáticos. (Trabajo fin de máster). Universidad Internacional de la Rioja, La Rioja, Recuperado de:https://reunir.unir.net/bitstream/handle/123456789/2828/arnedo%20blanco.pdf?sequence=1&isAllowed=y

[4] MOLINA KJM, MENESES JP, SILGADO IZ. Firewall - Linux: Una Solución De Seguridad Informática Para Pymes (Pequeñas Y Medianas Empresas). UIS Ingenierías.2009;8(2):155-165. Recuperado de: https://search-ebscohost-com.proxydgb.buap.mx/login.aspx?direct=true&db=asn&AN=48798424&lang=es&site=ehost-live

[5] La Criptografía como elemento de la seguridad informática. ACIMED. 2003;11(6):90-97. Recuperado de: https://search-ebscohost-com.proxydgb.buap.mx/login.aspx?direct=true&db=asn&AN=26302695&lang=es&site=ehost-live

[6] Hernández Encinas, Luis. La criptografía. (PP-147). Catarata; 1era Edición (2016).

[7] Cisco Networking Academy. Curso Cisco Networking Academy: Introduction to cybersecurity Español 0921a cga. 08 Septiembre 2021, de Cisco Networking Academy. Recuperado de: https://lms.netacad.com/course/view.php?id=741979

[8] Caneda Martínez, Fanl. (Julio 10,2020) Ramas de la ciberseguridad: divisiones de una profesión con futuro. Revista: Campus Training. Recuperado de: https://www.campustraining.es/noticias/ramas-ciberseguridad-profesion-futuro/

[9] Lewis, ELIJAH. CIBERSEGURIDAD, Guía completa para principiantes aprende todo de la ciberseguridad de la A a la Z. Idependently Published. 1era Edición (2020)

[10] García Garduño, Eladia Salgado Gallegos, Mireya. (2013). Análisis documental del Cómputo Forense y su situación en México. 20 Abril 2021, de IS-UAEM. Recuperado de: http://ri.uaemex.mx/bitstream/handle/20.500.11799/14288/404004.pdf?sequence=1&isAllowed=y

[11] CISCO. (2020). ¿Qué es la seguridad de red? 26 Mayo 2021, de CISCO. Recuperado de: https://www.cisco.com/c/es_mx/products/security/what-is-network-security.html

[12] Digital Guide IONOS, Seguridad. (Septiembre 4, 2019). Inyección SQL: la importancia de proteger tu sistema de base de datos. 2 Junio 2021, de Digital Guide IONOS. Recuperado de: http://ri.uaemex.mx/bitstream/handle/20.500.11799/14288/404004.pdf?sequence=1&isAllowed=y

[13] Lázaro Domínguez, Francisco. Introducción a la Informática Forense. (PP 329). Ra-Ma. (2014).

[14] B. Astudillo, Karina. Hacking Ético 101: Cómo Hackear Profesionalmente en 21 días o menos. (PP 300). CreateSpace Independent Publishing Platform, 2da Edición (2016).

[15] Oracle México. (2021). Definición de big data. 2 Junio 2021, de Oracle. Recuperado de: https://www.oracle.com/mx/big-data/what-is-big-data/

[16] González, Sofía. (Abril 12, 2016). Seguridad en Cómputo (LASC). Computo forense. Facultad de Estudios Superiores Acatlán. UNAM. Recuperado de: http://blogs.acatlan.unam.mx/lasc/2016/04/12/computo-forense/

[17] Cole, Arthur. Brett, Johnson. (Enero 9,2020). Lista de las mejores herramientas de informática forense, recuperación forense de datos, análisis forense digital. Clever How-To´s. Recuperado de: https://www.cleverfiles.com/howto/es/computer-forensic.html

[18] Coscollano, Carlos. (Marzo 3,2019). Análisis forense de dispositivos móviles. Revista: Red Seguridad. Recuperado de: https://www.redseguridad.com/especialidades-tic/auditoria-e-investigacion/analisis-forense-en-dispositivos moviles_20190313.html#:~:text=Al%20igual%20que%20para%20los,cada%20modelo%20de%20sistema%20operativo.

[19] Paus, Lucas. (Marzo 2, 2016). Análisis forense de redes con NetworkMiner 2.0 para identificar anomalías. Recuperado de: https://www.welivesecurity.com/la-es/2016/03/02/analisis-forense-de-redes-networkminer/

[20], [21] López Delgado, Miguel. (Junio 2007) Análisis Forense Digital. 2da Edición. Recuperado de: https://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf

[22] Louise L. Soe, Dan Manson y Marcy Wright. 2004. Establecimiento de clases de informática forense en red. En Actas de la 1ª conferencia anual sobre desarrollo curricular de seguridad de la información (InfoSecCD '04). Association for Computing Machinery, Nueva York, NY, EE. UU76–81. Recuperado de: https: //doi.org/10.1145/1059524.1059540

[23] Autopsy Digital Forensics. (2021). Autopsy para el entorno académico y de investigación. 21 Junio 2021, de Autopsy Digital Forensics. Recuperado de: https://www.autopsy.com/use-case/academic-research/

[24] Pérez Fernandez, Daniel. (Octubre 27, 2017). CAINE 9.0 “Quantum”: La nueva version de la distro de análisis forense digital. 22 Junio 2021, de Tecnonucleous. Recuperado de: https://tecnonucleous.com/2017/10/27/caine-9-0-quantum-la-nueva-version-de-la-distro-de-analisis-forense-digital/

[25] Montes Díaz, María José. (Abril 9,2014). NetworkMiner. 22 Junio 2021, de Hacking ético. Recuperado de: https://hacking-etico.com/2014/04/09/networkminer/

[26] Caballero Quezada, Alonso Eduardo. (Mayo 2, 2014). Crear la imagen forense desde una unidad utilizando FTK Imager. 23 Junio 2021, de ReYDeS. Recuperado de:http://www.reydes.com/d/?q=Crear_la_Imagen_Forense_desde_una_Unidad_utilizando_FTK_Imager

[27] NMAP.ORG. (2021). Capítulo 15. Guía de referencia de Nmap. 23 Junio 2021, de NMAP.ORG. Recuperado de: https://nmap.org/book/man.html#man-description

[28] Paus, Lucas. (Febrero 23, 2016). 3 distribuciones gratuitas recomendadas para el análisis forense. 23 Junio 2021, de WELIVESECURITY by ESET. Recuperado de: https://www.welivesecurity.com/la-es/2016/02/23/distribuciones-gratuitas-analisis-forense/

[29] KALI. (2021). ¿Qué es Kali Linux?. 28 Junio 2021, de Kali. Recuperado de: https://www.kali.org/docs/introduction/what-is-kali-linux/

[30] Rizaldos, Hector. (Octubre 22, 2018). Qué Metasploit framework. 30 Junio 2021, de OpenWebinars. Recuperado de: https://openwebinars.net/blog/que-es-metasploit/

[31] NMAP.ORG. (2021). Introducción. 30 Junio 2021, de NMAP.ORG. Recuperado de: https://nmap.org/

[32] WIRESHARK. (2021). Acerca de Wireshark. 30 Junio 2021, de Wireshark.org. Recuperado de: https://www.wireshark.org/

[33] OWASP. (2021). Acerca de la Fundación OWASP. 30 Junio 2021, de Owasp.org. Recuperado de: https://owasp.org/about/

[34] Caballero Quezada, Alonso Eduardo. Pruebas de penetración con Zed Attack Proxy. (Noviembre 23, 2016). Recuperado de: https://owasp.org/www-pdf-archive//OWASP_ZAP_Alonso_ReYDeS.pdf

[35 Lorenzo, Antonio José. (Agosto 18, 2020). Mejores herramientas gratuitas de informática forense. 1 Julio 2021, de RZ redes zone. Recuperado de: https://www.redeszone.net/tutoriales/seguridad/mejores-herramientas-gratuitas-informatica-forense/

[36] Nigel, Jones. Völzow, Victor. Bradley, Andrea. Stamenkovic, Branko. (Octubre, 2016). Forense digital. Una guía básica para gestión y procedimientos de un laboratorio digital forensics. 8 Julio 2021, de COUNCIL OF EUROPE (Cybercrime). Recuperado de:https://rm.coe.int/glacy-dfl-guide-version-aug-2017-v8/16809ebf68

[37] López Molina, Karen Hapue. Vindell Olivas, Juan Carlos. (2017) INFORMÁTICA FORENSE. LABORATORIO DE COMPUTACIÓN FORENSE PARA EL DEPARTAMENTO DE CRIMINALÍSTICA DE LA POLICÍA NACIONAL DE NICARAGUA. [Tesis de Licenciatura, Universidad Nacional Autónoma de Nicaragua-UNAN-Managua.] Recuperado de: https://repositorio.unan.edu.ni/6161/1/93526.pdf

[38] Grupo ATLAS De Seguridad Integral. (2021). ¿Qué es la informática forense? En Alas ya contamos con un laboratorio. 17 Agosto 2021, de Grupo ATLAS De Seguridad Integral. Recuperado de: https://lp.atlas.com.co/que-es-informatica-forense-en-atlas-ya-contamos-con-un-laboratorio#seccion7

ANEXOS

Apéndice A

CÓMPUTO FORENSE BAJO LINUX

"HERRAMIENTAS DE CÓMPUTO FORENSE"

INTRODUCCIÓN

Estas herramientas son elementos que pertenecen al sistema operativo de Kali-Linux. Se emplean mediante una máquina virtual dentro de nuestra PC las cuales vamos a utilizar y ver qué es lo que nos ofrecen.

Mostraremos breves imágenes describiendo algunas de las funciones que tienen estas herramientas para poderlas comparar con los diferentes sistemas que nos ayudan a realizar el cómputo forense.

OBJETIVO:

Analizar el entorno de las herramientas y su debido proceso de utilidad, siguiendo los estándares para verificar su funcionamiento.

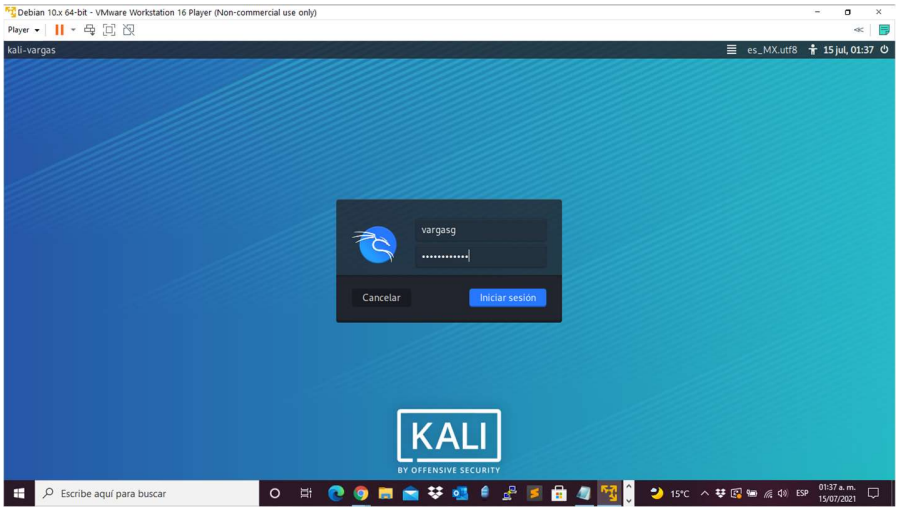
MATERIALES:

Pc personal.
Máquina virtual con S.O Kali Linux.
Conexión a internet.

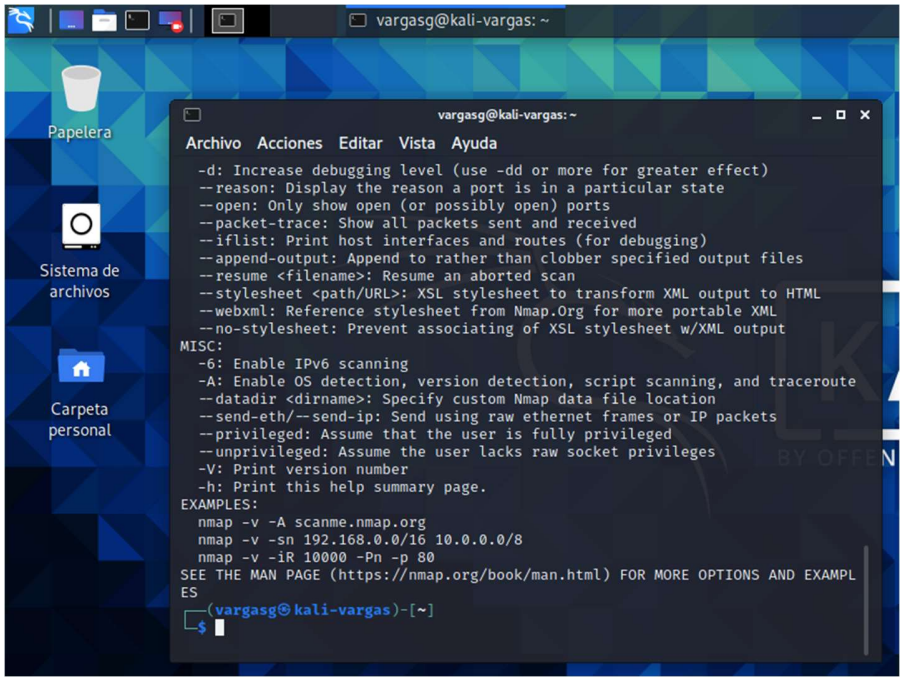
METODOLOGÍA

EJEMPLO DE DESCRIPCIÓN DE LA HERRAMIENTA NMAP.

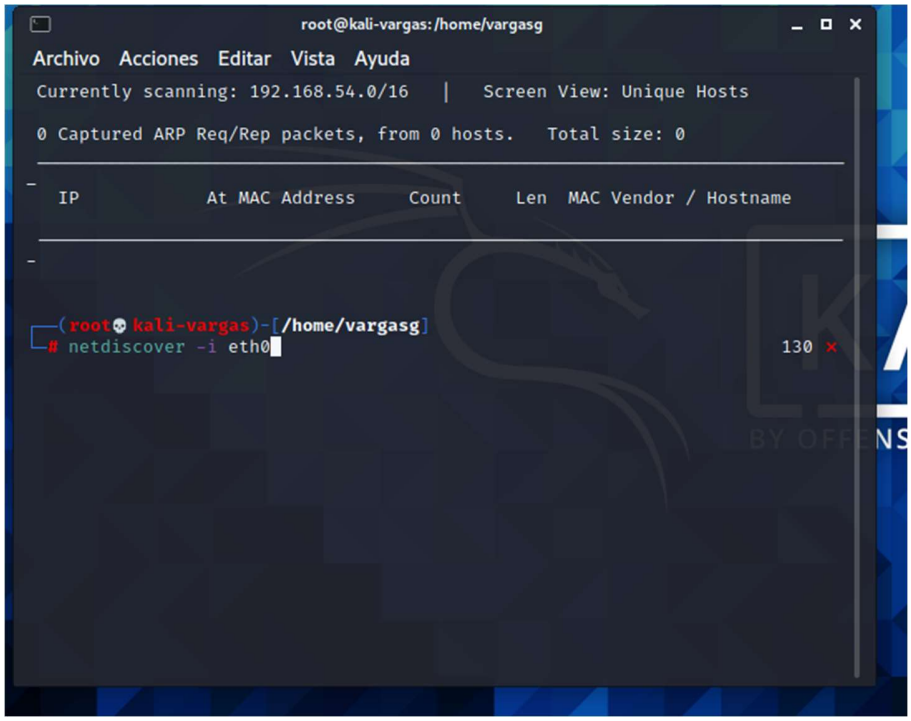
1. Iniciaremos nuestra máquina virtual accediendo al sistema Kali-Linux.



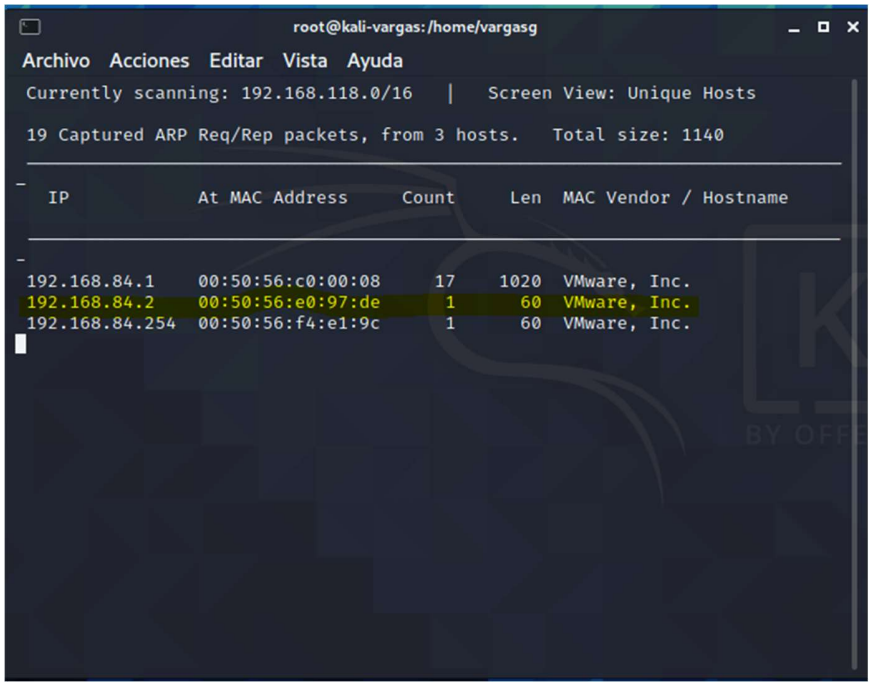
2. Una vez iniciada la sesión de nuestra máquina virtual nos fijamos en una terminal del sistema, **probando la herramienta de inspección de red y auditoría de seguridad NMAP**. La cual se encarga de enviar y recibir paquetes del tráfico de red, analizando y escaneando cada respuesta.



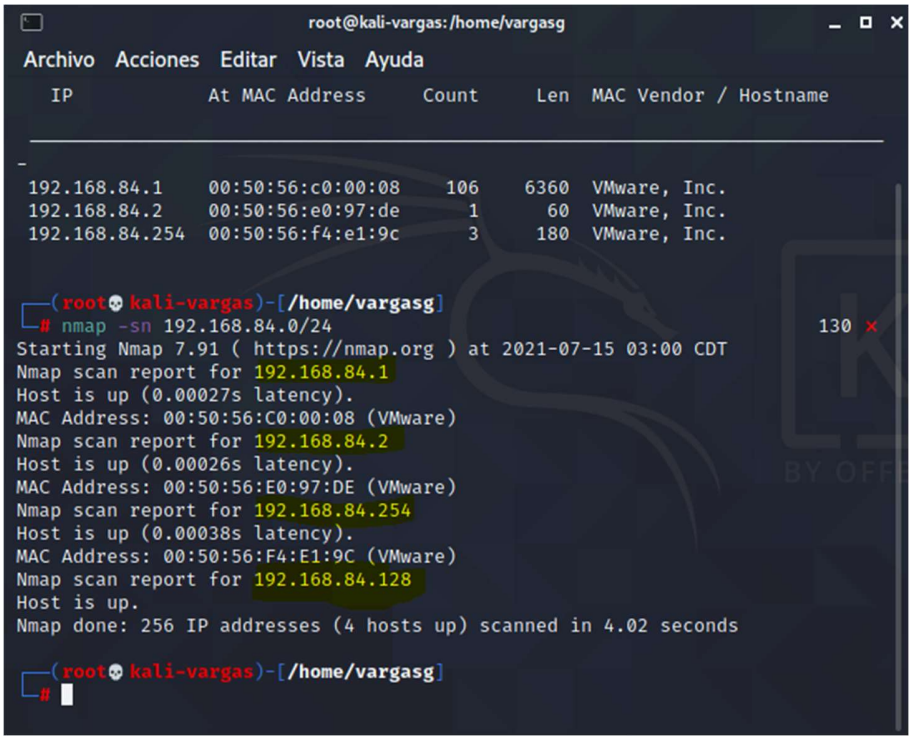
3. Vamos a empezar analizando el host de nuestra PC (máquina virtual VMware) que estamos ocupando por medio de la dirección IP en modo NAT. Ocupamos el comando **netdiscover -ieth0** para buscar que otros hosts están en nuestro segmento o subredes de red local. (eth0 es nuestro adaptador de red).



4. Una vez introducido el comando anterior podemos analizar que la red que tenemos en nuestro adaptador de red es la **192.168.84.2** en caso de no saber cuál es y sea un ataque a cierto host podríamos realizar un barrido de ping de cierta red que va desde la IP **192.168.84.0/24**.

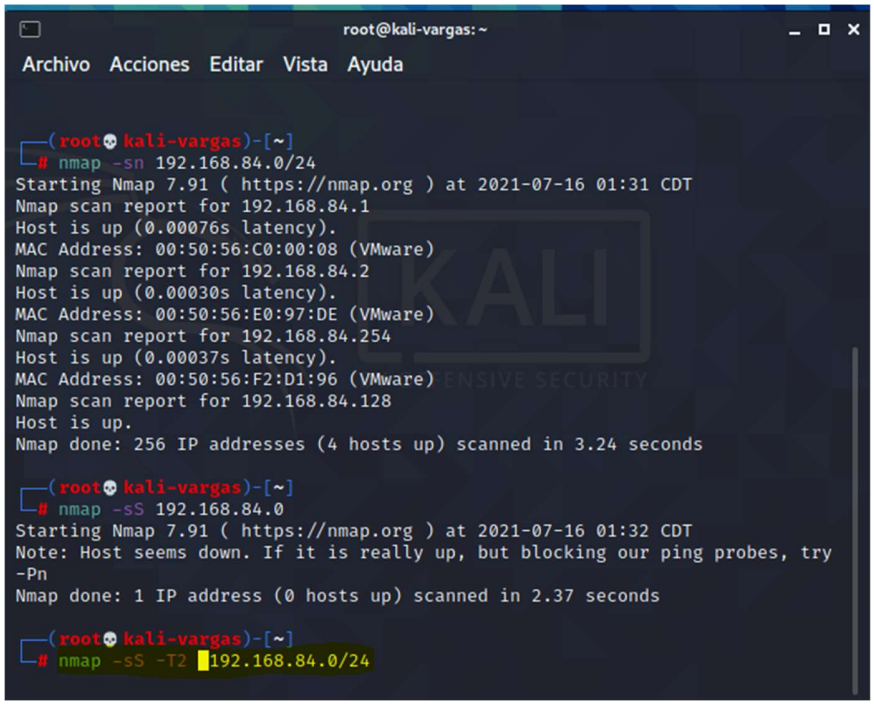


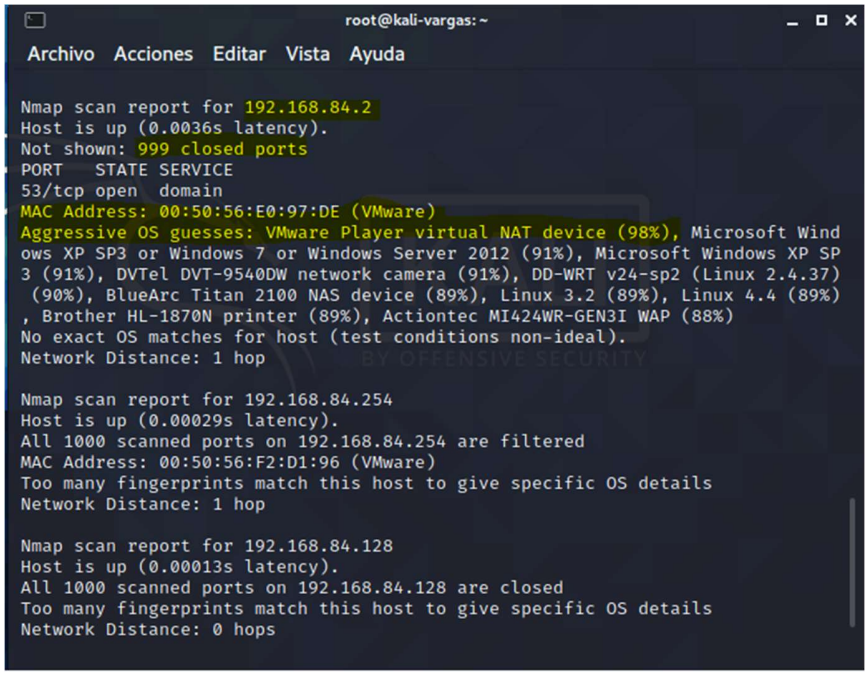
En la imagen anterior podemos darnos cuenta de los tres hosts que están en nuestra red y que dispositivo es el dueño. Hay veces que no podemos ver con facilidad a todos los hosts, por esa razón haremos un barrido de ping más profundo dónde podríamos darnos cuenta de que otros host existen en toda la red. El siguiente comando nos ayudará: **nmap -sn 192.168.84.0/24** dónde nos mostrará los hosts completos de esta red.



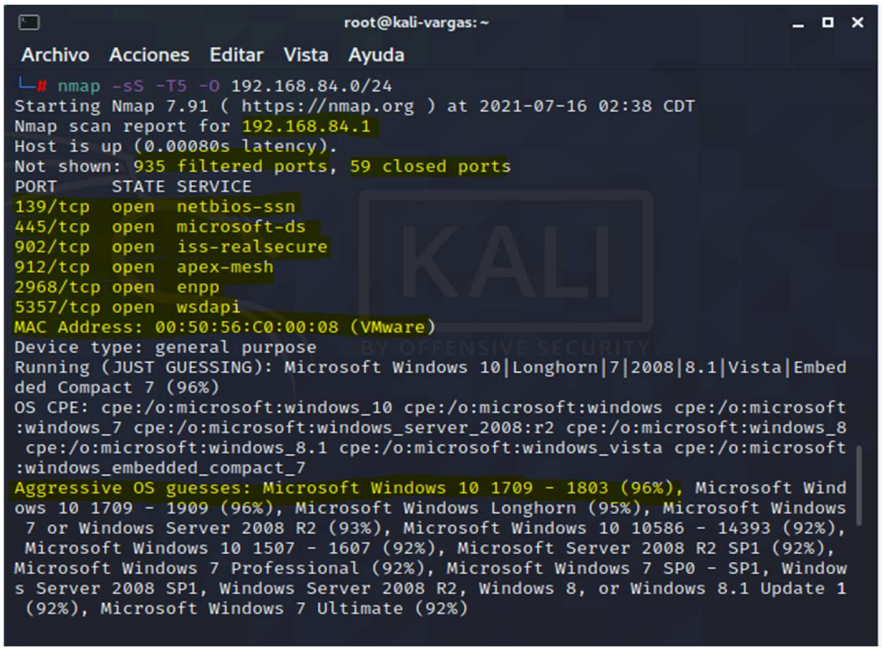
Podemos notar que apareció un nuevo host **192.168.84.128** el cual corresponde a nuestra máquina física determinando que con esta herramienta podemos hacer búsquedas más minuciosas de la red, determinando qué hosts existen y podemos analizar posteriormente.

5.De otra manera también podemos realizar un barrido de ping de todos los equipos que se encuentran en la red con más profundidad, determinando el tiempo de escaneo entre más bajo sea puede ser más cauto y podemos también saber el tipo de sistema que ocupa cada equipo conectado a la red. Eso lo podemos realizar con el comando **nmap –sS -T2 -O 192.168.84.0/24.**

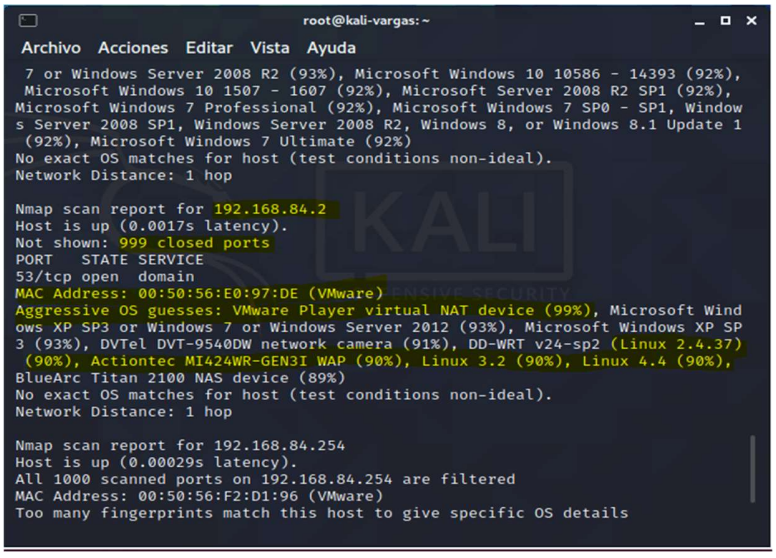




Podemos observar en la imagen anterior que después del escaneo que encontró diferentes hosts dentro de la red, como los resultados la subred **192.168.84.2** a su vez podemos ver que hay **999 puertos cerrados** e identificamos que el servicio que se está ocupando para salir a internet es nuestra tarjeta de red de la máquina física, donde la **máquina virtual (VMware)** está conectada al router simulado de la máquina física para poder tener acceso a diferentes sitios web.



En la anterior imagen encontramos la subred **192.168.84.1** la cual indica que tiene **59 puertos cerrados,** pero **935 están abiertos (filtrados),** como también **los sistemas que pueden estar dentro de la máquina física** en este caso podemos ver que es **windows 10**. Esta subred sería el gateway de la máquina física que brinda servicios a las máquinas virtuales conectadas a esta red y sería nuestro primer objetivo para ver qué es lo que contiene y ver de qué manera nos podrían atacar.

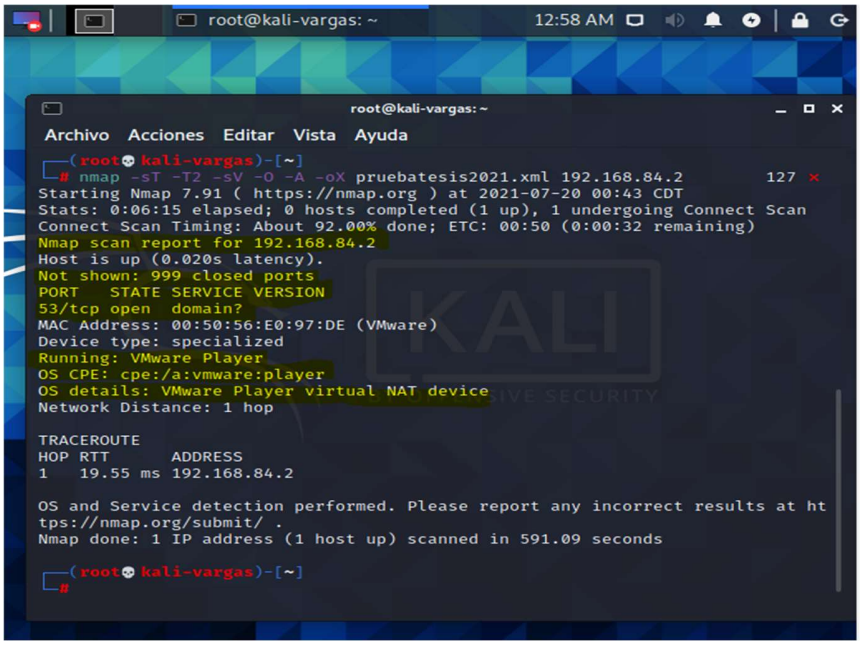


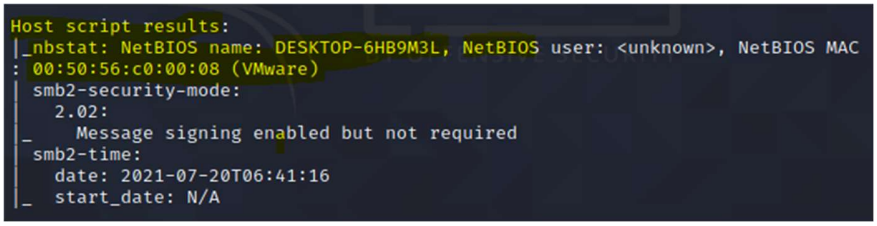
Podemos notar que hay diferentes hosts, el anterior es el **192.168.84.2 con 999 puertos cerrados**, nos indica que el sistema operativo como la máquina virtual que se está

ocupando y arrojando los resultados de los posibles sistemas operativos que cuenta esa máquina virtual como: **Linux 4.4 asegurando que es un 90% de efectividad que sea esa distribución.**

Es entonces donde nosotros podemos identificar qué máquina podría ser la posible qué está ocupando un atacante e indagar qué es lo que contiene y que trata de hacer.

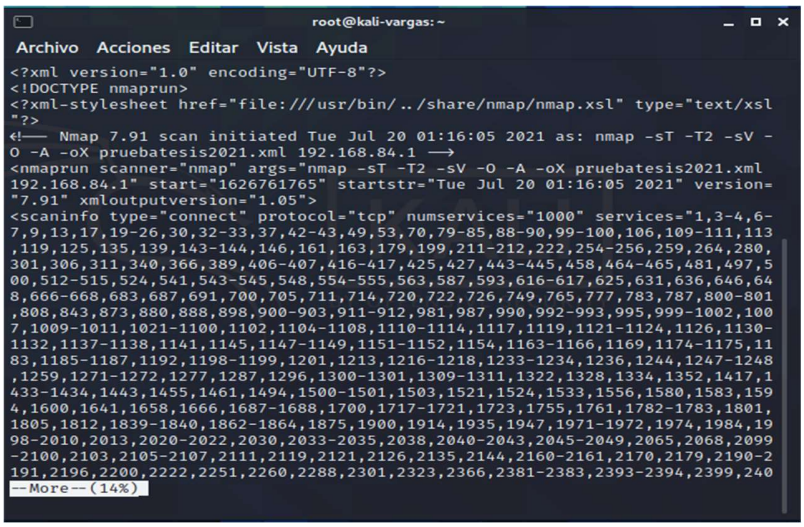
6. Analizando lo anterior después de realizar un barrido de ping profundo con temporizador bajo, podemos notar que el tiempo de escaneo fue satisfactorio y no nos denegó la inspección es por ello que podemos realizar un escaneo TCP más detallado de la máquina virtual identificada en la red, para averiguar los nombres de servicios como los nombres de las aplicaciones como la versión que están utilizando los usuarios conectados a la red. El comando que debemos utilizar es **nmap -sT -T2 -sV -O -A -oX pruebatesis2021.xml 192.168.84.2** el cual nos brindará un formato de archivo **xml** donde nos informará lo mencionado anteriormente. El cual también podemos ocuparlo en otros frameworks de explotación y poder utilizar esta información para realizar un reporte completo de evidencias.





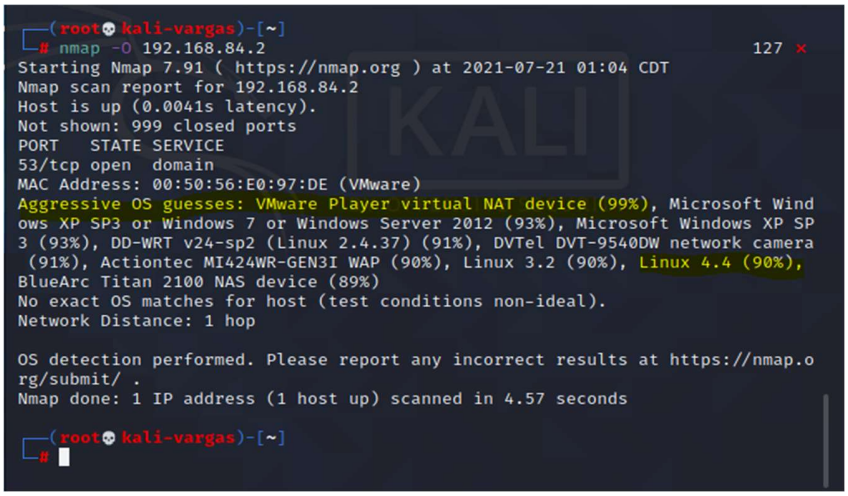
En las imágenes anteriores vemos cómo escaneo nuestro host de la máquina virtual identificada con el sistema Linux, **192.168.84.2 detallando** los puertos en este caso solo está abierto el 53/TCP (servicios DNS, Email, HTTPS) el cual no cuenta con una (configuración) conexión, por ello es que no muestra la versión y los servicios de dominio de la red NAT de nuestra máquina virtual, si tuviera un dominio configurado nos mostrará el nombre del servicio y las aplicaciones que ejecuta, es muy importante tener cerrado este puerto para que un externo (atacante) no tenga respuesta del servicio DNS y evitemos posibles ataques por este medio, también observamos la dirección MAC de la máquina virtual y el script el cual nos muestra el nombre de la máquina física que estamos utilizando.

Visualizando el contenido del **archivo XML** podemos notar todo el escaneo que se realizó y la información que almacena.

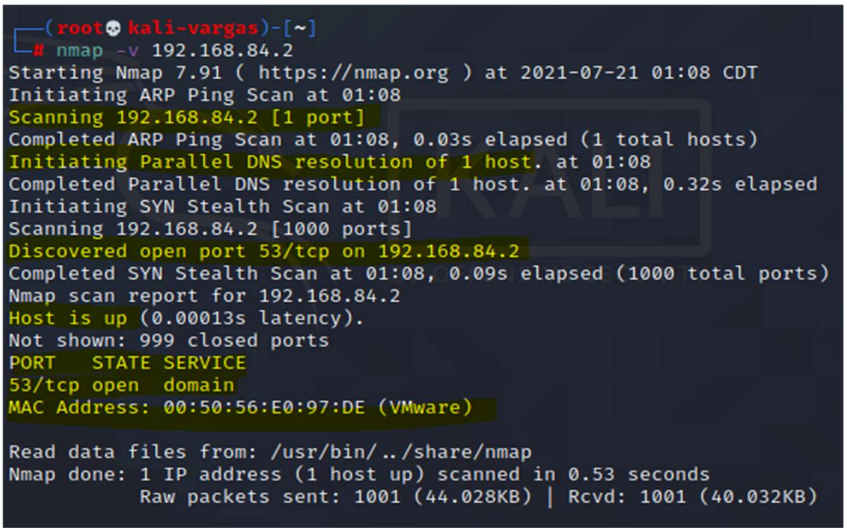


7. Parámetros de **NMAP** los más utilizados y para qué sirven.

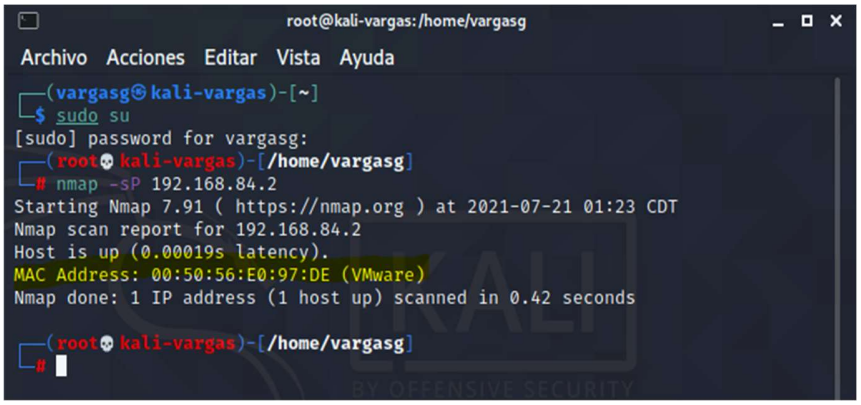
- **nmap -O 192.168.84.2** habilita la detección del sistema operativo



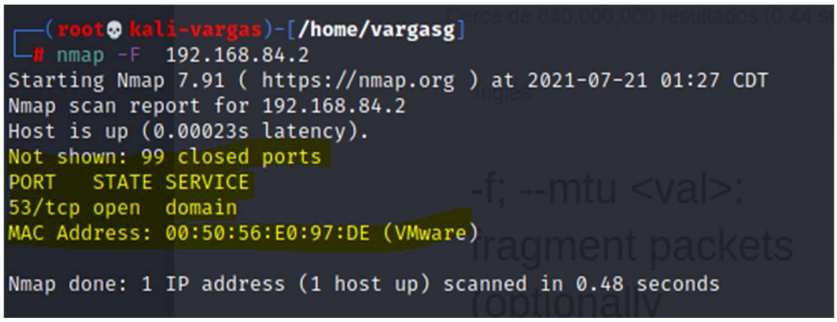
- **nmap -v 192.168.84.2** identifica las versiones de los servicios y aplicaciones que se están ocupando en el host.



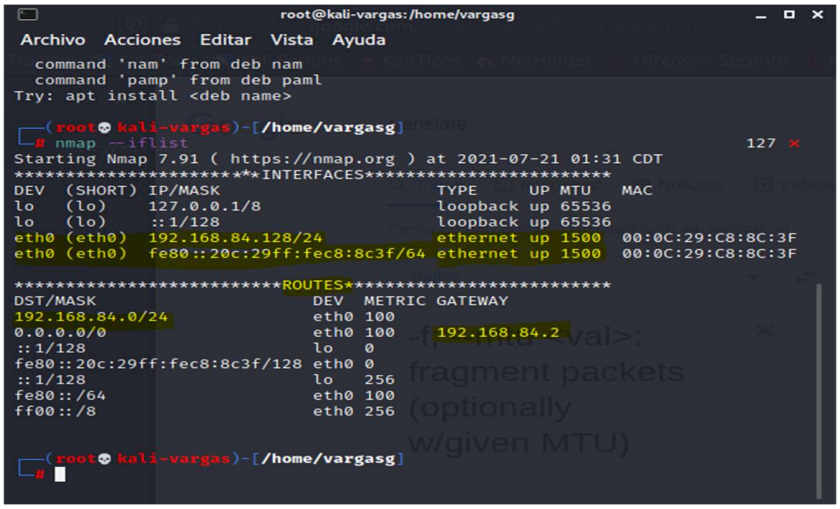
- **nmap -sP 192.168.84.2 este** comando nos sirve para identificar la dirección MAC de nuestra máquina física o virtual.



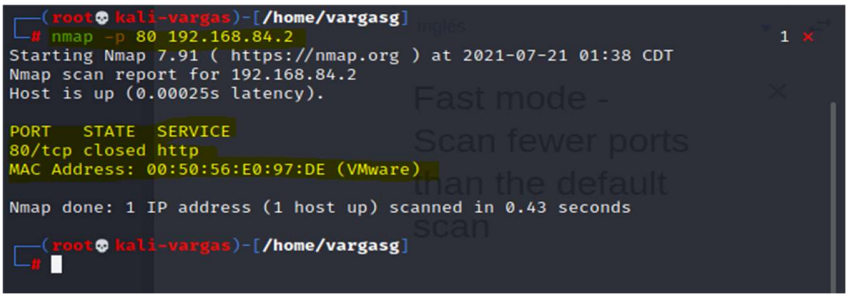
- **nmap -F 192.168.84.2 podemos** identificar los puertos y su estado, el nombre del servicio que está utilizando, así como la dirección MAC del host escaneado.



- **nmap --iflist** arroja una tabla en forma de lista donde nos informará el nombre de nuestra tarjeta de red en este caso es (eth0), identificando el gateway el cual está conectado nuestra máquina virtual y nos ofrece los servicios de conexión a internet y su vez la ruta de la red que utilizamos.



- **nmap -p 80 192.168.84.2** escanea el puerto indicado brindarnos información del estado y el servicio que utiliza.



CONCLUSIONES: Con NMAP pode

mos identificar desde el sistema operativo, host, puertos filtrados, versiones de los servicios que ocupa una máquina física o virtual, gateways internos de las máquinas que ocupan diferentes usuarios lo cual nos sirve para recabar (escanear) información de una red y quienes son los que la utilizan. Esta la podemos utilizar para explotar diferentes situaciones como investigaciones, hacking ético, aprendizaje etc. Detectando las vulnerabilidades analizarlas y ver de qué manera podemos actuar de la mejor manera.

BIBLIOGRAFIA:

B. Astudillo, Karina. Hacking Ético 101: Cómo Hackear Profesionalmente en 21 días o menos!. (PP 300); CreateSpace Independent Publishing Platform, 2da Edición (2016).

NMAP.ORG. (2021). Introducción. 21 Julio 2021, de NMAP.ORG. Recuperado de: Nmap: the Network Mapper - Free Security Scanner

Apéndice B

CÓMPUTO FORENSE BAJO LINUX

"HERRAMIENTAS DE CÓMPUTO FORENSE"

INTRODUCCIÓN

Estas herramientas son elementos que pertenecen al sistema operativo de Kali-Linux. Se emplean mediante una máquina virtual dentro de nuestra PC las cuales vamos a utilizar y ver qué es lo que nos ofrecen.

Mostraremos breves imágenes describiendo algunas de las funciones que tienen estas herramientas para poderlas comparar con los diferentes sistemas que nos ayudan a realizar el cómputo forense.

OBJETIVO:

Analizar el entorno de las herramientas y su debido proceso de utilidad, siguiendo los estándares para verificar su funcionamiento.

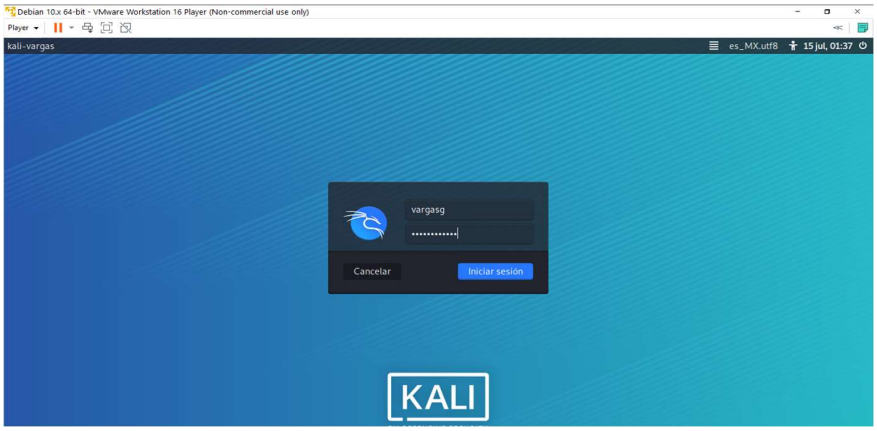
MATERIALES:

Pc personal.
Máquina virtual con S.O Kali Linux.
Conexión a internet.

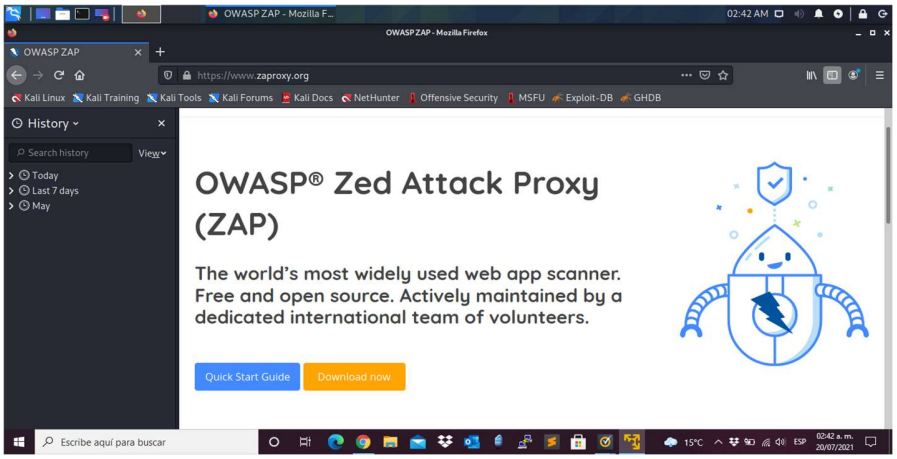
METODOLOGÍA

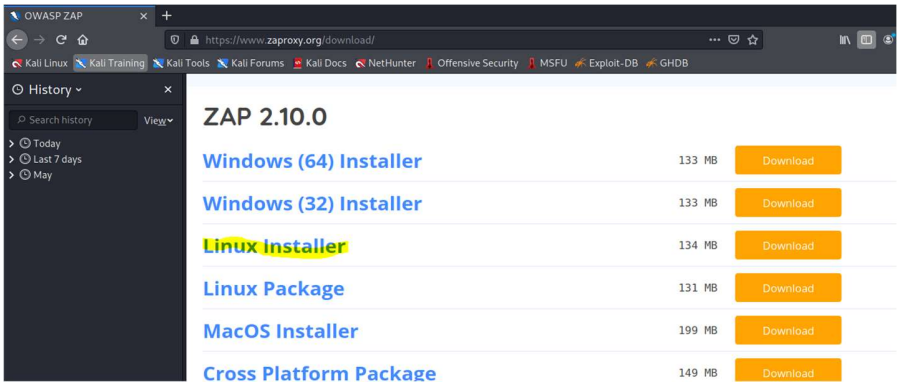
EJEMPLO DE DESCRIPCIÓN DE LA HERRAMIENTA OWASP.

1.Iniciaremos nuestra máquina virtual y accederemos a nuestro sistema operativo Kali-Linux.

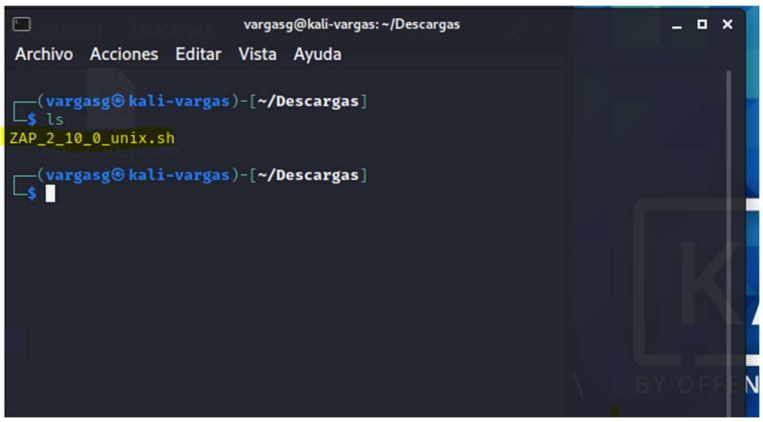


2. Una vez iniciada nuestra sesión, procederemos a ir a nuestro navegador web buscando la herramienta que utilizaremos, en la página oficial https://www.zaproxy.org/ .

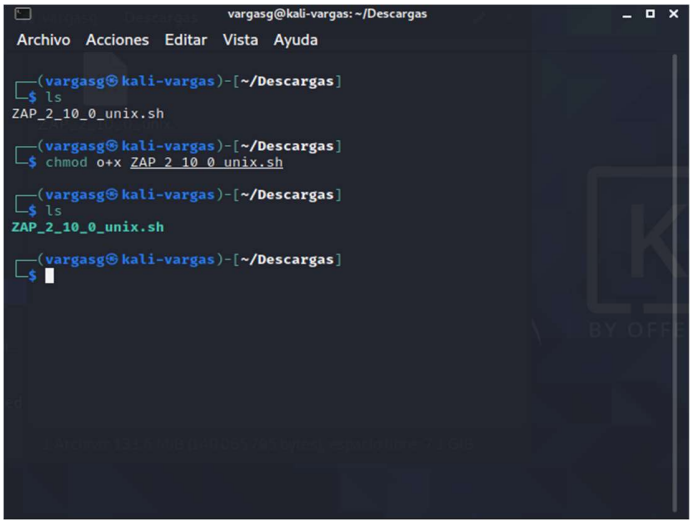


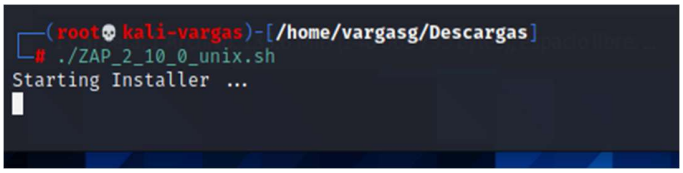


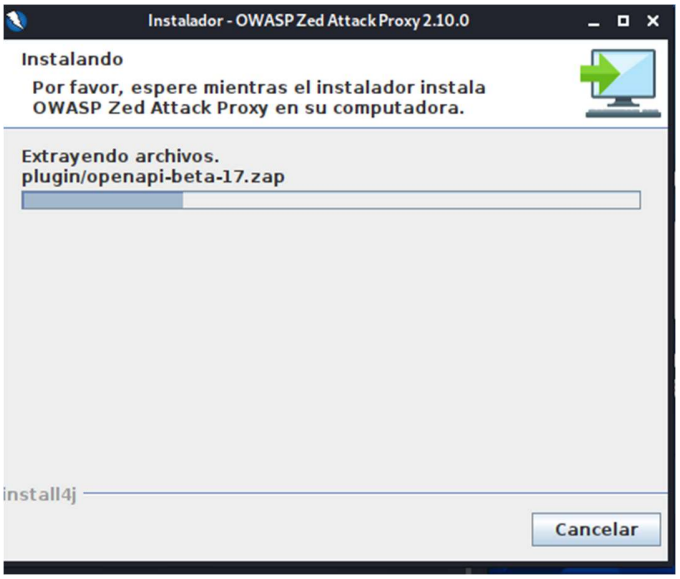
3. Una vez se haya descargado el archivo correctamente, abriremos una terminal para poder instalar correctamente nuestra herramienta.



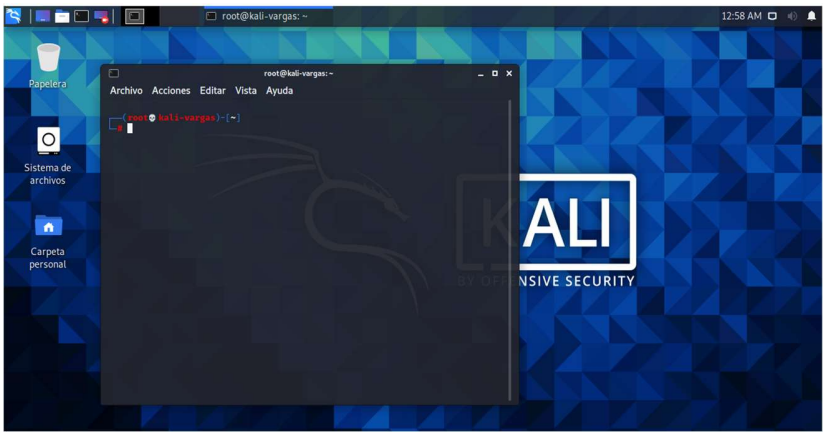
Procederemos a darle permiso de ejecución con el comando **chmod o+x 'y el nombre del archivo'.** El cual notaremos un cambio en las letras del archivo pasando a un color verde el cual indica que podemos ejecutarlo.

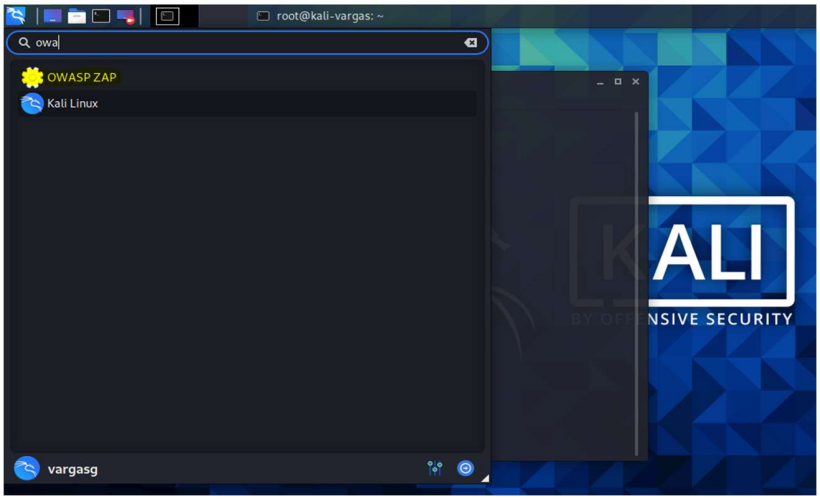






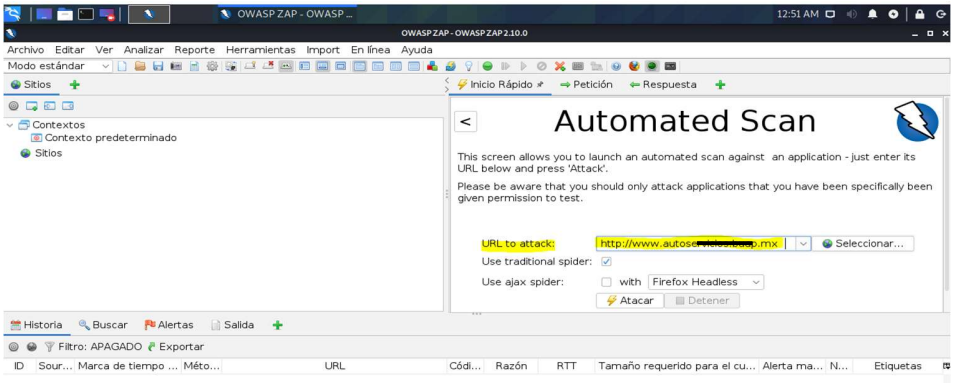
4. Una vez instalada la herramienta también podemos visualizarla en una terminal de nuestro S.O. Para posteriormente hacer uso de las cosas más eficientes e importantes que ofrece esta.





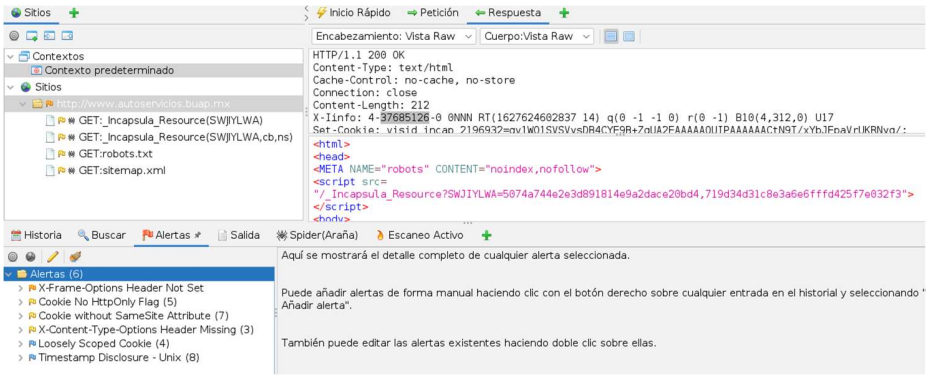
Algo importante que nos ofrece esta herramienta es realizar descubrimientos de motores de búsqueda los cuales pueden exponer información que pueden servir para comenzar un ataque malicioso. La herramienta tiene diversidad de utilidades, pero utilizaremos las más importantes.

5. Comenzaremos utilizando nuestra herramienta visualizando los modos de ataque con los que cuenta, los cuales son el **modo activo o pasivo.**

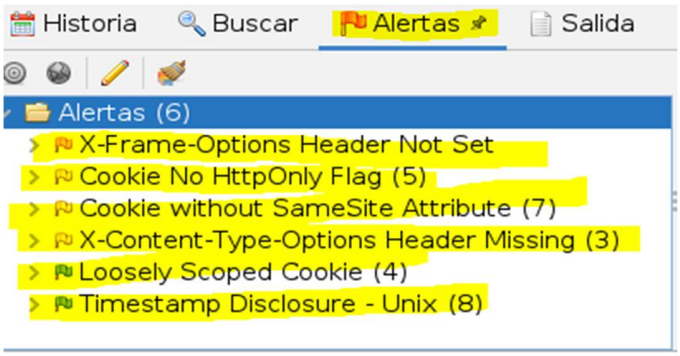


- **En la imagen anterior podemos observar cómo el modo activo funciona simplemente estableciendo la dirección web que queremos auditar.**

Cuando la herramienta comience a hacer el ataque hará demasiadas peticiones hacia los diferentes archivos que tiene ese sitio web, incluyendo el directorio de robots mostrándonos diferente información que contiene cada carpeta. Permitiéndonos descubrir formularios o información confidencial que contenga el sitio, también el servidor que ocupa y que lenguajes ocuparon para diseñar la página web. Dependerá del certificado de seguridad del sitio para ver qué tan efectivo es contra este tipo de ataques.

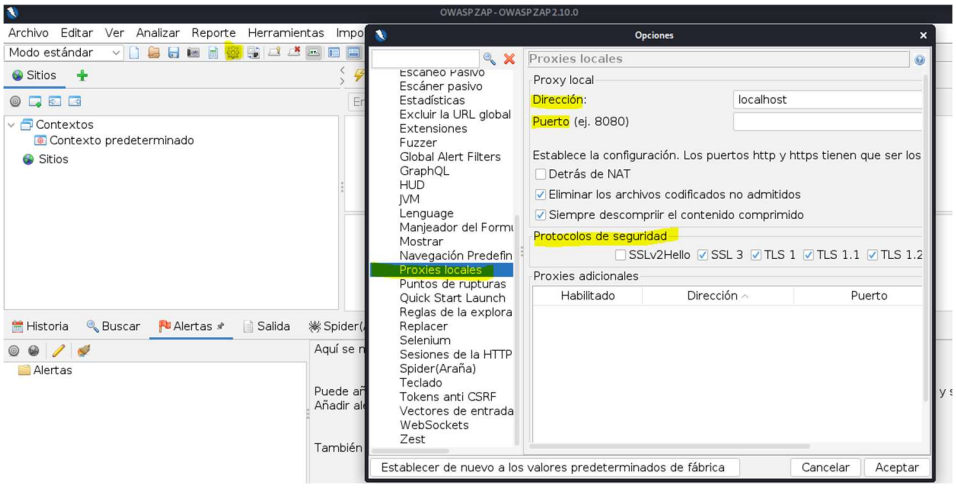


Podemos visualizar en la imagen las alertas de seguridad encontradas y de qué modo está comprometido el sitio web atacado.

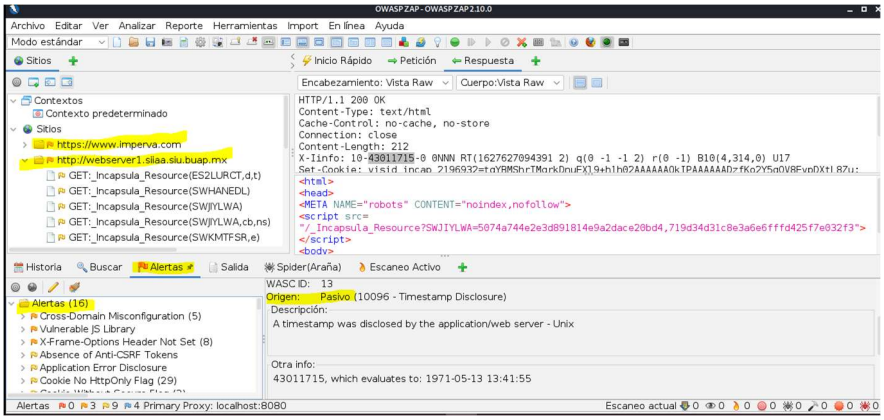


Un atacante lo que busca siempre es descubrir las vulnerabilidades de un sitio, aplicación y usuarios en especial, posteriormente buscará explotar los accesos que desee dentro de esas vulnerabilidades, siendo un factor clave para realizar un ataque mayor dejando diferentes secuelas en el sitio.

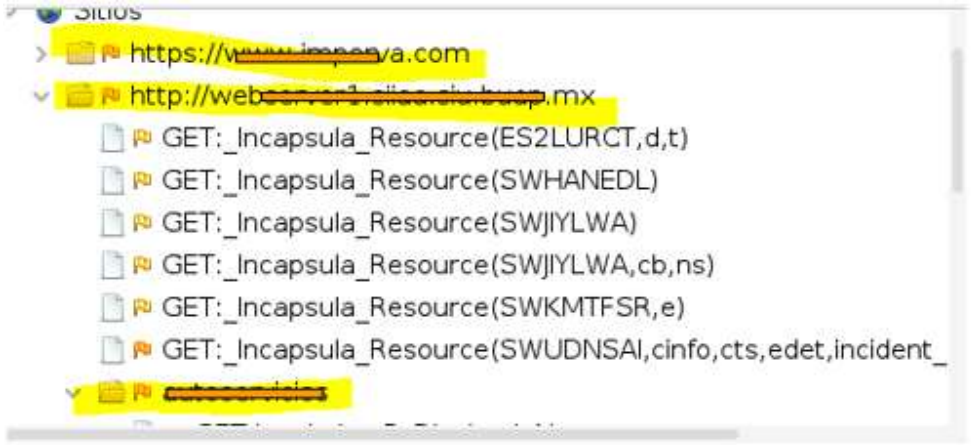
6. Ataque pasivo: su funcionamiento consiste en la configuración de un proxy dónde nos permite establecer los puertos (http, https), la dirección IP (X.X.X.X), junto con la seguridad de protocolos.



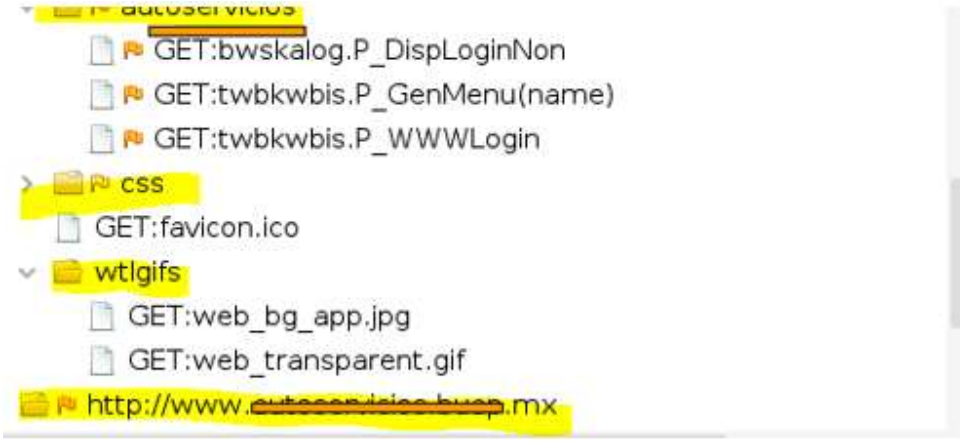
Configuraremos nuestro proxy seleccionando el icono de engrane y elegiremos la opción “Proxies locales”, donde podremos establecer la IP, puertos, protocolos de seguridad, etc.



En la imagen anterior observamos las carpetas subrayadas en amarillo donde podremos encontrar desde archivos de la página web atacada y su código fuente y que conforma.



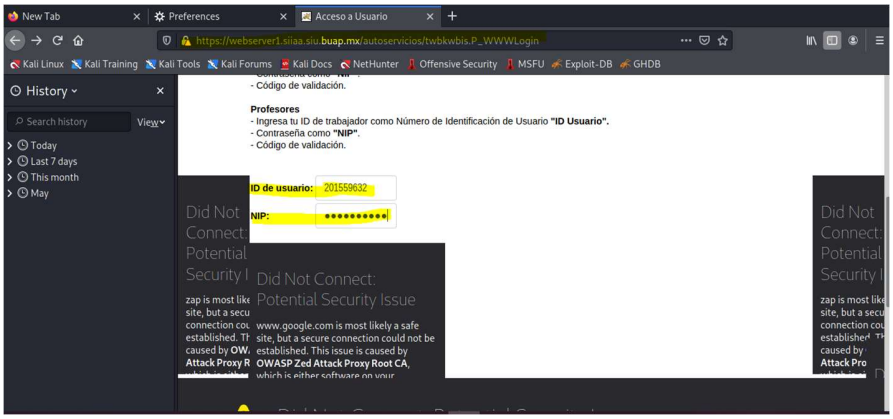
En esta imagen observamos lo que contiene la carpeta y las peticiones que hace al servidor.



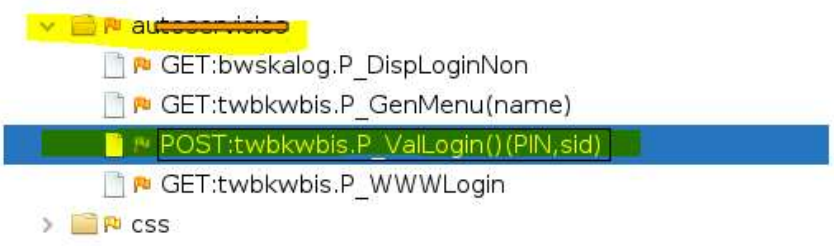
De igual manera podemos encontrar el nombre de las imágenes que conforman parte del sitio, al igual que cuando se modificaron en el servidor.

En la siguiente imagen notamos que el sitio web atacado hizo algunas actualizaciones de imágenes en el mes de abril del presente año (2021).

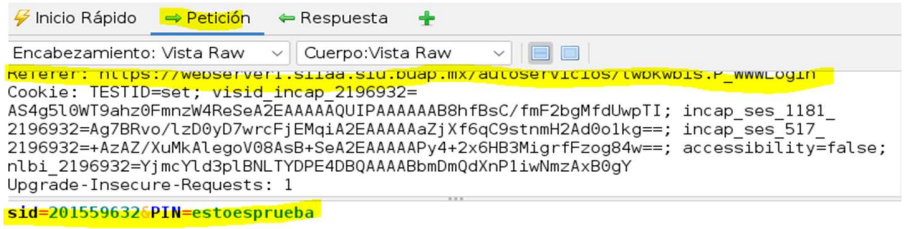
En la imagen podemos notar las peticiones que hemos hecho al servidor, en este caso son las credenciales para poder acceder al sitio web dónde en cada cabecera introducimos un ID y una contraseña.



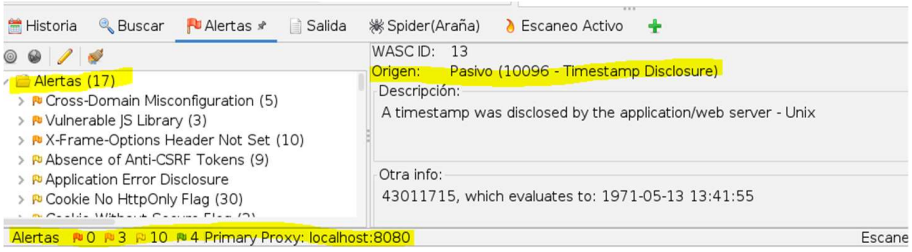
Posteriormente en nuestra herramienta notamos la petición que hicimos al servidor la cual nos permitirá ver qué credenciales introducimos para poder acceder al sitio web.



Notamos que el **ID** fue una serie de números y la **credencial** que se escribe de manera protegida para la vista de los internautas nos la muestra dentro de esta petición al servidor, lo cual nos podría servir para poder robar datos de los usuarios que pudiesen ocupar una PC con esta herramienta y esta configuración habilitada.



A su vez pudimos encontrar 17 vulnerabilidades en el sitio que lo hacen comprometedor para ataques de ingeniería inversa o simplemente explotando cada debilidad un atacante pueda en un tiempo determinado conseguir un acceso al servidor que contiene la información de este sitio web.



CONCLUSIONES: El propósito de esta herramienta es ayudar a los profesionales, investigadores o diferentes usuarios a comprender el por qué, cuándo, dónde, contra fallos en ataques de sitios o aplicaciones web. Mediante procesos los cuales conforman un conjunto de pruebas que utilizan esta información para determinar una solución a los problemas que surjan durante una investigación en específico. Ha sido mayormente utilizada para evaluar pruebas de seguridad de redes, a estas se les puede llamar de caja negra o hacking ético. A su vez en estas pruebas de seguridad en sitios web se ocupan métodos que evalúan el nivel de seguridad de diferentes sistemas (software o red), que se encargan de verificar la efectividad y seguridad de diferentes sitios.

Cabe resaltar que ningún curso, diplomado, bibliografía o algún otro material de capacitación puede determinar todos los inconvenientes que puedan surgir en una investigación de ciberseguridad, por lo cual pueden aparecer diferentes pruebas con diferentes escenarios para llegar a un objetivo en específico y destacar que fue lo que ocurrió dentro de una investigación.

BIBLIOGRAFIA:

B. Astudillo, Karina. Hacking Ético 101: Cómo Hackear Profesionalmente en 21 días o menos!. (PP 300); CreateSpace Independent Publishing Platform, 2da Edición (2016).

Caballero Quezada, Alonso Eduardo. (Enero 30, 2020). Webinar Gratuito: Escanear Vulnerabilidades Web con Zed Attack Proxy. 06 Agosto 2021, de ReYDeS. Recuperado de: https://www.reydes.com/d/?q=videos_2020

Apéndice C

CÓMPUTO FORENSE BAJO LINUX

"HERRAMIENTAS DE CÓMPUTO FORENSE"

INTRODUCCIÓN

Estas herramientas son elementos que pertenecen al sistema operativo de Kali-Linux. Se emplean mediante una máquina virtual dentro de nuestra PC las cuales vamos a utilizar y ver qué es lo que nos ofrecen.

Mostraremos breves imágenes describiendo algunas de las funciones que tienen estas herramientas para poderlas comparar con los diferentes sistemas que nos ayudan a realizar el cómputo forense.

OBJETIVO:

Analizar el entorno de las herramientas y su debido proceso de utilidad, siguiendo los estándares para verificar su funcionamiento.

MATERIALES:

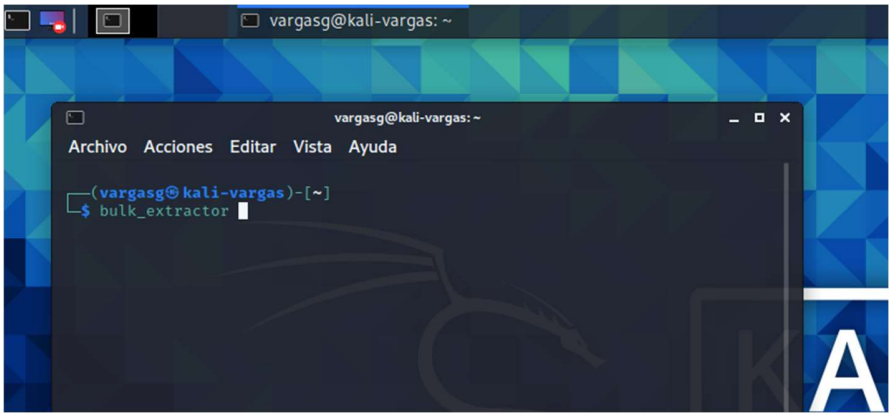
Pc personal.
Máquina virtual con S.O Kali Linux.
Conexión a internet.

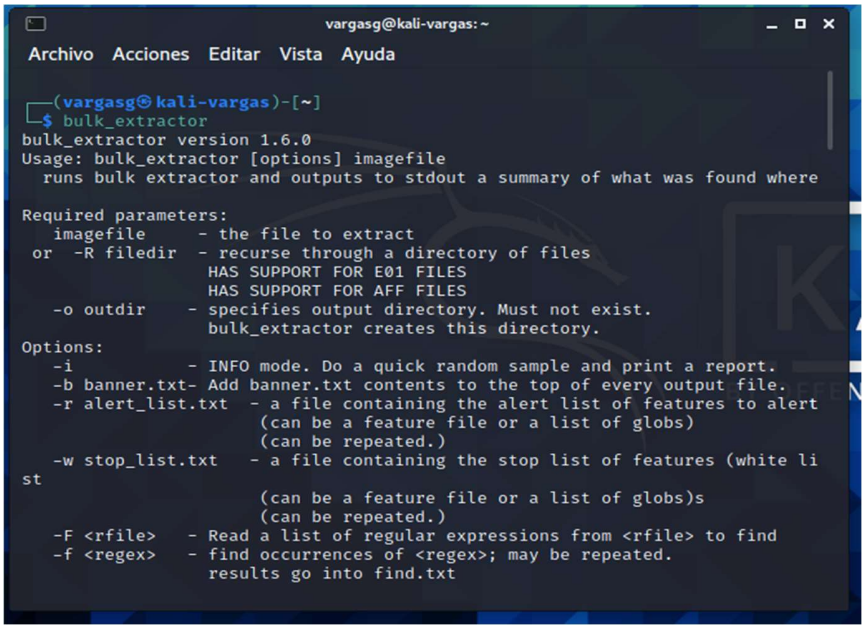
METODOLOGÍA

EJEMPLO DE DESCRIPCIÓN DE LA HERRAMIENTA BULK EXTRACTOR.

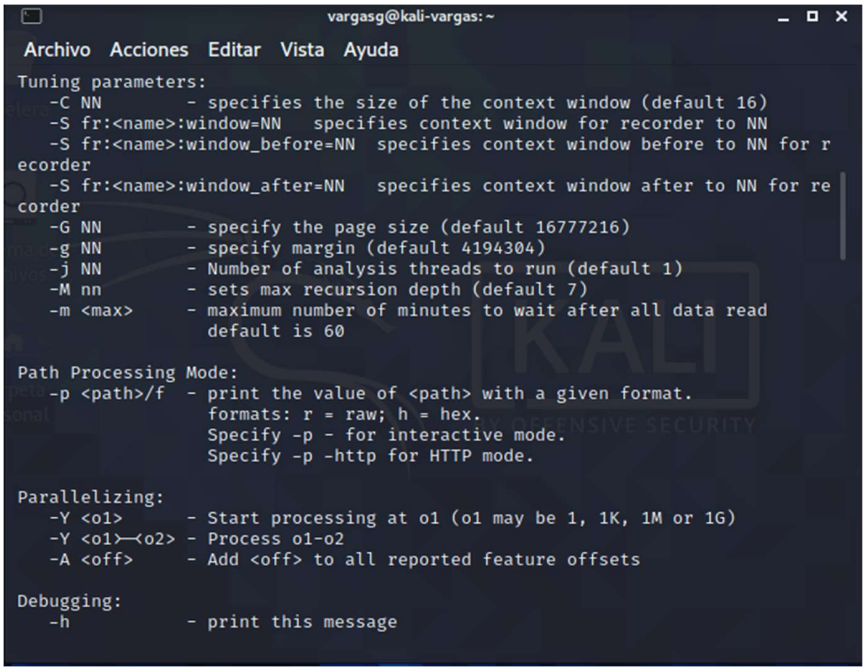
1.Iniciaremos nuestra máquina virtual y accederemos a nuestro sistema operativo Kali-Linux.

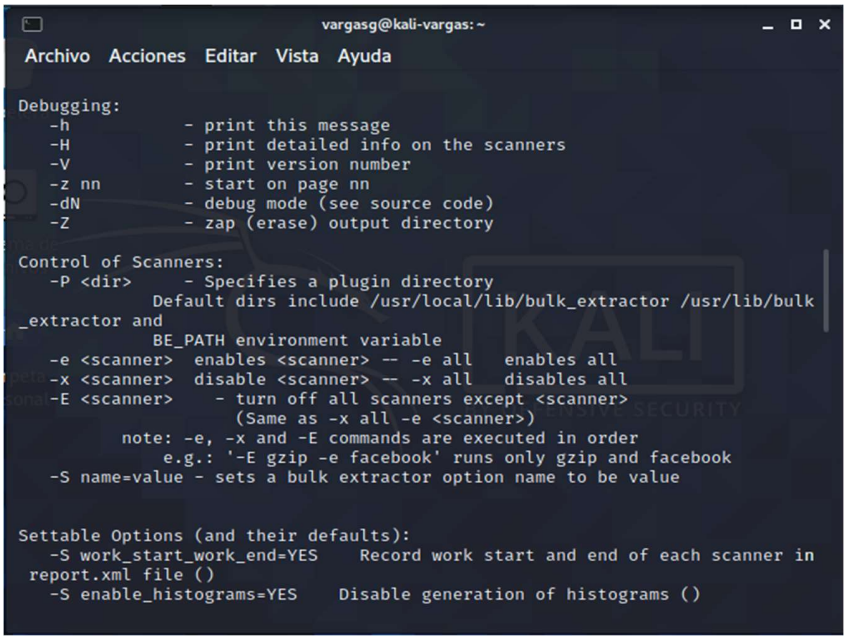
2. Una vez iniciada nuestra sesión, procederemos a abrir una terminal dentro de nuestro S.O Kali, para inicializar nuestra herramienta.

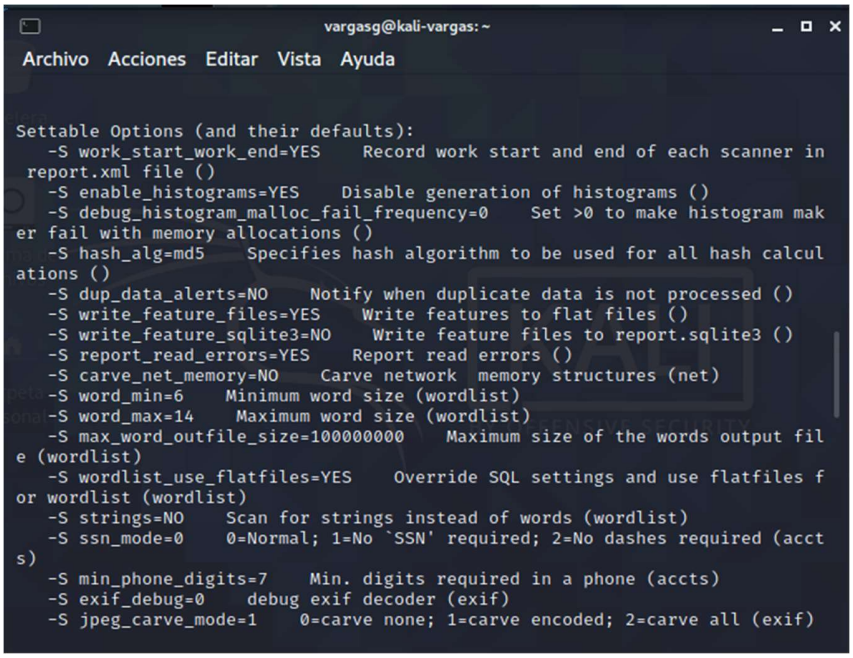




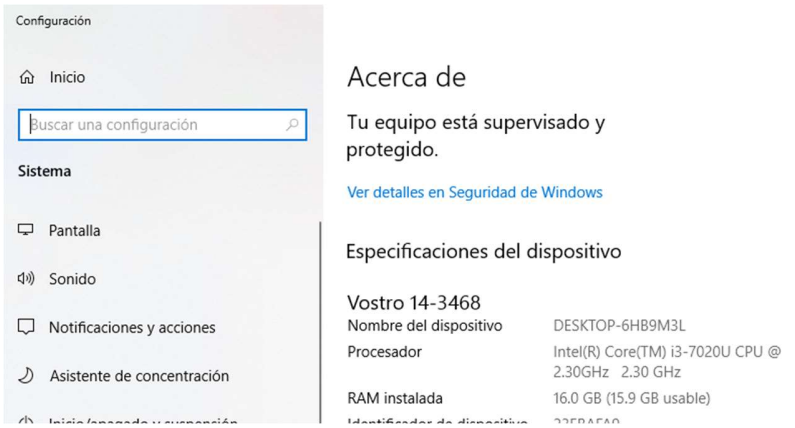
3. Una vez ejecutado el comando en la terminal señalando el nombre de la herramienta como en la imagen anterior, podremos visualizar las diferentes opciones de análisis de memoria RAM, como: **características de archivos, parámetros de afinamiento, paralelismo, control de escáner y otros ajustes que nos ofrece esta.**

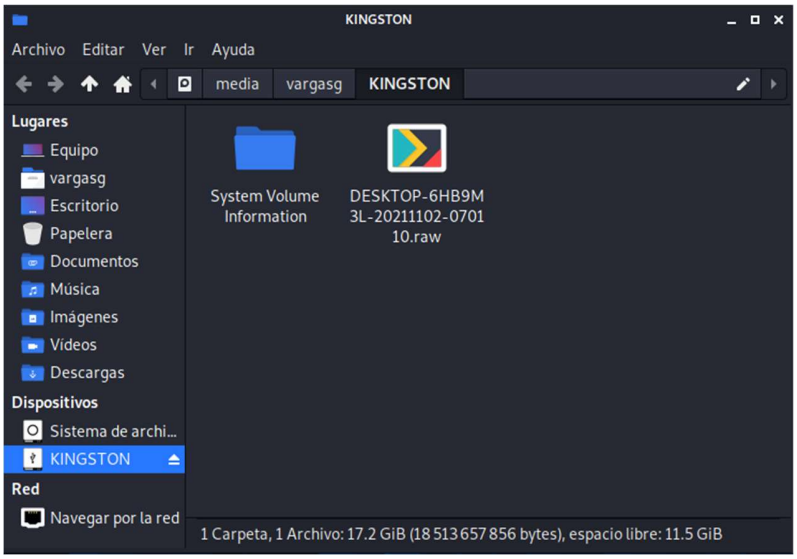






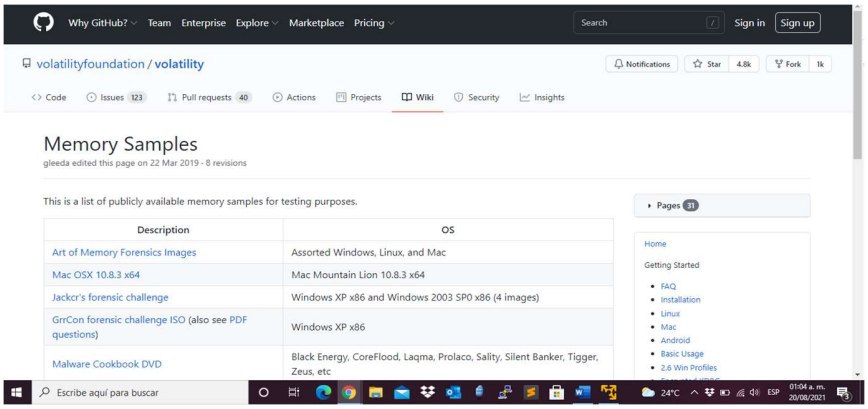
Para comenzar a trabajar en nuestro análisis de memoria RAM necesitaremos un archivo de volcado de memoria la cual podemos llamar una “imagen forense” de memoria RAM de alguna computadora, en este caso ocuparemos en un **archivo de volcado de memoria** de nuestra computadora física y otro archivo de volcado de memoria que nos ofrecen un repositorio de investigación para hacer realizar estas prácticas de estudio.

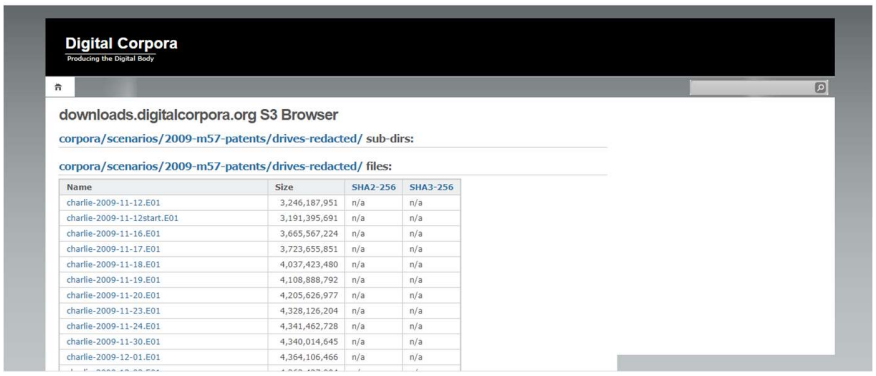




También hay algunos archivos que existen como apoyo académico e investigación simple, que nos brindan diferentes sitios, como de volatility aportando diferentes archivos de volcados de memoria para realizar pruebas de cómputo forense, las podremos encontrar en los siguientes enlaces:

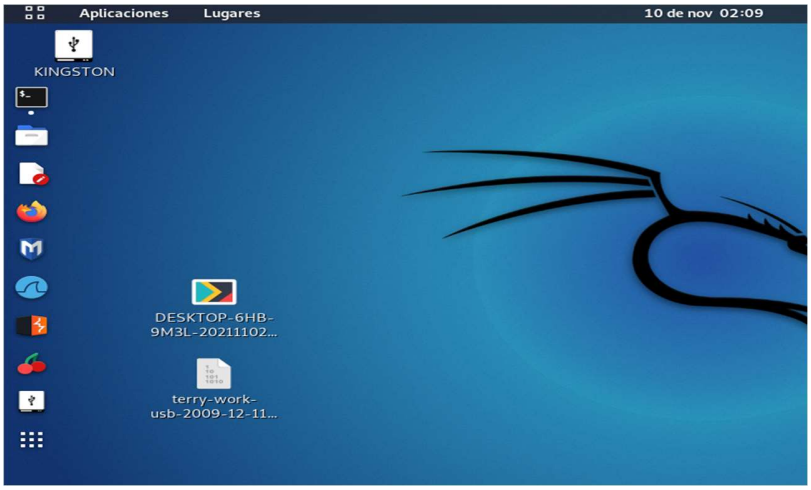
- https://github.com/volatilityfoundation/volatility/wiki/Memory-Samples
- https://downloads.digitalcorpora.org/corpora/scenarios/2009-m57-patents/drives-redacted/



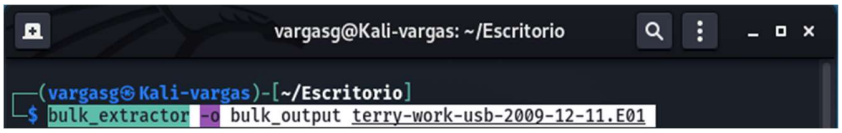


4. Una vez tengamos nuestro archivo de volcado de memoria podremos realizar una investigación exhaustiva de la información que contenga, esto lo haremos en una terminal de nuestra máquina virtual kali-linux. Para posteriormente indagar en el archivo la información que contiene y comprender la eficiencia e importancia que ofrece esta herramienta.

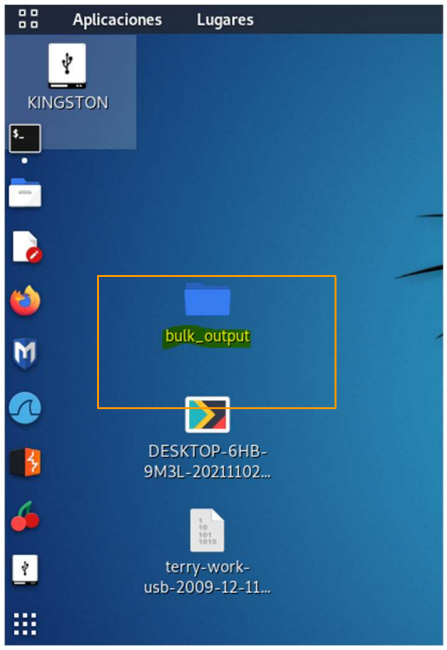
Primero deberemos ubicarnos en nuestro directorio de escritorio, donde estarán ubicados los archivos de volcado de memoria. Eso lo haremos en nuestra terminal con el comando **cd /home/vargasg/Escritorio.**



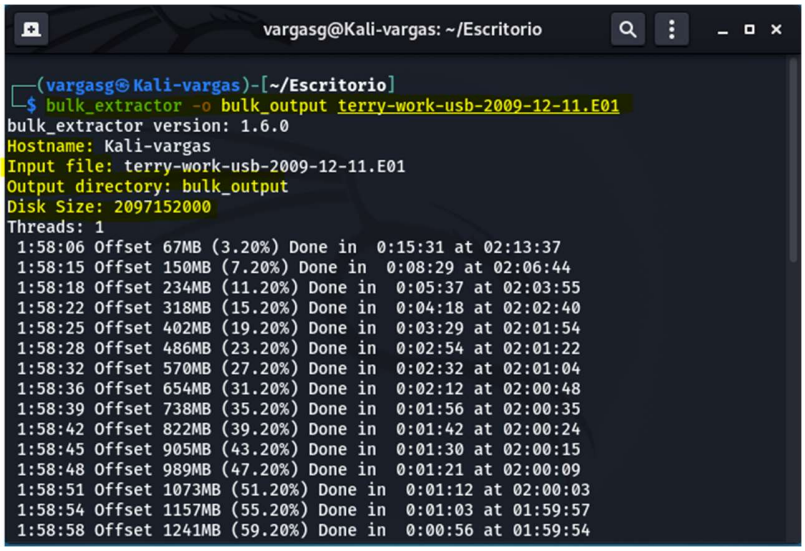
Posteriormente crearemos una carpeta de salida donde se almacenará la información de extracción de la información del archivo de volcado de memoria. Con la instrucción en la terminal **bulk_extractor -o bulk_output terry-work-usb-2009-12-11.E01.**



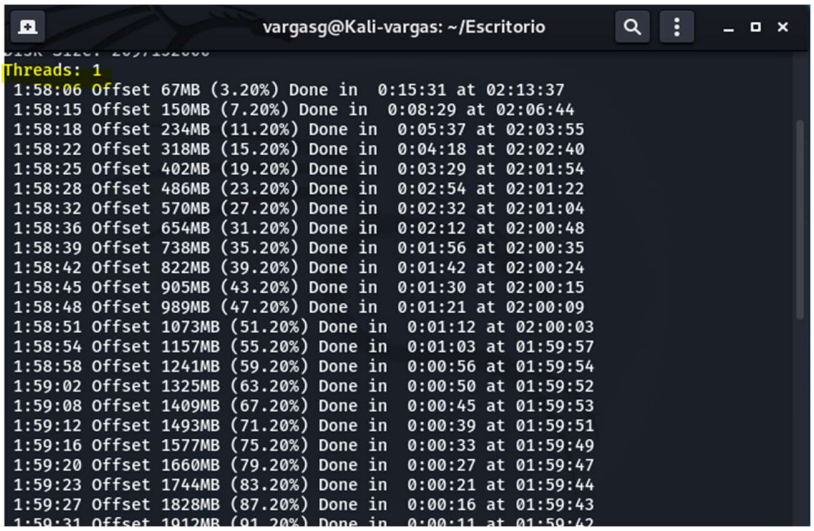
La cual contendrá información de la extracción del archivo de volcado de memoria RAM que estamos analizando.



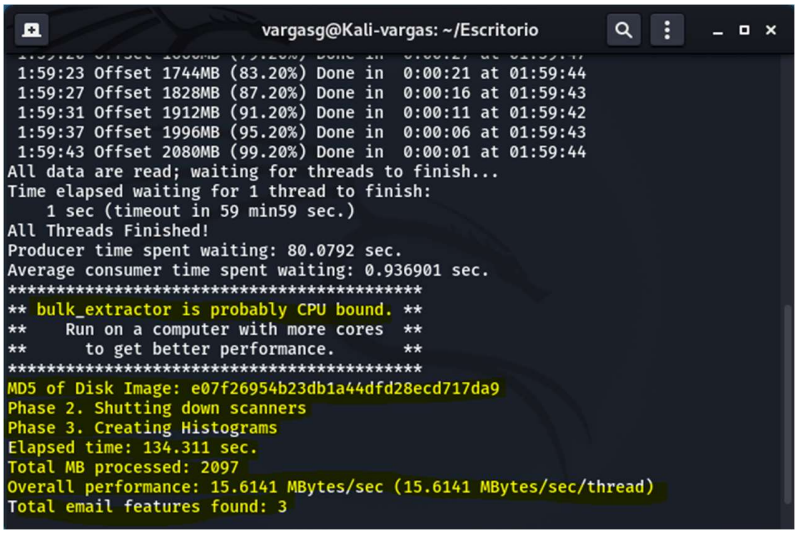
5. Una vez ejecutado el comando en nuestra terminal, la herramienta 'BULK-EXTRACTOR' comenzará con la extracción de la información donde nos arrojará: **nombre de la máquina, nombre del archivo que se está analizando, el directorio de salida donde se almacena la información y su tamaño.**



Dependerá del tamaño del archivo de volcado de memoria y de nuestra memoria RAM el tiempo de extracción de la información, ya que los procesos de extracción deben ser minuciosos. En nuestra prueba estaremos utilizando el tamaño de la memoria RAM que tiene nuestra máquina virtual que es de 4GB.

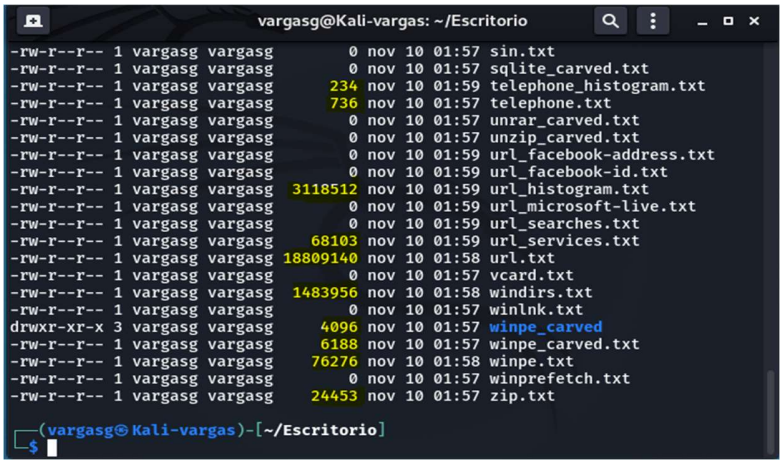


6. Posteriormente visualizaremos la recolección de resultados. **La extracción de clave AES del archivo de volcado de memoria, escaneo de archivos, creación de los histogramas, tiempo de análisis, total de MB procesados, rendimiento global de Mbytes/sec y el total de correos electrónicos encontrados.**

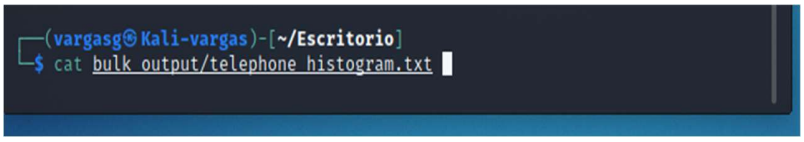


7. A continuación visualizamos la recolección de la información que se generó en nuestra carpeta de salida **"bulk_output" ubicada en el escritorio de nuestro sistema.** Con el comando **ls -l bulk_output.**

En estas imágenes observamos más de un total de **30,600 datos que están almacenados en archivos.txt,** donde encontramos información confidencial, indagando en cada uno de los archivos podemos saber ver qué información se estuvo utilizando en la memoria RAM de esa computadora.



8. De igual manera podemos indicar con el comando: **cat bulk_output/telephone_histogram.txt** o el nombre de cada archivo.txt dentro de la terminal para hacer un análisis de los datos que se ocuparon o modificaron dentro de esa computadora.

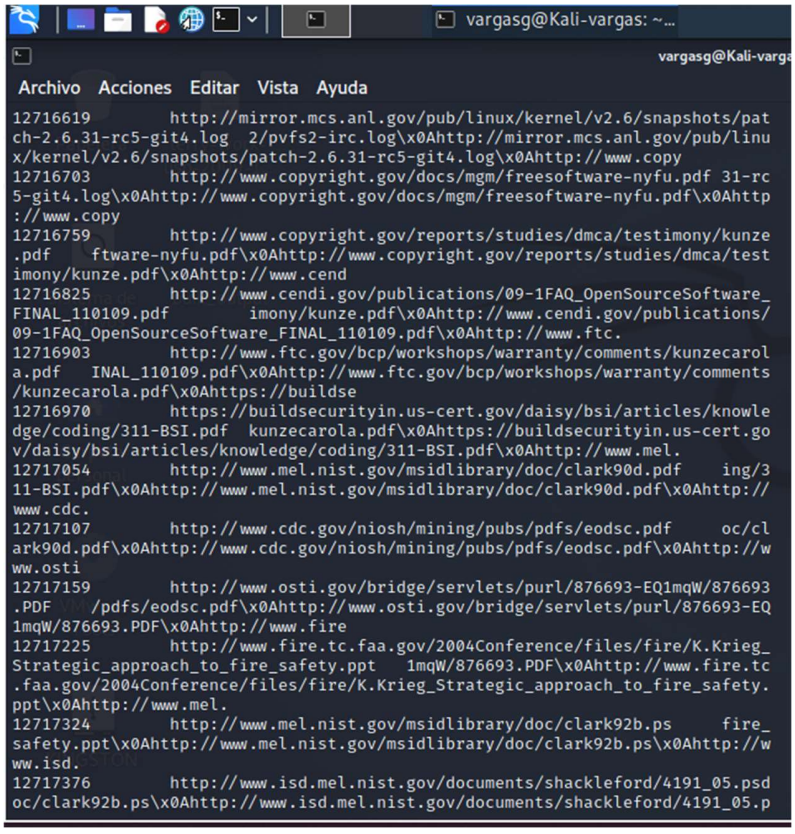


En la siguiente imagen visualizamos los teléfonos almacenados que contenía esta imagen de volcado de memoria.

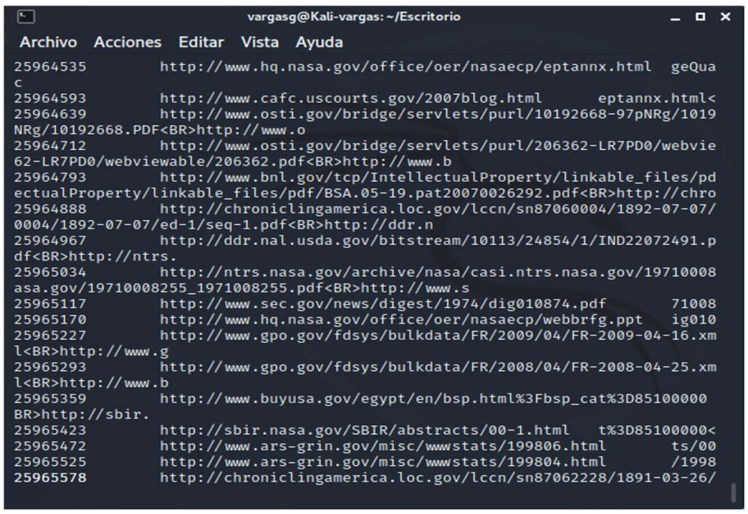
En las siguientes imágenes visualizaremos la información de distintos archivos en específico, conteniendo información confidencial de la imagen de la memoria RAM analizada.

- Información de sitios web visitados

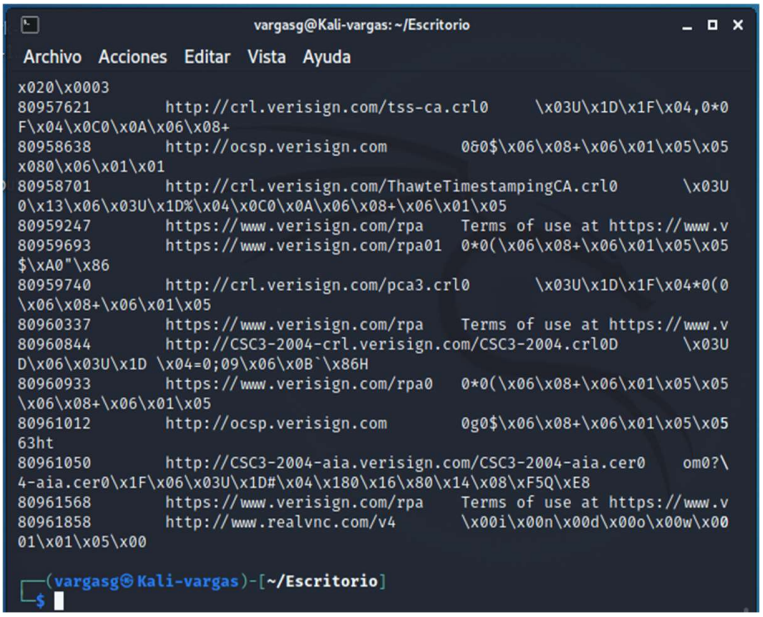
- Sitios web dentro del archivo **url.txt**



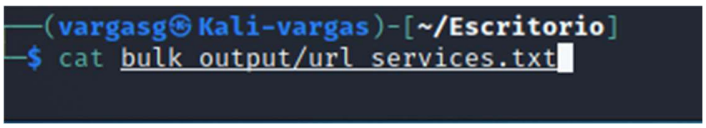
- Sitios web dentro del archivo **url.txt**



- Sitios web dentro del archivo **url.txt**



- En la siguiente imagen podemos notar las peticiones que realizó a diferentes servidores.

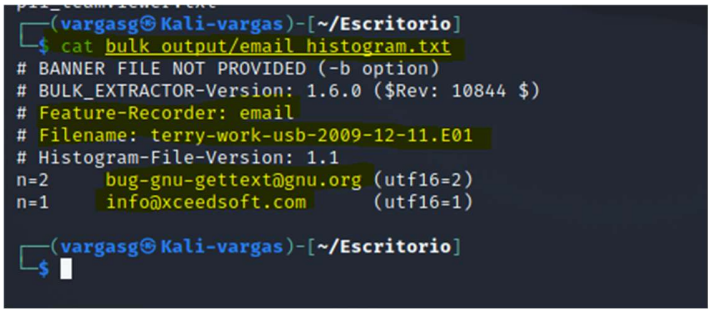


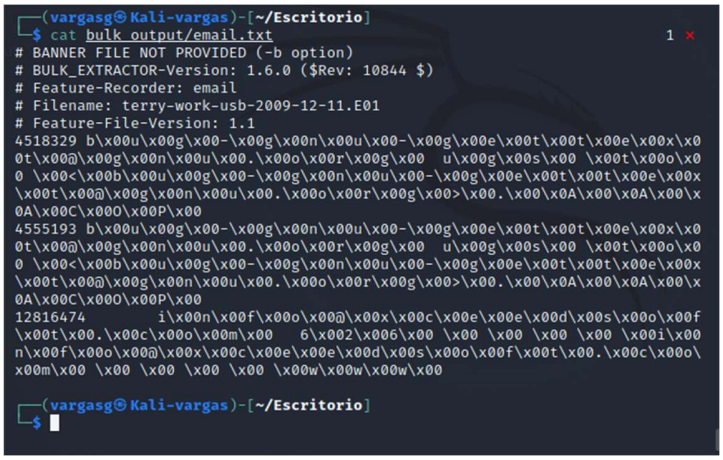
- Acceso a diferentes sitios web

```
n=1     www.sbmtd.gov
n=1     www.sdd.uscourts.gov
n=1     www.sensornet.gov
n=1     www.sestak.house.gov
n=1     www.sidney.ars.usda.gov
n=1     www.slashdot.org
n=1     www.solids.bnl.gov
n=1     www.sos.wv.gov
n=1     www.southbendin.gov
n=1     www.srmt-nsn.gov
n=1     www.srpmic-nsn.gov
n=1     www.sshs.samhsa.gov
n=1     www.ssi.nrcs.usda.gov
n=1     www.st.nmfs.noaa.gov
n=1     www.star.nesdis.noaa.gov
n=1     www.stateuse.wv.gov
n=1     www.steelers.com
n=1     www.stlucieco.gov
n=1     www.stocktonca.gov
n=1     www.stonington-ct.gov
n=1     www.sullivancountynh.gov
n=1     www.sumtersc.gov
n=1     www.surgeongeneral.gov
n=1     www.swpc.noaa.gov
n=1     www.t4.lanl.gov
n=1     www.tf.nist.gov
n=1     www.thinkingtelescopes.lanl.gov
```

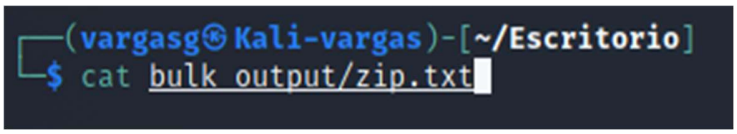
```
vargasg@Kali-vargas: ~/Escritorio
Archivo  Acciones  Editar  Vista  Ayuda
n=67    dtd.nlm.nih.gov
n=67    www.cendi.gov
n=67    www.fms.treas.gov
n=67    www.usatradeonline.gov
n=66    search.loc.gov:8765
n=66    www.emc.ncep.noaa.gov
n=66    www.senate.gov
n=65    rs6.loc.gov
n=65    rsb.info.nih.gov
n=64    hongkong.usconsulate.gov
n=64    www.nws.noaa.gov
n=62    docdb.fnal.gov
n=62    rulings.cbp.gov
n=62    www.fema.gov
n=61    tsapps.nist.gov
n=61    www.bioethics.gov
n=61    www.eric.ed.gov
n=60    vision.arc.nasa.gov
n=60    www.disasterhousing.gov
n=60    www.epm.ornl.gov
n=60    www.usgs.gov
n=60    www3.cancer.gov
n=59    geo.arc.nasa.gov
n=59    sti.srs.gov
n=59    www.ncs.gov
n=58    bxa.ntis.gov
n=58    jazz.nist.gov
```

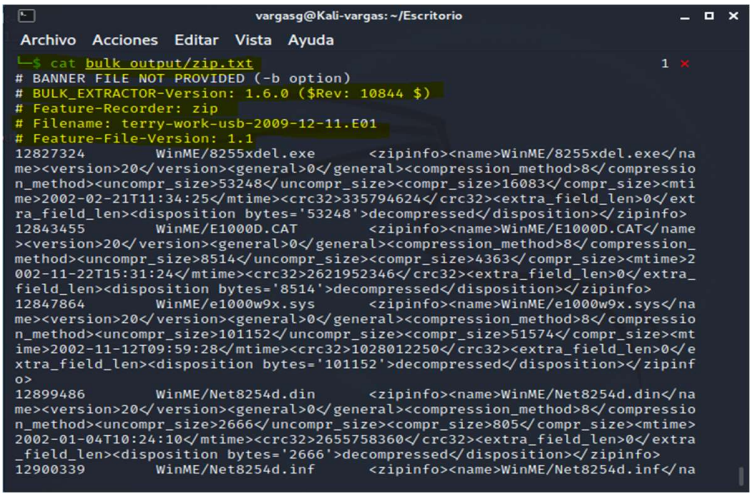
- Emails ocupados en la computadora alojados en el archivo de volcado de memoria RAM

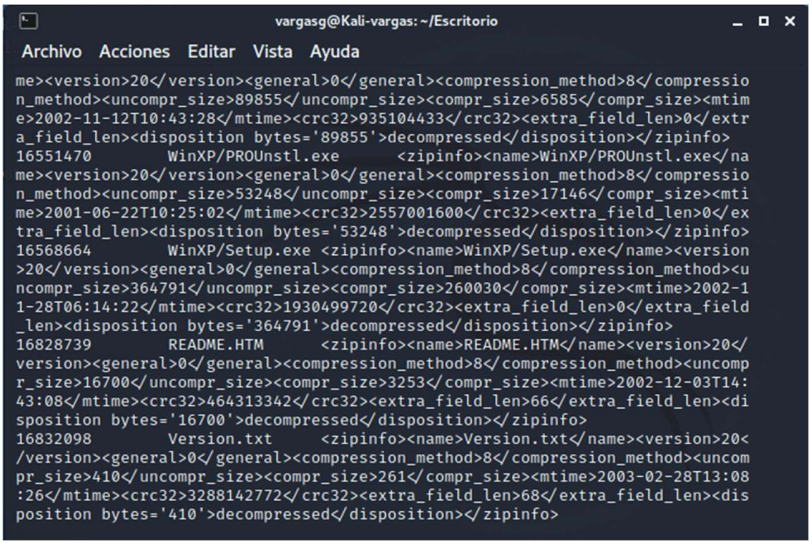


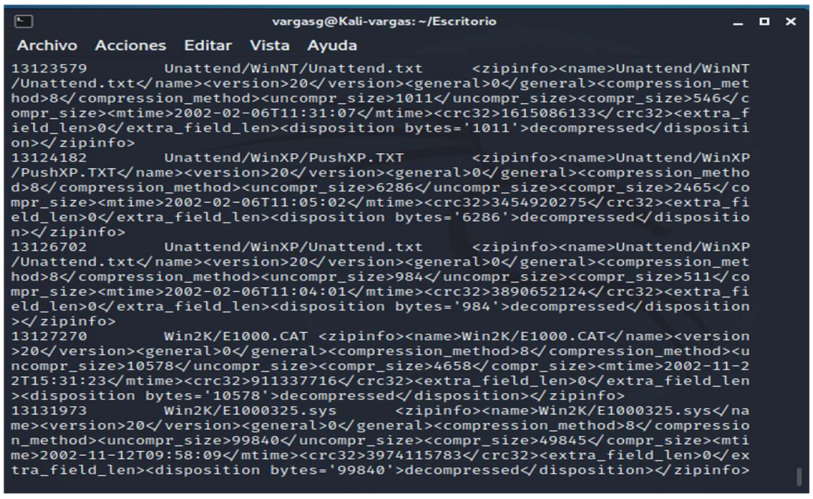


En la siguiente imagen podemos notar los archivos .zip que contiene la imagen de volcado de la memoria RAM.





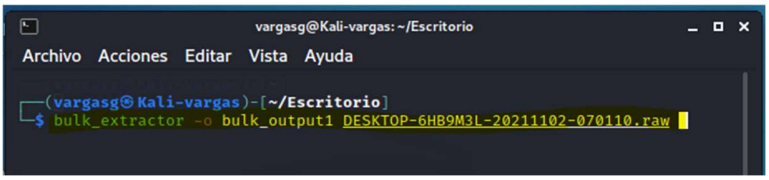




A su vez podemos indagar y encontrar diferentes vulnerabilidades dentro de los **archivos.txt** comprometiendo los datos de la computadora donde se obtuvo el archivo de volcado de memoria. Este tipo de técnicas se ocupan para ataques de ingeniería inversa, “cold boot attack”, para que simplemente en un ciberataque encuentren datos que conlleven a una debilidad y el atacante pueda en un tiempo determinado conseguir un acceso a diferente información que contiene una computadora en específico.

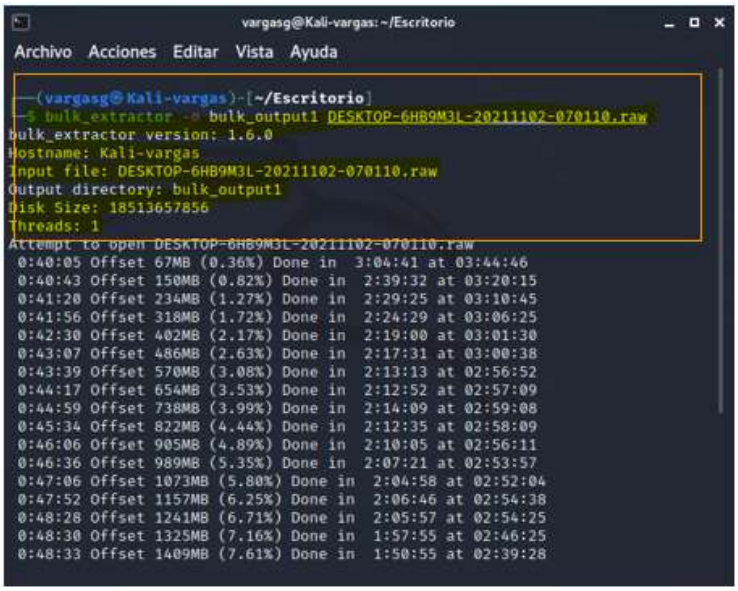
En una investigación de cómputo forense esta herramienta es muy importante ya que nos permite analizar una imagen de volcado de memoria completa, dañada o incompleta, para analizar la información de una computadora en específico sabiendo qué información utilizó el usuario que le pertenecía el dispositivo y deducir qué intención tenía o si realizó uno o más ciberataques a diferentes usuarios que navegan en la web.

9. **Segundo análisis:** directorio de salida donde almacenará el análisis del archivo de volcado de memoria RAM de **nuestra máquina física.**

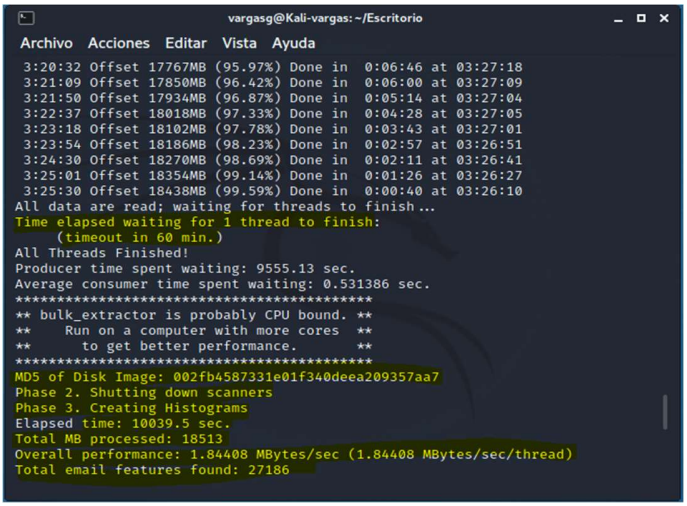


- Directorio donde se almacenarán los datos del análisis de memoria.

- Extracción de la información donde nos arrojará después del escaneo de archivos el: **nombre de la máquina, nombre del archivo que se está analizando, el directorio de salida donde se almacena la información y su tamaño.**

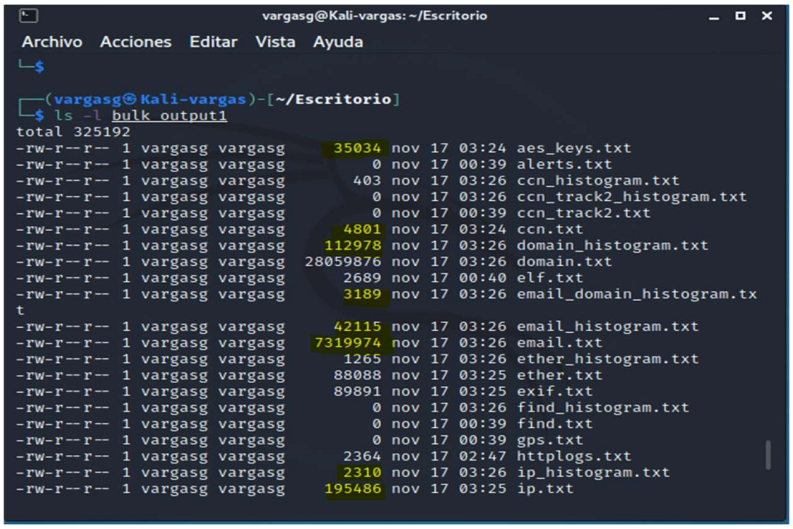


- Extracción de clave AES del archivo de volcado de memoria RAM, escaneo de información digital, creación de los histogramas, tiempo de análisis, total de MB procesados, rendimiento global de Mbytes/sec y el total de correos electrónicos encontrados.



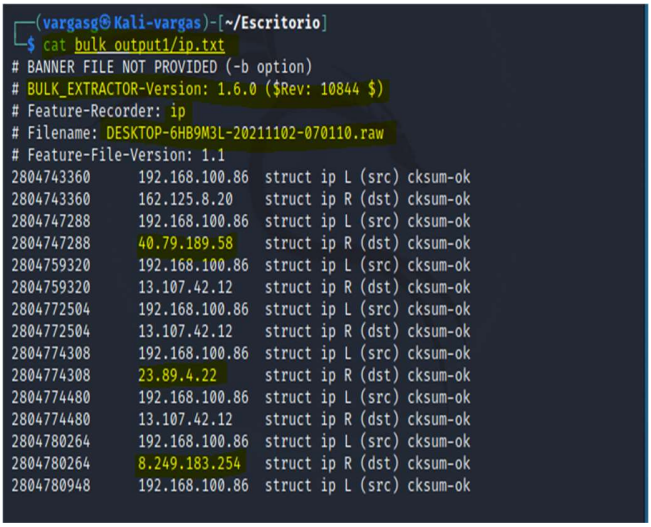
A continuación, visualizamos la recolección de la información que se generó en nuestra carpeta de salida **"bulk_output1" ubicada en el escritorio de nuestro sistema.** Con el comando **ls -l bulk_output1.**

- Podemos visualizar la cantidad de datos con los que cuenta nuestro archivo de volcado de memoria de nuestra memoria RAM física. Esto se puede realizar dentro de una investigación de cómputo forense y sería muy efectivo para analizar la diferente información recolectada.



Con el comando: **cat bulk_output1/ip.txt** o diferente archivo.txt dentro de la terminal podremos hacer un análisis de los datos que se ocuparon o modificaron dentro de esa computadora.

- En la siguiente imagen visualizamos las direcciones IP que se visitaron en la máquina física, solo basto analizar el archivo de volcado de memoria de esa máquina para saber qué direcciones ha visitado.



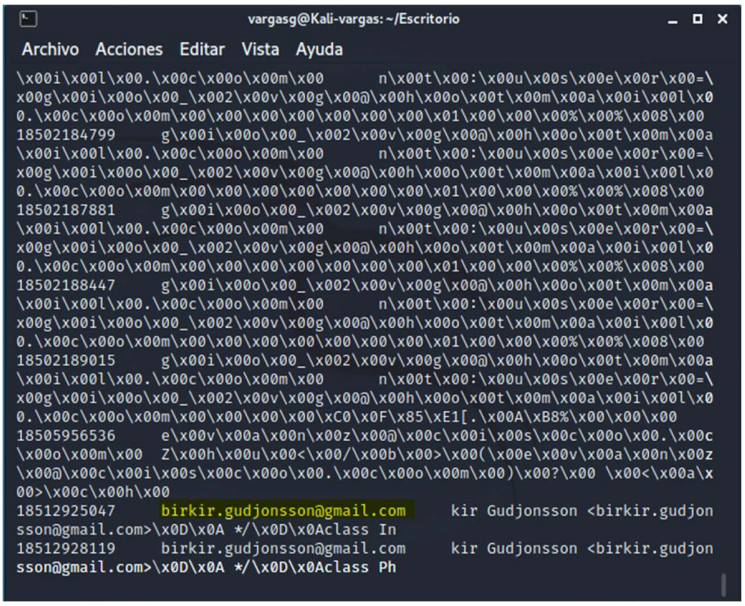
```
┌──(vargasg㉿Kali-vargas)-[~/Escritorio]
└─$ cat bulk_output1/ip.txt
# BANNER FILE NOT PROVIDED (-b option)
# BULK_EXTRACTOR-Version: 1.6.0 ($Rev: 10844 $)
# Feature-Recorder: ip
# Filename: DESKTOP-6HB9M3L-20211102-070110.raw
# Feature-File-Version: 1.1
2804743360      192.168.100.86  struct ip L (src) cksum-ok
2804743360      162.125.8.20    struct ip R (dst) cksum-ok
2804747288      192.168.100.86  struct ip L (src) cksum-ok
2804747288      40.79.189.58    struct ip R (dst) cksum-ok
2804759320      192.168.100.86  struct ip L (src) cksum-ok
2804759320      13.107.42.12    struct ip R (dst) cksum-ok
2804772504      192.168.100.86  struct ip L (src) cksum-ok
2804772504      13.107.42.12    struct ip R (dst) cksum-ok
2804774308      192.168.100.86  struct ip L (src) cksum-ok
2804774308      23.89.4.22      struct ip R (dst) cksum-ok
2804774480      192.168.100.86  struct ip L (src) cksum-ok
2804774480      13.107.42.12    struct ip R (dst) cksum-ok
2804780264      192.168.100.86  struct ip L (src) cksum-ok
2804780264      8.249.183.254   struct ip R (dst) cksum-ok
2804780948      192.168.100.86  struct ip L (src) cksum-ok
```

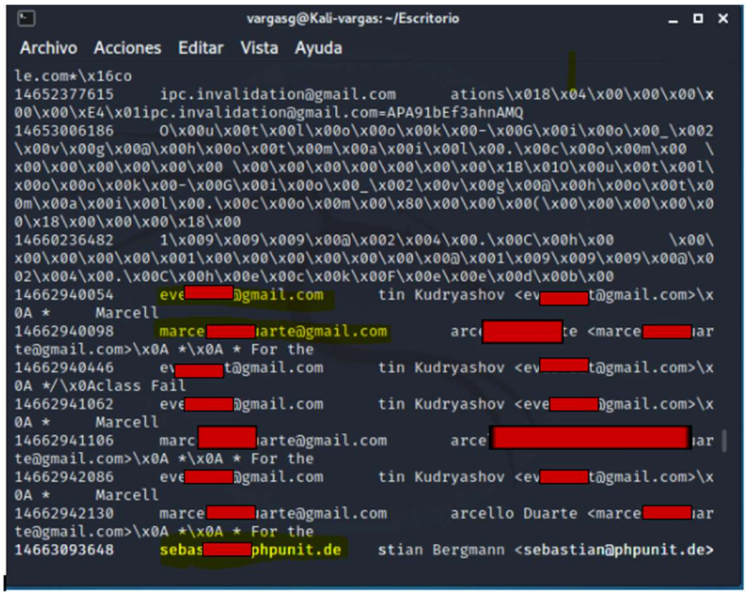
- En la siguiente imagen podemos notar los teléfonos almacenados encontrados durante la extracción de la información.

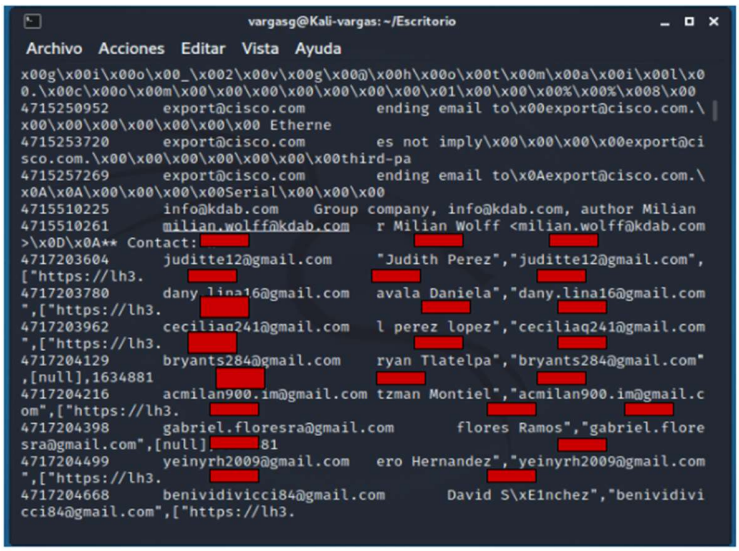
```
┌──(vargasg㉿Kali-vargas)-[~/Escritorio]
└─$ cat bulk_output1/telephone.txt
# BANNER FILE NOT PROVIDED (-b option)
# BULK_EXTRACTOR-Version: 1.6.0 ($Rev: 10844 $)
# Feature-Recorder: telephone
# Filename: DESKTOP-6HB9M3L-20211102-070110.raw
# Feature-File-Version: 1.1
881014221-PDF-1073      05000021558     n8(5selar 5n--\x0D\x0A05000021558 5 E
5l.l9T.5[(.7
1103413806      (999) 999-9999  rol" data-mask="(999) 999-9999" placeholder="
"
1103413911      (999) 999-9999  ss="help-block">(999) 999-9999</span>\x0A

1153600601-PDF-23763    0320455606444   650o4 B_1036434 0320455606444a651c04o
4 B_1036
1153600601-PDF-23796    0320455606444   c04o4 B_1036434 0320455606444a651c04o
4 B_1036
1153600601-PDF-23829    032045560847444 c04o4 B_1036434 0320455608474444a651c0
4147350536
1154976569-PDF-18847    03450635067     674103406341  3 03450635067l6l6.76Z7l
6 4103
```

```
vargasg@Kali-vargas: ~/Escritorio
Archivo  Acciones  Editar  Vista  Ayuda
4388151296-ZIP-120157   01211471111     41111131FCDF311 01211471111V4.2111113
111131
4450155676      01234567808     \x08\x00\x08\x00\x00\x139\x02abcdef\x09\x0A01
234567808x\xFF\x1E\x00\x00\x00\x00\xFF?\x00\x00\x00\x00\xBB\x01\x00
4496088622      252.227-7013    e at DFARS sec. 252.227-7013.\x00\x00\x00\x00
\x00
4496092438      252.227-7013    e at DFARS sec. 252.227-7013.\x00\x00\x00\x00
\x00
4496094900      252.227-7013    e at DFARS sec. 252.227-7013.\x0A\x0A
   ci
4481717925-PDF-1208     Tel: 5583231064         de Lenguas BUAP Tel: 55832310
64 alma.sanchezlina
4568339164      mobile          padding-top-8x-mobile       ">\x0A\x0A    \x
0A    \x0A
4568340259      mobile          padding-top-0x-mobile       ">\x0A\x0A    \x
0A    \x0A
4629138516      252.227-7013    e at DFARS sec. 252.227-7013.\x0A\x0A
   ci
4629144899      252.227-7013    e at DFARS sec. 252.227-7013.\x0A          c
is
4629165860      252.227-7013    e at DFARS sec. 252.227-7013.\x0A\x0A
   ci
4715252934      252.227-7013    e at DFARS sec. 252.227-7013.\x00\x00\x00\x00
\x00
4715256100      252.227-7013    e at DFARS sec. 252.227-7013.\x0A\x0A
   ci
4763624192      Fax                     ──────────┤\x0D\x0A├ Fax
```

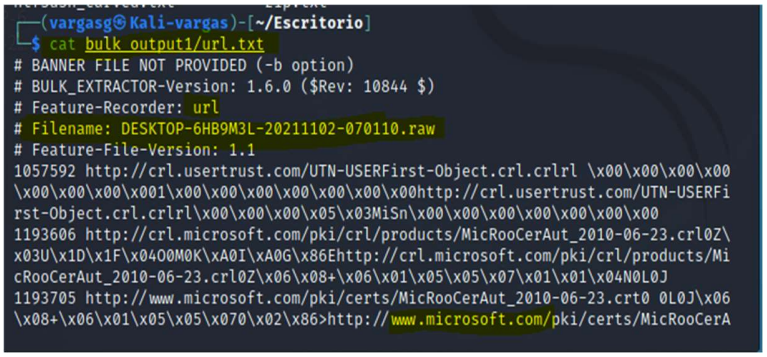
- Emails ocupados en la computadora alojados en el archivo de volcado de memoria RAM

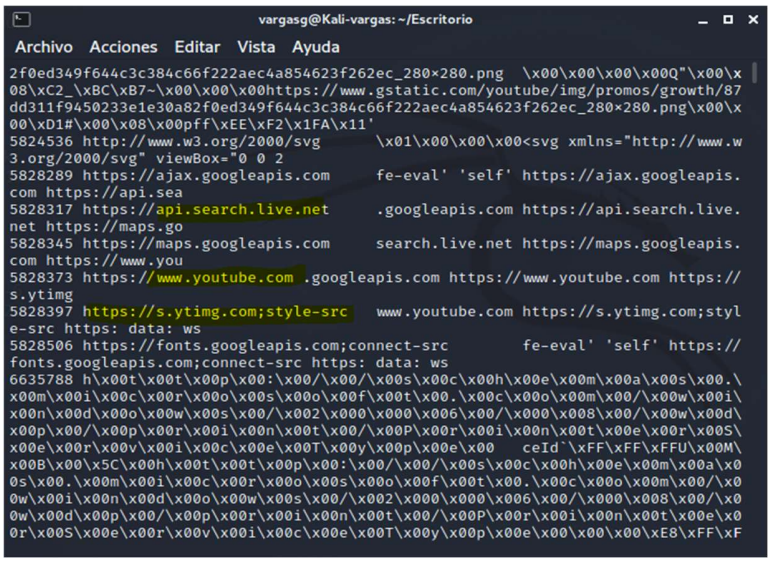


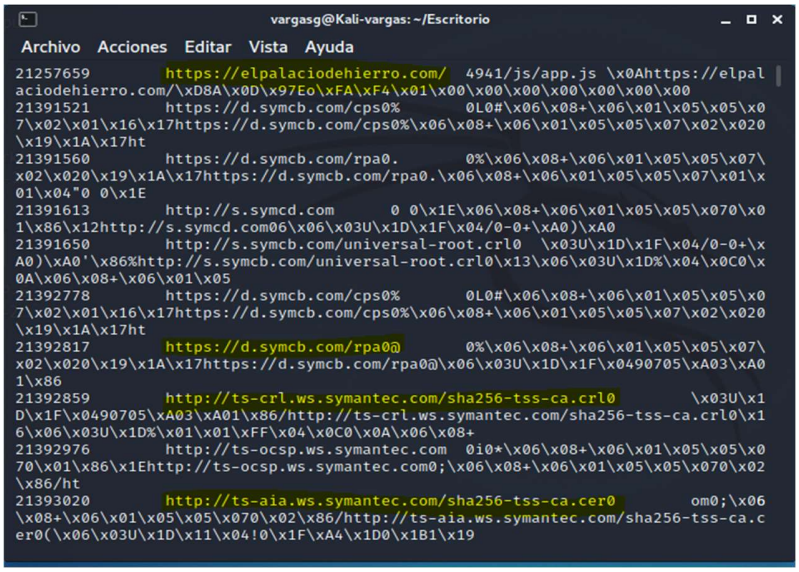


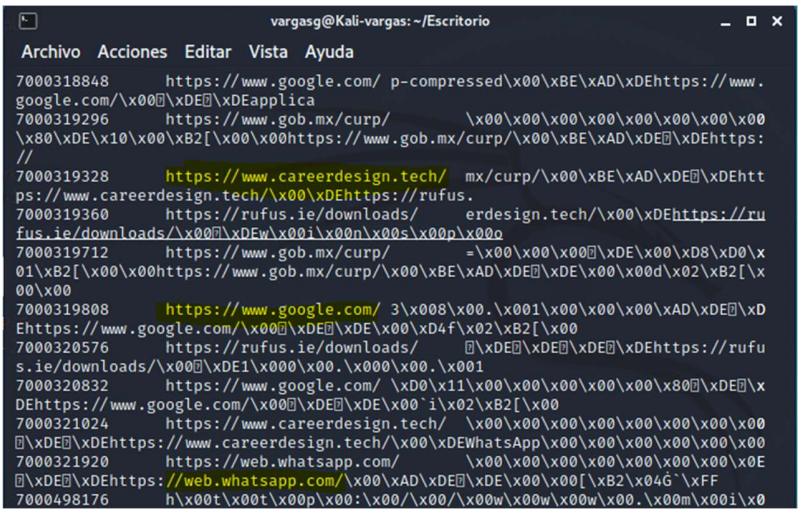


- Acceso a diferentes sitios web

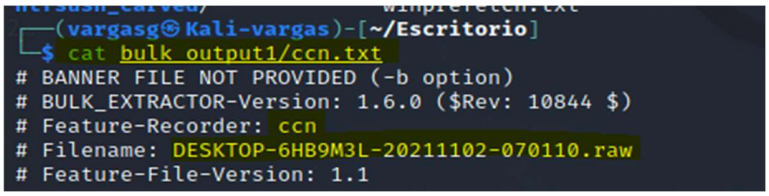


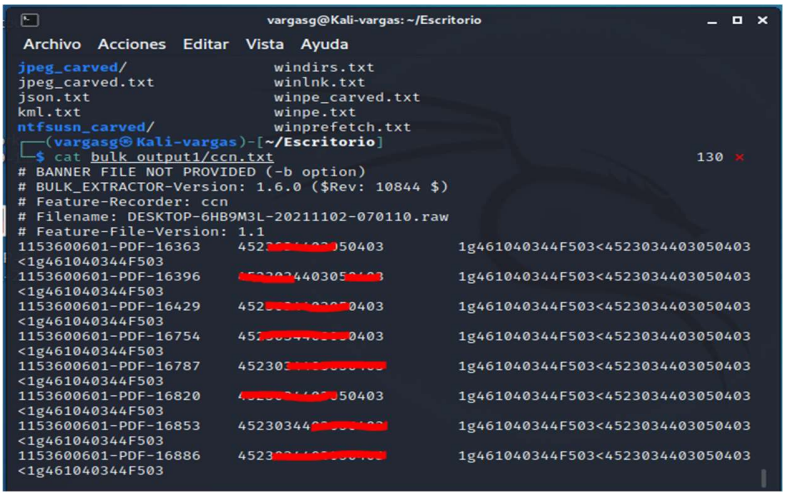


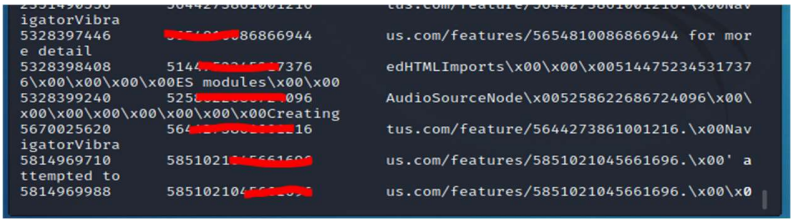




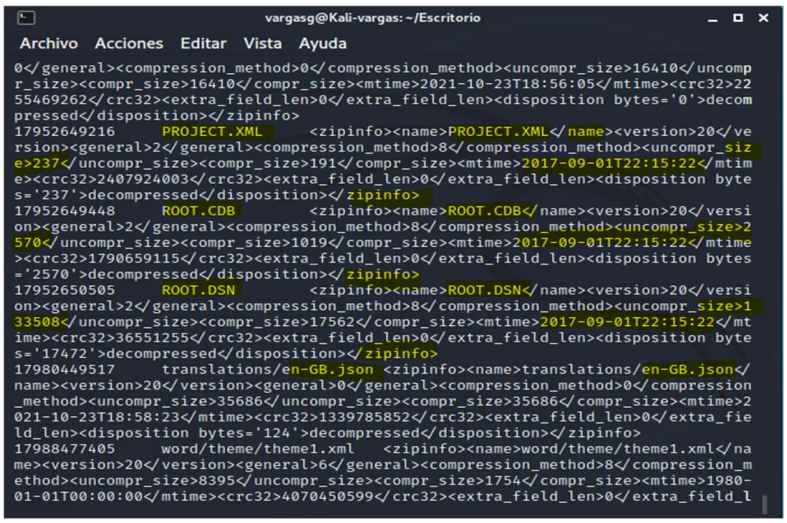
- Números de tarjetas bancarias almacenadas en el archivo de volcado de memoria de la máquina física.



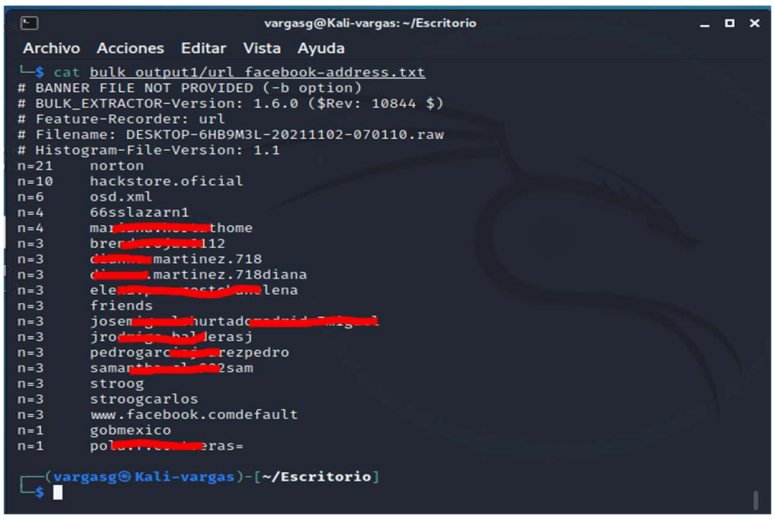




- Nombre de archivos .ZIP almacenadas en el archivo de volcado de memoria de la máquina física. Donde podemos visualizar el nombre del archivo, fecha del archivo y su tamaño.



- URL´S de Facebook almacenadas en el archivo de volcado de memoria de la máquina física. Donde podemos visualizar el nombre de los perfiles visitados por el usuario quien manipuló la máquina física.



CONCLUSIONES: El objetivo de probar esta herramienta es ayudar a los profesionales, investigadores o diferentes usuarios a comprender la recolección de diferentes datos (información) que podemos encontrar en una computadora en específico. Esta nos permite analizar archivos de volcado de memoria donde podemos indagar qué información se utilizó para posteriormente determinar las actividades de una persona que trató de dar mal uso a diferentes dispositivos, llamando a esto ciberataques que se pueden resolver con el cómputo forense.

Existen diferentes herramientas de software libre para el análisis y recolección de datos, pero podemos decir que BULK-EXTRACTOR es una herramienta muy completa que hace posible la examinación de diferentes tipos de archivos desde su extensión hasta el estado en el que se encuentren, permitiéndonos mejorar los procesos de recolección de evidencias de información digital, que nos sirven para resolver diferentes casos de cómputo forense.

BIBLIOGRAFIA:

Caballero Quezada, Alonso Eduardo. (Febrero 27, 2020). Webinar Gratuito: Analizar una imagen RAM con Bulk Extractor. 16 Noviembre 2021, de ReYDeS. Recuperado de: https://www.reydes.com/d/?q=videos_2020