HALLAZGOS DE VULNERABILIDADES EN LOS SISTEMAS OPERATIVOS Y BASE DE DATOS DE LA EMPRESA ALDIM ACCIONES LOGÍSTICAS EN DISTRIBUCIÓN DE MERCANCÍAS S.A.S.

Ing. DIEGO FERNANDO CADAVID ROMERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

VICERRECTORÍA ACADÉMICA Y DE INVESTIGACIÓN - VIACI

CIENCIAS BASICAS TECNOLOGIA E INGENIERIA

ESPECIALIZACION EN SEGURIDAD INFORMATICA

Guadalajara de Buga

2018

HALLAZGOS DE VULNERABILIDADES EN LOS SISTEMAS OPERATIVOS Y BASE DE DATOS DE LA EMPRESA ALDIM ACCIONES LOGÍSTICAS EN DISTRIBUCIÓN DE MERCANCÍAS S.A.S.

Ing. DIEGO FERNANDO CADAVID ROMERO

Proyecto de grado para optar por el título de Especialista en Seguridad Informática

Ing. Mauricio Ramírez V

Magister en Educación Virtual

Phd(C) Ciencias de la Electrónica

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

VICERRECTORÍA ACADÉMICA Y DE INVESTIGACIÓN - VIACI

CIENCIAS BASICAS TECNOLOGIA E INGENIERIA

ESPECIALIZACION EN SEGURIDAD INFORMATICA

Guadalajara de Buga

2018

Nota de aceptación:

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Guadalajara de Buga, 17 de febrero de 2018

DEDICATORIA

Este trabajo es dedicado a mi familia, por cuanto todo su apoyo en la formación académica fue esencial para sacar adelante mis sueños para un futuro mejor. A mis amigos, y a Dios por darnos la posibilidad de llegar a esta meta.

AGRADECIMIENTOS

Agradezco a los profesores de la Universidad Nacional Abierta y a Distancia – UNAD, quienes fueron guía y apoyo para el desarrollo personal y en la formación académica adquirida a lo largo de este proyecto.

A mi familia, por enseñarme la importancia de la perseverancia en la consecución de nuestros objetivos.

A Ing. Mauricio Ramírez V, director del presente desarrollo quien con su apoyó, guio para direccionar y culminar el trabajo en el que se representa toda nuestra formación.

A la empresa ALDIM, por permitirme poner en pie este proyecto en su organización.

En general a todos los que se vieron involucrados con este trabajo, les agradezco profundamente por su apoyo y compromiso.

CONTENIDO

Pag.

LISTA DE ILUSTRACIONES

Pag.

LISTA DE TABLAS

Pag.

GLOSARIO

PENTESTING: Las pruebas de penetración (también llamadas “pentesting”) son una práctica para poner a prueba un sistema informático, red o aplicación web para encontrar vulnerabilidades que un atacante podría explotar.[1]

VULNERABILIDAD: Las vulnerabilidades son puntos débiles del software que permiten que un atacante comprometa la integridad, disponibilidad o confidencialidad del mismo. Algunas de las vulnerabilidades más severas permiten que los atacantes ejecuten código arbitrario, denominadas vulnerabilidades de seguridad, en un sistema comprometido.[2]

HACKERS: persona o a una comunidad que posee conocimientos en el área de informática y se dedica a acceder a sistemas informáticos para realizar modificaciones en el mismo. Los hackers también son conocidos como “piratas informáticos”. [3]

[1] Prueba de penetración (pen test), Margaret Rouse, testo consultado en septiembre de 2017 http://searchdatacenter.techtarget.com/es/definicion/Prueba-de-penetracion-pen-test

[2] Wikipedia la enciclopedia libre, Vulnerabilidad, consultado en septiembre de 2017 https://es.wikipedia.org/wiki/Vulnerabilidad#cite_note-2

[3] "Hacker". En: significados.com. Disponible en: https://www.significados.com/hacker/ Consultado: septiembre de 2017.

INTRODUCCIÓN

Con el uso de la informática y la tecnología en las organizaciones, los procesos se efectúan de una manera sistemática, ágil y sencilla; sin embargo, estos procesos deben ser confiables y seguros. Con el paso del tiempo, las redes empresariales, su crecimiento y la complejidad de las mismas, surge la necesidad de crear sistemas más seguros ante la presencia de posibles ataques informáticos, que amenacen su estabilidad en el sector productivo y económico.

Dichos avances tecnológicos e informáticos y las innumerables posibilidades de acceder a la información de forma libre para cualquier persona. Las empresas han identificado la necesidad de proteger gran parte de la información que no es pública, como uno de sus activos más valiosos. Por ello la intención de ofrecer servicios de seguridad informática preventiva, y a su vez construir estrategias que garanticen la seguridad en sistemas de información y la infraestructura tecnológica de las redes empresariales.

La empresa ALDIM Acciones Logísticas en Distribución de Mercancías S.A.S. es una organización que ha venido funcionando de manera estable en el mercado durante los últimos 7 años; a su vez en los últimos dos años ha demostrado un evidente crecimiento en la información registrada en su base de datos, y en el préstamo de sus servicios, por tanto quiere garantizar un óptimo cubrimiento al acceso de su red a través de un sistema seguro que los proteja de cualquier ataque informático que se presente.

El presente proyecto aplicado tiene por objetivo identificar las vulnerabilidades, amenazas y los riesgos que se presentan en los sistemas operativos y base de datos de la empresa ALDIM Acciones Logísticas en Distribución de Mercancías S.A.S., por medio de procesos de pentesting aplicados a la seguridad informática estableciendo recomendaciones que permitan un enfoque de un sistema de control eficiente por parte de la empresa donde se aseguren los sistemas operativos y la base de datos.

1 PLATEAMIENTO DEL PROBLEMA

La empresa ALDIM Acciones Logísticas en Distribución de Mercancías S.A.S. a lo largo de los 7 años de funcionamiento se ha destacado por la prestación de un buen servicio en entrega de mercancías en venta directa de productos que se ofertan por catálogo a nivel departamental.

Luego de observar y dialogar con algunos colaboradores se identifica que actualmente, el director es quien manipula, registra, usa y reúsa la información en un solo computador, el cual, a su vez, hace las veces de servidor. Esto demuestra la falta de asesoría empresarial, en lo correspondiente al uso de herramientas ofimáticas y el manejo informático de las bases de datos y sus necesidades.

Además, la empresa no posee ningún tipo de resguardo de información[4], lo cual es un grave problema si en algún momento llegara a tener problemas de un hackeo o hasta por un simple virus por el mal uso de los sistemas, puedan llegar a terminar con toda la información que posee la empresa e incluso no han precavido el riesgo de que la empresa tenga una catástrofe natural y el medio en cómo pueden llegar a solucionar todos estos problemas.[5]

Por otro lado, desde la perspectiva funcional en el mercado regional y nacional en seguridad informática, el presente proyecto aplicado sirve como antecedente al desarrollo de pentesting en sistemas operativos y bases de datos; enfocado a mejorar las prácticas laborales de la empresa ALDIM Acciones Logísticas en

[4] Ser Informática, Computer Solutions Company. La importancia del respaldo de la información [en línea], 8 septiembre del 2015 [noviembre 2017]. Disponible en Internet: https://serinformatica.com.ar/actualidad/la-importancia-del-respaldo-de-informacion/

[5] emprende pyme. Tipos de riesgos empresariales [en línea], [noviembre 2017]. Disponible en Internet: https://www.emprendepyme.net/tipos-de-riesgos-empresariales.html

Distribución de Mercancías S.A.S. las cuales se aportarán técnicas de análisis de riesgos y evaluación de controles de seguridad de la información.

Lo anterior como punto de partida para brindar soluciones efectivas y actuales a empresas que no posean mucho en infraestructura ni en capital o bienes, ni en la instalación de sistemas de seguridad informática. Para así, salvaguardar, uno de los activos más valiosos de las mismas. Porque se halla que estas dificultades dejan ver, a las nuevas empresas en estados de vulnerabilidad con acceso libre al personal no autorizado, permitiendo a su vez la modificación o hurto de su información.

1.1 FORMULACIÓN DEL PROBLEMA

¿Qué vulnerabilidades se encuentran expuestas del sistema operativo y base de datos por la ausencia de la asesoría y uso efectivo de recursos tecnológicos y herramientas para la protección de la información en la empresa ALDIM Acciones Logísticas en Distribución de Mercancías S.A.S?

2 JUSTIFICACIÓN

El principio de la informática, comenzó cuando varios equipos fueron conectados entre sí, haciendo que en las redes comenzara a haber vulnerabilidad y amenazas, por ellos surgió la necesidad de implementar medidas de seguridad informática y formar gente capacitada para implementar procesos y políticas de seguridad.

Los primeros virus informáticos surgieron alrededor del año 1985[6], el cual fue creado por un estudiante el cual infectaba a los sistemas apple, los virus fueron evolucionando y existiendo diferentes tipos de virus y generando a su vez en el ámbito delincuencial también diversas formas de hacerlo a medida que la red evolucionaba.

El mundo va evolucionando y a la misma medida aumentan las amenazas, actualmente la seguridad de la información es necesaria por el alto grado de riesgos ante posibles ataques ante el hurto de información importante en el ámbito personal y empresarial.[7] Existen múltiples amenazas informáticas a las cuales la empresa es vulnerable día a día mientras navega en la Internet.[8] Haciendo que la amenaza más común sean los virus, los cuales son programas que han sido creados para alterar algo.[9]

---

[6] seguinfo2012, Timeline, "HISTORIA DE LA SEGURIDAD INFORMATICA", consultado en noviembre 2017, retomado de https://www.timetoast.com/timelines/historia-de-la-seguridad-informatica--2

[7] SGSI - Blog especializado en Sistemas de Gestión de Seguridad de la Información. ISO 27001: ¿Qué significa la Seguridad de la Información?, consultado en noviembre 2017, disponible en: http://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/

[8] Iván Luzardo, conozca las amenazas informáticas más comunes (DISI 2010), consultado en noviembre 2017, disponible en: http://www.enter.co/chips-bits/seguridad/conozca-las-amenazas-informaticas-mas-comunes-disi2010/

[9] eset. Definición de virus, códigos maliciosos y ataques remotos, consultado en noviembre 21017, disponible en: https://support.eset.com/kb186/?viewlocale=es_ES

Teniendo en cuenta lo anterior es importante realizar este proyecto, colocando a la empresa ALDIM Acciones Logísticas En Distribución De Mercancías S.A.S. como el principal beneficiario, ya que la realización de un análisis a los sistemas operativos y la base de datos, le ayudará a establecer políticas sobre la seguridad de la información tanto interna como externamente, implementando un sistema de gestión de seguridad sobre los activos de información manejados y que son responsabilidad de la organización, además beneficiara a sus clientes y proveedores dándoles mayor seguridad y confianza en la empresa.

El desarrollo de dicho proceso de seguridad informática a los sistemas operativos y bases de datos red de datos de la empresa ALDIM Acciones Logísticas en Distribución de Mercancías S.A.S., permitirá identificar vulnerabilidades y corregir los fallos de seguridad de la red antes de que sean explotados, con lo que la empresa podrá asegurar la calidad en su red informática. Además, se verán beneficiados los funcionarios de la empresa ya que contarán con un sistema de red confiable en el manejo y gestión de la información.

3 OBJETIVOS

3.1 OBJETIVO GENERAL

Analizar la seguridad de la empresa ALDIM Acciones Logísticas en Distribución de Mercancías S.A.S., para identificar vulnerabilidades que puedan afectar la información que posee en los sistemas operativos y base de datos.

3.2 OBJETIVOS ESPECÍFICOS

- Identificar los activos que conforma los sistemas de la empresa ALDIM Acciones Logísticas en Distribución de Mercancías S.A.S. y con los cuales se les realizara pruebas de seguridad.
- Realizar las pruebas de seguridad para encontrar las vulnerabilidades a la empresa ALDIM Acciones Logísticas en Distribución de Mercancías S.A.S.
- Presentar un informe sobre las vulnerabilidades encontradas y las recomendaciones de mejora relacionadas con la seguridad de información de los sistemas operativos y base de datos para la empresa ALDIM Acciones Logísticas en Distribución de Mercancías S.A.S.
- Recomendar las mejoras a la empresa ALDIM Acciones Logísticas en Distribución de Mercancías S.A.S. para evitar las vulnerabilidades encontradas a el sistema operativo y base de datos.

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

En la historia de la seguridad informática; viene creciendo cada día, hacia los años 80 y principios de los 90 la seguridad informática se centraba en proteger simplemente que el usuario no dañara el sistema operativo y como máxima protección el colocar un antivirus para que no dañara información.

Con la aparición de la internet la seguridad informática se fue centrando en las redes, protegiendo servidores, equipos y controlando la seguridad a través de firewall, lo cual había que hubiera nuevas posibilidades de aparición de vulnerabilidades que podrían ser explotadas por aquellas personas que sabían que hacer para obtener información.[10]

El perfil de los atacantes antes se centraba en acceder a un sitio donde nadie más podía llegar o simplemente infectar un sistema con un virus pero todo sin ánimo de lucro, en la actualidad los atacantes lo que les importa es la información. Estos se aprovechan de las vulnerabilidades en los sistemas y las redes para acceder a la información sensible de una empresa.

Ante esta situación las empresas se protegen con nuevas tecnologías: Sistemas IDS[11] (Intrusion Detection System). Sistemas de monitorización y detección de

[10] LÓPEZ, David. Evolución de la Seguridad Informática [en línea], [noviembre 2017]. Disponible en Internet: https://www.grupocontrol.com/evolucion-de-la-seguridad-informatica

[11] BRADLEY, Tony. Introduction to Intrusion Detection Systems (IDS) [en línea], agosto 13, 2017 [noviembre 2017]. Disponible en Internet: https://www.lifewire.com/introduction-to-intrusion-detection-systems-ids-2486799

accesos no permitidos en una red, Sistemas IPS [12](Intrusion Prevention System). Sistemas de prevención de intrusión. No solo monitoriza el tráfico para detectar vectores de ataque en una red, sino que el sistema es capaz de bloquearlos.

Honey pot.[13] Instalación de equipos aparentemente vulnerables que en realidad no contienen ninguna información sensible de la empresa, sino que están diseñados para atraer y detectar a los atacantes, protegiendo los sistemas realmente críticos.

SIEM[14] (Security Information and Event Management). Sistemas de correlación de eventos y generación de alertas, capaces de integrar diferentes dispositivos, lanzar acciones en función de las alertas, y almacenar los registros para un posterior análisis de los mismos.

Los sistemas operativos. Son un programa que después de que arranca o inicia es capaz de gestionar todos los recursos tanto de hardware (disco, teclado, pantalla, etc.) como el software (programas), permitiendo la comunicación entre las personas y el computador.

La función principal de los sistemas operativos es administrar los recursos, coordinar el hardware, organizar archivos y dispositivo de almacenamiento en nuestro ordenador. Permite hacer múltiples tareas al mismo tiempo, se ocupa de la entra y la salida de los dispositivos; entre los sistemas operativos se encontró

[12] techopedia. Intrusion Prevention System (IPS) [en línea], [noviembre 2017]. Disponible en Internet: https://www.techopedia.com/definition/15998/intrusion-prevention-system-ips
[13] candytraps. ¿Qué es un honeypot? [en línea], [noviembre 2017]. Disponible en Internet: https://candytraps.wordpress.com/que-es-un-honeypot/
[14] ShutterStock. ¿Qué es un SIEM? [en línea], enero 10 de 2016 [noviembre 2017]. Disponible en Internet: https://www.tripwire.com/state-of-security/incident-detection/log-management-siem/what-is-a-siem/

diferentes tipos como lo son Windows, Linux que son los más conocidos y los que más trabajan los usuarios, además están los sistemas operativos para móviles.[15]

Las bases de datos el termino surgió en los años 60, donde una base de datos es una especie de almacén el cual nos permite guardar información de forma ordenada donde nos permite buscar y utilizar fácilmente, actualmente existen números bases de datos dependiendo de la necesidad de los usuarios.[16]

La Seguridad Informática es la disciplina que se encarga del diseño de normas, métodos, técnicas, procedimientos dirigidos a establecer condiciones de seguridad óptimas para el tratamiento de datos en un sistema informático. Va dirigida al aseguramiento de los activos tecnológicos de una organización, para que estos sean utilizados de la manera correcta y por el personal acreditado para ello.

La seguridad informática tiene sus bases en tres pilares fundamentales, los cuales se deben cumplir en cualquier sistema informático: La confidencialidad; este pilar hace referencia a la privacidad de la información, la seguridad informática debe proteger un sistema informático de acceso a la información por parte de personal o programas no autorizados.

La Integridad; este pilar hace referencia a la veracidad y validez de los datos almacenados o guardados en un sistema informático. La disponibilidad; Este pilar hace referencia a las condiciones óptimas que deben estar establecidas para que los datos y/o la información se puedan, consultar, verificar, se pueda acceder a la misma en el momento que sea requerido y por personal autorizado.

---

[15] areatecnologia. Sistemas Operativos [en línea], [noviembre 2017]. Disponible en Internet: http://www.areatecnologia.com/sistemas-operativos.htm

[16] VALDÉS, Damián P. ¿Qué son las bases de datos? [en línea], octubre 26 2007 [noviembre 2017]. Disponible en Internet: http://www.maestrosdelweb.com/que-son-las-bases-de-datos/

Una vulnerabilidad son las debilidades o fallos de una empresa donde puede ser utilizadas para causar un daño a la red de datos o un sistema de información, estas vulnerabilidades pueden aparecer en cualquier momento tanto en el hardware como en el software.[17]

Una amenaza es una acción capaz de atentar contra la seguridad de la información. Las amenazas surgen a partir de la existencia de vulnerabilidades, es decir que una amenaza sólo puede existir si existe una vulnerabilidad que pueda ser aprovechada, e independientemente de que se comprometa o no la seguridad de un sistema de información.[18]

Los riesgos informáticos se refieren a la incertidumbre existente por la posible realización de un suceso relacionado con la amenaza de daño respecto a los bienes o servicios informáticos como por ejemplo los equipos informáticos, periféricos, instalaciones, proyectos, programas de cómputo, archivos, información, datos confidenciales, entre otros.[19]

[17] PRANDINI, Patricia. Vulnerabilidades, amenazas y riesgo en “texto claro” [en línea], mayo 25 2013 [noviembre 2017]. Disponible en Internet: http://www.magazcitum.com.mx/?p=2193#.WhNW41WWaM8

[18] UNIVERSIDAD NACIONAL DE LUJAN. Departamento de Seguridad Informática. Amenazas a la Seguridad de la Información. Recopilado de: http://www.seguridadinformatica.unlu.edu.ar/?q=node/12

[19] Seguridad informática, Riesgos, recopilado de https://carrmen.jimdo.com/riesgo-informatico/

Los tipos de ataques están destinados a páginas y/o portales web; dado que pueden obtener control parcial o total sobre este medio también esta los ataques a personas y/o usuarios donde pueden perder información valiosa como puede ser hasta su propia identidad.[20]

Cross Site Scripting (XSS): lo que se hace es fijar un código en un sitio web de la persona que se va atacar, hacer que esa persona ingrese al sitio web al que se le fijo el código para poder que se ejecute y este cumpla su función para lo que fue creado, como lo son robos de sesiones o datos vulnerables.[21]

Fuerza bruta: para este se crea procesos automáticos donde el atacante mediante prueba y error logra dar con el usuario y la contraseña, generados al azar, este ataque se puede realizar en cualquier sitio web donde nos pida un usuario y una contraseña para ingresar.[22]

Inyección de código: con este método los atacantes inyectan código fuente como SQL, SSI, HTML al sitio web que se desea atacar, cambiando su funcionalidad original o revelando datos que se encuentran almacenados en las bases de datos que utilizan.[23]

Denegación del servicio (DOS): este ataque aprovecha algún error de la programación del sitio web que se está atacando, haciendo que el servidor utilice

[20] URREGO, Jonatán. Tipos de ataque y cómo prevenirlos [en línea], mayo 1, 2013 [noviembre 2017]. Disponible en Internet: https://colombiadigital.net/actualidad/articulos-informativos/item/4801-tipos-de-ataque-y-como-prevenirlos.html

[21] PÉREZ, Ignacio. Comprendiendo la vulnerabilidad XSS (Cross-site Scripting) en sitios web [en línea], abril 29 2015 [noviembre 2017]. Disponible en Internet: https://www.welivesecurity.com/la-es/2015/04/29/vulnerabilidad-xss-cross-site-scripting-sitios-web/

[22] GARCÍA, Juan. Qué es un ataque por fuerza bruta [en línea], mayo 7 del 2013 [noviembre 2017]. Disponible en Internet: http://faqoff.es/que-es-un-ataque-por-fuerza-bruta/

[23] OWASP. Inyección de Código [en línea], julio 30 2015 [noviembre 2017]. Disponible en Internet: https://www.owasp.org/index.php/Inyecci%C3%B3n_de_C%C3%B3digo

los recursos como es el procesador y la memoria, hasta el punto donde el servidor no da más y colapsa el servidor web por no tener más recursos. En consecuencia, logra sacar el sitio web del aire.[24]

Fuga de información: a pesar de que es un ataque es la consecuencia del error del administrador del sitio web, el cual consiste en dejar público el registro de errores, lo que facilita al atacante ver las fallas exactas del sistema, tomar provecho de estas, y obtener el control parcial o total del sitio web.[25]

Phishing (pesca de datos): el atacante a través de diversos métodos intenta obtener datos personales de su víctima, una de las más conocidas es suplantar páginas web, crean un sitio similar al sitio original con el fin de que el visitante ingrese y deje sus datos personales como claves, números de tarjeta etc. Obviamente estos datos llegan al atacante el cual los aprovecha. Por lo general dichos ataques llegan al correo, suplantando empresas y entidades financieras, haciéndolos ingresar al sitio web falso.[26]

Spoofing: este ataque consiste en suplantar la identidad de la máquina de una persona, a través de sustitución de datos. Por lo general se realiza cuando se crea la conexión entre dos máquinas y una tercera ingresa en medio de la comunicación, haciéndose pasar por la otra utilizando datos como la IP de la máquina.[27]

---

[24] ROUSE, Margaret. Ataque de denegación de servicio (DDoS) [en línea], noviembre 2012 [noviembre 2017]. Disponible en Internet: http://searchdatacenter.techtarget.com/es/definicion/Ataque-de-denegacion-de-servicio

[25] BORTNIK, Sebastián. ¿Qué es la fuga de información? [en línea], abril 13 de 2010 [noviembre 2017]. Disponible en Internet: https://www.welivesecurity.com/la-es/2010/04/13/que-es-la-fuga-de-informacion/

[26] avast. Qué es el phishing [en línea], [noviembre 2017]. Disponible en Internet: https://www.avast.com/es-es/c-phishing

[27] Muñoz, Ana. ¿Qué es spoofing? [en línea], septiembre 2016 [noviembre 2017]. Disponible en Internet: http://computerhoy.com/noticias/software/que-es-spoofing-51236

Scam: cuando se regala dinero a cambio de más dinero, el atacante ofrece extrañas recompensas, herencias de origen desconocido o premios de otros países, los cuales para ser reclamados tienen que dar una suma de dinero inferior a la que se recibirá a cambio. Por eso es importante verificar la identidad de las personas que circulan esta información a través de Internet.[28]

Ingeniería social: el atacante busca suplantar personas y entidades para obtener datos personales, por lo general, estos ataques se realizan mediante llamadas telefónicas, mensajes de texto o falsos funcionarios. Su objetivo no es otro que el de obtener datos importantes para después manipularlos, analizarlos y utilizarlos en contra de la persona. Otros métodos que buscan estafar a las personas son falsos correos que prometen premios.[29]

Troyano: haciendo referencia al famoso "caballo de Troya" de la Odisea, este ataque informático consiste en instalar programas espías dentro del computador afectado, para realizar diversas acciones en él como manejo remoto, cambio de archivos, robo de información, captura de datos personales, entre otras.[30]

[28] infobae. El scam, otra forma de estafar ingenuos [en línea], septiembre 10 de 2005 [noviembre 2017]. Disponible en Internet: https://www.infobae.com/2005/09/10/208271-el-scam-otra-forma-estafar-ingenuos/

[29] ENTER.CO. La ingeniería social: el ataque informático más peligroso [en línea], julio 25 de 2016 [noviembre 2017]. Disponible en Internet: http://www.enter.co/guias/lleva-tu-negocio-a-internet/ingenieria-social/

[30] pandasecurity. ¿Qué es un troyano? [en línea], diciembre 10, 2013 [noviembre 2017]. Disponible en Internet: https://www.pandasecurity.com/spain/mediacenter/consejos/que-es-un-troyano/

Riesgos de seguridad a nivel de sistema operativo: Muchas veces se comete el error de pensar que la seguridad consiste en evitar que intrusos entren en nuestro sistema, toca ver a fondo los factores que ayudan a mejorar la seguridad; detectar cuando nos están entrando al sistema, poder restaurar nuestro sistema e identificar qué es lo que está haciendo el intruso, dicho en otras palabras, es el mecanismo de prevención, detención, restauración y análisis lo que garantiza la seguridad.[31]

4.2 MARCO CONCEPTUAL

El Pentesting es la práctica de atacar diversos entornos con la intención de descubrir fallos, vulnerabilidades u otros fallos de seguridad, para así poder prevenir ataques externos hacia esos equipos o sistemas.[32] El software de una computadora es todo aquel que le permite al usuario ordenarle a la misma que realice una tarea.

También se deben subdividir en diversas categorías en base a las funciones que realizan en el sistema. “Software es una secuencia de instrucciones que son interpretadas y/o ejecutadas para la gestión, redireccionamiento o modificación de un dato/información o suceso”.[33]

[31] ADMINSO. Medidas de seguridad en los sistemas operativos [en línea], [noviembre 2017]. Disponible en Internet: http://www.adminso.es/index.php/4._Medidas_de_seguridad_en_los_sistemas_inform%C3%A1ticos

[32] ¿Qué es un Pentest?, Gianfranco Lemmo, consultado en junio de 2017, retomado de https://www.webbizarro.com/noticias/2658/que-es-un-pentest/

[33] Que es Hardware y Software, Informática Hoy, consultado en junio 2017, retomado de http://www.informatica-hoy.com.ar/aprender-informatica/Que-es-Hardware-y-Software.php

Nmap es una utilidad de software libre para explorar, administrar y auditar la seguridad de redes de ordenadores. Detecta hosts online, sus puertos abiertos, servicios y aplicaciones corriendo en ellos, su sistema operativo, que firwalls/filtros corren en una red y de qué tipo son.

Es excelente para hacer trabajos de auditoria de red y fue diseñado para llevar acabo escaneos rápidos en una gran cantidad de redes, pero es igualmente usable en hosts individuales. Es reconocido como el scanner de puertos más poderoso y se lo usa básicamente para 3 cosas: Auditorias de seguridad, Pruebas rutinarias de redes y Recolector de información para futuros ataques. (hackers)[34]

Un Ataque informático es una acción intencionada o no, mediante la cual se accede a un sistema informático o red sin autorización alguna, este ataque se puede llevar a cabo por parte de personas con grandes conocimientos en informática e incluso con conocimientos básicos, y que buscan causar algún tipo de daño como puede ser el robo, copia, daño, alteración, borrado de información importante para el propietario de la misma.

SQLmap es una herramienta desarrollada para realizar inyección de código SQL automáticamente. Su objetivo es detectar y aprovechar las vulnerabilidades de inyección SQL en aplicaciones web y explotar todas las falles posibles en la base de datos.[35]

[34] Paraíso Linux. “Que es y cómo usar NMAP”, consultado en octubre 2017, retomado de https://paraisolinux.com/que-es-y-como-usar-nmap/

[35] DragonJAR. SQLMap – Herramienta Automática de Inyección SQL [en línea], [noviembre 2017]. Disponible en Internet: http://www.dragonjar.org/sqlmap-herramienta-automatica-de-inyeccion-sql.xhtml

Nessus es escáner para la prevención de ataques de red, identificación de vulnerabilidades y detección de problemas de configuración que utilizan los hackers para entrar en la red. Es utilizado por gran cantidad de personas a nivel mundial de evaluación de la vulnerabilidad, configuración de seguridad y cumplimiento de las normas de seguridad.[36]

4.3 MARCO CONTEXTUAL

La empresa ALDIM Acciones Logísticas en Distribución de Mercancías S.A.S. surge de la necesidad de entrega y despacho mercancía (productos para el hogar, ropa, etc.) que viene presentando el mercado en la Venta Directa de revistas por catálogo a nivel Departamental, donde procura establecer con cada uno de sus clientes, ofreciéndoles sus servicios innovadores, eficientes, oportunos y confiables, con tarifas competitivas en el mercado, soportado en un equipo humano experto.

ALDIM Acciones Logísticas en Distribución de Mercancías S.A.S.[37] se ha caracterizado en el cumplimento de entregas y promoviendo un buen servicio, nombre y prestigio ante los clientes, todo soportado por un equipo de trabajo capacitado en su labor, con sentido de pertenencia ante la compañía.

ALDIM Acciones Logísticas En Distribución De Mercancías S.A.S., es una compañía de transporte de carga y distribución, especializada en prestar servicios a empresas de venta directa a nivel del Departamento. Conocemos a fondo las necesidades de las empresas dedicadas a la venta directa y nos hemos fortalecido en los

[36] gb-advisors, Nessus Escáner de Vulnerabilidad [en línea], [noviembre 2017]. Disponible en Internet: https://www.gb-advisors.com/es/gestion-de-vulnerabilidades/nessus-escaner-vulnerabilidad/

[37] ALDIM Acciones Logísticas En Distribución De Mercancías S.A.S., tomado del interior de la empresa

pormenores que marcan la diferencia en los servicios convencionalmente ofrecidos en el mercado.

Las entregas en un menor tiempo, ya que esto repercute directamente en las ventas de las asesoras, las cuales tienen este como su principal fuente de ingresos, y obtener un vínculo más estrecho con las Asesoras, percibiendo así sus necesidades en el servicio y un servicio de distribución exclusivo por Empresa; con cobertura a nivel Departamental. Haciendo que el objetivo principal sea la satisfacción de las necesidades de los clientes, garantizando la simpleza y transparencia del servicio, en un mercado de responsabilidad y respeto hacia nuestros clientes y colaboradores.

Según la ACIS "Asociación Colombiana de Ingenieros De Sistemas", presenta una lista de empresas dedicadas a la seguridad informática en Colombia, la cual está para brindar ayuda a toda aquella persona que desee una empresa reconocida en el medio para realizar todo tipo de seguridad informática; a continuación, se puede observar algunas empresas de forma informativa para todo aquel que lo solicite, retomado de la página oficial.[38]

Tabla 1. Lista de Empresas de Seguridad Informática

Nombre Empresa	Sitio Web
Netdata Networks	www.netdatanetworks.com
S2 Grupo Colombia	www.s2grupo.co
0 Riesgos Consultores	https://sites.google.com/site/hadm88
360 Security Group S.A	www.360sec.com
360 Integral Security S.A.S.	www.360isg.com
2Secure S.A.S	www.2secure.org
A	
ACT Tecnología Informática	www.act.com.co

[38] ACIS, "Asociación Colombiana de Ingenieros De Sistemas". Lista de Empresas de Seguridad Informática [en línea], [diciembre 2017]. Disponible en Internet: http://acis.org.co/portal/content/lista-de-empresas-de-seguridad-inform%C3%A1tica-en-colombia

Activos TI SAS	www.activosti.com
Adalid Corp S.A.S	www.adalid.com
Addintech	www.addintech.com
Adistec Colombia	www.adistec.com/co
Antai Group Ltda	www.antai-group.com
Antifraude	www.antifraude.co
Aerolen	www.arolen.com
ASR Soluciones	www.asr-la.com
ASTAF –TICS – División Tecnologías de la información y las comunicaciones	www.astaf.com
ASSURE IT SAS	https://assureit.co
Afina	www.afina.com.co
Azuan Technologies S.A	www.azuan.com
A3SEC	www.a3sec.com
B	
B-Secure	www.b-secure.co
Binary TI	www.binaryti.co
BDO Audit S.A.	www.bdo.com.co/es/
BLT Colombia	www.bltcolombia.com
BSolution Group S.A.S.	www.bsolutiongroup.com
C	
Centro de Soluciones Tecnológicas Siglo XXI	www.cstsigloxxi.com
CISCO (Security consulting)	www.cisco.com/global/CO
CLM Colombia S.A.S	www.clm.com.co
Cloud Seguro	www.cloudseguro.co
Consultores de sistemas de información CSI COLOMBIA	www.csi-internacional.com
Creange	www.creangel.com
Consulting Network Security	www.cns.com.co
Cross Border Technology	http://www.crossbordertech.com
CSIETE	http://www.csiete.org/
CONTROL IT	www.controlit.com.co
Complex Security Networks	www.complexsn.com
D	
Deloitte & Touche (Security services)	www.deloitte.com
Desca	www.desca.com
Digiware S.A.	www.digiware.net
Digital Business DBX Ltda	www.digital01.com.co
DragonJAR Soluciones y Seguridad Informática SAS	www.dragonjar.biz

DSTEAM Seguridad Informática	www.dsteamseguridad.com
E	
Easysolutions Inc.	www.easysol.net
The Eagle Labs	www.theeaglelabs.com
Ecomil S.A.S.	www.solucionesecomil.com
EC Security Solutions SAS	www.ec-sec.com.co
Efeyce Integrales S.A.S	www.efeyceintegrales.com
Elliptical Ltda	www.elliptical.com.co
Enfocus	www.en-focus.com
ERC Colombia SAS	www.erc.com.co/site
Ernest & Young (Riesgos en Tecnología y Seguridad)	www.ey.com/global
Estéganos International Group	www.esteganos.com
ETEK S.A.	www.etek.com.co
Everis	www.soceveris.com www.everis.com/global/es/industries/aerospace-defense
F	
Fast & ABS Auditores Ltda.	www.fastauditores.com
FoxNet Sistemas Ltda	www.foxnetsistemas.com
Fluidsignal Group	www.fluidsignal.com
G	
Gamma Ingenieros S.A.	www.gammaingenieros.com
Global Crossing	www.globalcrossing.com
Globaltek Security	www.globalteksecurity.com
GMTECH	www.gmtech.es
Grupo Oruss	www.grupooruss.com
H	
Hack&Secure SAS	www.hackandsecure.net
IT Government Hambar	www.hambar.com.co
Human Hacking	www.humanhacking.com.co
I	
IBM (Servicios de Seguridad y Privacidad)	www.ibm.com/co/services/security
Icon Company	www.iconcompany.com
Identian	www.identian.co
IQ Information Quality	www.iqcol.com
Imaginanda	www.imaginanda.com.co
Infocomunicaciones	www.infocomunicaciones.net
Information Technology Security Solutions (ITSS) Ltda	www.itss.com.co
Soluciones Inteligentes para Negocios Masivos - Inteligensa	www.inteligensa.com

Information Security Systems - ISS	www.iss.com.co
Innovativa	www.innovativa.biz/index_archivos/Page354.htm
Ingeniería Telemática S.A.S	www.ingenieriatelematica.com.co
Integrar S.A	www.integrar.com.co
InterLAN	www.interlan.com.co
Internet Solutions	www.internet-solutions.com.co
Intergrupo S.A	www.intergrupo.com
Isec Information Security Inc	www.isec-global.com
IT Forensic SAS	www.itforensic-la.com
ITECH S.A.S	www.itechsas.com
Internet Security Auditors Colombia S.A.S.	www.isecauditors.com
IT SECURITY	www.itsecurity.com.co
J	
J2K Security Group	www.j2ksec.com
K	
KPMG	www.kpmg.com.co
Kinetic Solutions	www.kineticsl.com
L	
Latinus Ne	www.latinus.net
Lia Solutions Ltda	www.liacolombia.com
Locknet S.A.	www.lock-net.net
M	
Mareigua	www.mareigua.com
Millán C. & Asociados	www.millanyasociados.com
Multisoft	www.multisoft.com.co
Mnemo	www.mnemo.com
N	
NeoSecure Colombia	www.neosecure.com
Némesis S.A.	www.nemesis.com.co
NetSecure Colombia	www.netsecure.com.co
Newnet S.A.	www.newnetsa.com
Niterix	www.niterix.com
Network Security Team	www.nst.com.co
O	
Ona Systems SAS	www.onasystems.net
Olimpia	www.olimpiait.com
OBIKUZ S.A.S Integrador Tecnológico	www.obikuz.net
P	
Password Safe S.A.S	www.passwordsafesas.net

Password Seguridad Informática S.A.	www.password.com.co
PyP Servicios y Sistemas Integrados	www.pypservi.com
Power Link	powerlink.shorturl.com
PricewaterhouseCoopers - PwC	www.pwc.com/co
PCM	www.pcm-ti.com
R	
Red Colombia	www.redcolombia.com.co
Red Segura	www.redsegura.com
Ricardo Bernate y Compañia Ltda	www.rbcia.net
S	
SAFETY IN DEEEP SAS	www.safeid-sas.com
Scientech - Seguridad e Inteligencia Informática	www.scientechsecurity.com
SecTorch S.A.S.	www.sectorch.com
SeguraTec S.A.S	www.seguratec.com.co
SSP (Secure Solutions Provider)	www.securesolutionsprovider.com
Seltika, Seguridad Informática	www.seltika.com
Siemens S.A.	www.siemens.com.co/security
SISEL Ingeniería S.A.S.	www.siselingenieria.com
Sciotec s.a.s	www.sciotec.net
SlabInfo	www.slabinfo.com
Softnet S.A.	www.softnet.com.co
System Security Hardening	www.ssh-consulting.com
Software Channel - Symantec Partner	www.softwarechannel.net
Sotecsa Colombia S.A.S.	www.gruposotecsa.com
SSE Ltda	www.sse.com.co
SWAT Security IT	www.swatsecurityit.com
Systematic Solutions	www.systematicsolutions.com.co
Secure Information Systems s.a.s (GERSAFE)	www.gersafe.com.co
SecuriTIC Group	www.securitic.com.co
T	
Tecnología en Sistemas Avanzados	www.tsaconsultores.com.co
Teknii	www.teknii.com
Terremark	www.terremark.com.co
Trustwave	www.trustwave.com
U	
Unisys	www.unisys.com/unisys

V	
Vilsol	www.vilsol.com

Fuente: ACIS. Disponible en Internet: http://acis.org.co/portal/content/lista-de-empresas-de-seguridad-inform%C3%A1tica-en-colombia

4.4 MARCO LEGAL

4.4.1 Ley 1273 de 2009 – "De la Protección de la Información y los Datos"

Con esta ley se preservan integralmente los sistemas que utilicen de las tecnologías de la información y la comunicación, entre otros. En esta ley se tipificaron como delitos, el uso abusivo de los datos personales por lo que es de resulta de gran importancia para las empresas que se blinden jurídicamente en este ámbito para evitar incurrir en ciertas conductas estipuladas como delitos penales. La Ley 1273 de 2009 se compone de dos (2) capítulos y de diez (10) artículos. A continuación, se sintetizarán aquellos artículos que correspondan al desarrollo del presente proyecto:

Artículo 269A: Acceso abusivo a un sistema informático toda persona que acceda a un sistema informático y permanezca en el sin autorización.

Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación incurrir en este delito toda persona que sin estar autorizado no permita el acceso a una red, sistema informático o los datos informáticos.

Artículo 269C: Interceptación de datos informáticos incurrirá en este delito toda persona que sin tener orden judicial intercepte ya sea en su origen, trasmisión, destino o al interior de un sistema informático los datos informáticos.

Artículo 269D: Daño Informático este delito contempla que toda persona quien no tenga la debida autorización que borre, altere, suprima o modifique datos informáticos o dentro de un sistema sus partes o componentes lógicos.

Artículo 269E: Uso de software malicioso aquí se contempla como delito la producción, tráfico, venta, distribución importación o exportación de software considerado como dañino o malicioso.

Artículo 269F: Violación de datos personales, incurrirá en este delito toda persona que obtenga beneficio para sí mismo o para terceros de información personal contenida en bases de datos, ficheros.

Artículo 269G: Suplantación de sitios web para capturar datos personales, este delito contempla el diseño, creación distribución o venta de sitios web, enlaces o ventanas emergentes diseñados para capturar ilegalmente datos personales.

Artículo 269I: Hurto por medios informáticos y semejantes, incurrirá en este delito toda persona que, a través de un sistema informático, red de un sistema electrónico o telemático cometa hurto.

Artículo 269J: Transferencia no consentida de activos. Este delito contempla la trasferencia no autorizada de activos en perjuicio de otra persona, mediante manipulaciones de tipo informático.[39]

Entre los delitos más comunes en Colombia se encuentran: Hurto por medios informáticos y semejantes, uso de software malicioso, violación de datos personales y acceso abusivo a un sistema informático.

[39] Código Penal. Ley 1273 de 2009 De la Protección de la Información y de los Datos. Colombia, 2009. Ministerio de la Información y las Comunicaciones de Colombia

4.4.2 Ley 1581 de 2012 - Protección de Datos Personales

Esta ley que complementa la regulación vigente para la protección del derecho fundamental que tienen todas las personas naturales a autorizar la información personal que es almacenada en bases de datos o archivos, así como su posterior actualización y rectificación. Esta ley se aplica a las bases de datos o archivos que contengan datos personales de personas naturales.

El régimen de protección de datos personales que se establece en la presente ley no será de aplicación: A las bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico, cuando estas bases de datos o archivos vayan a ser suministrados a terceros se deberá, de manera previa, informar al titular y solicitar su autorización. En este caso los responsables y encargados de las bases de datos y archivos quedarán sujetos a las disposiciones contenidas en la presente ley.

A las bases de datos y archivos que tengan por finalidad la seguridad y defensa nacional, así como la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo, a las Bases de datos que tengan como fin y contengan información de inteligencia y contrainteligencia, a las bases de datos y archivos de información periodística y otros contenidos editoriales.[40]

[40] CÓDIGO PENAL. Ley 1581 de 2012. la protección de datos personales, 2012. Disponible en la URL, http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

5 METODOLOGÍA

5.1 MÉTODO DE INVESTIGACIÓN

Teniendo en cuenta el planteamiento del problema propuesto en este proyecto, el enfoque que se quiere buscar en esta investigación es cuantitativo, ya que se busca medir las variables de seguridad de la información en la red de la empresa ALDIM Acciones Logísticas En Distribución De Mercancías S.A.S., observando los métodos que utilizan para preservar la confidencialidad, integridad y disponibilidad.

El proyecto tendrá como tipo de investigación, Exploratoria: por cuanto se pretende identificar vulnerabilidades, amenazas y riesgos de la seguridad de los sistemas operativos y base de datos de la empresa ALDIM Acciones Logísticas En Distribución De Mercancías S.A.S.

5.2 FUENTES Y TÉCNICAS DE RECOLECCION DE INFORMACIÓN

5.2.1 Fuentes primarias

La primera fuente de información será a través de las visitas a las instalaciones de la red de la empresa ALDIM Acciones Logísticas en Distribución de Mercancías S.A.S. y mediante el contacto con el personal de sistemas. La recolección de la información será mediante entrevistas, cuestionarios y listas de chequeo, las cuales permitirán conocer el estado de la red de la empresa. Se utilizarán datos obtenidos de búsqueda bibliográfica, artículos científicos, monografías, tesis, libros o artículos de revistas especializadas originales, relacionados al objeto de estudio.

5.2.2. Fuentes secundarias.

Se utilizará resúmenes, compilaciones o listados de referencias, preparados en base a las fuentes primarias sobre herramientas de pentesting para el análisis de vulnerabilidades a los sistemas operativos y la base de datos de la empresa ALDIM Acciones Logísticas En Distribución De Mercancías S.A.S.

5.3 DELIMITACIÓN Y ALCANCE

El proyecto se llevará a cabo en los sistemas operativos y base de datos de la empresa ALDIM Acciones Logísticas En Distribución De Mercancías S.A.S. ubicada en la ciudad de Guadalajara de Buga – Valle del Cauca. Para la aplicación del proyecto se tendrán en cuenta herramientas de pentesting; la metodología a trabajar será penetración ISSAF, posteriormente se aplicarán pruebas de penetración que sirvan de evidencia y posibles amenazas existentes en los sistemas operativos y base de datos de la empresa ALDIM Acciones Logísticas En Distribución De Mercancías S.A.S.

5.4 TÉCNICAS E INSTRUMENTOS

Para esta investigación y la realización del pentesting, se tiene previsto utilizar las siguientes herramientas y técnicas:

- Visitas técnicas: Se realizarán visitas técnicas para verificar aspectos físicos y administrativos de la red.
- Entrevistas al encargado de sistemas y a los usuarios de la red de datos
- Cuestionarios aplicados a los usuarios y encargado de sistemas.

- Listas de chequeo para determinar que controles existen dentro de la seguridad en la red.
- Pruebas de Penetración: se realizarán pruebas para identificar vulnerabilidades de la red de la empresa ALDIM Acciones Logísticas en Distribución de Mercancías S.A.S.

5.5 POBLACIÓN Y MUESTRA

La población lo conforman los usuarios que integran la planta de trabajo y que se conectan a la red de la empresa ALDIM Acciones Logísticas En Distribución De Mercancías S.A.S., además de todas las entidades en las distintas ciudades del país que tienen convenio con la empresa para ejecutar los proyectos. Para la muestra se seleccionará solamente al personal encargado del departamento de sistemas.

5.6 ACTIVIDADES

Las actividades para realizar el plan de desarrollo para los objetivos serían los siguientes.

Tabla 2. Actividades.

ETAPA	OBJETIVO	ACTIVIDAD
1	Identificar los activos que conforma los sistemas de la empresa ALDIM Acciones Logísticas en Distribución de Mercancías S.A.S. y con los	Para ellos se realizará visitas técnicas o para conocer la infraestructura de la red de datos de la empresa, se solicitará la documentación de la red para

	cuales se les realizara pruebas de seguridad.	identificar puntos de acceso, topología, la distribución de los equipos y servidor, las características de los equipos.
2	Realizar las pruebas de seguridad para encontrar las vulnerabilidades a la empresa ALDIM Acciones Logísticas en Distribución de Mercancías S.A.S.	Donde se realizará un plan de pruebas de penetración, donde se escogerán las más relevantes que se acojan al caso del proyecto con el fin de determinar vulnerabilidades, riesgos y amenazas existentes en la seguridad de la red de la empresa ALDIM Acciones Logísticas en Distribución de Mercancías S.A.S., por medio de las herramientas
3	Presentar un informe sobre las vulnerabilidades encontradas y las recomendaciones de mejora relacionadas con la seguridad de información de los sistemas operativos y base de datos para la empresa ALDIM Acciones Logísticas en Distribución de Mercancías S.A.S.	Para aplicar las pruebas seleccionadas, donde siguiendo las fases del test de penetración se realizará reconocimiento, identificación y análisis de las vulnerabilidades encontradas y realizar un análisis y gestión de riesgos sobre los hallazgos y vulnerabilidades encontrados con los métodos e instrumentos seleccionados y las pruebas de penetración.
4	Recomendar las mejoras a la empresa ALDIM Acciones	Donde se examinará y recopilará la información y los resultados

	Logísticas en Distribución de Mercancías S.A.S. para evitar las vulnerabilidades encontradas a el sistema operativo y base de datos	obtenidos en las pruebas de pentesting y se presentará el informe de pentesting a la oficina de sistemas y la dirección de la empresa ALDIM Acciones Logísticas en Distribución de Mercancías S.A.S.

Fuente: El autor

6 RESULTADOS

6.1 APLICACIONES SELECCIONADAS

Para el desarrollo de la presente investigación fue seleccionado el sistema operativo Kali Linux el cual contiene programas gratuitos especializados que permiten hacer vulneraciones para realizar diversas pruebas de seguridad con el fin de identificar posibles vulnerabilidades que puedan afectar al sistema operativo y la base de datos de la empresa ALDIM Acciones Logísticas En Distribución De Mercancías S.A.S.

A continuación, se caracteriza cada una de las aplicaciones seleccionadas:

Tabla 3. Aplicación con objetivo de estudio

APLICACIÓN	DESCRIPCIÓN
NMAP	Es una aplicación que nos permite administrar y auditar las redes de los computadores; nos detecta todos los puertos que estén abiertos con sus respectivos servicios y aplicaciones que estén corriendo sobre ellos, es el programa que escanea puertos más rápido y poderoso.
Metasploit	Es un programa que sirve para explotar las vulnerabilidades de los equipos donde su fuerte es hacer penetraciones a las bases de datos.
Nessus	Programa para el escaneo de vulnerabilidades, es categorizada como la mejor herramienta de seguridad de red, el cual nos permite identificar las debilidades y errores de configuración que pueden ser usados para ataques

SQLMAP	Esta herramienta se utiliza en inyección de SQL, para obtener listas y registros de las bases de datos

Fuente: el autor

6.2 CONFIGURACIÓN DEL AMBIENTE DE PRUEBAS

El objetivo de la configuración del ambiente de pruebas es proveer el hardware y software necesario para realizar la ejecución de las pruebas de las aplicaciones en escenarios que cumplan con los requisitos necesarios para su funcionamiento normal con el fin de obtener resultados acertados.

A continuación, se describe la configuración, de hardware y software, del ambiente para la ejecución de las pruebas de pentesting realizadas a ALDIM Acciones Logísticas En Distribución De Mercancías S.A.S. para el desarrollo del proyecto:

1. El equipo utilizado para realizar las pruebas tienen las siguientes características: procesador Intel Core I7 (3,60 Ghz), memoria RAM de 8GB, Disco duro de 1 Tera

2. Para el ambiente de pruebas se seleccionó como sistema operativo base la distribución Kali Linux de 64 bits. Donde desde este sistema operativo mirara los sistemas operativos de la empresa y la base de datos. La descarga realizada de la página oficial https://www.kali.org/downloads/

3. Sobre el sistema operativo Kali linux se instaló Oracle VM VirtualBox versión 5.2, para usar una máquina virtual donde se ejecuten las herramientas de pruebas. La máquina virtual tiene la siguiente configuración: procesador de 2 Core, 4 GB de memoria RAM, 20 GB de disco duro. Oracle VM VirtualBox fue descargado de la página oficial del fabricante https://www.virtualbox.org/

6.3 HERRAMIENTAS SELECCIONADAS PARA REALIZAR LAS PRUEBAS

Para la realización de las pruebas de las aplicaciones móviles fueron seleccionadas las siguientes herramientas

Tabla 4. Herramientas seleccionadas

HERRAMIENTA	DESCRIPCIÓN	LICENCIA
Kali Linux	Es una distribución de Linux derivada de Debian diseñada para análisis forense digital y pruebas de penetración.	Free
Nmap	Es un software de uso libre de código abierto que se utiliza para detectar puertos abiertos.	Free
Metasploit	Es un programa que sirve para explotar las vulnerabilidades de los equipos donde su fuerte es hacer penetraciones a las bases de datos.	Free
SQLMap	Esta herramienta se utiliza en inyección de SQL, para obtener listas y registros de las bases de datos.	Free
Nessus	Programa para el escaneo de vulnerabilidades, es categorizada como la mejor herramienta de seguridad de red, el cual nos permite identificar las debilidades y errores de configuración que pueden ser usados para ataques.	Free

Fuente: el autor

6.4 PLAN DE PRUEBAS

Para hallar las vulnerabilidades en los sistemas operativos y base de datos de la empresa ALDIM Acciones Logísticas en Distribución de Mercancías S.A.S., se debe diseñar, organizar e implementar una guía que contribuya a mantener el enfoque y objetivo del proceso, por esta razón, se ha creado un plan de pruebas basado en la penetración que ofrece las herramientas seleccionadas como lo es NMAP, Nessus, que se encuentran dentro del sistema operativo Kali Linux, el cual nos brinda una gran variedad de información sobre las vulnerabilidades encontradas y ver que permite hacer con ellas.

Tabla 5. Proceso plan de prueba

Paso	Objetivo	Proceso
Recopilación de información sobre la Aplicación	Reconocimiento de la aplicación para identificar la magnitud y alcance.	Encuesta sobre el proceso a desarrollar. 1. Nombre 2. Función 3. La herramienta es de licencia gratuita Si _____ No _____ 4. La herramienta necesita registrarse para su funcionamiento Si _____ No _____ 5. La herramienta es fácil de manejar Si _____ No _____ 6. Que necesita para que funcione la herramienta _____

Análisis estático	Identificación de vulnerabilidades de seguridad en las herramientas seleccionadas.	1. Configurar permisos sobre el sistema operativo a trabajar 2. Analizar con que herramienta se va a trabajar en cada punto a acceder 3. Configurar acceso a la red y a la base de datos.
Análisis dinámico	Identificación de vulnerabilidades de seguridad de la herramienta durante el proceso de ejecución de la misma.	1. Instalar, configurar y utilizar la herramienta. 2. Identifica la red que se va a vulnerar 3. Identifica la base de datos

Fuente: el autor

6.5 RESULTADOS OBTENIDOS EN LA EJECUCIÓN DE LAS PRUEBAS

Luego de instalar y configurar el ambiente de pruebas, se procede a desarrollar el plan de pruebas de seguridad sobre las herramientas seleccionadas y definidas previamente, los resultados obtenidos de este proceso se encuentran en el Anexo A. resultados ejecución de pruebas detallado por cada aplicación, allí se puede observar el resultado de cada una de los ítems evaluados para las herramientas.

6.6. ANÁLISIS DE LOS RESULTADOS

Finalizado el proceso de ejecución del plan de pruebas sobre cada una de las herramientas, los resultados obtenidos se organizan, consolidan y analizan los resultados de analizar la seguridad de la empresa ALDIM Acciones Logísticas en

Distribución de Mercancías S.A.S., para identificar vulnerabilidades que puedan afectar la información que posee en los sistemas operativos y base de datos; resultados se exponen a continuación:

El hallazgo encontrado en el área de informática, sobre el control de acceso al área de informática y el entorno físico, se encontró que no tiene ningún tipo de restricción, donde cualquier persona de la empresa puede acceder a la sala de informática donde está el sistema operativo de la empresa y la base de datos.

El hallazgo encontrado a la red de datos, se pudo comprobar que el ingreso al computador posee un protocolo de seguridad para acceder al sistema operativo, donde para poder ingresar al sistema operativo de la empresa a la persona se le solicita una clave alfa numérica de más de 8 caracteres, lo cual hace que las claves sean fuertes y difíciles de descifrar. Ya depende de cada usuario que al pararse de su puesto de trabajo cierre sesión para mantener la seguridad en el área de red de datos y área física con el fin de que ningún ente ajeno a la empresa haga algo indebido.

Los hallazgos encontrados con las herramientas de pentesting, se encontró que con la herramienta NMAP; que está incorporada en el sistema operativo de Kali Linux, se pudo hacer un escaneo a la IP donde están alojados la base de datos, y permite ver que puertos se encuentran abiertos, que servicios y aplicaciones están corriendo sobre ellos, en su mayoría puertos de comunicación (ver ilustraciones 41, 42, 43 y 44) donde cualquier persona ajena a la empresa y con conocimientos informáticos podría acceder a información.

Con el solo hecho de permitir hacer el escaneo y dar la información de que puertos tiene abiertos y mostrar su servicio que posee cada puerto se desarrollaría una

penetración al sistema, todos esos puertos en una computadora la hacen vulnerable y puede tener un alto potencial de ataque.

Tabla 6. Puertos principales vulnerados

PUERTO	PROTOCOLO	DESCRIPCIÓN
21	Puerto de FTP	Usado para la descarga de archivos al equipo.
23	Puerto Telnet	Protocolo usado para comunicación.
25	Puerto SMTP	Usado por los clientes de email para enviar correo electrónico.
80	Puerto HTTP	Es el usado por los navegadores para cargar las páginas web.
110 y 995	Puertos POP3	Usados por los clientes de email para la recepción del correo.
119	Puerto NNTP	Servidor de noticias.
139	NetBIOS	Usado para compartir servicios compartidos de impresoras y/o archivos.
443	Puerto HTTPS	Usado para la carga segura de páginas web.
445	MSFT DS	Server Message Block.
531	Puerto IRC	Usado para servicios de chat.
1527	tlisrv	Puerto para Oracle y SQL.
1723	PPTP	Virtual private network (VPN). Puerto usado para conectar equipos por medio de Red Privada Virtual.
3306	MySQL	Puerto para Mysql (Bases de datos)
4661, 4662, 4665		Puertos usados para Conexiones Peer to Peer como Emule y otros.

Fuente: el autor

Las asignaciones de los puertos se encuentran organizados mediante las reglamentaciones asignadas por la IANA[41] (Agencia de Asignación de Números de Internet) esta asignación la hacen mediante tres categorías o rangos donde se encontró puertos reservados, registrados y privados.

Tabla 7. Rangos de los puertos

Categoría	Descripción
0 - 1023	Se denominan puertos reservados para usos específicos que se encuentran reglamentados, el sistema operativo los abre para permitir su empleo por diversas aplicaciones mediante los llamados protocolos, por ejemplo: HTTP, FTP, TELNET, IRC, POP3, etc.
1024 – 49151	Se denomina "Registrados" estos puertos pueden ser usados por cualquier aplicación.
49152 – 65535	Se denominan "Dinámicos o privados", estos puertos los usa el sistema operativo cuando una aplicación tiene que conectarse a un servidor y se le realiza la solicitud de un puerto.

Fuente: el autor

La importancia de los puertos es que ellos son las puertas de la computadora, sin ellos gran cantidad de programas no podrían funcionar y hasta el mismo sistema operativo los necesita para poder trabajar, y la empresa no posee ningún firewall que sirva de protección, ni un sistema de monitoreo “snort”[42] que nos vaya informan resultado en tiempo real de lo ocurre en la red.

[41] IANA, Agencia de Asignación de Números de Internet [en línea], [diciembre 2017]. Disponible en Internet: https://www.iana.org/

[42] Snort. Sistemas de Detección de intrusos [en línea], diciembre2017]. Disponible en Internet: https://www.snort.org/

Muchos de esos puertos no se pueden cerrar, puesto que deben de estar abiertos para que haya comunicación entre los aplicativos que lo necesitan como es el caso del puerto 80 que pertenece al navegador y es necesario para tener acceso hacia internet, el puerto 21 que se usa para la descarga de archivos, el puerto 110 que se usa para que el correo funcione; entre otros; lo ideal sería un monitoreo constante de lo que sucede en la red y un firewall.

Con la herramienta SQLMAP; se le hizo una penetración a la base de datos y observar que esta no posee ningún tipo de seguridad, por el contrario, todos los datos están expuestos a que cualquier persona con nociones de informática (hacker) que pueda acceder a la información de la empresa.

Por medio de comandos se pudo hacer un escaneo a la base de datos y encontrar información sobre sus tablas creadas, las cuales están alojadas en la base de daos de la empresa, una vez estando dentro de las tablas se siguió la penetración para listas información sobre el contenido de cada una de ella, pero no fue posible que arrojara dicha información, debido a las políticas de seguridad que tiene registrada la base de datos.

Con la herramienta NESSUS, permitió hacer un escaneo de las vulnerabilidades a todo el sistema operativo, encontrar errores de configuración, puertos por donde se pueden vulnerar, fallos de software instalado. Una vez configurado la misma herramienta arroja un listado de vulnerabilidades donde las clasifica y mide el riesgo que puede tener cada una de ellas, además permite clasificarla en un rango de bajo, medio y alto las vulnerabilidades; la misma herramienta da un informe detallado de lo que hace cada vulnerabilidad y como podría solucionarse dicha vulnerabilidad, error o falla del sistema.

7 PERSONAS QUE PARTICIPAN EN EL PROCESO

En el desarrollo del presente proyecto aplicado para la empresa ALDIM Acciones Logísticas en Distribución de Mercancías S.A.S. para culminar el proceso se necito una serie de personas con las cuales tuvo interacción para poder llevarlo a cabo y lograr su totalidad de lo planteado.

El rol de investigador, que es la persona encargada de hacer toda la investigación, consultas e informe sobre el desarrollo de todo el proyecto, además se tiene el rol de director que es el encargado de guiar y dirigir al investigador del camino que debe tomar el proyecto y delimitaciones sobre el mismo.

Tabla 8. Personas que intervienen en el proyecto

Rol	Datos personales
Investigador	Diego Fernando Cadavid Romero, Ingeniero de Sistemas y Telemática, estudiante de la especialización en seguridad informática de la UNAD, con experiencia en el área logística del sector de transporte.
Director	Ing. Gabriel Mauricio Ramírez Villegas, Magister en Educación Virtual, Phd(C) Ciencias de la Electrónica y docente de la UNAD.

Fuente: el autor

8 RECURSOS NECESARIOS PARA EL DESARROLLO

8.1 RECURSO HUMANO

El proyecto lo llevara a cabo en su totalidad el estudiante de la especialización en seguridad informática Diego Fernando Cadavid Romero, en un lazo de 14 semanas.

8.2 RECURSO FÍSICO Y FINANCIERO

En la siguiente tabla se describe el recurso físico y financiero que se requiere para llevar a cabo el proyecto, igualmente se ilustra la fuente de financiación.

Tabla 9. Recurso físico y financiero

Cantidad	Recurso Físico	Valor
Recurso tecnológico		
1	Equipo de cómputo, core i7-4790 3.60 GHz, 8 Gb en RAM, 1 Tera en Disco duro	$3.000.000
1	Impresora HP Laserjet P1102w	$550.000
1	Toner Impresora	$350.000
1	Disco Duro externo de 500 GB	$150.000
1	Internet	$250.000
	Subtotal	**$4.300.000**
Recurso material		
1	Papelería	$100.000

	Subtotal	**$100.000**
	Total Recurso Financiero	**$4.400.000**

Fuente: El autor.

8.3 RECURSO TÉCNICO

Herramientas de Pentesting: Nmap, Metasploit, Nessus, Kali Linux

9 CRONOGRAMA DE ACTIVIDADES

Tabla 10. Cronograma de actividades.

Actividad Planteada	Semana													
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**
Inicio de Proyecto aplicado	X													
Revisión observaciones planteadas por tutor		X												
Planeamiento trabajo en sitio			X											
Recolección de información				X										
Aplicación Pentesting a sistema operativo y base de datos					X									
Sistematización de resultados						X								
Análisis de resultados							X	X						
Redacción del Documento									X	X				
Presentación Documento al tutor para revisión											X			
Corrección del documento												X		

Entrega del documento final al tutor del curso													X	
Entrega del documento en versión digital o impreso para la evaluación del jurado														X

Fuente: El autor.

10 INFORME DE VULNERABILIDADES Y RECOMENDACIONES

La red de empresa ALDIM Acciones Logísticas en Distribución de Mercancías S.A.S., no presenta ningún grado de complejidad para la administración y control de seguridad informática. A continuación, se presentarán las vulnerabilidades y recomendaciones que se le sugieren a la empresa para mejorar su seguridad en sus sistemas operativos y base de datos.

DIRECTIVAS Y PERSONAL DE LA EMPRESA

Tabla 11. Recomendación Directiva y Personal

PROCESO	RECOMENDACIÓN
Concientizar a los empleados de la empresa de la importancia que tiene la manipulación y confidencialidad de la información.	Los funcionarios y empleados adquieren las responsabilidades y cuidados que se deben tener al manipular información confidencial de la empresa.
Todas las claves y privilegios que tienen los empleados de la empresa deben ser bloqueados a la hora que se termine el contrato de forma definitiva.	En caso que el contrato termine en malos términos se debe impedir que el afectado despedido manipule la información.
Prohibir cualquier actividad de personal no autorizado en las áreas donde hay información y acceso a los equipos de cómputo.	Se evitará daños en los equipos ya sea por derramamiento de líquidos o comida sobre ellos provocando la pérdida del equipo y de la información, además se evitará que personal no

	autorizado pueda acceder a la información de los usuarios.
Los empleados de la organización que ejercen funciones en los sistemas de información deberán ser capacitados periódicamente en materia de seguridad.	El departamento de seguridad informática deberá difundir las políticas de seguridad implementadas por la empresa a todos los empleados en general.
Los usuarios de la empresa que tienen correo electrónico deberán conocer la importancia del uso del mismo, ya que, si no le damos un buen uso, se puede ser víctima de virus por descargas de archivos adjuntos.	Los empleados deberán tomar conciencia del uso del correo electrónico, del riesgo a que están expuestos por el mal uso del mismo, solo se deberá utilizar para intercambiar información exclusiva de la empresa.
Es necesario que los empleados tengan claro los aspectos de integridad, disponibilidad y confiabilidad de los bienes y servicios de la entidad.	Los empleados deberán adquirir el compromiso al momento de ser contratados de proteger y salvaguardar los activos informáticos, ya que es lo más valiosos que posee la organización y así se evitaran fugas de información.

Fuente: el autor

BASE DE DATOS

Como resultados de las pruebas se identificaron las siguientes vulnerabilidades a la base de datos:

Tabla 12. Recomendación a la Base de datos

PROCESO	RECOMENDACIÓN
Algunos usuarios cuentan con políticas de contraseñas débiles. • **Permite asignar contraseñas iguales al nombre de usuario fáciles de identificar.** • **No cuenta con la longitud mínima de caracteres.** • **Para la construcción de la contraseña no cuenta con criterios de asignación de caracteres especiales como condición obligatoria.**	Se recomienda establecer políticas más fuertes en la definición de contraseñas, contar con una longitud mínima, no asignar el mismo nombre de usuario a la clave y asignar un mínimo de caracteres especiales
Usuarios en desuso	Se requerirá contar con tareas periódicas de monitoreo de la base de datos para identificar usuarios en desuso.
La información contenida en las bases de datos deberá ser usada únicamente para asuntos relacionados con actividades de la empresa.	Los funcionarios y empleados deben dar buen uso a la información de las bases de datos y no utilizarla para su beneficio personal que no tiene nada que ver con la actividad de la empresa.
Todos los datos de gran importancia deberán ser respaldados y almacenados en un lugar seguro.	El departamento de sistemas deberá estar pendiente de realizar copias de respaldo de la información más importante de la empresa, ya que de esta forma se protegerá la información

	y en caso de desastre se pueda recuperar.
La información contenida en las bases de datos solo la podrá utilizar y modificar el personal autorizado.	Se deberá crear una política de control de acceso la cual debe ser gestionada por el administrador de base de datos.
Incorporar a la base de datos un proceso que registre todos los accesos y las actividades realizadas.	Actualizar las bases de datos, de esta forma la empresa contara con un historial de acceso a las bases de datos de los empleados en caso de un uso inadecuado de la información.
Implementar una política que administre y controle la eliminación de información de la base de datos que ya no sea necesaria.	La base de datos no se recargará con información innecesaria y serán más rápidas las consultas.

Fuente: el autor

INFRAESTRUCTURA Y RED

Tabla 13. Recomendación Infraestructura y red

PROCESO	RECOMENDACIÓN
Socializar los procedimientos de prevención y mitigación de los riesgos informáticos.	Difundir las políticas de riesgos tanto a las directivas como a los empleados de las diferentes áreas de la empresa, para prevenir futuros desastre en la red que puedan conllevar a la perdida en la información por culpa de ignorancia o desconocimiento de las políticas de

	seguridad informática implementada por la organización.
Cumplir con todas las políticas de seguridad establecidas por la organización.	El departamento de seguridad informática está encargado, de que todos los empleados cumplan con las políticas de seguridad implementadas, para evitar riesgos informáticos, que puedan ocasionar daño a la red y fuga de su información.
Actualizar el cronograma de mantenimiento de equipos preventivo y correctivo.	La empresa deberá realizar un cronograma de mantenimiento periódico a los equipos, así se evitará futuros daños en los computadores y la red será más eficiente.
Se cuenta con un antivirus que no realiza una buena protección a los equipos, en ocasiones se pierde información por la existencia de código malicioso.	La empresa deberá establecer un plan de protección del registro, establecer procedimientos de detención, prevención y corrección de software malicioso (Virus, troyanos, spyware, etc.), actualizando el sistema operacional y el antivirus periódicamente.
Mejorar la seguridad física, el ingreso de personal no autorizado.	La empresa deberá hacer cumplir la política de control de acceso a las instalaciones, definir el perímetro de seguridad física, establecer mecanismos de protección contra amenazas externas y personal no

	autorizado en las diferentes áreas de la entidad.
Los equipos que no estén en uso deberán ser almacenados en un lugar seguro donde se restrinja el acceso al personal no autorizado.	Se deberán destruir los equipos almacenados y que ya no son útiles, para evitar la pérdida o sustracción de la información que pueda ocasionar daño a la entidad.
Los equipos de cómputo serán asignados a un responsable para evitar el uso inadecuado del mismo.	Así se mejorará la administración y mantenimiento de los recursos informáticos de la organización.
El área de sistemas es la encargada de realizar los diferentes mantenimientos preventivo y correctivo de los quipos de cómputo.	Para evitar deterioro de los equipos y una mala manipulación por personal no calificado.
Se deberá establecer controles de acceso en áreas donde se ubican los servidores y equipos de comunicación de la empresa.	De esta forma se llevará un control de quien y a qué hora ingresa el personal autorizado a estas áreas.
Las contraseñas usadas para la configuración de equipos de red y telecomunicaciones deberán estar basadas en un estándar que defina aspectos como: estructura, tiempo de validez y reusabilidad.	La utilización de contraseñas fuertes y difíciles de descifrar evitara el acceso no autorizado de personal a los equipos y a la información confidencial de la empresa.
El personal que realiza trabajos de configuración de los dispositivos de red deberá poseer una certificación que avale sus capacidades.	El personal que manipule, configure y repare los equipos deberán estar calificados debidamente para que no comprometan la seguridad de la red.

Se deberá llevar un documento que registre todas las configuraciones que se realicen sobre los dispositivos de red, debidamente codificados e identificados.	Facilitará y agilizará el proceso de reparación o mantenimiento de los dispositivos de Red.
Los puertos que no estén en uso deberán ser bloqueados adecuadamente.	De esta forma se evitarán accesos internos y externos de personal no autorizado a la red que puedan ocasionar daños y la manipulación de la información.
El acceso a Internet será restringido, solo para realizar labores propias de la empresa.	Se deberán de bloquear algunas páginas de internet que no son necesarias para el desarrollo de la actividad de la empresa, para que los trabajadores no puedan acceder y empleen su tiempo más eficientemente en actividades propias de la empresa.
Deberá cifrarse la información que circule a través de la red.	Evitará que personal no autorizado puedan acceder a la información confidencial que circula a través de la red y la puedan manipular en contra de la organización.

Fuente: el autor

UTILIZACIÓN DEL SOFTWARE

Tabla 14. Recomendación uso del software

PROCESO	RECOMENDACIÓN
La instalación de software en el equipo deberá ser instalado solo por el personal del área de sistemas autorizado.	Los usuarios no podrán instalar programas que no sean de la organización para realizar su trabajo diario, ya que pueden poner en riesgo los equipos y la seguridad de la red de datos.
Todos los equipos deberán tener configurado la opción de cierre de sesión después de un lapso de inactividad.	Se preverá que usuarios no autorizados puedan acceder, modificar o borrar información confidencial, mientras el usuario no está en su sitio de trabajo.
Crear una política de revisión periódica del funcionamiento del software.	Se mejorará la vida útil, el rendimiento de los equipos, la seguridad en la red y se actualizara el software que ya no es eficiente.
Se permitirá únicamente instalar software licenciado a los equipos.	Se borrará el software inútil y se dará buen uso de los recursos informáticos utilizando únicamente el software licenciado, así se mejorará la seguridad de la red y se evitará la propagación de virus informáticos.
Todo software nuevo antes de ser instalado en el equipo deberá ser probado y evaluado.	De esta forma se evitará un software defectuoso que pueda modificar la información o bloquee los equipos de la

	entidad y la red de datos será más eficiente y segura.

Fuente: el autor

CONCLUSIONES

Finalizado el análisis de los resultados de las pruebas de seguridad ejecutadas se puede concluir que el objeto de estudio del presente proyecto aplicado ha sido cumplido, se pudo dar solución al problema planteado de analizar la empresa para encontrar las vulnerabilidades del sistema operativo y base de datos de la empresa ALDIM Acciones Logísticas en Distribución de Mercancías S.A.S.

Se pudo identificar que la empresa ALDIM Acciones Logísticas en Distribución de Mercancías S.A.S. durante todo el proceso del proyecto se encontró que posee vulnerabilidades como cualquier otra empresa que no contiene seguridad informática (sistema operativo y base de datos), ni en su infra estructura, a la empresa se le puede hacer penetración y encontrar puertos que alguien con mayor conocimiento del tema pueda aprovechar y acceder a información que es vital para la empresa.

Es importante que la empresa implante un sistema de monitoreo que permita ver en tiempo real lo que está ocurriendo en la red y si es posible instalar y configurar un firewall que permita detener cualquier posible ataque a las vulnerabilidades que la empresa posee para llegar a prevenir un siniestro.

La empresa debe estar más involucrada en cumplir y divulgar el cumplimiento de las políticas de seguridad implementadas por la empresa, además debe definir la forma clara los procesos y roles a las personas responsables del departamento de seguridad informática.

La empresa debe invertir en recurso económico periódicamente para que todo el personal de la empresa reciba una adecuada capacitación y actualización en

materia de seguridad informática y de los riesgos a que está expuesta toda la empresa, además de sus sistemas operativos y la base de datos. Todo el personal de la empresa tanto interno como externo que manipule información confidencial y sensible de la empresa, debe comprometerse a protegerla, para evitar fugas de información, la cual pueda ser utilizada indebidamente.

Los resultados obtenidos en el presente proyecto aplicado la puerta para que la comunidad académica de la UNAD continúe el desarrollo de proyectos futuros que aporten a mejorar la seguridad en la empresa ALDIM Acciones Logísticas en Distribución de Mercancías S.A.S., se proponen temas como: estándares de calidad tales como ITIL, COBIT, ISO entre otros.

BIBLIOGRAFÍA

ROUSE, Margaret. Prueba de penetración (pen test) [en línea], [septiembre de 2017]. Disponible en Internet: http://searchdatacenter.techtarget.com/es/definicion/Prueba-de-penetracion-pen-test

WIKIPEDIA, La Enciclopedia Libre. Vulnerabilidad [en línea], [septiembre de 2017]. Disponible en Internet: https://es.wikipedia.org/wiki/Vulnerabilidad#cite_note-2

SIGNIFICADOS.COM. Hacker [en línea], [septiembre de 2017]. Disponible en Internet: https://www.significados.com/hacker/

SER INFORMÁTICA, Computer Solutions Company. La importancia del respaldo de la información [en línea], 8 septiembre del 2015 [noviembre 2017]. Disponible en Internet: https://serinformatica.com.ar/actualidad/la-importancia-del-respaldo-de-informacion/

SEGUINFO2012, Timeline. Historia de la seguridad informática [en línea], [noviembre de 2017]. Disponible en Internet: https://www.timetoast.com/timelines/historia-de-la-seguridad-informatica—2

SGSI. Blog especializado en Sistemas de Gestión de Seguridad de la Información. ISO 27001: ¿Qué significa la Seguridad de la Información [en línea], [noviembre de 2017]? Disponible en Internet: http://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/

LUZARDO, Iván. conozca las amenazas informáticas más comunes (DISI 2010) [en linea], [noviembre de 2017]. Disponible en Internet: http://www.enter.co/chips-bits/seguridad/conozca-las-amenazas-informaticas-mas-comunes-disi2010/

ESET. Definición de virus, códigos maliciosos y ataques remotos, consultado en noviembre 21017, disponible en: https://support.eset.com/kb186/?viewlocale=es_ES

LÓPEZ, David. Evolución de la Seguridad Informática [en línea], [noviembre 2017]. Disponible en Internet: https://www.grupocontrol.com/evolucion-de-la-seguridad-informatica

BRADLEY, Tony. Introduction to Intrusion Detection Systems (IDS) [en línea], agosto 13, 2017 [noviembre 2017]. Disponible en Internet: https://www.lifewire.com/introduction-to-intrusion-detection-systems-ids-2486799

TECHOPEDIA. Intrusion Prevention System (IPS) [en línea], [noviembre 2017]. Disponible en Internet: https://www.techopedia.com/definition/15998/intrusion-prevention-system-ips

CANDYTRAPS. ¿Qué es un honeypot? [en línea], [noviembre 2017]. Disponible en Internet: https://candytraps.wordpress.com/que-es-un-honeypot/

SHUTTERSTOCK. ¿Qué es un SIEM? [en línea], enero 10 de 2016 [noviembre 2017]. Disponible en Internet: https://www.tripwire.com/state-of-security/incident-detection/log-management-siem/what-is-a-siem/

AREATECNOLOGIA. Sistemas Operativos [en línea], [noviembre 2017]. Disponible en Internet: http://www.areatecnologia.com/sistemas-operativos.htm

VALDÉS, Damián P. ¿Qué son las bases de datos? [en línea], octubre 26 2007 [noviembre 2017]. Disponible en Internet: http://www.maestrosdelweb.com/que-son-las-bases-de-datos/

PRANDINI, Patricia. Vulnerabilidades, amenazas y riesgo en “texto claro” [en línea], mayo 25 2013 [noviembre 2017]. Disponible en Internet: http://www.magazcitum.com.mx/?p=2193#.WhNW41WWaM8

UNIVERSIDAD NACIONAL DE LUJAN. Departamento de Seguridad Informática. Amenazas a la Seguridad de la Información. Recopilado de: http://www.seguridadinformatica.unlu.edu.ar/?q=node/12

CARRMEN. Seguridad informática [en línea], [noviembre de 2017]. Disponible en Internet: https://carrmen.jimdo.com/riesgo-informatico/

URREGO, Jonatán. Tipos de ataque y cómo prevenirlos [en línea], mayo 1, 2013 [noviembre 2017]. Disponible en Internet: https://colombiadigital.net/actualidad/articulos-informativos/item/4801-tipos-de-ataque-y-como-prevenirlos.html

PÉREZ, Ignacio. Comprendiendo la vulnerabilidad XSS (Cross-site Scripting) en sitios web [en línea], abril 29 2015 [noviembre 2017]. Disponible en Internet: https://www.welivesecurity.com/la-es/2015/04/29/vulnerabilidad-xss-cross-site-scripting-sitios-web/

GARCÍA, Juan. Qué es un ataque por fuerza bruta [en línea], mayo 7 del 2013 [noviembre 2017]. Disponible en Internet: http://faqoff.es/que-es-un-ataque-por-fuerza-bruta/

OWASP. Inyección de Código [en línea], julio 30 2015 [noviembre 2017]. Disponible en Internet: https://www.owasp.org/index.php/Inyecci%C3%B3n_de_C%C3%B3digo

ROUSE, Margaret. Ataque de denegación de servicio (DDoS) [en línea], noviembre 2012 [noviembre 2017]. Disponible en Internet: http://searchdatacenter.techtarget.com/es/definicion/Ataque-de-denegacion-de-servicio

BORTNIK, Sebastián. ¿Qué es la fuga de información? [en línea], abril 13 de 2010 [noviembre 2017]. Disponible en Internet: https://www.welivesecurity.com/la-es/2010/04/13/que-es-la-fuga-de-informacion/

AVAST. Qué es el phishing [en línea], [noviembre 2017]. Disponible en Internet: https://www.avast.com/es-es/c-phishing

MUÑOZ, Ana. ¿Qué es spoofing? [en línea], septiembre 2016 [noviembre 2017]. Disponible en Internet: http://computerhoy.com/noticias/software/que-es-spoofing-51236

INFOBAE. El scam, otra forma de estafar ingenuos [en línea], septiembre 10 de 2005 [noviembre 2017]. Disponible en Internet: https://www.infobae.com/2005/09/10/208271-el-scam-otra-forma-estafar-ingenuos/

ENTER.CO. La ingeniería social: el ataque informático más peligroso [en línea], julio 25 de 2016 [noviembre 2017]. Disponible en Internet: http://www.enter.co/guias/lleva-tu-negocio-a-internet/ingenieria-social/

PANDASECURITY. ¿Qué es un troyano? [en línea], diciembre 10, 2013 [noviembre 2017]. Disponible en Internet: https://www.pandasecurity.com/spain/mediacenter/consejos/que-es-un-troyano/

ADMINSO. Medidas de seguridad en los sistemas operativos [en línea], [noviembre 2017]. Disponible en Internet: http://www.adminso.es/index.php/4._Medidas_de_seguridad_en_los_sistemas_inform%C3%A1ticos

LEMMO, Gianfranco. ¿Qué es un Pentest? [en línea], marzo 15 del 2017 [consultado en junio de 2017], disponible en internet: https://www.webbizarro.com/noticias/2658/que-es-un-pentest/

INFORMÁTICA HOY. Que es Hardware y Software [en línea], [consultado en junio 2017], disponible en internet: http://www.informatica-hoy.com.ar/aprender-informatica/Que-es-Hardware-y-Software.php

PARAÍSO LINUX. “Que es y cómo usar NMAP”, consultado en octubre 2017, retomado de https://paraisolinux.com/que-es-y-como-usar-nmap/

DRAGONJAR. SQLMap – Herramienta Automática de Inyección SQL [en línea], [noviembre 2017]. Disponible en Internet: http://www.dragonjar.org/sqlmap-herramienta-automatica-de-inyeccion-sql.xhtml

GB-ADVISORS, Nessus Escáner de Vulnerabilidad [en línea], [noviembre 2017]. Disponible en Internet: https://www.gb-advisors.com/es/gestion-de-vulnerabilidades/nessus-escaner-vulnerabilidad/

ALDIM Acciones Logísticas En Distribución De Mercancías S.A.S., tomado del interior de la empresa

CÓDIGO PENAL. Ley 1273 de 2009 De la Protección de la Información y de los Datos. Colombia, 2009. Ministerio de la Información y las Comunicaciones de Colombia, disponible en http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

CÓDIGO PENAL. Ley 1581 de 2012. la protección de datos personales, 2012. Disponible en la URL, http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

KALI LINUX. Nuestra distribución más avanzada de pruebas de penetración [en línea], 2017. Disponible en internet: https://www.kali.org/

NMAP ("Network Mapper"), [en línea], 2017. Disponible en internet: https://nmap.org/

MARDELBIT y CREANGEL. Que es y cómo usar NMAP [en línea], marzo 29 del 2010 [consultado en junio 2017], disponible en internet: https://paraisolinux.com/que-es-y-como-usar-nmap/

VERGARA, Kervin. Seguridad informática: principios básicos y software [en línea], mayo 27 del 2007 [consultado en junio 2017]. Disponible en internet: http://bloginformatico.com/seguridad-informatica-principios-basicos-y-software.php

CAITORA, Fernando. Penetration Test, ¿en qué consiste? [en línea], julio 24 del 2012 [consultado en junio 2017], disponible en internet: https://www.welivesecurity.com/la-es/2012/07/24/penetration-test-en-que-consiste/

EMPRENDE PYME. Tipos de riesgos empresariales [en línea], [noviembre 2017]. Disponible en Internet: https://www.emprendepyme.net/tipos-de-riesgos-empresariales.html

IANA, Agencia de Asignación de Números de Internet [en línea], [diciembre 2017]. Disponible en Internet: https://www.iana.org/

Snort. Sistemas de Detección de intrusos [en línea], diciembre2017]. Disponible en Internet: https://www.snort.org/

ACIS, “Asociación Colombiana de Ingenieros De Sistemas”. Lista de Empresas de Seguridad Informática [en línea], [diciembre 2017]. Disponible en Internet: http://acis.org.co/portal/content/lista-de-empresas-de-seguridad-inform%C3%A1tica-en-colombia

ANEXO A. RESULTADOS EJECUCIÓN DE PRUEBAS

1. IDENTIFICACIÓN DE LA INFORMACIÓN PARA EL DESARROLLO DEL PROYECTO

Se realizaron entrevistas, charlas, reuniones e inspección visual en los puestos de trabajo con el ingeniero que administra la red y demás personal de la empresa para identificar las posibles vulnerabilidades a las que esta es puesta la red de datos de la organización.

Además, se identificaron algunas de las políticas de seguridad:

1. Seguridad de la Información: realiza la creación de usuarios donde se definen las acciones permitidas para cada usuario, tipo de acceso a qué objetos y sobre que esquema.
2. Seguridad de Usuarios: Cada usuario tiene un nombre de usuario definido, con rol y/o perfil específico definido para cada sistema. De acuerdo al rol y/o perfil de cada usuario se asigna la respectiva política a regir en él; cada usuario es responsable de su contraseña ya que esta es personal e intransferible.

   Los usuarios están divididos en los siguientes grupos: Usuario de Consulta, Usuario Administrado y Usuario Desarrollador – Pruebas.
3. Listado de usuarios con su respectivo estado, rol y permisos asignados.
4. Administración de Contraseñas: Para la asignación de usuarios y contraseñas tiene un procedimiento general, donde el jefe de área tiene conocimiento de todo el personal con perfil.

2. IDENTIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN QUE CONFORMAN LA RED DE DATOS DE LA EMPRESA

En Guadalajara de Buga se encuentra la sede, en la cual se encuentra una oficina para el departamento de sistemas, encargada de mantener el sistema de red funcionando, en ella se identificaron los activos de información de la red de datos de la entidad.

Identificación de activos de información

Tabla 15. Activos de Información

Activo	Tipo de Activo
Terminal de Usuario	Hardware
Base de datos	Software
Computador de Escritorio	Hardware
Router	Red
Empleados	Personal
Antivirus	Software
Modem	Hardware
Fuente de alimentación	Hardware
Programas	Software

Fuente: El autor.

3. HERRAMIENTAS DE SOFTWARE UTILIZADAS PARA EL DESARROLLO DEL ANALISIS DE LA RED DE DATOS

3.1. HERRAMIENTAS DE SOFTWARE UTILIZADAS

Para la realización de las pruebas de seguridad se utilizaron las siguientes herramientas:

Herramientas de software Pentesting: Es una herramienta que sirve para evaluar la seguridad de las redes, sistemas de computación y aplicaciones involucradas en los mismos, para poder descubrir las vulnerabilidades en el sistema estudiado.

Programa NMAP: Es un software de uso libre de código abierto que se utiliza para detectar puertos abiertos.

Herramienta SQLMAP: Esta herramienta se utiliza en inyección de SQL, para obtener listas y registros de las bases de datos.

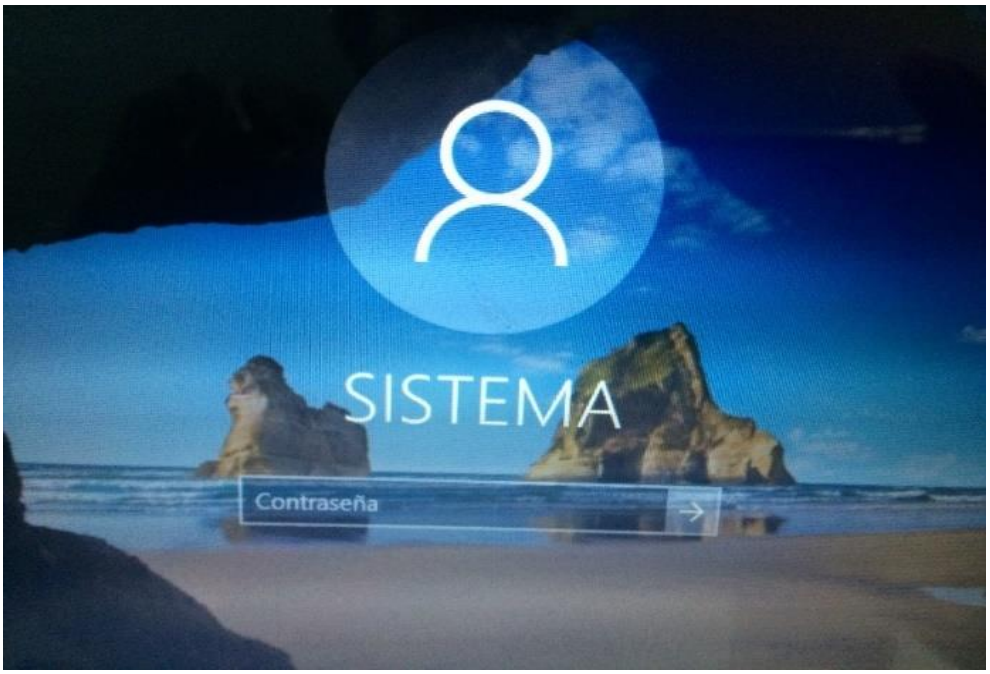
3.2. PRUEBAS DE DETECCIÓN DE VULNERABILIDADES A LA RED DE DATOS

3.2.1. Pruebas de contraseña valida y nombre de usuario incorrecto.

Contraseña valida

En las figuras se puede visualizar que al escribir la contraseña correcta la terminal permite el acceso a los programas y aplicativos del sistema.

Ilustración 1. Terminal del usuario

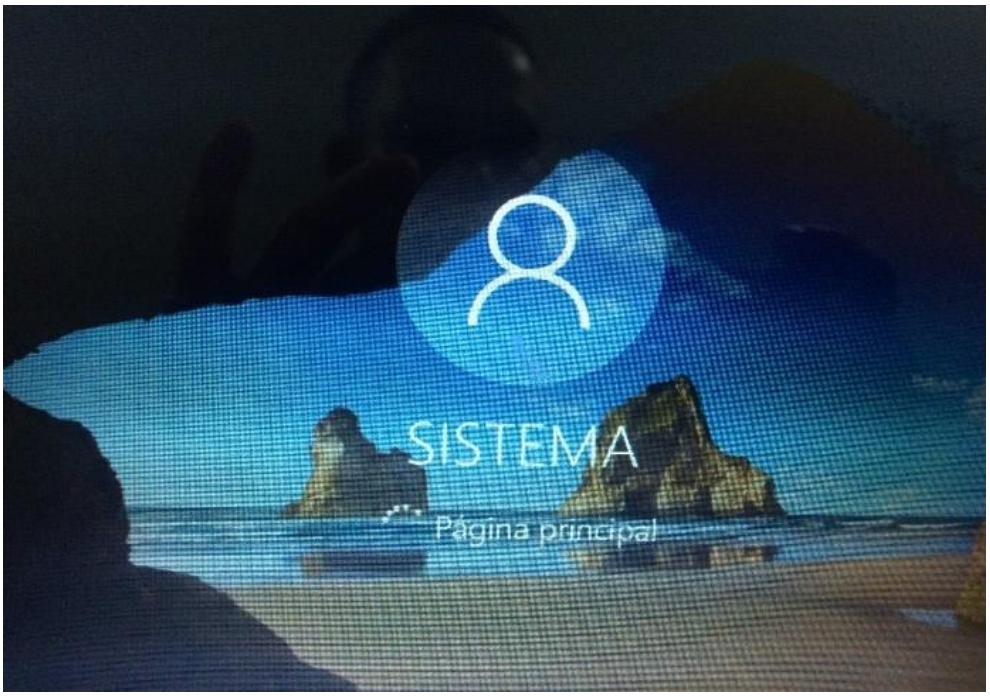


Fuente: El autor.

Ilustración 2. Contraseña de usuario

Fuente: El autor.

Ilustración 3. Inicio a la plataforma

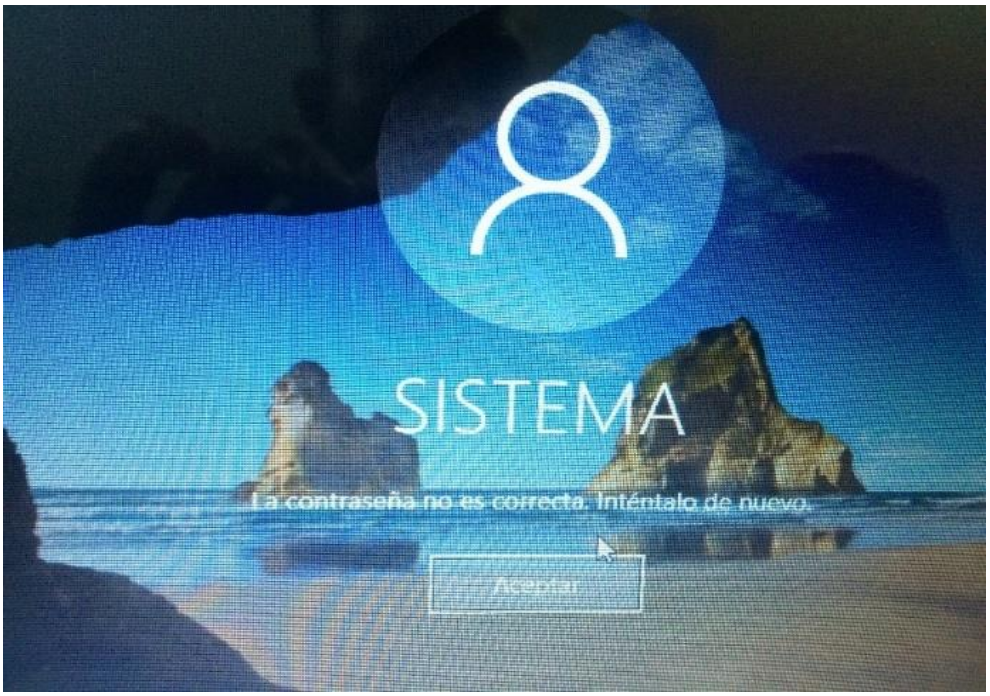


Fuente: El autor.

En las figuras se puede observar que la contraseña tiene más de 8 caracteres, numéricos, letras y alfanuméricos lo cual determina que las contraseñas son fuertes y difíciles de descifrar.

Contraseña incorrecta

Ilustración 4. Contraseña incorrecta



Fuente: el autor

En las figuras se puede observar que al escribir la contraseña de usuario incorrecta la terminal no permite el acceso a los aplicativos.

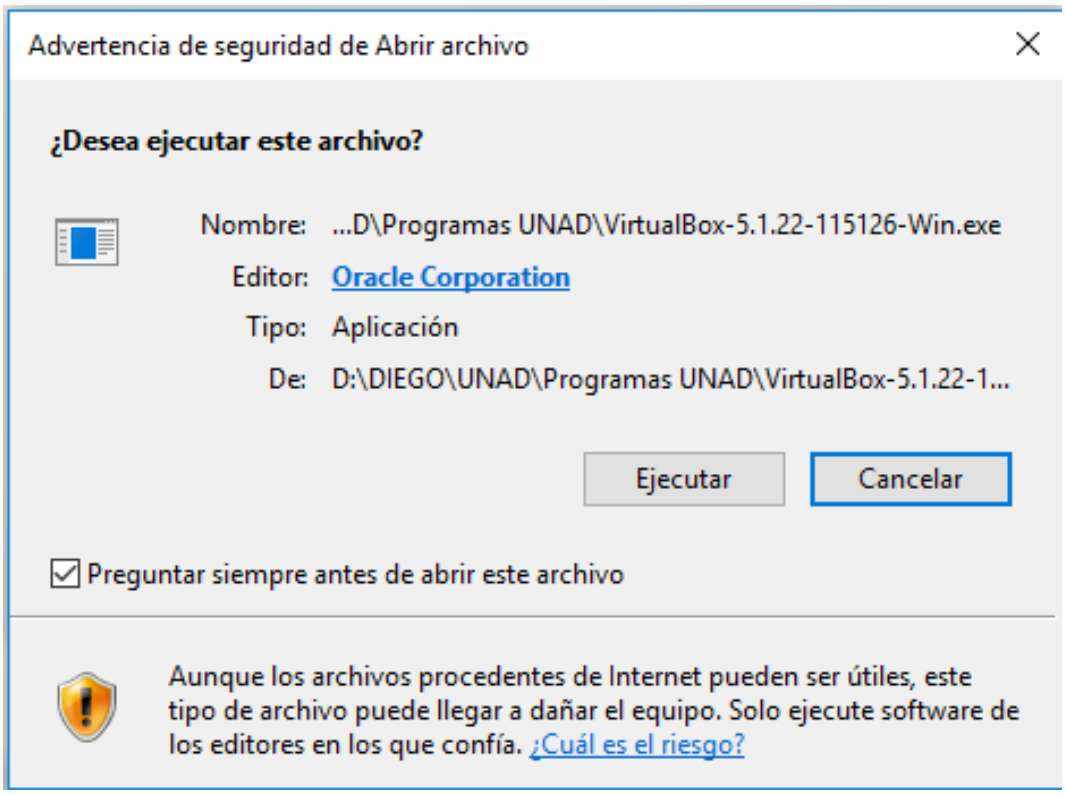
La contraseña tiene más de 8 caracteres, numéricos, letras y alfanuméricos lo cual determina que las contraseñas son fuertes y difíciles de descifrar.

4. INSTALACIÓN Y CONFIGURACIÓN DEL AMBIENTE DE TRABAJO

4.1. INSTALACIÓN DEL APLICATIVO VIRTUALBOX

El primer paso será arrancar el programa de instalación, para ello hacer doble clic en el fichero VirtualBox-5.1.22-115126-Win.exe desde don lo hallamos descargado.

Ilustración 5. Instalación VirtualBox



Fuente: el autor

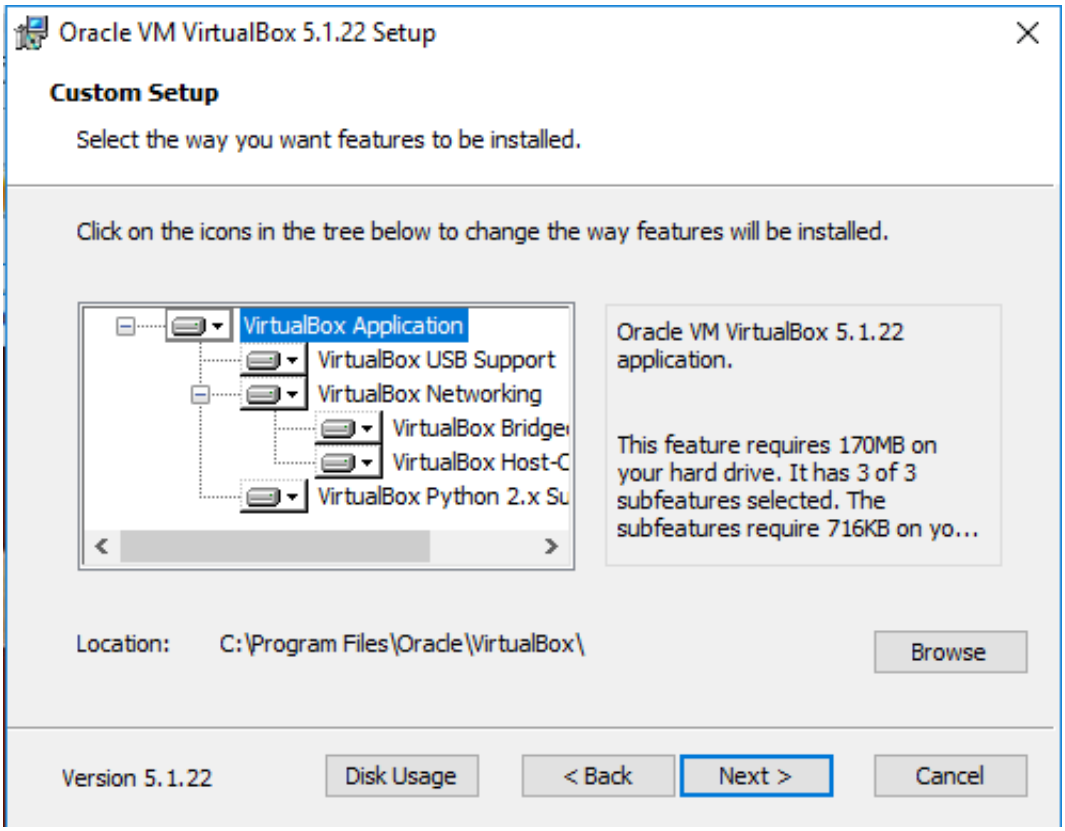
Luego nos aparecerá una ventana del asistente de instalación. Como se puede ver el asistente de instalación aparece en ingles pero el programa Oracle VirtualBox está en español.

Ilustración 6. Asistente de instalación del VirtualBox

Fuente: el autor

Pulsamos el botón next para continuar. En la siguiente ventana del asistente nos aparece en forma de árbol la información de las características de Oracle VirtualBox que se van a instalar.

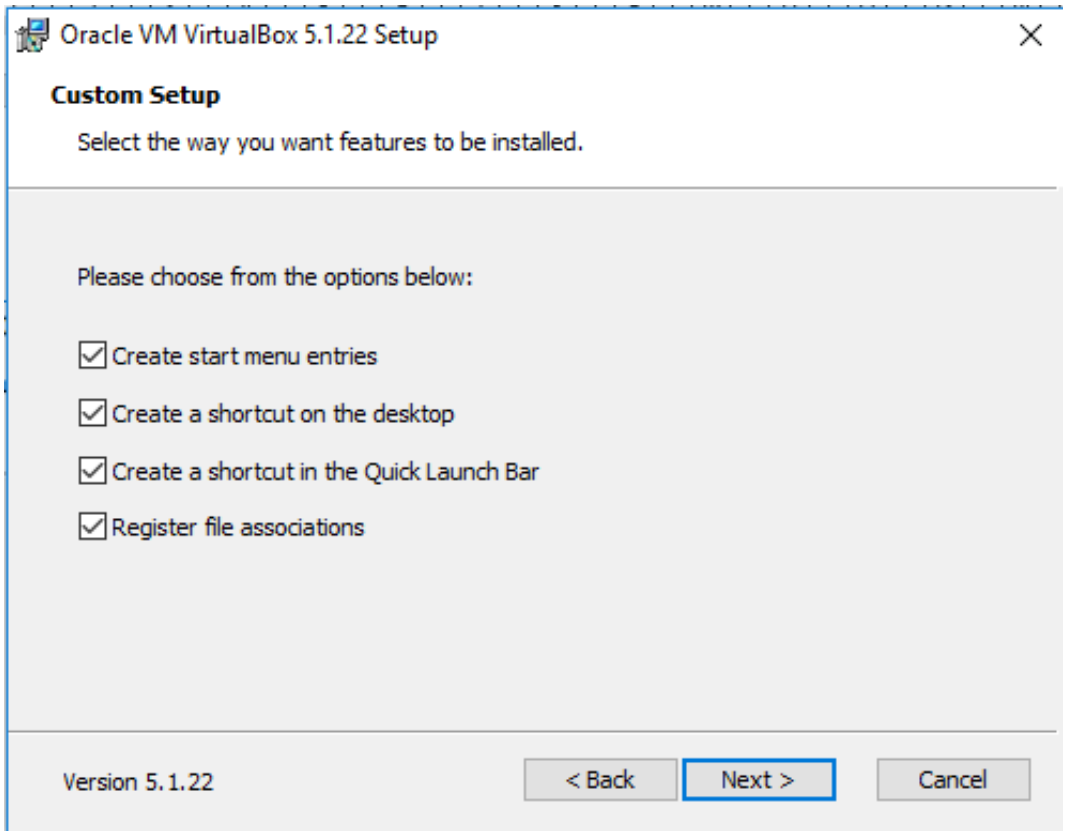
Ilustración 7. Características del VirtualBox



Fuente: el autor

Las opciones que aparecen en la ventana siguiente del asistente vienen marcadas por defecto, donde nos dice que va a crear un acceso directo en el escritorio del ejecutable de Oracle VirtualBox, que creara un acceso directo en la barra de inicio rápido, etc., se puede seleccionar la que queramos que nos instale los accesos directos.

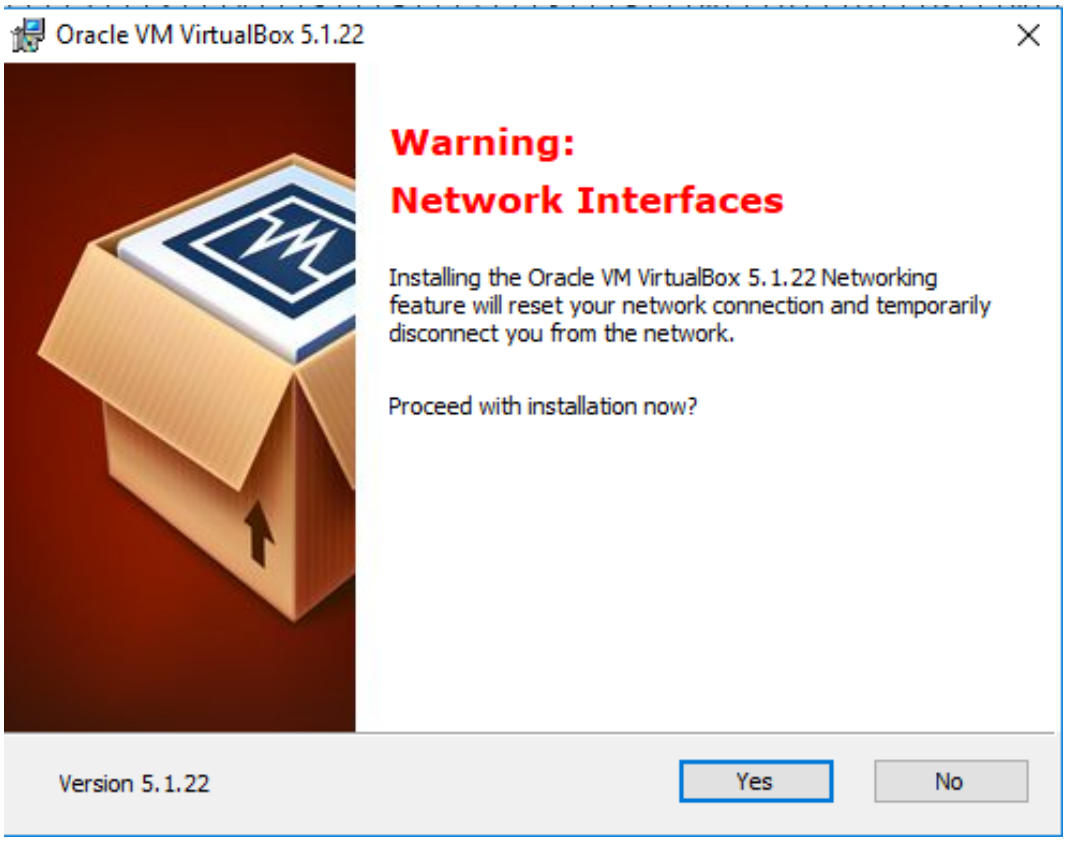
Ilustración 8. Opciones de instalación del VirtualBox



Fuente: el autor

Pulsamos el botón siguiente para continuar. En este punto el asistente de instalación de Oracle VirtualBox realiza la instalación de las características de red, esta operación deshabilitará temporalmente los servicios de red, pulsamos el botón Yes para continuar.

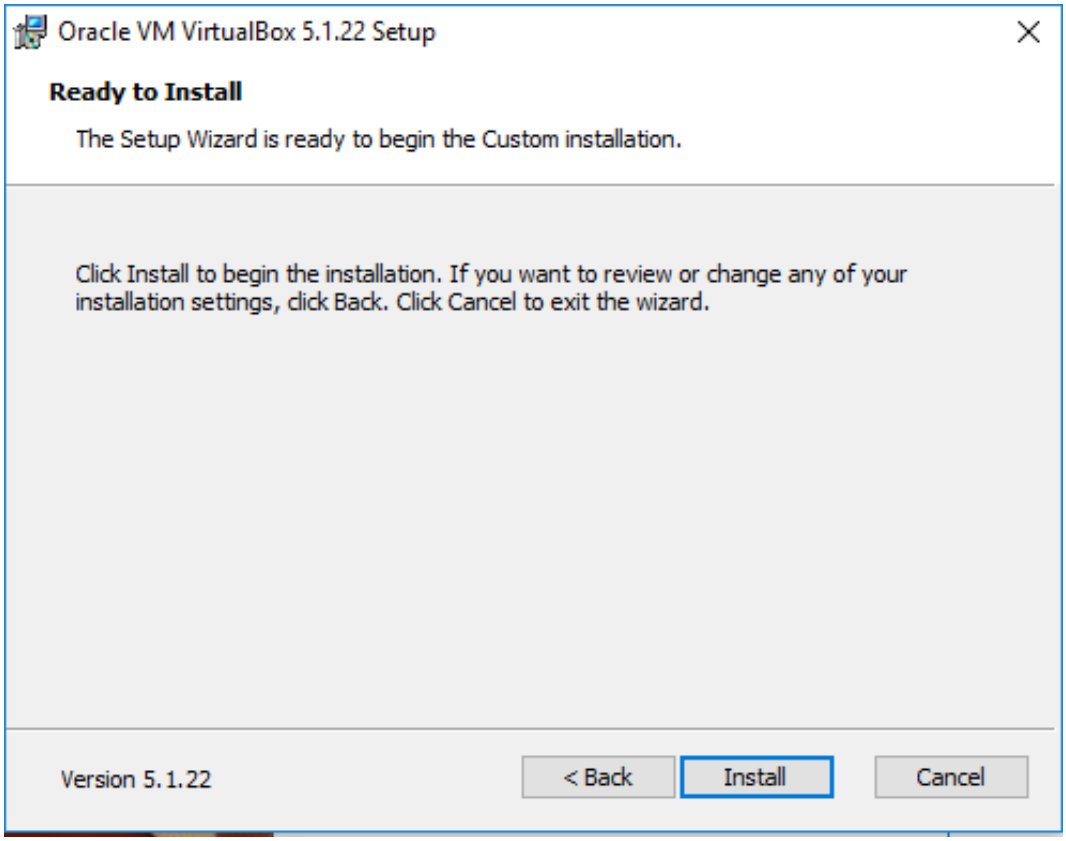
Ilustración 9. Instalación característica de Red



Fuente: el autor

El asistente está preparado para iniciar la instalación, pulsamos el botón install y la instalación se iniciará.

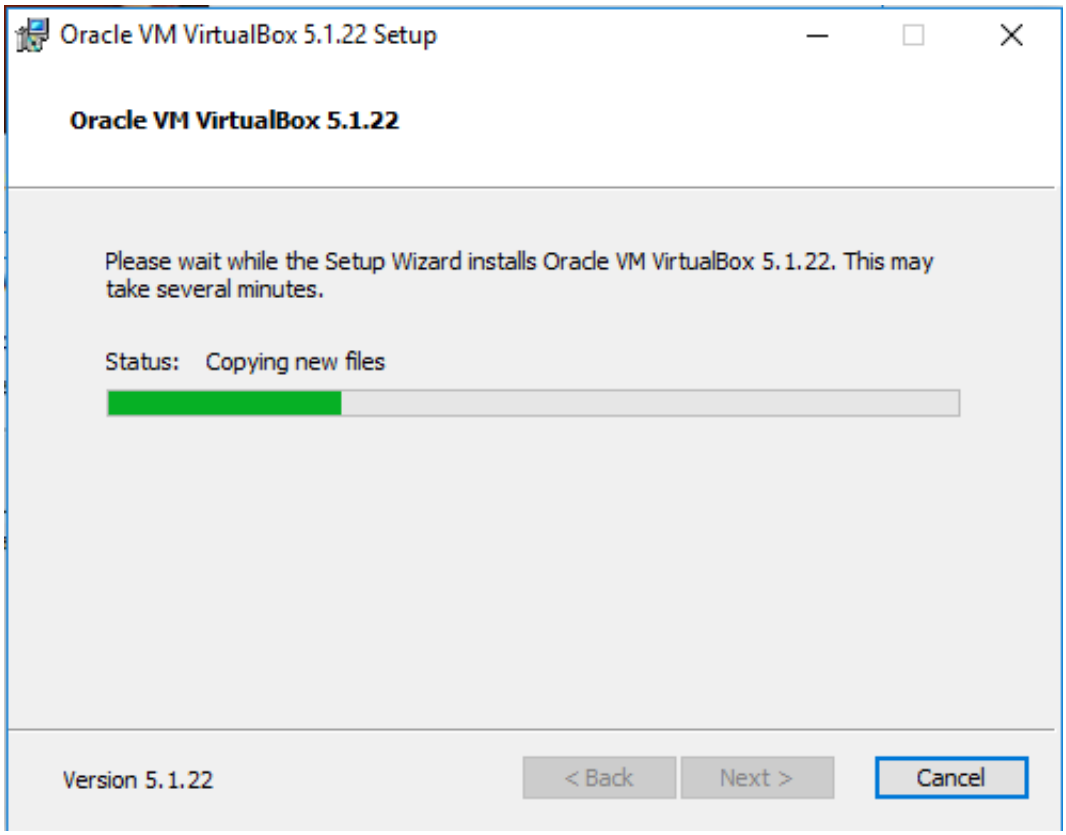
Ilustración 10. Inicio de instalación del virtualBox



Fuente: el autor

El asistente nos va dando información del avance de la instalación, esperamos hasta que la instalación finalice.

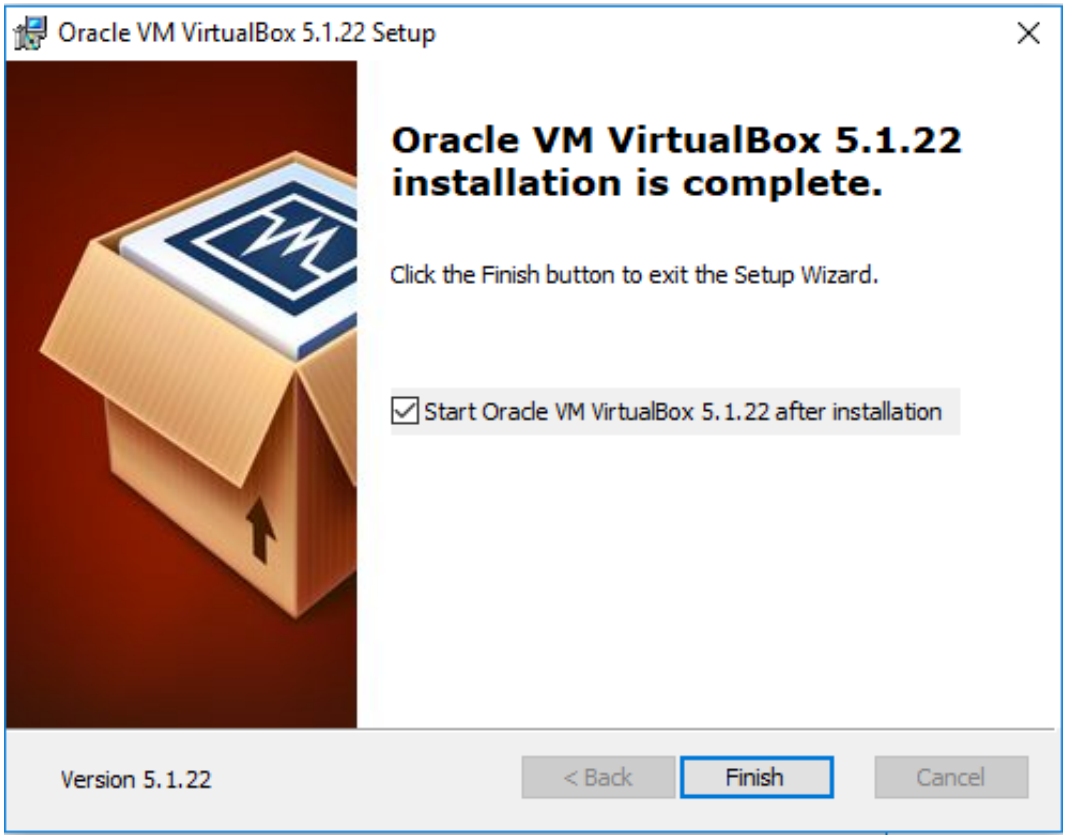
Ilustración 11. Proceso de la instalación del VirtualBox



Fuente: el autor

Cuando la instalación haya finalizado, en la ventana del asistente nos aparece la opción '**Start Oracle VM VirtualBox ….**''Seleccionada, esto hará que cuando pulsemos el botón finish abrirá automáticamente la aplicación.

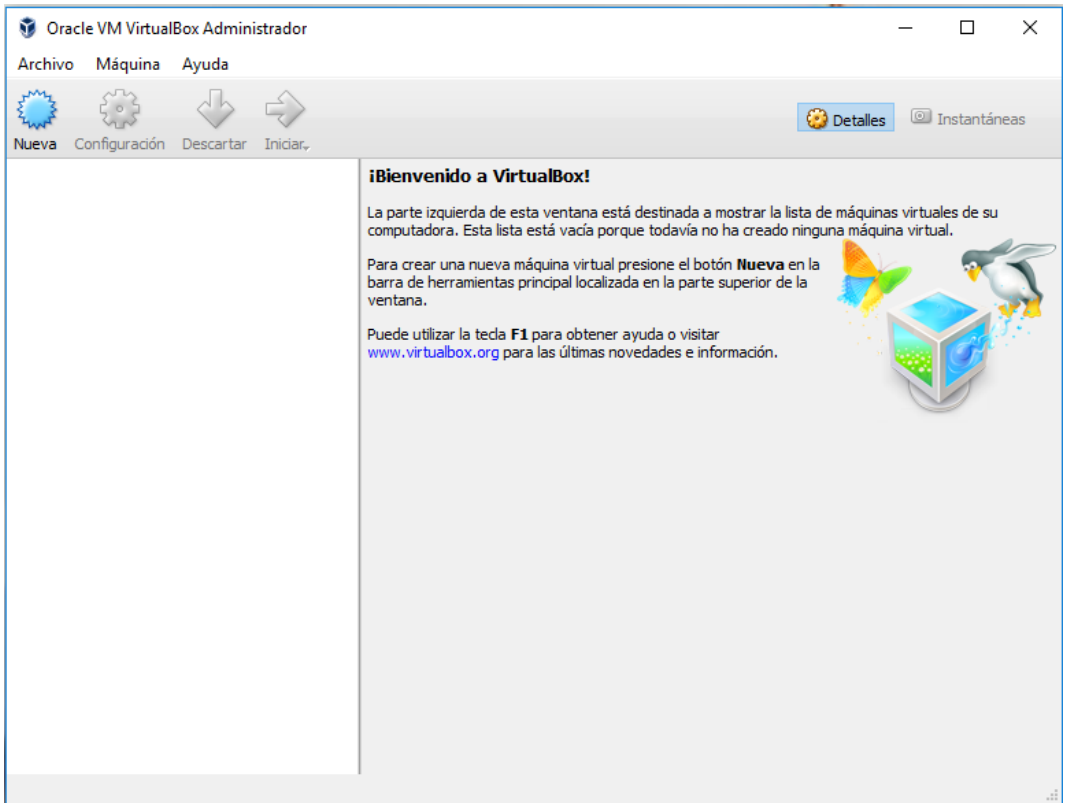
Ilustración 12. Finaliza Instalación virtualBox



Fuente: el autor

Ya estamos en la ventana principal de Oracle VM VirtualBox.

Ilustración 13. Página Principal del VirtualBox

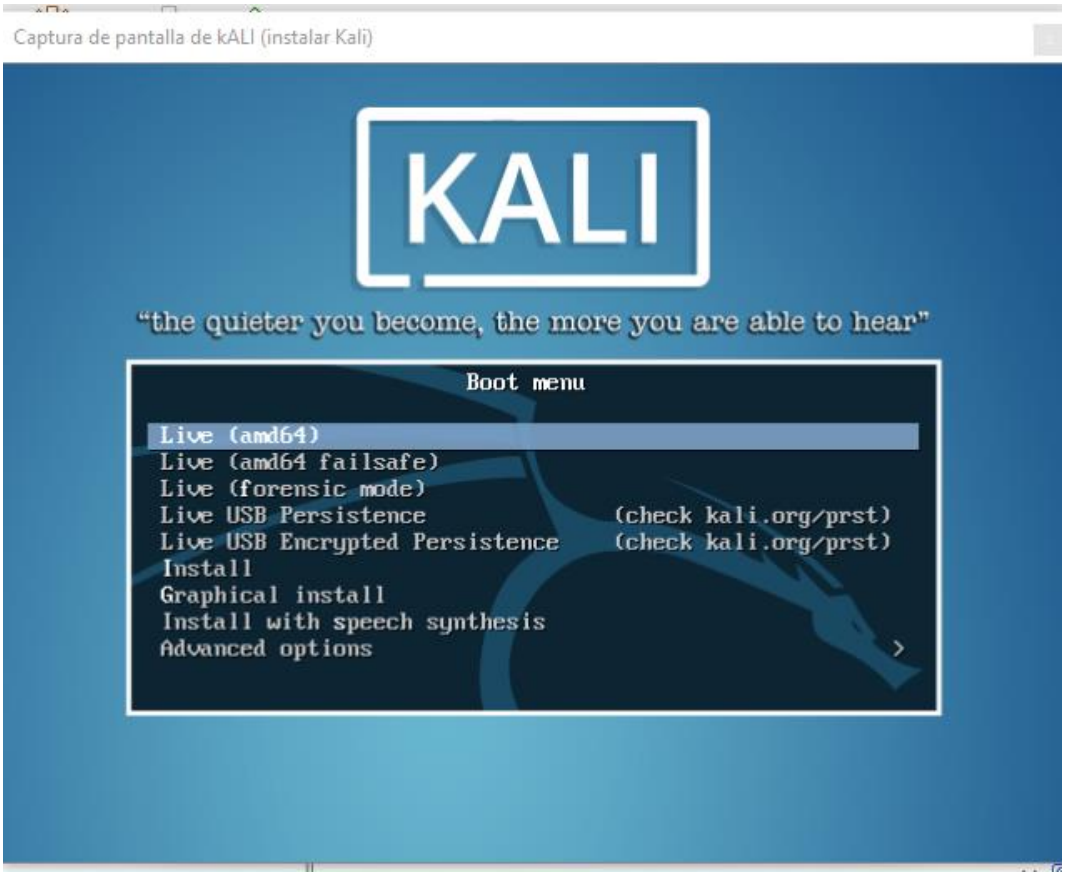


Fuente: el autor

4.2. INSTALACIÓN Y CONFIGURACIÓN DEL SISTEMA OPERATIVO KALI LINUX

Para inicar debemos de tener ya configurado el virtualbox para instalar kali linux.

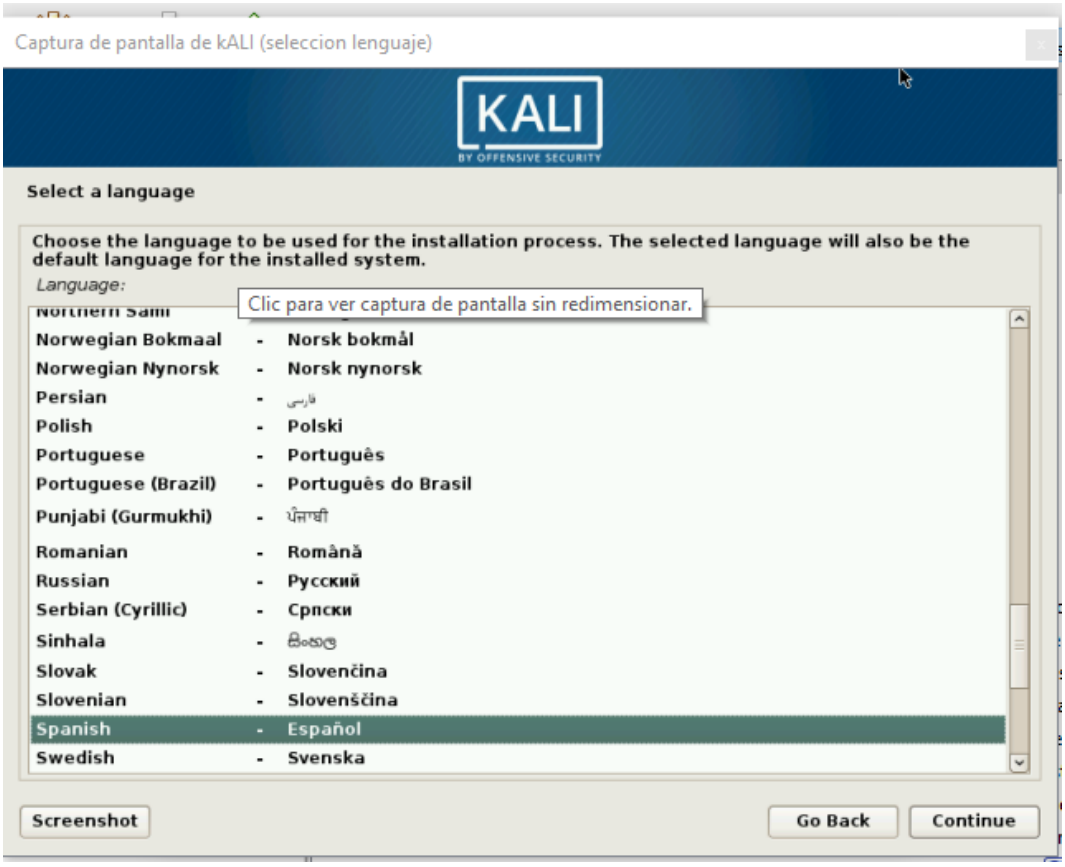
Ilustración 14. Inicio instalación Kali linux



Fuente: el autor

Escogemos install y procedemos a escoger el lenguaje

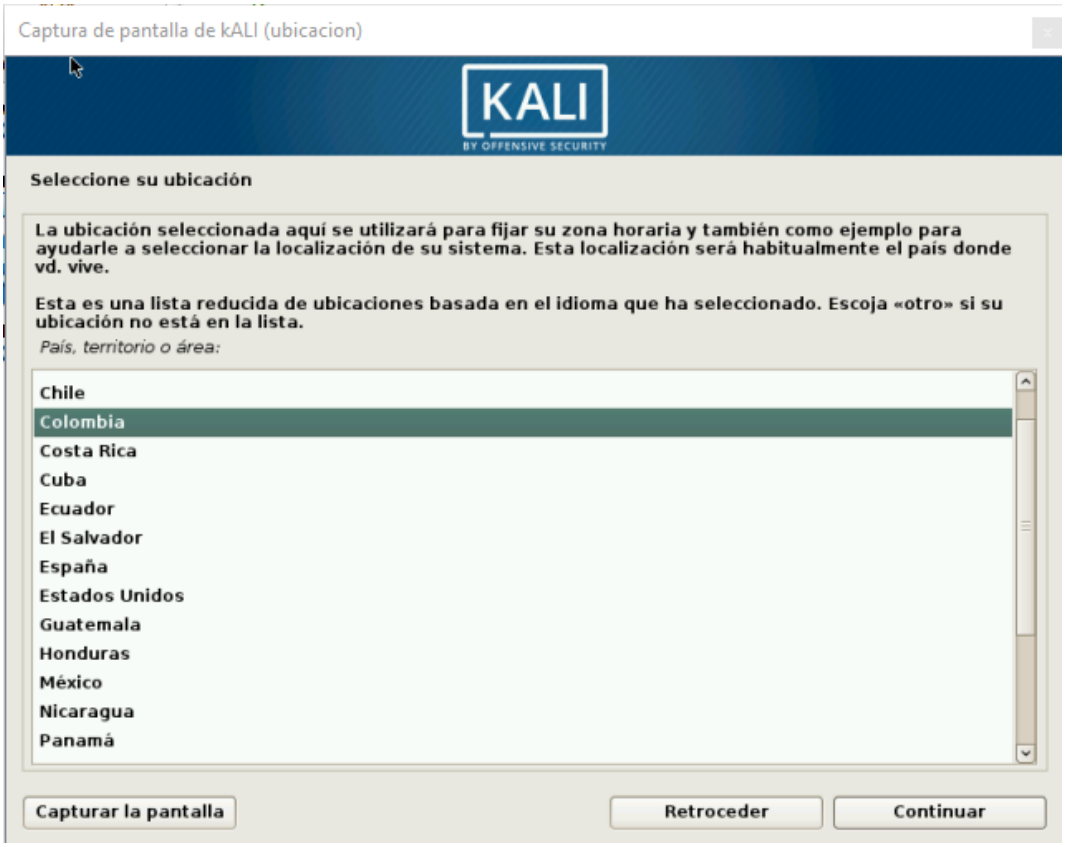
Ilustración 15. Selección del lenguaje



Fuente: el autor

Seleccionamos nuestra ubicación

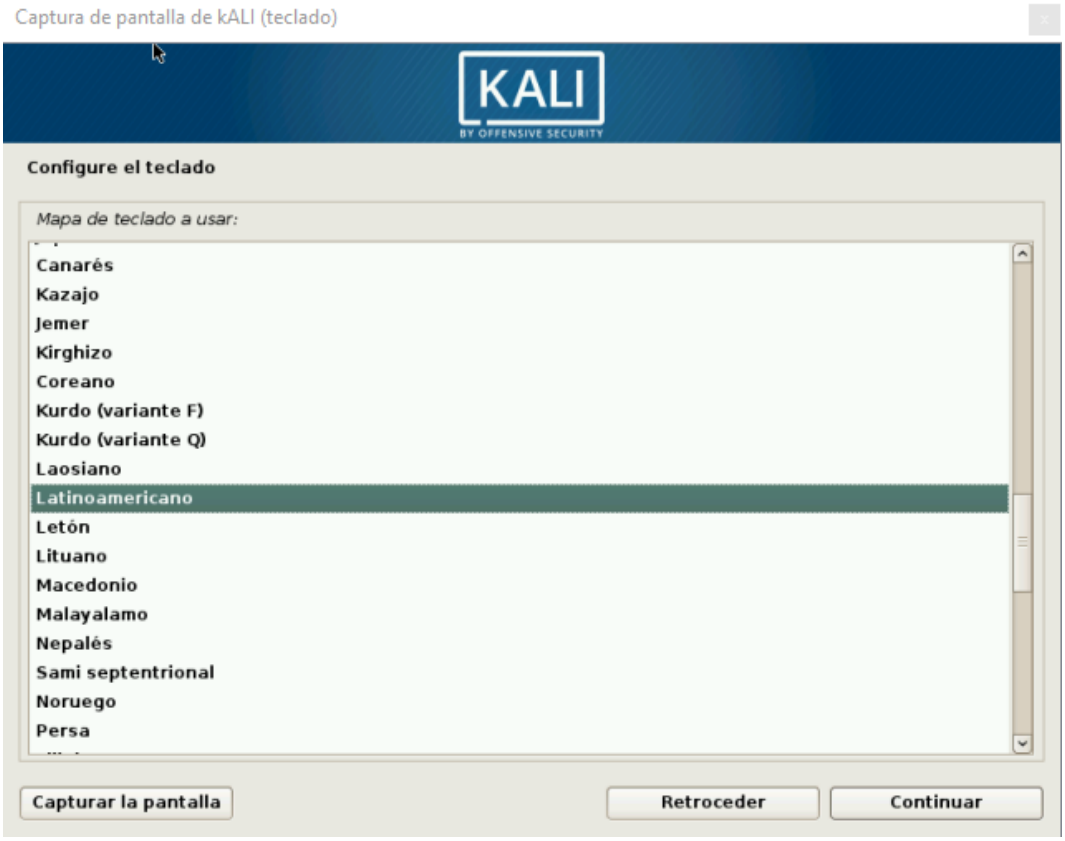
Ilustración 16. Selección de la ubicación



Fuente: el autor

Escogemos el teclado que vamos a instalar

Ilustración 17. Configuración del teclado



Fuente: el autor

Nos pide asignarle nombre a la maquina

Ilustración 18. nombre maquina

Fuente: el autor

Luego vemos la configuración de dominio, no tenemos en nuestro caso por ende lo dejamos en blanco.

Ilustración 19. Configuración del dominio

Fuente: el autor

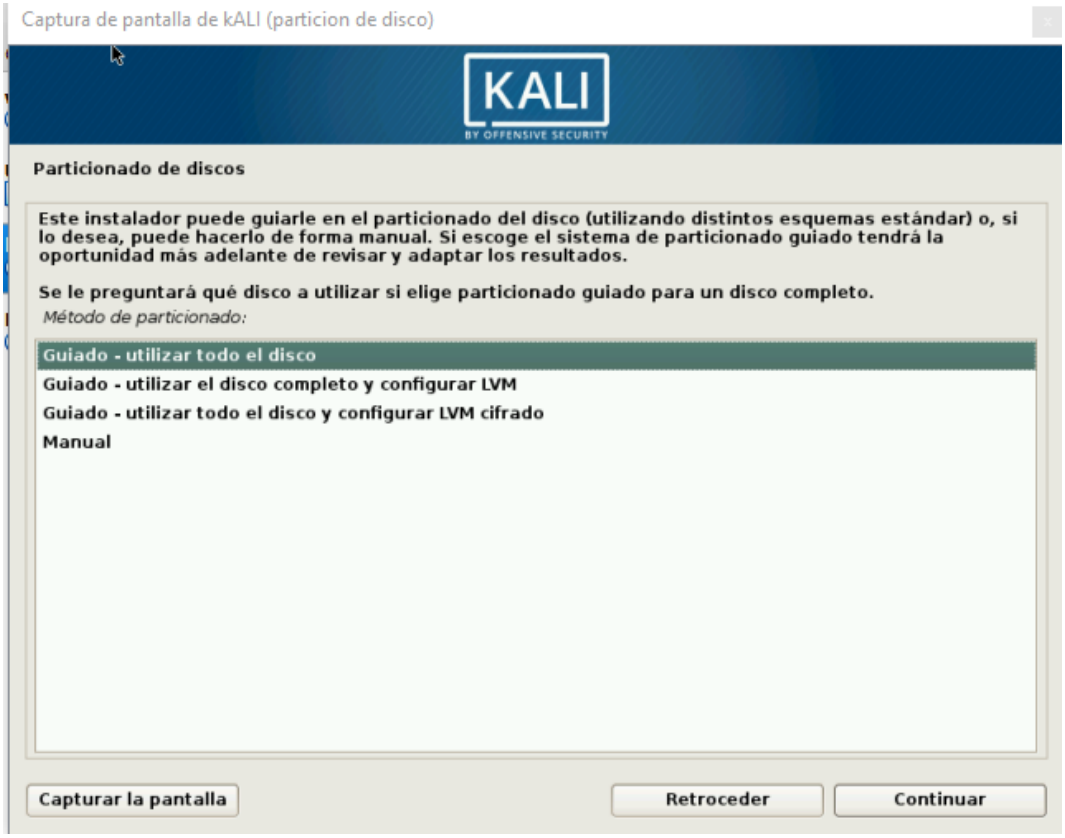
Luego vamos a darle una clave al super usuario

Ilustración 20. clave super usuario

Fuente: el autor

Luego vamos a particionar el disco en donde se va a grabar nuestro Kali Linux

Ilustración 21. partición disco



Fuente: el autor

Me dice el disco que encontró y donde se va hacer la instalación

Ilustración 22. configuración partición de disco

Fuente: el autor

Nos informa donde va a grabar en esa parte de disco los ficheros del kali linux

Ilustración 23. lugar grabarcion kali linux en el disco

Fuente: el autor

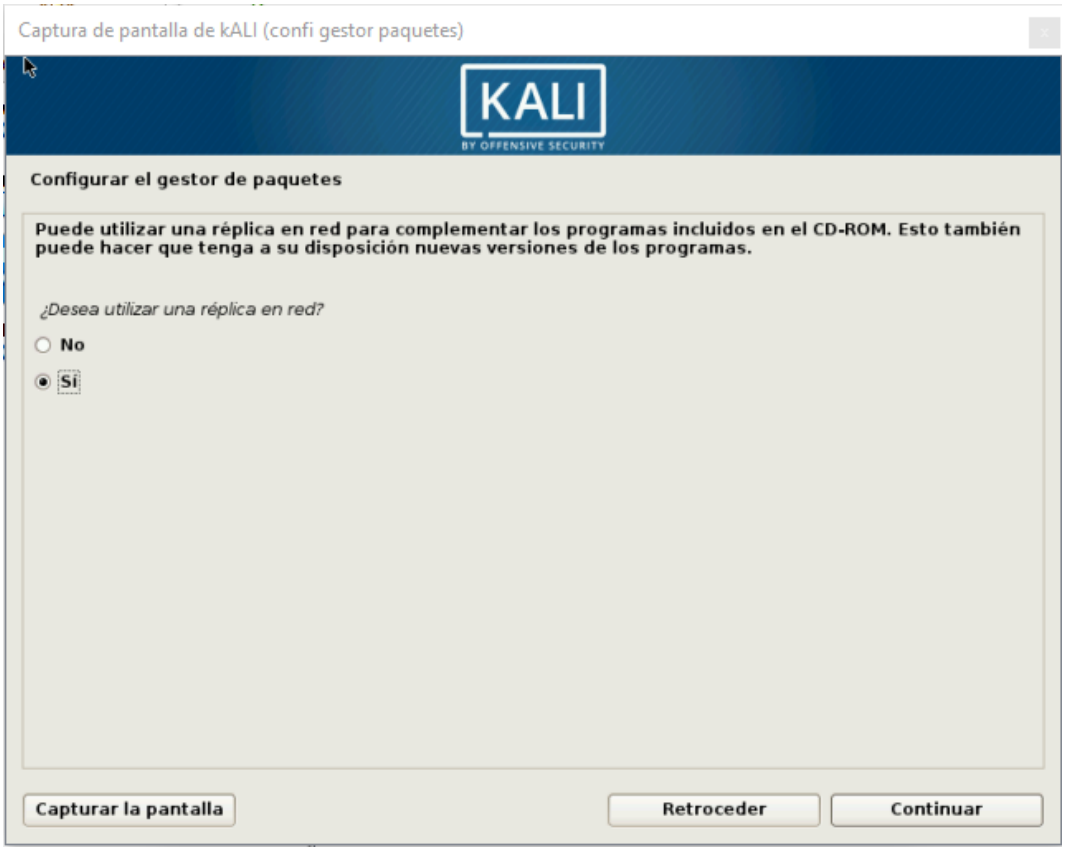
Nos informa donde va a gravar el Kali Linux y su ubicación y si estamos de acuerdo continuar con el proceso.

Ilustración 24. Confirma con seguir con la instalación

Fuente: el autor

Que si deseamos configurar el gestor de paquetes

Ilustración 25. configuración de gestor de paquetes



Fuente: el autor

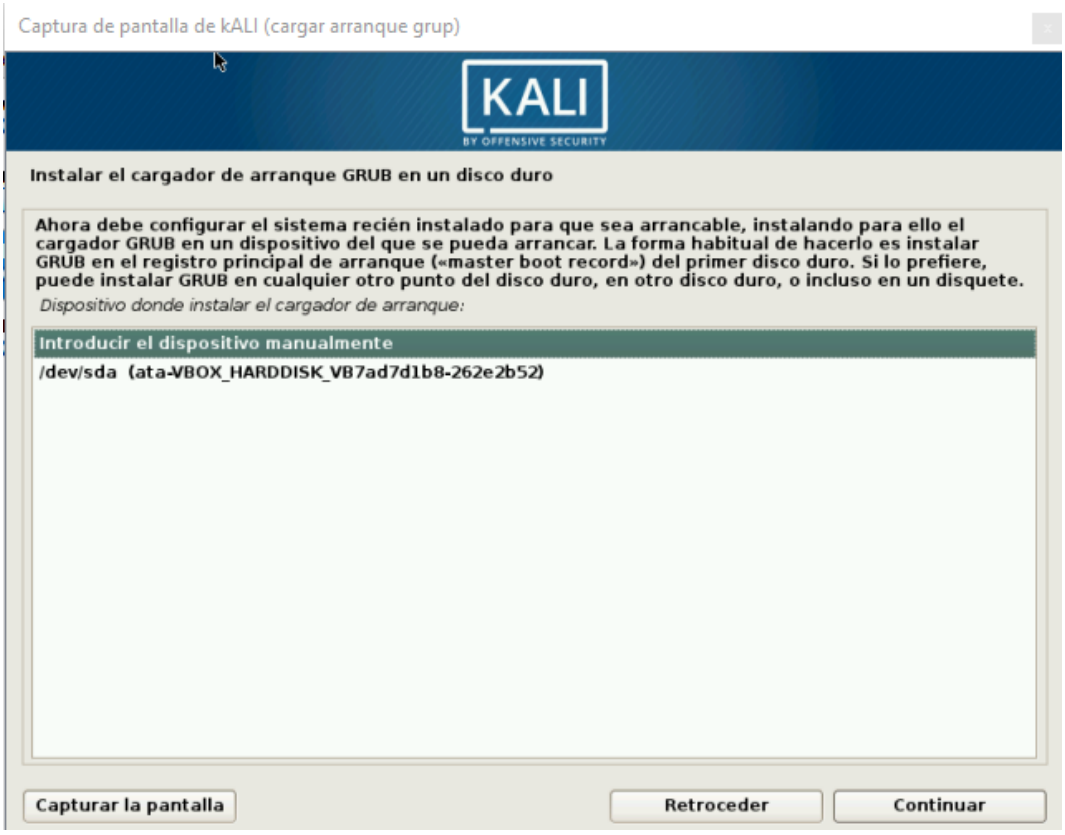
Instalar el arranque del grup

Ilustración 26. instalación del GRUP

Fuente: el autor

Instalar del cargador de arranque grup, la ruta que nos aparece allí

Ilustración 27. ruta de donde nos va a cargar el GRUP



Fuente: el autor

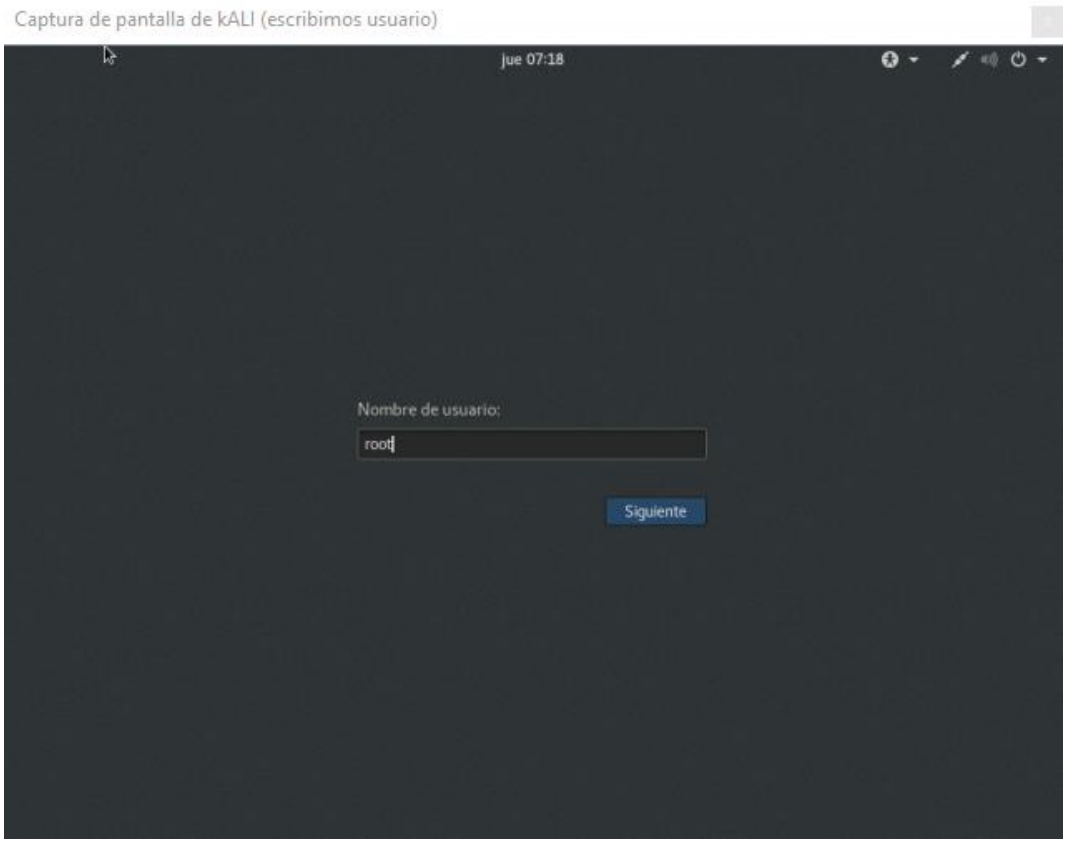
Termina la instalación y reinicia

Ilustración 28. fin de instalación

Fuente: el autor

Nos carga la primera pantalla donde nos pide el usuario por defecto el super usuario es root

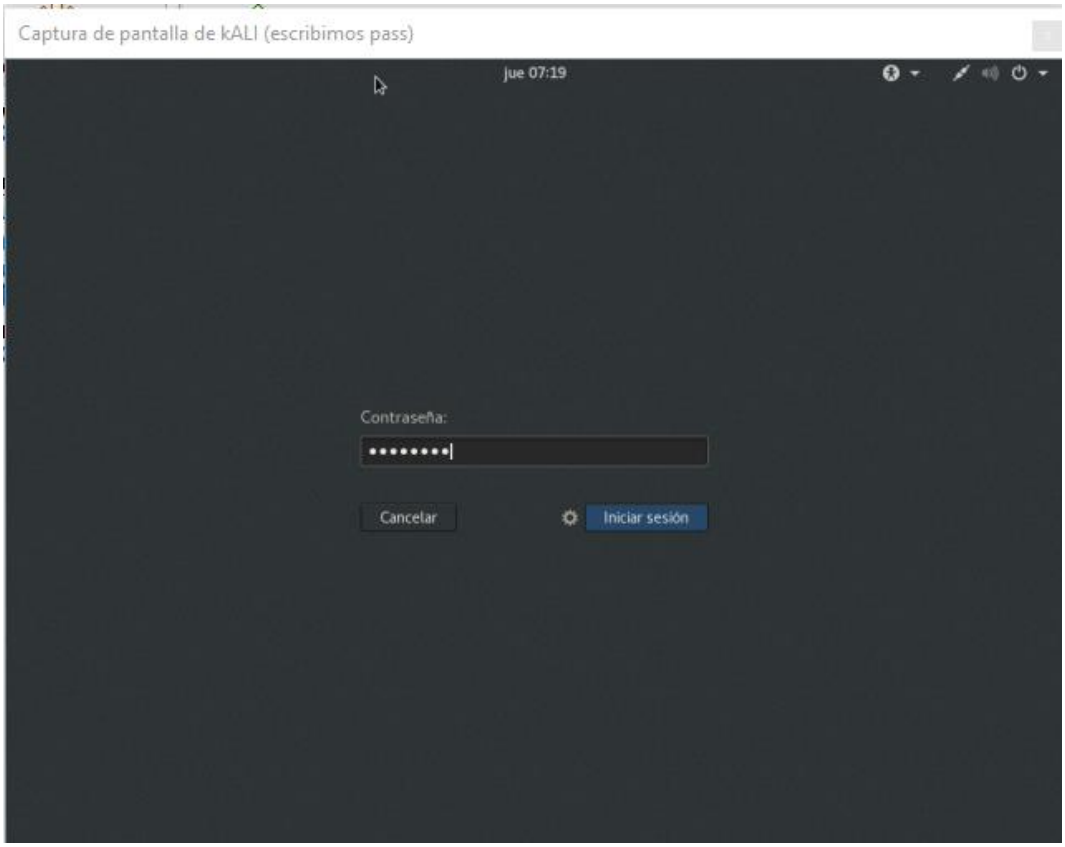
Ilustración 29. primera pantalla Kali linux



Fuente: el autor

En la primera pantalla nos pide el usuario por defecto el super usuario es root y la contraseña

Ilustración 30. validación de usuarios



Fuente: el autor

Nos carga la primera pantalla del sistema operativo KALI Linux

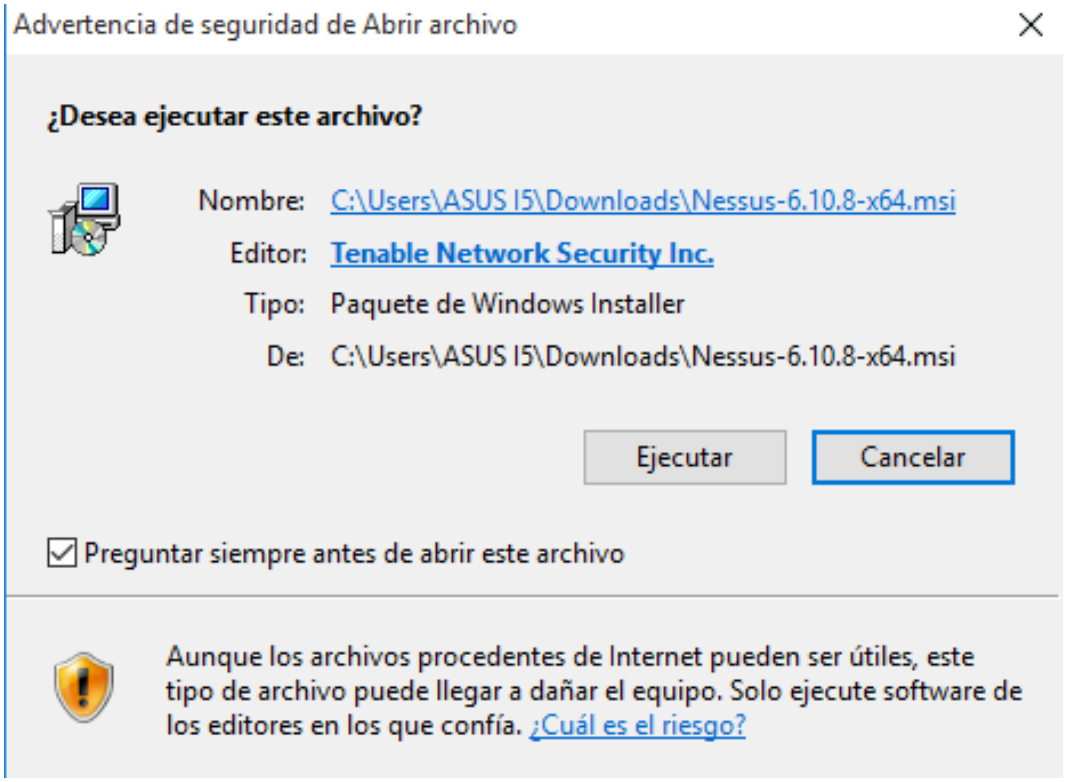
Ilustración 31. pantalla grafica Kali linux

Fuente: el autor

4.3. INSTALACIÓN Y CONFIGURACIÓN DEL NESSUS

Iniciamos la instalación de Nessus

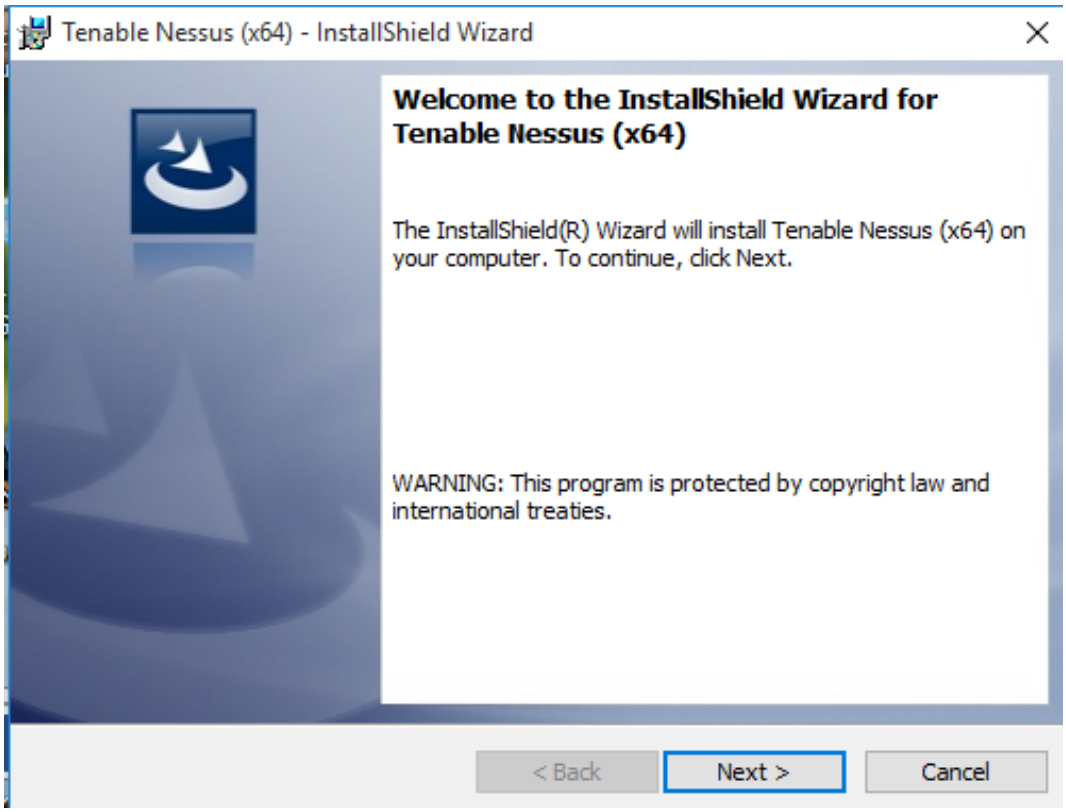
Ilustración 32. Inicio Instalación



Fuente: el autor

En la primera pantalla lo que nos pide es ejecutar

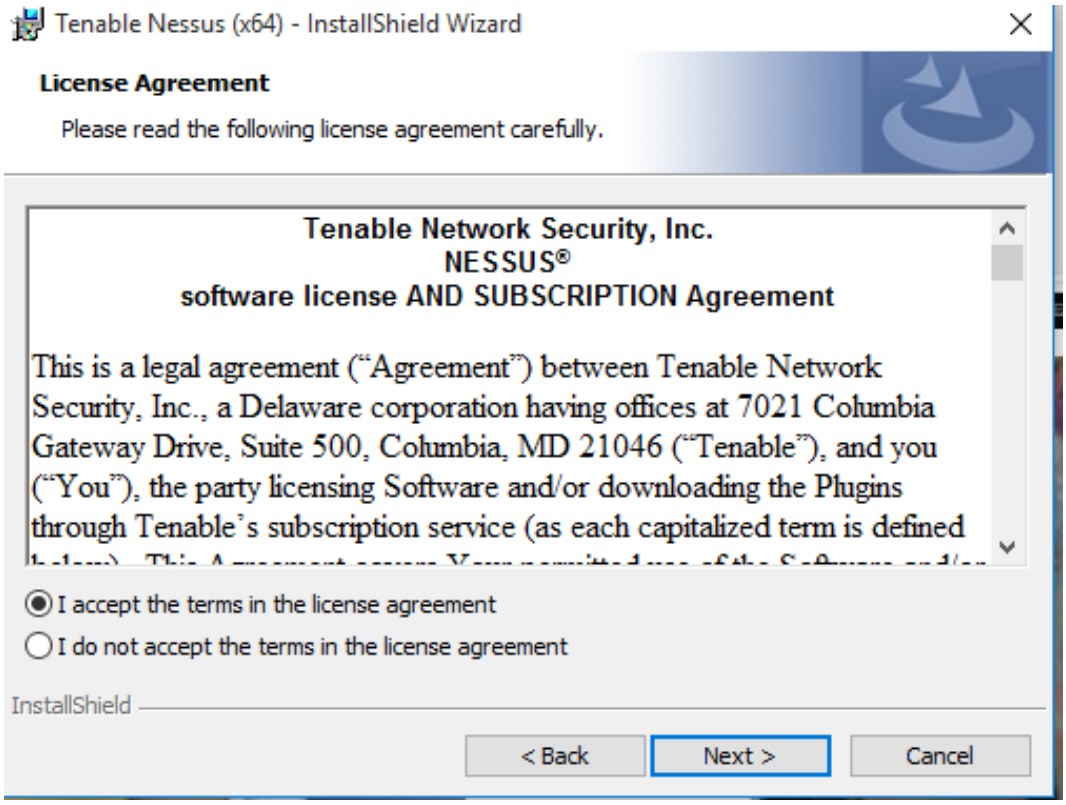
Ilustración 33. Bienvenida a la instalación



Fuente: el autor

En la segunda pantalla le damos siguiente

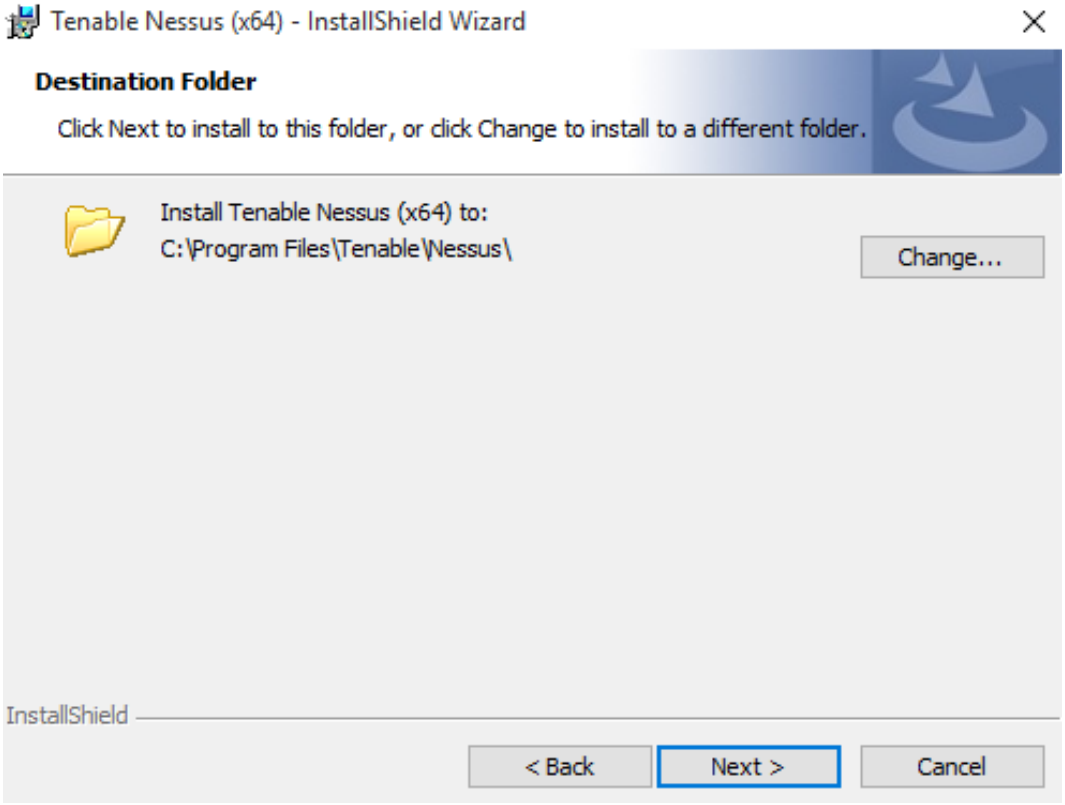
Ilustración 34. Términos de licencia



Fuente: el autor

En la tercera nos pide aceptar las condiciones de licencia y términos y le damos en siguiente

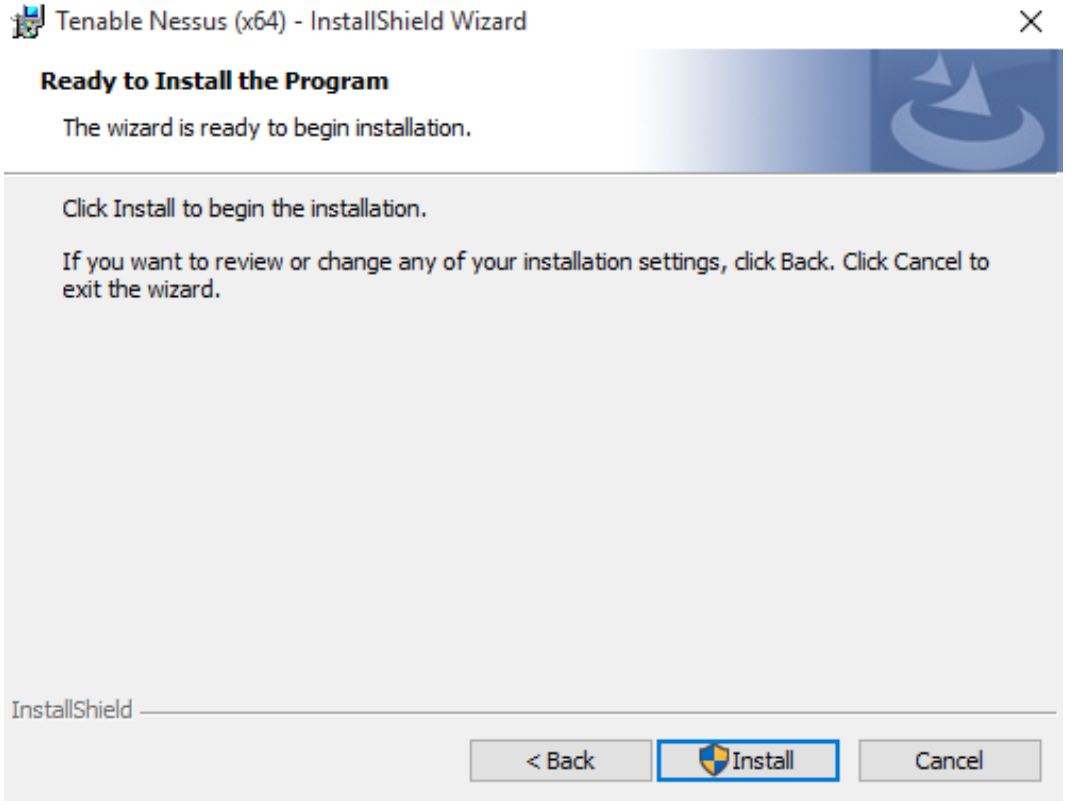
Ilustración 35. Ubicación de instalación



Fuente: el autor

En esta pantalla lo que nos dice es la ruta donde se va a instala en Nessus y siguiente

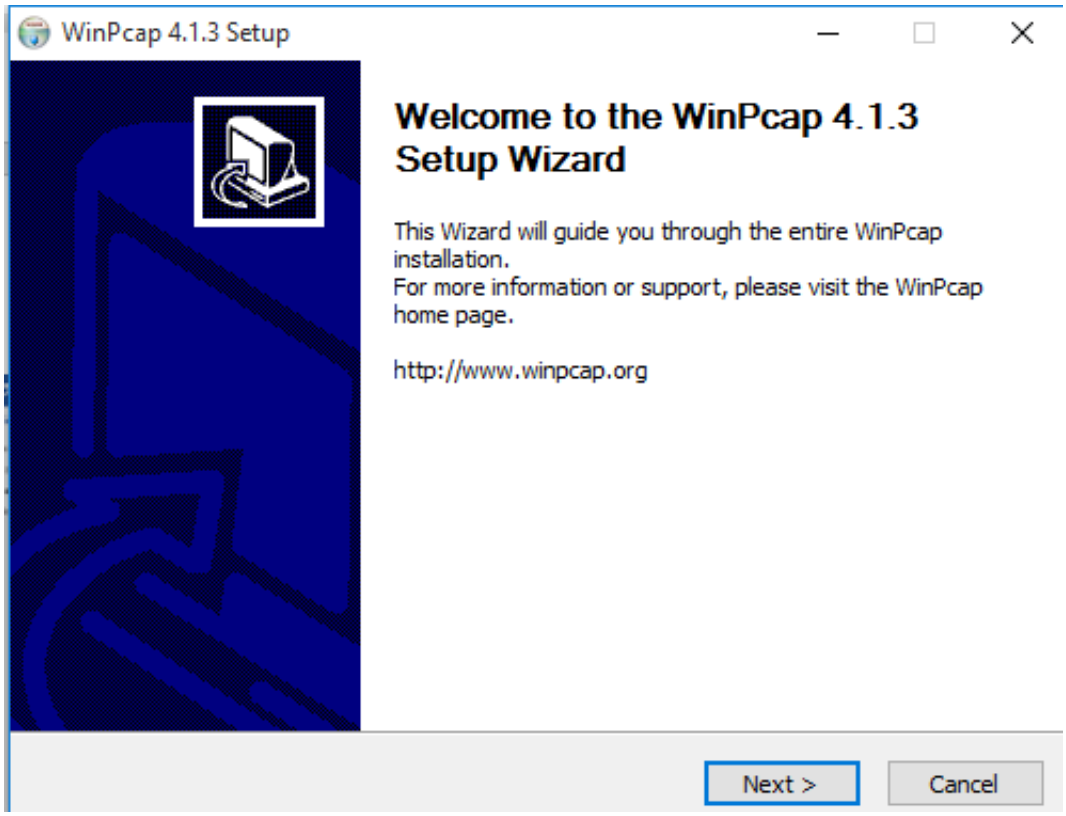
Ilustración 36. Inicia proceso de instalación Nessus



Fuente: el autor

En esta pantalla nos confirma que inicia la instalación de Nessus

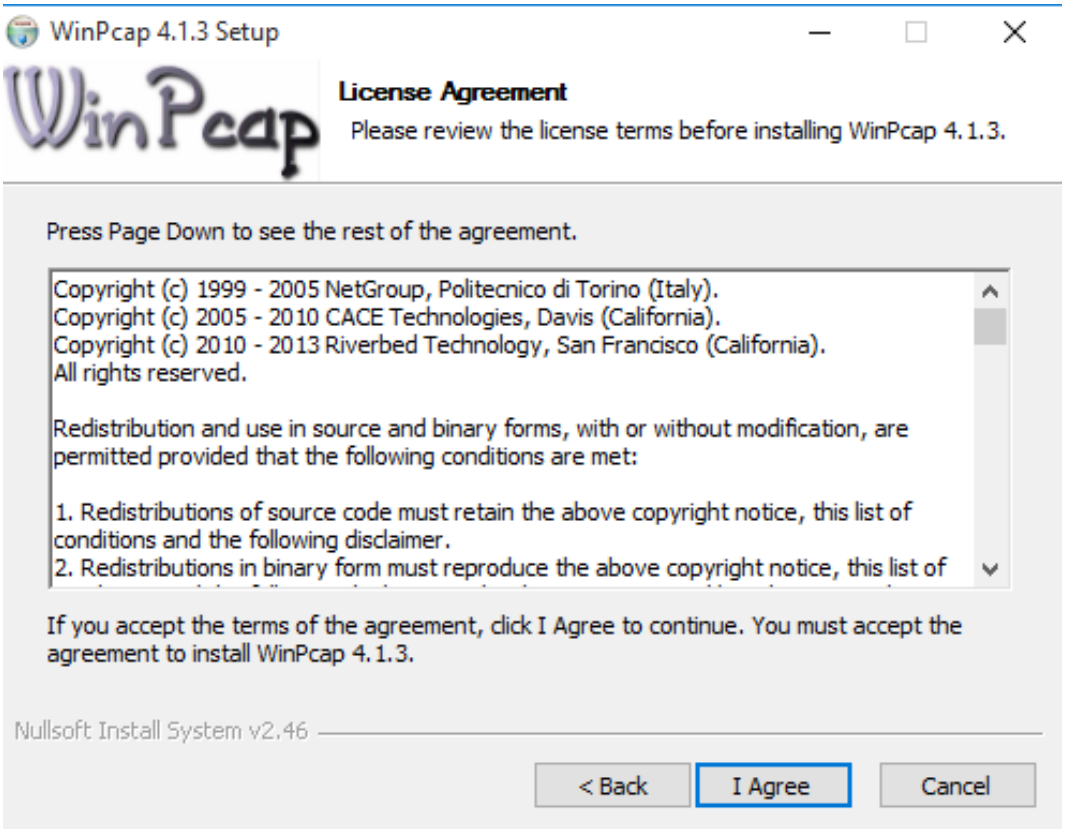
Ilustración 37. Instala herramienta WinPcap



Fuente: el autor

Nos pide instalar una herramienta, en mi caso me desinstala nmap para actualizarlo

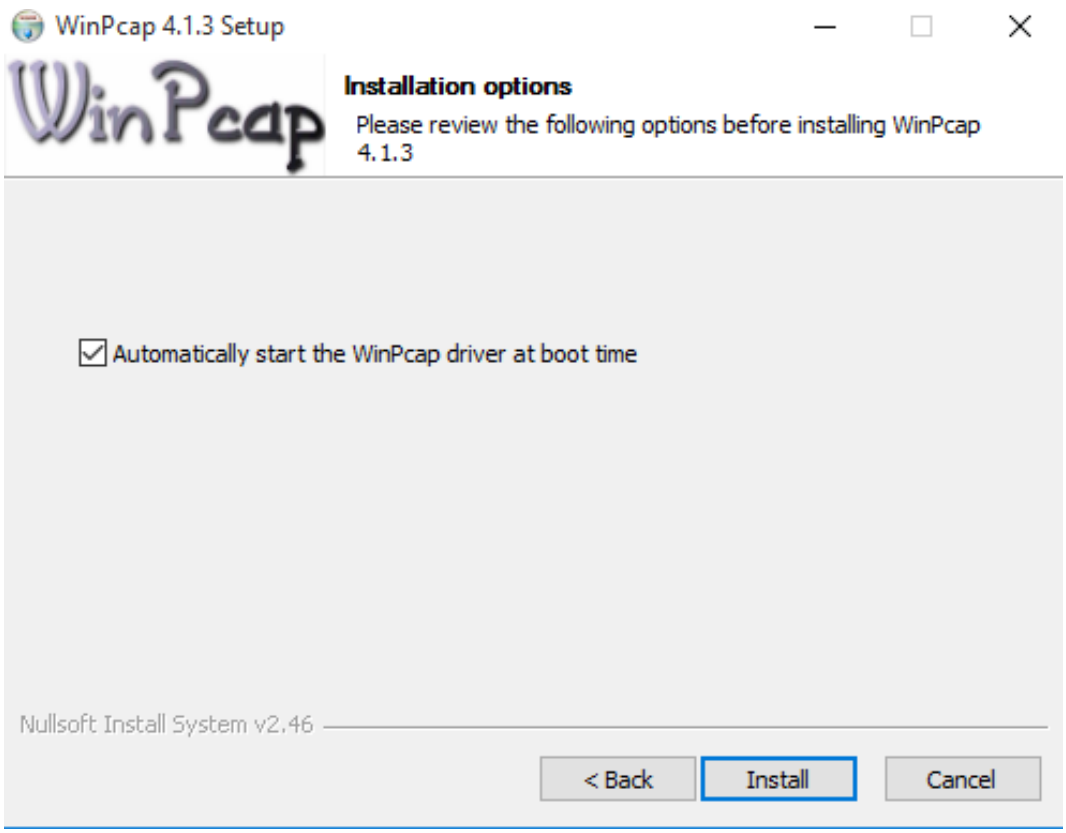
Ilustración 38. términos y licencia de herramienta WinPcap



Fuente: el autor

Nos pide aceptar las condiciones de licencia de la herramienta a instalar

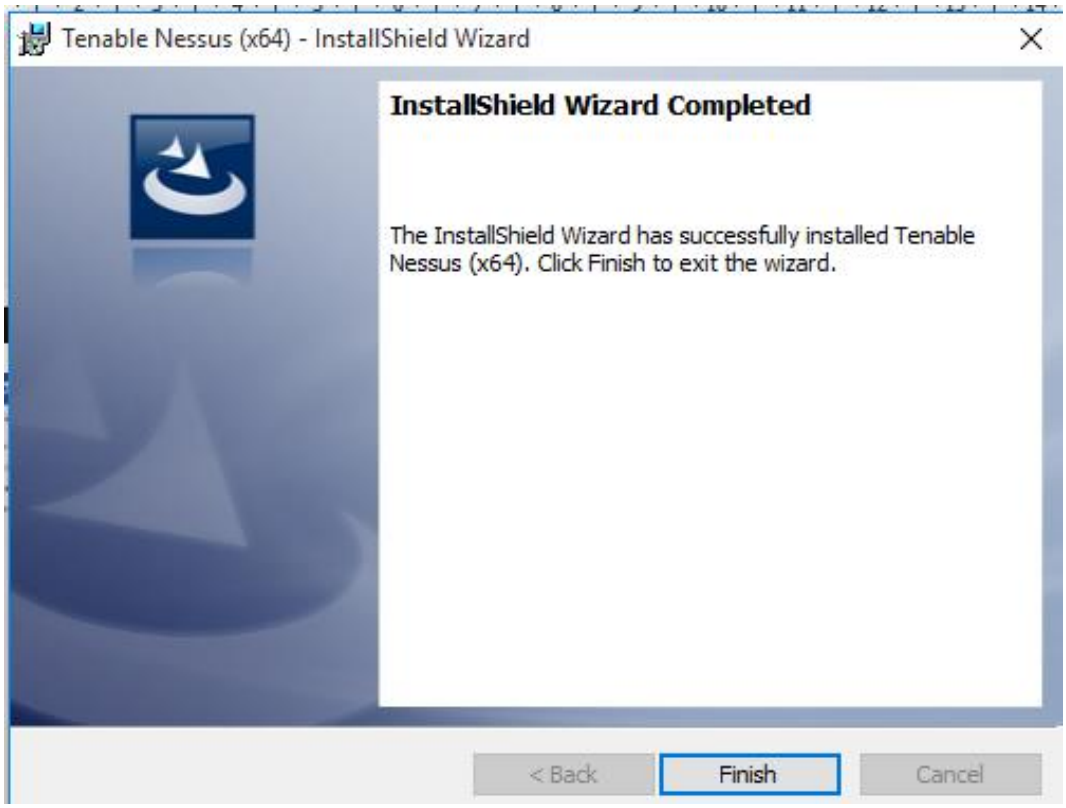
Ilustración 39. Instalación de la herramienta WinPcap



Fuente: el autor

Se instala la herramienta

Ilustración 40. Finalización de la herramienta Nesuus



Fuente: el autor

Y finaliza la instalación del Nessus

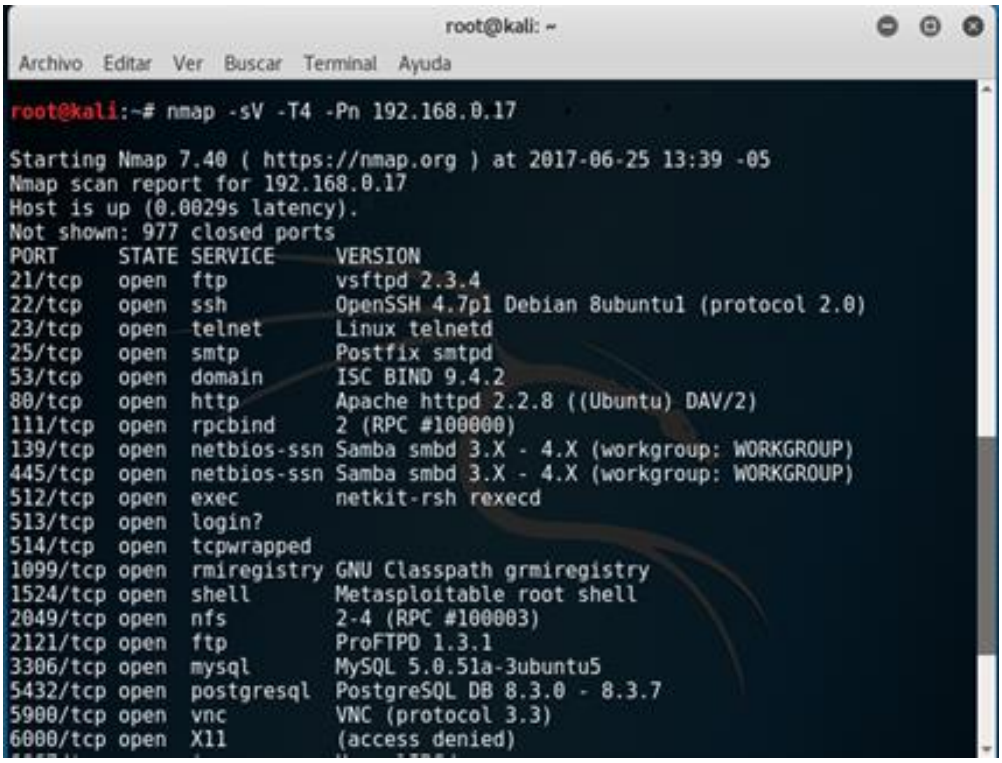
5. PRUEBAS REALIZADAS CON HERRAMIENTAS DE PENTESTING

5.1. NMAP

Utilizando la herramienta de Pentesting o herramienta de penetración la cual sirve para detectar vulnerabilidades en los sistemas, en este caso se utiliza la Suite de Kali Linux y algunos de sus componentes de Software para evaluar la red y determinar posibles vulnerabilidades.

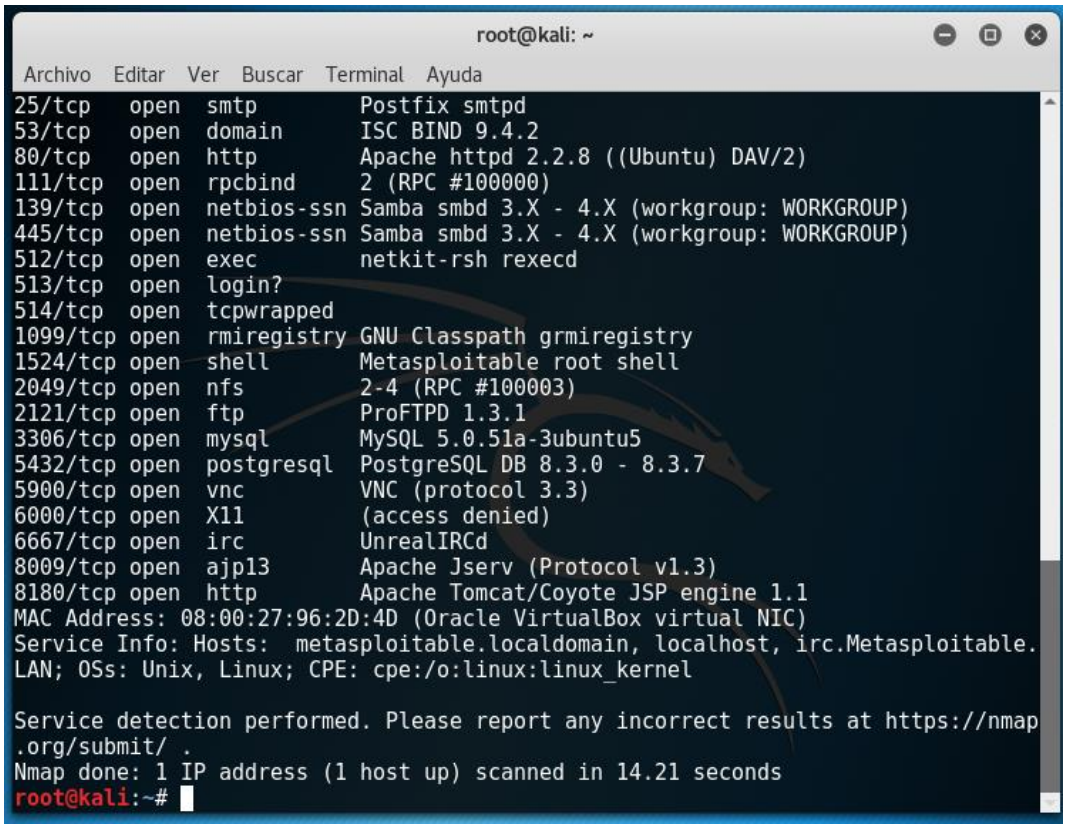
Usando la herramienta de Kali Linux con el programa NMAP, para escanear los puertos que están abiertos, usando el comando: Nmap -sV -T4 -Pn “IP maquina a vulnerar”. En nuestro caso Nmap -sV -T4 -Pn 192.168.0.17

Ilustración 41. Comando de escaneo de puertos a la IP victima



Fuente: el autor

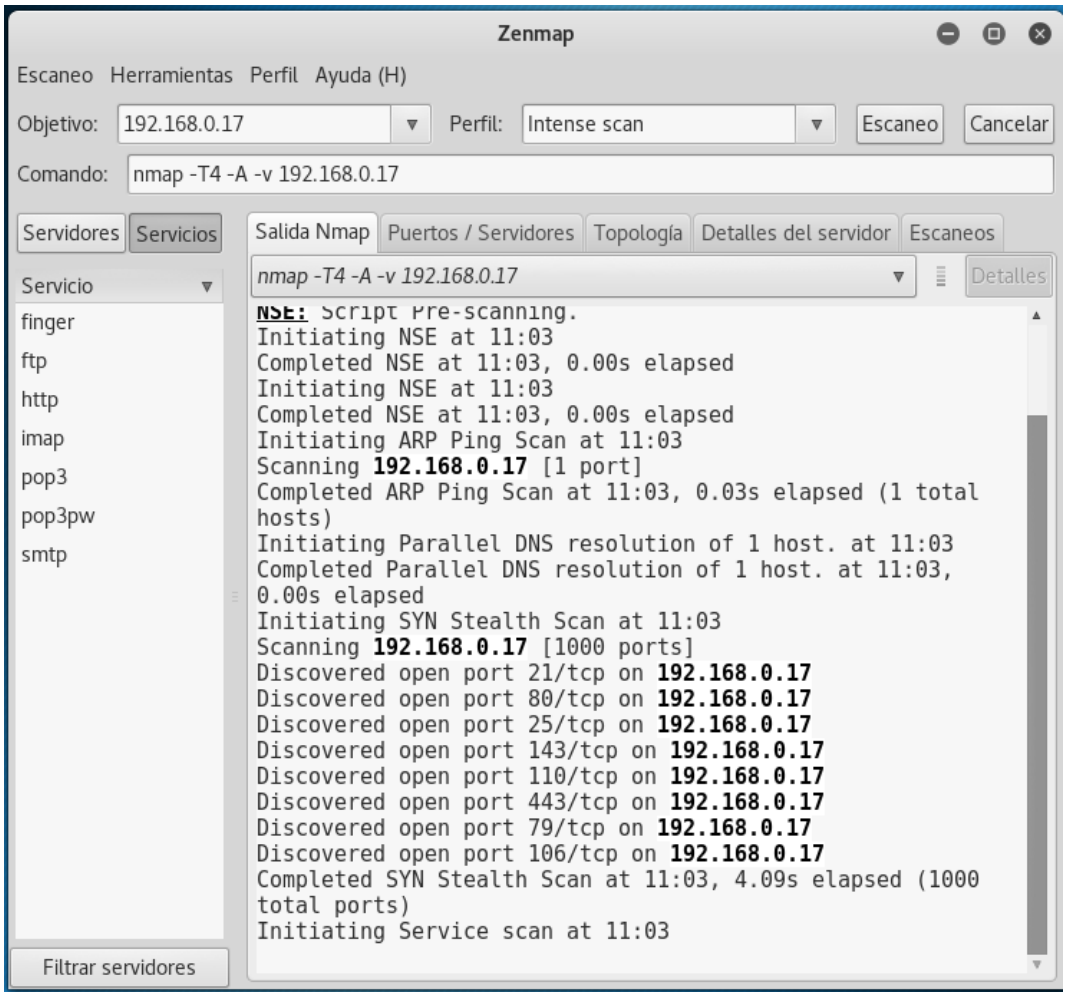
Ilustración 42. Comando de escaneo de puertos a la IP victima 1



Fuente: el autor

Aquí nos arroja la revisión de los puertos y sus servicios. Otra forma de hacer el mismo escaneo es por la interfaz gráfica de ZENMAP

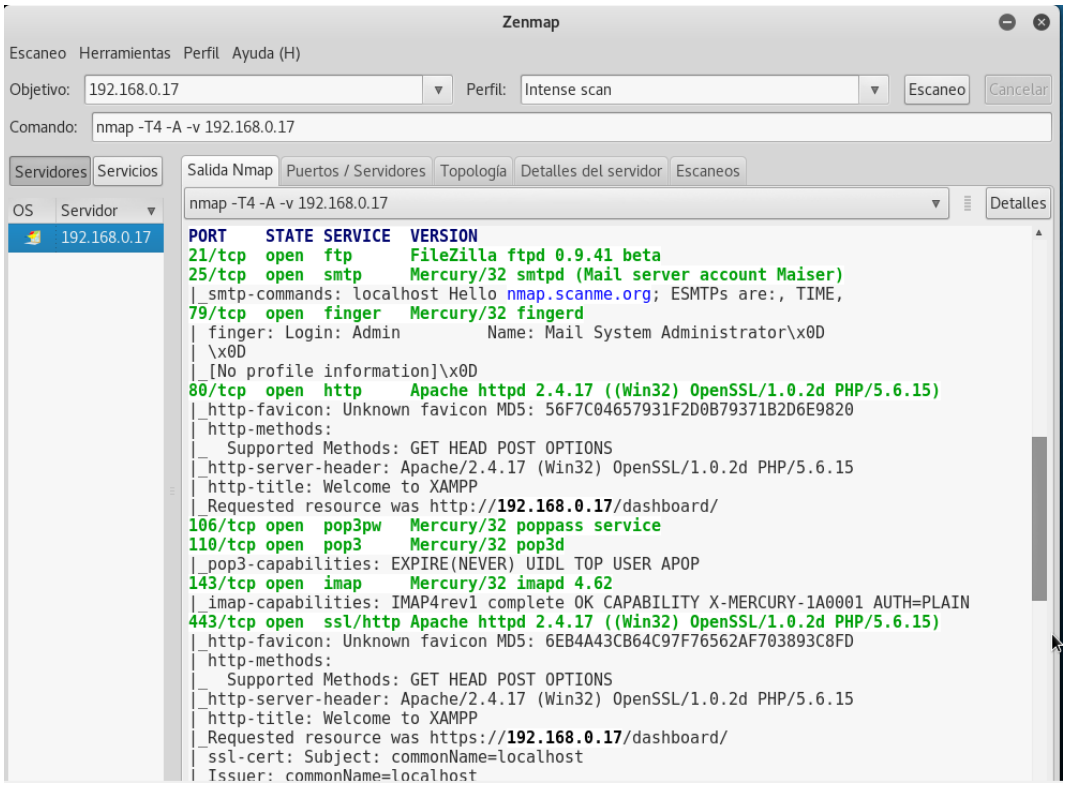
Ilustración 43. Escaneo de Puertos con la herramienta ZENMAP



Fuente: el autor

Donde por medio de la herramienta me permite ver que puertos tiene abierto y que servicio está usando.

Ilustración 44. Lista de puertos y servicios



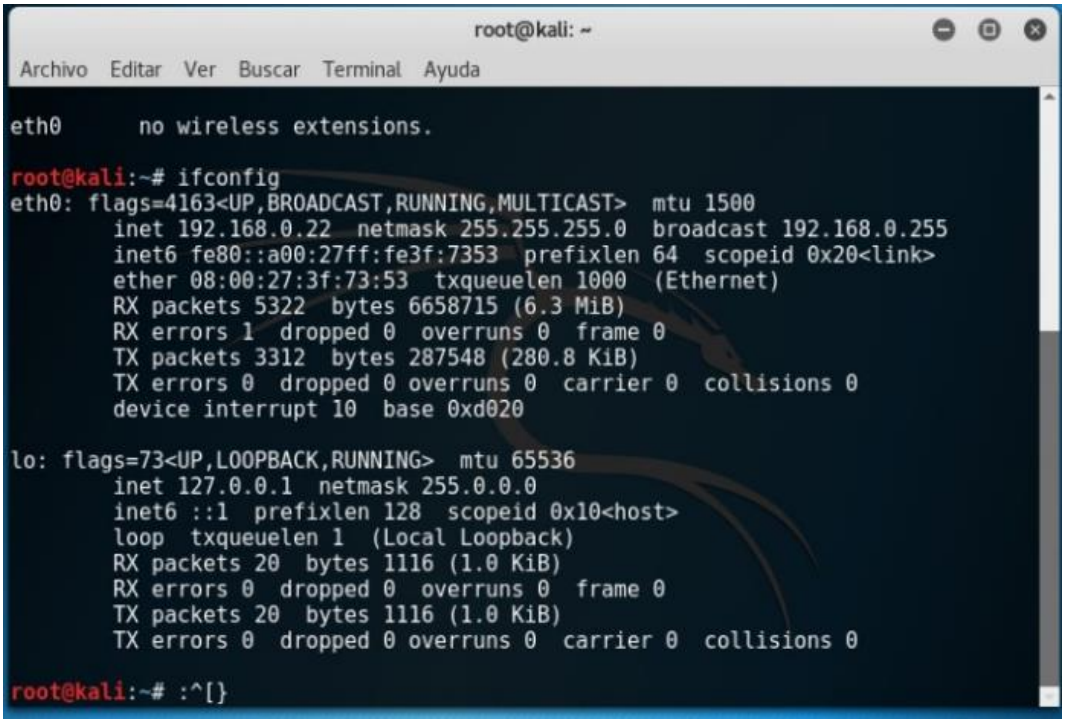
Fuente. El autor

5.2. SQLMAP

Primero abrimos un terminal root@kali y procedemos a cargar información e instalar

Se hace un ifconfig para saber si tengo red y cuál es la IP

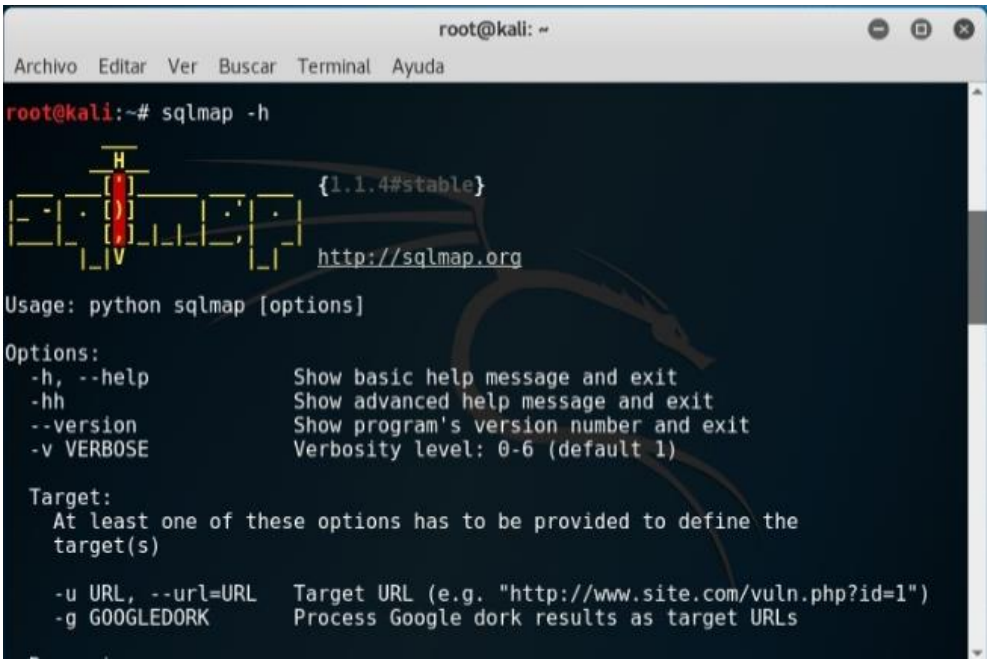
Ilustración 45. IP Kali linux



Fuente: el autor

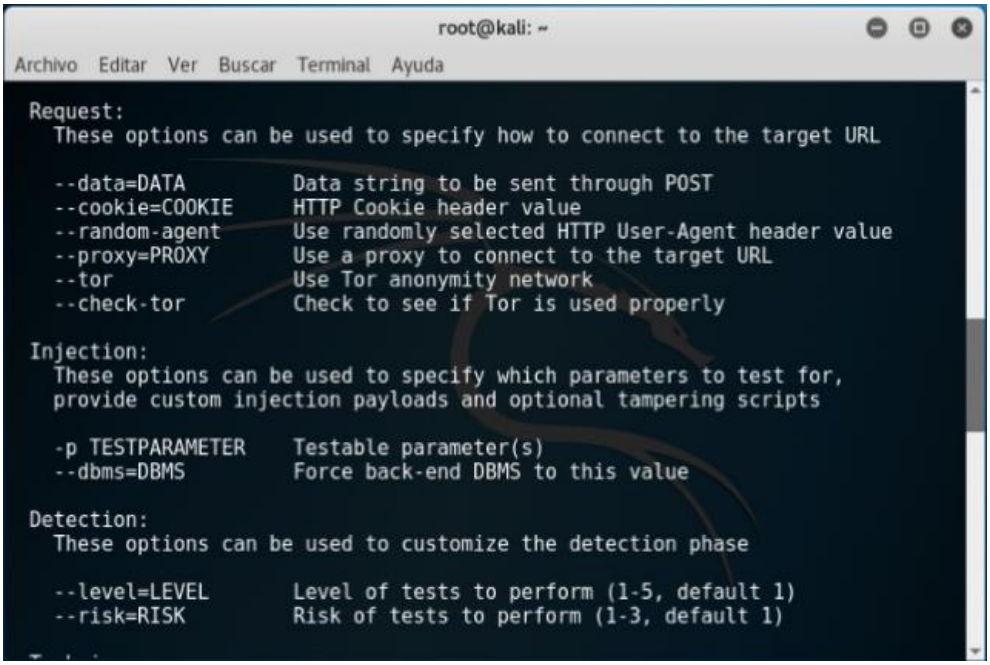
Ahora entramos a sqlmap con la opción -h para ver sus opciones

Ilustración 46. Herramienta SQLmap



Fuente: el autor

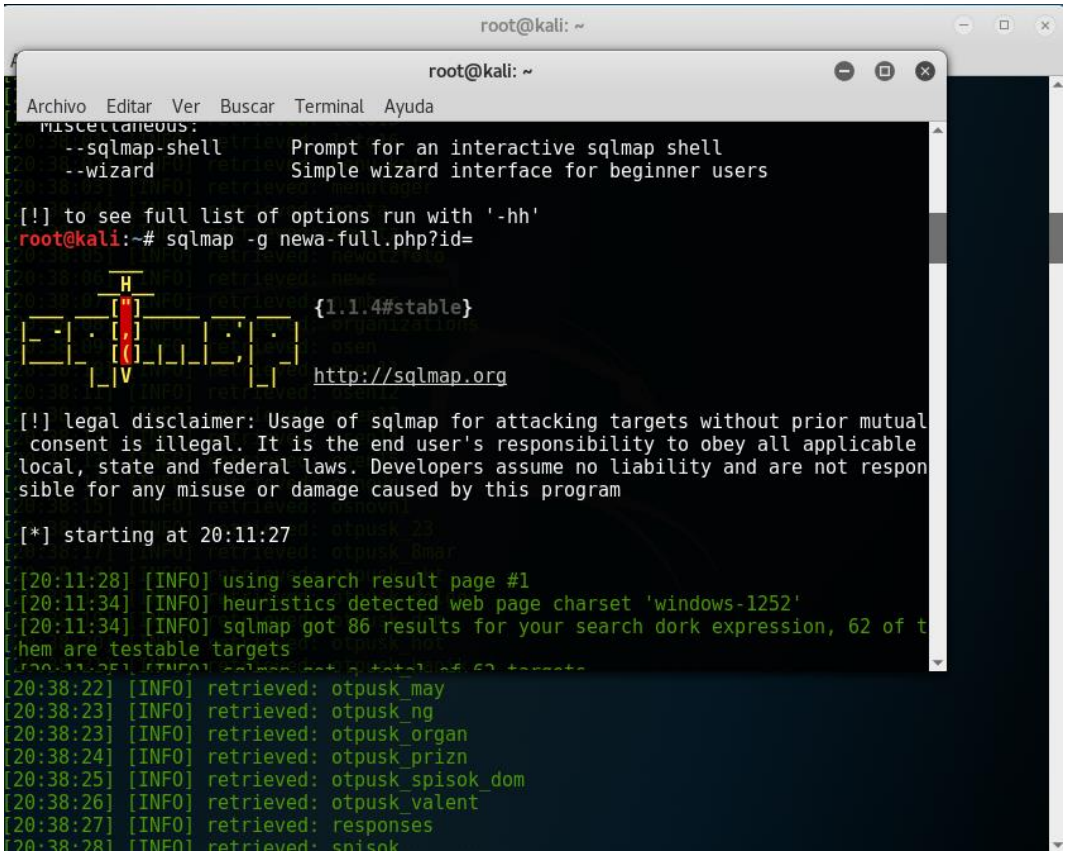
Ilustración 47. Opciones de la herramienta SQLmap



Fuente: el autor

Ahora iniciamos una búsqueda para poder vulnerar. Con el comando sqlmap -g y la URL en nuestro caso “newa-full.php?id=”

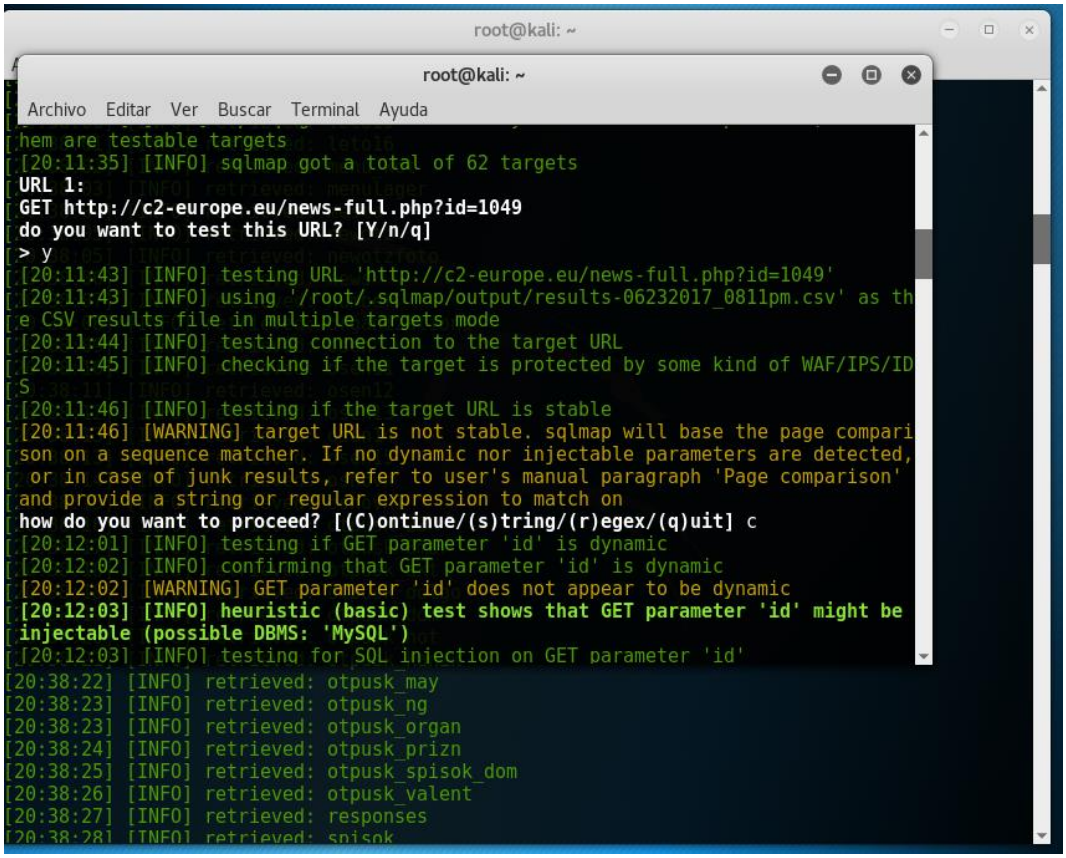
Ilustración 48. Búsqueda de la base de datos



Fuente: el autor

Lo cual me va mostrando URL que hay allí

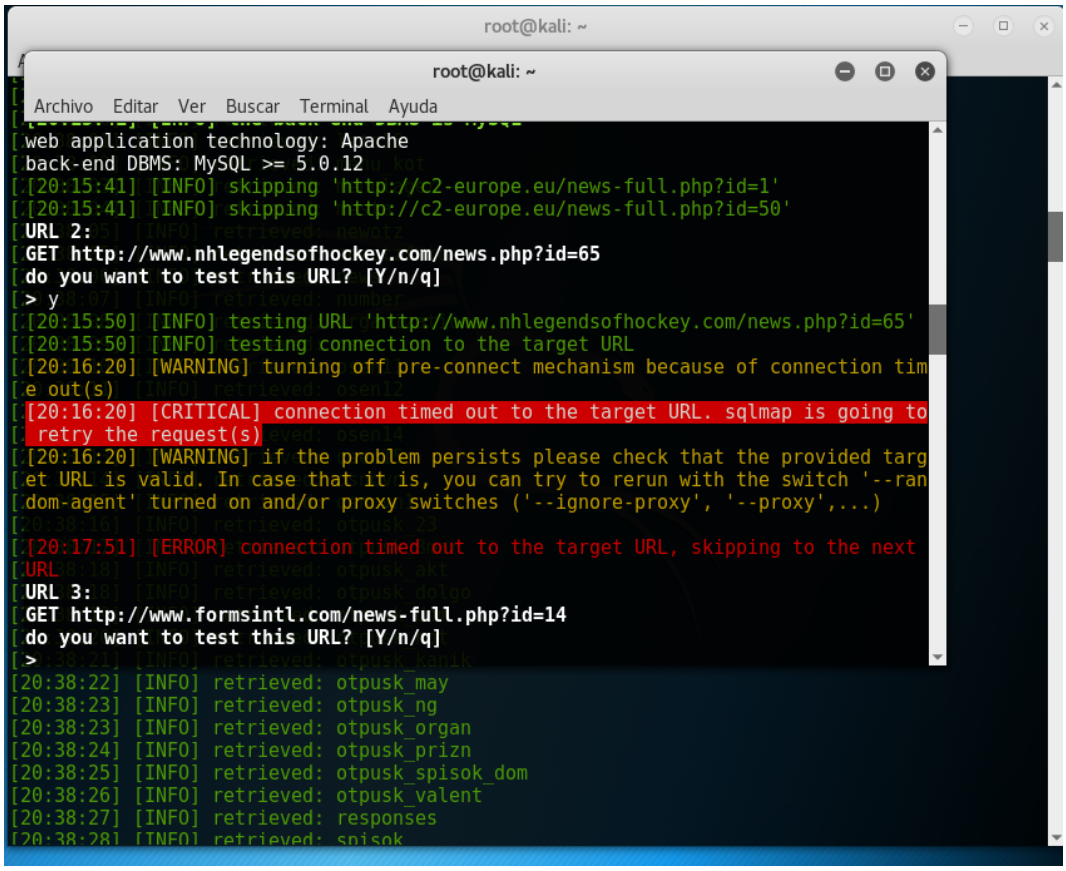
Ilustración 49. Información obtenida de la búsqueda



Fuente: el autor

Nos va dando una lista de URL y nos da la información de lo que contiene, en el ejemplo que a continuación vemos nos está diciendo que en esa URL tenemos una cantidad de páginas y otra información.

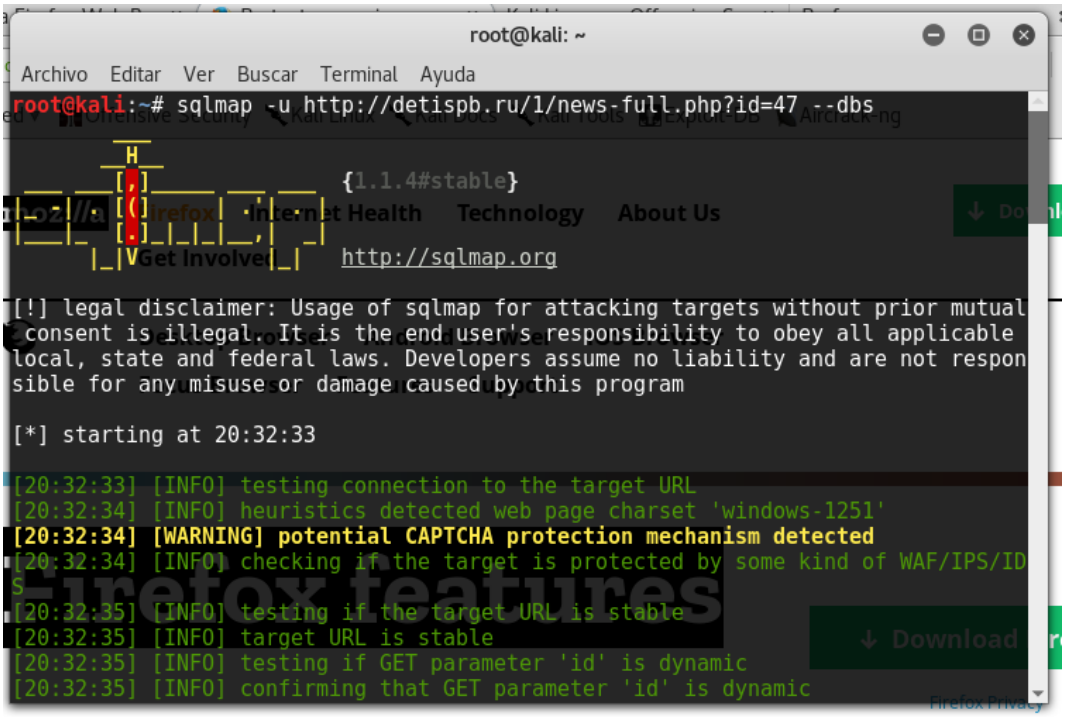
Ilustración 50. Información obtenida de la búsqueda – parte 1



Fuente: el autor

Procedemos a coger una URL de las que está escaneando para ver si tienen bases de datos, con el comando sqlmap -u “URL” –-dbs

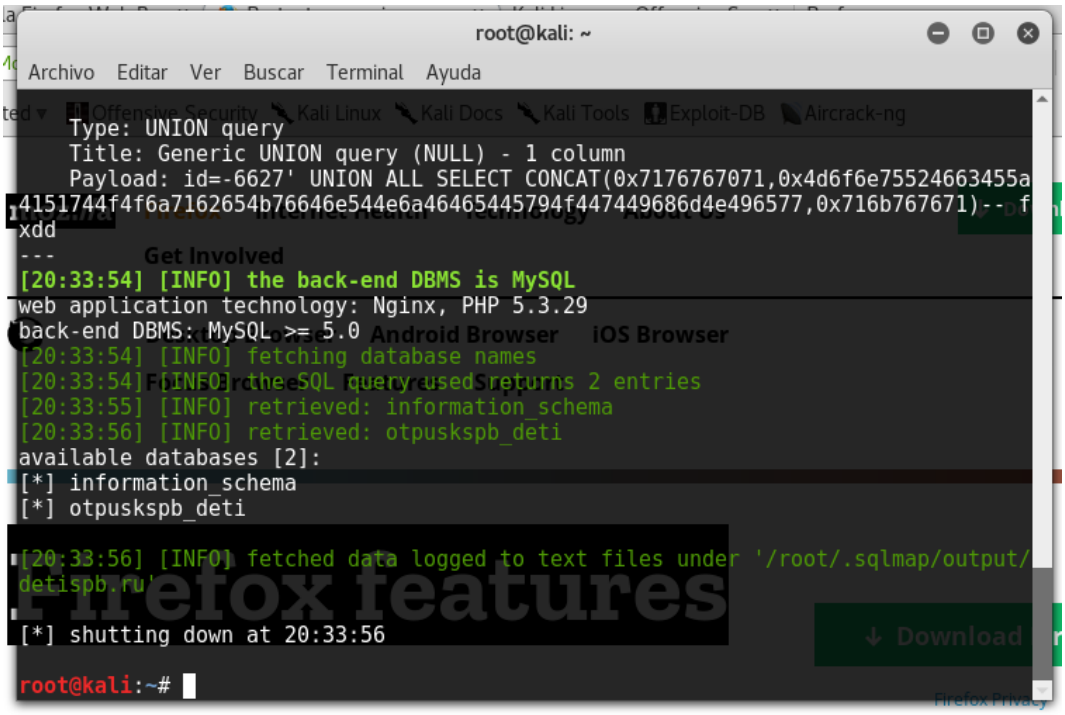
Ilustración 51. Escaneo para encontrar la Base de datos



Fuente: el autor

Con el comando -u es para que nos pueda ubicar la URL y con el comando –dbs es para que nos liste las bases de datos que encuentra en esa URL

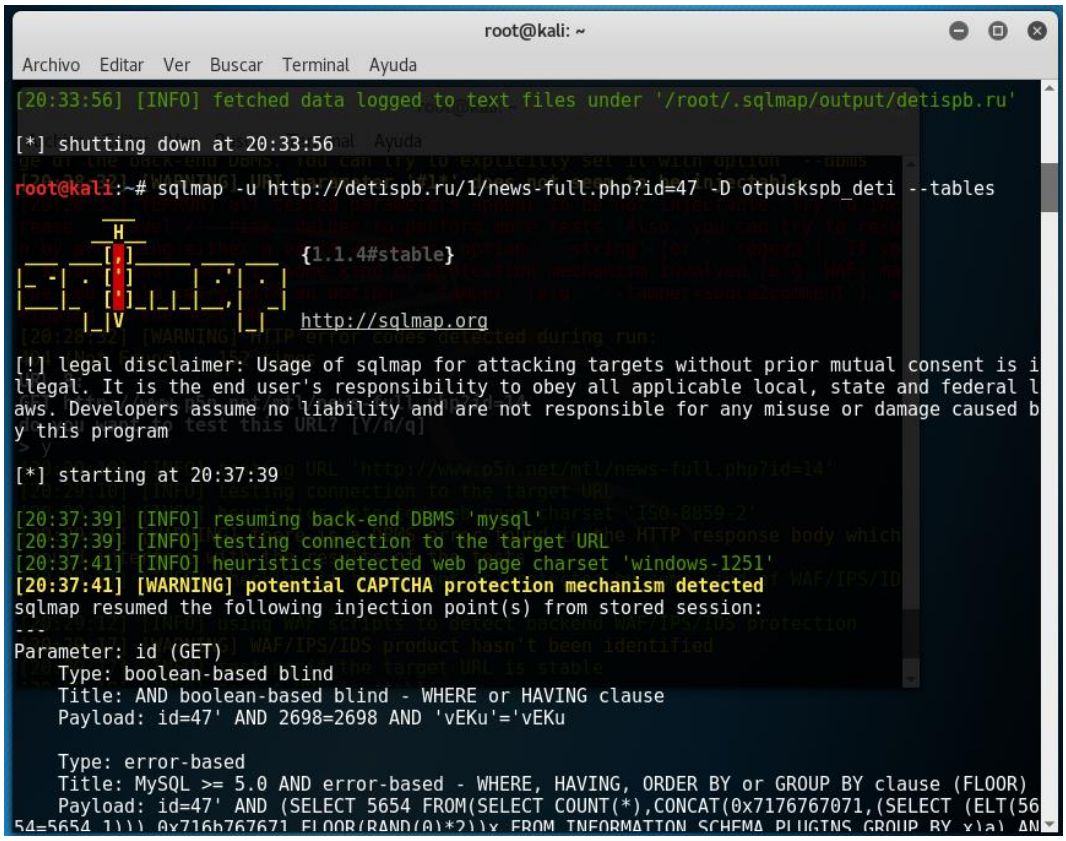
Ilustración 52. Ver contenido de la Base de Datos



Fuente: el autor

En nuestro caso encontró 2 bases de datos en esa URL. Ahora con el comando sqlmap -u “URL” -D “nombre de Base de datos” –table. Nos hará el escaneo para mostrarnos que tablas encontró en esa base de datos

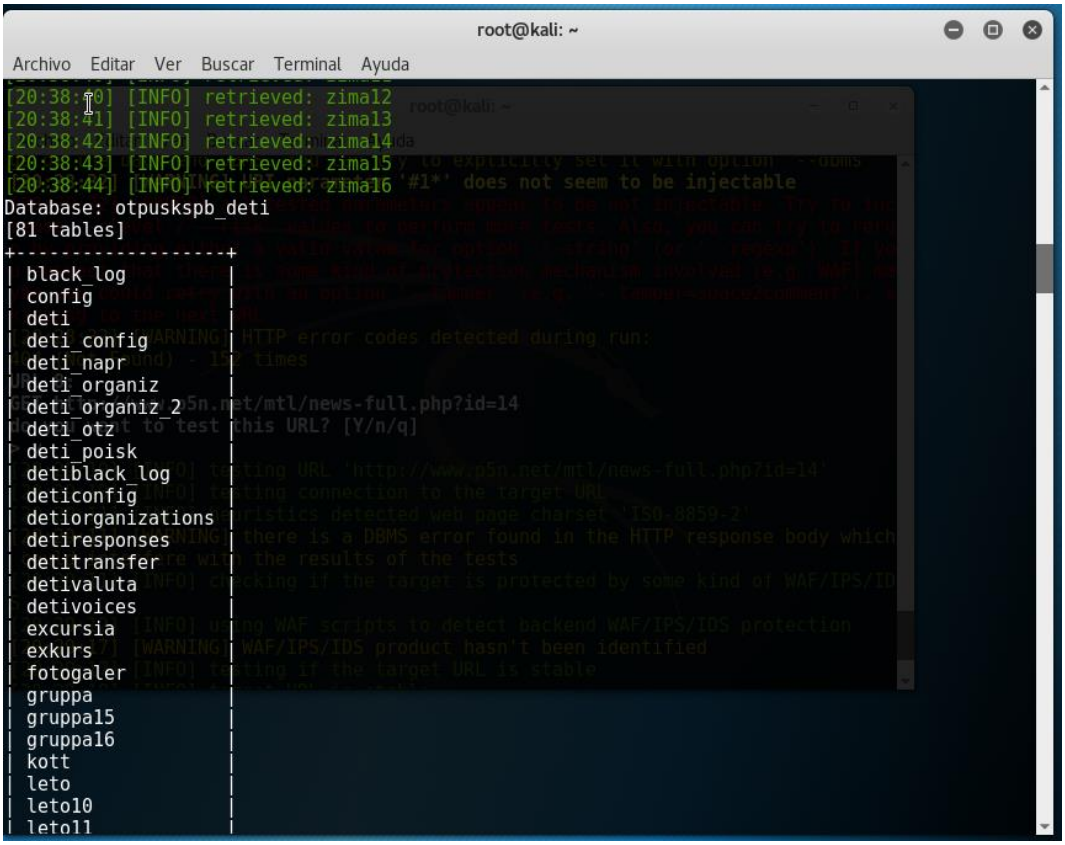
Ilustración 53. Muestra las bases de datos encontradas



Fuente: el autor

El escanea hasta que nos da la lista de las tablas encontradas en esa base de datos

Ilustración 54. Escaneo de las tablas a la base de datos encontrada



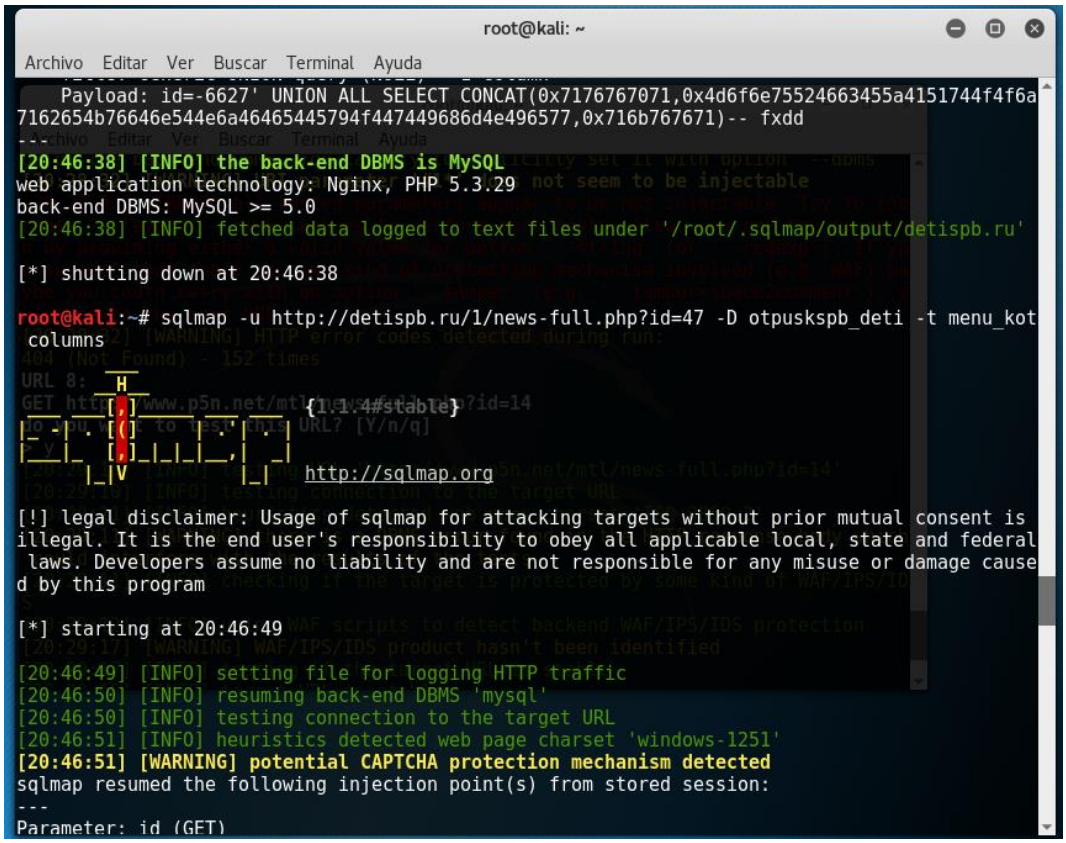
Fuente: el autor

En nuestro caso nos está diciendo que en esa base de datos se encontró 81 tablas

Ya teniendo las tablas se puede seleccionar una y ver que datos encuentra en ellas

Con el comando sqlmap -u “URL” -D “nombre de Base de datos” –t “nombre de la tabla” -columns

Ilustración 55. Visualizar información de las tablas



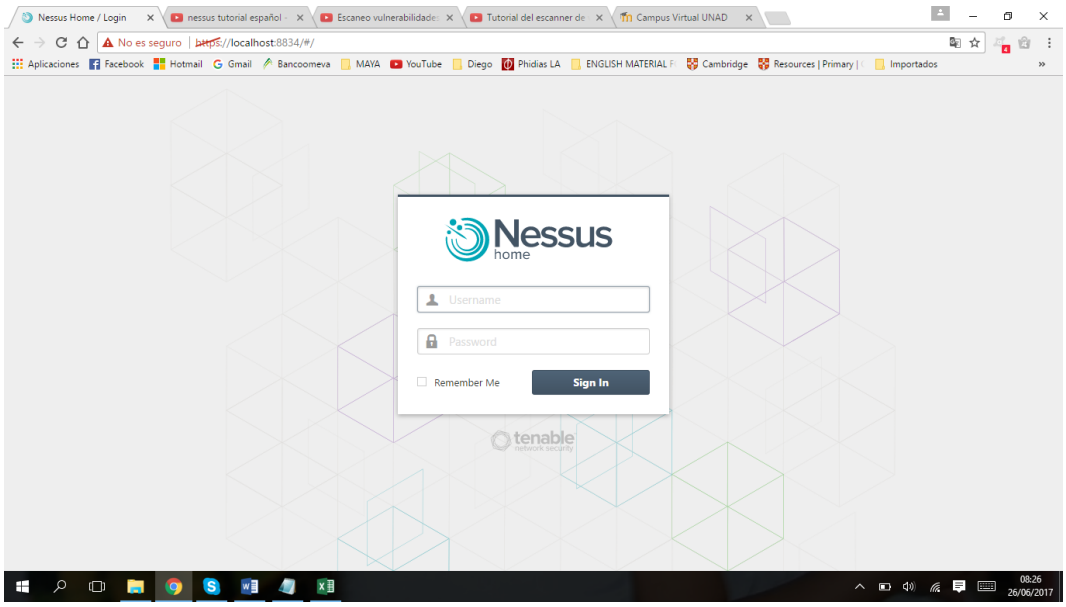
Fuente: el autor

En el caso nos deja entrar a ver el contenido de las tablas, pero no me permite manipularlas, lo cual con todo este proceso permite vulnerar base de datos, pues con el solo fin que me permita ver las tablas que hay dentro de una base de datos y su contenido, así no se pueda manipular el contenido estamos vulnerando la información y obteniendo respuesta a lo que hemos pedido que es encontrar información dentro de una base de datos.

5.3. NESSUS

Procedemos a entrar al Nessus por medio de la URL http://localhost:8834

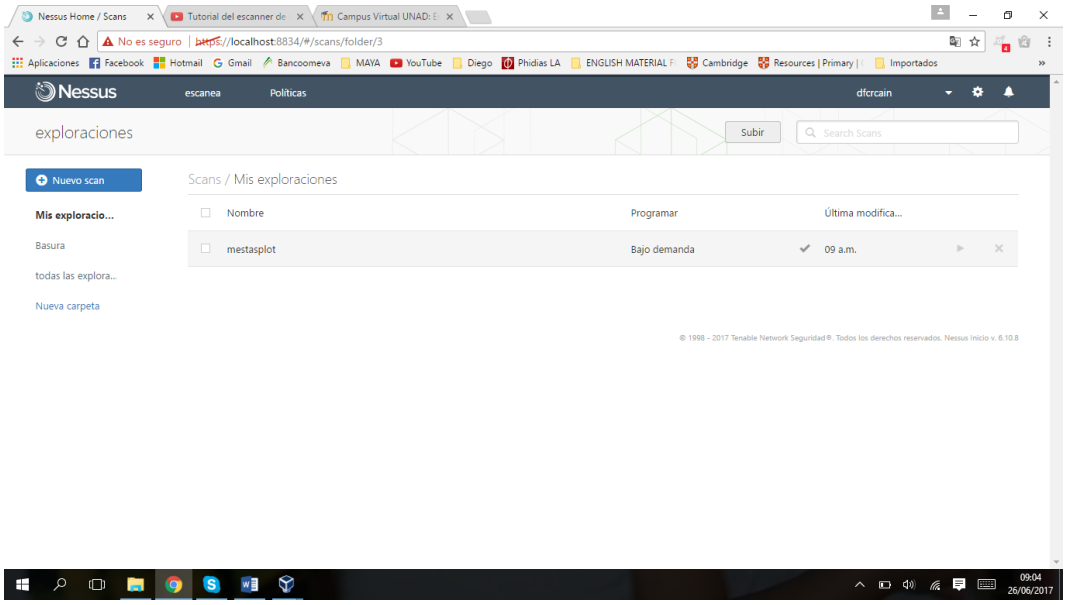
Ilustración 56. Ingreso a la plataforma de Nessus



Fuente: el autor

Entramos a Nessus con nuestro Id y nuestros Pass

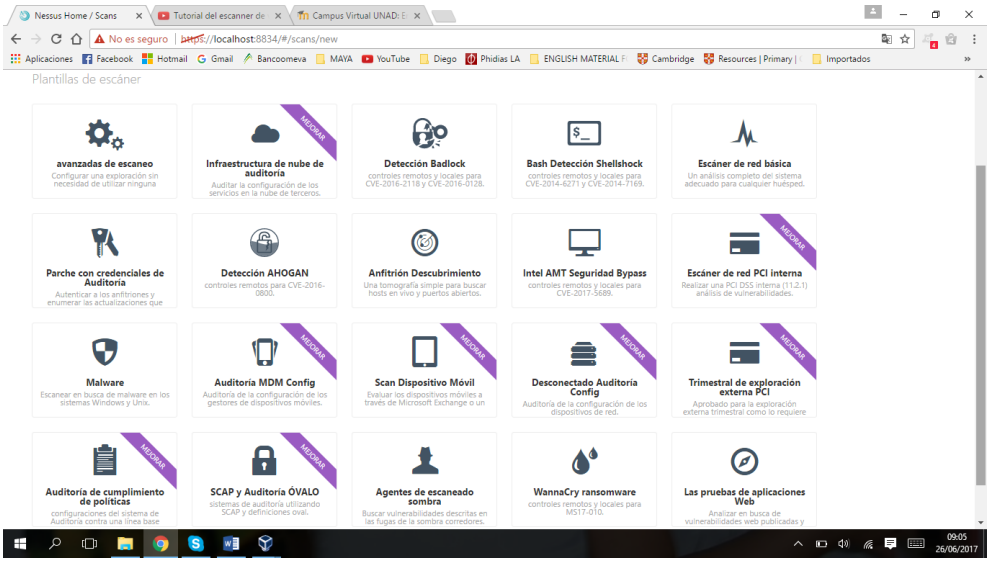
Ilustración 57. Página principal de Nessus



Fuente: el autor

Nos carga la página principal de Nessus y posteriormente vamos a escaneo para ver las opciones

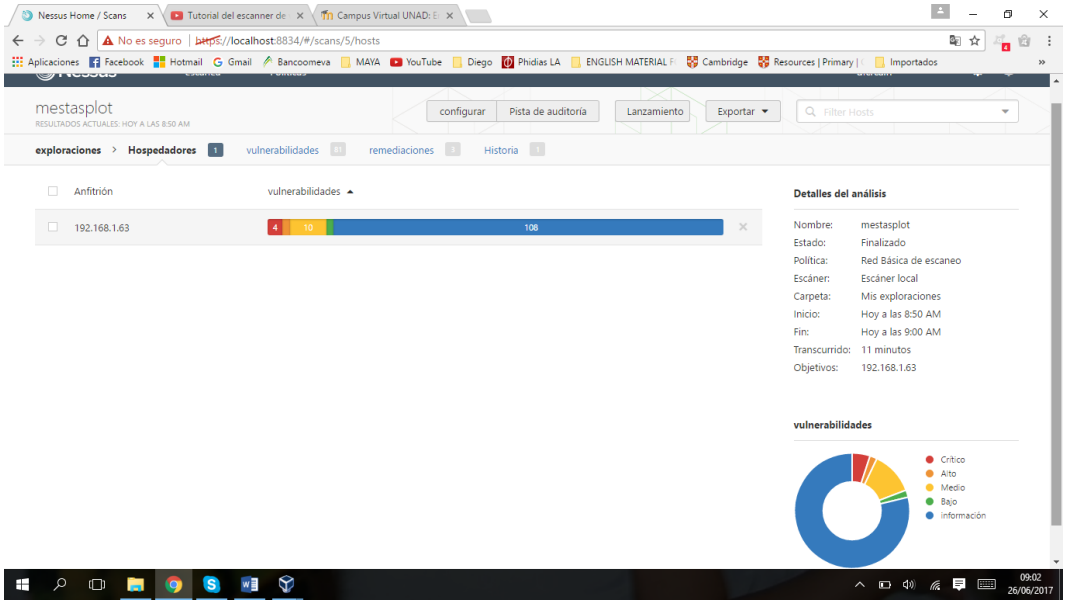
Ilustración 58. Opciones y configuración de Nessus



Fuente: el autor

Escogemos que opción o políticas queremos hacer para ver las vulnerabilidades, en mi caso escogí escanear una red básica, donde nos pide definir el escaneo, donde nos pide el nombre que queremos asignarle al escaneo y la IP que vamos escáner en mi caso el mi maquina principal tiene la IP 192.168.0.17. Una vez iniciamos el scan Nessus nos muestra los resultados

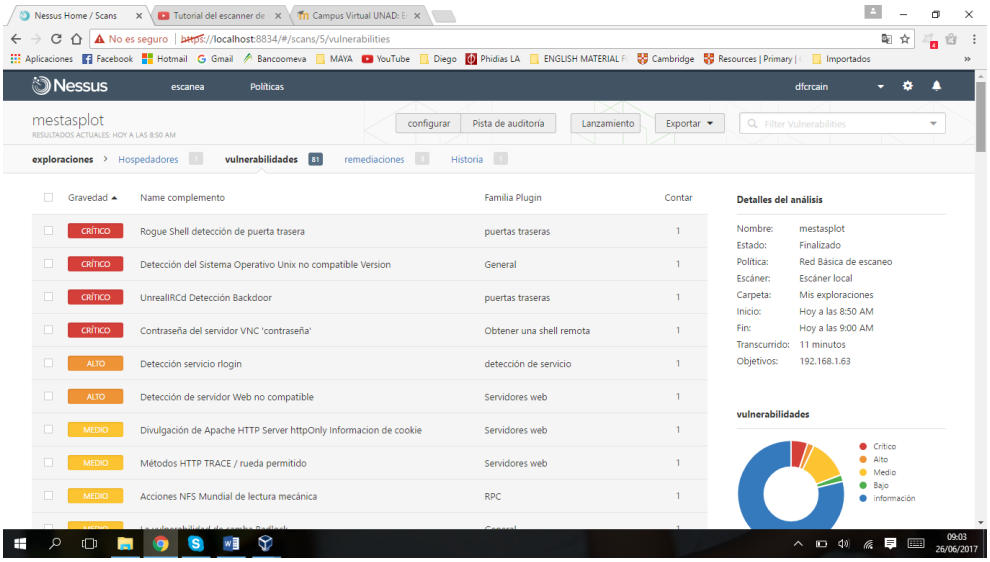
Ilustración 59. Escaneo de vulnerabilidades encontradas



Fuente: el autor

En la primera pantalla nos muestra los porcentajes de cada tipo de vulnerabilidad, donde vamos a encontrar desde información color azul, bajo de color verde, medio de color amarillo, alto de color naranja y crítico de color rojo

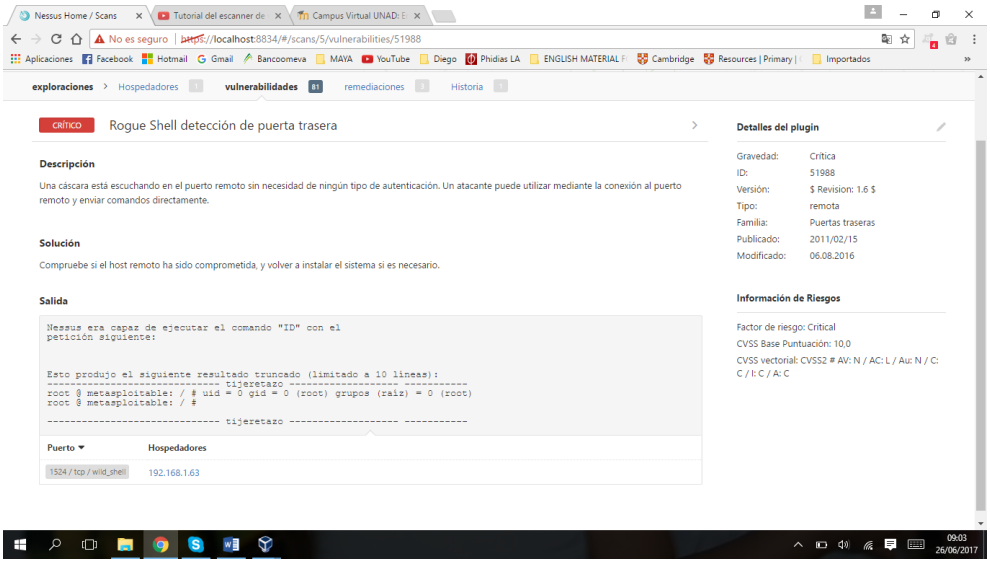
Ilustración 60. Información de las vulnerabilidades encontradas



Fuente: el autor

Si entramos a la pestaña de las vulnerabilidades nos va a listar cada una de ellas y dando clic sobre la vulnerabilidad nos va arrojar la información pertinente

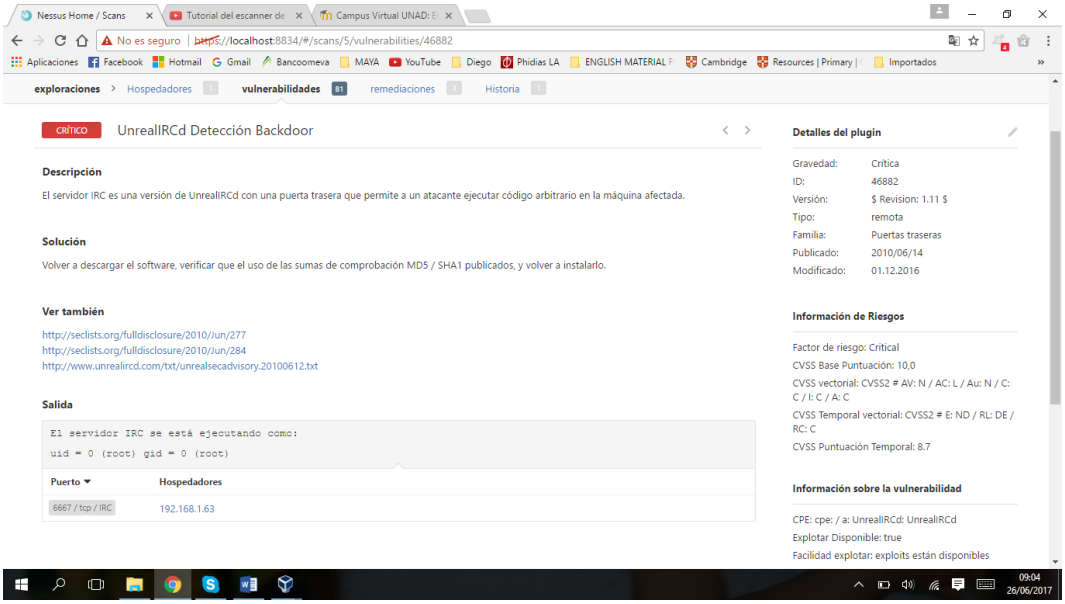
Ilustración 61. Informacion sobre la vulneravilidad



Fuente: el autor

Para este caso vemos una vulnerabilidad de tipo critico donde nos describe el problema y también nos da una solución para corregir

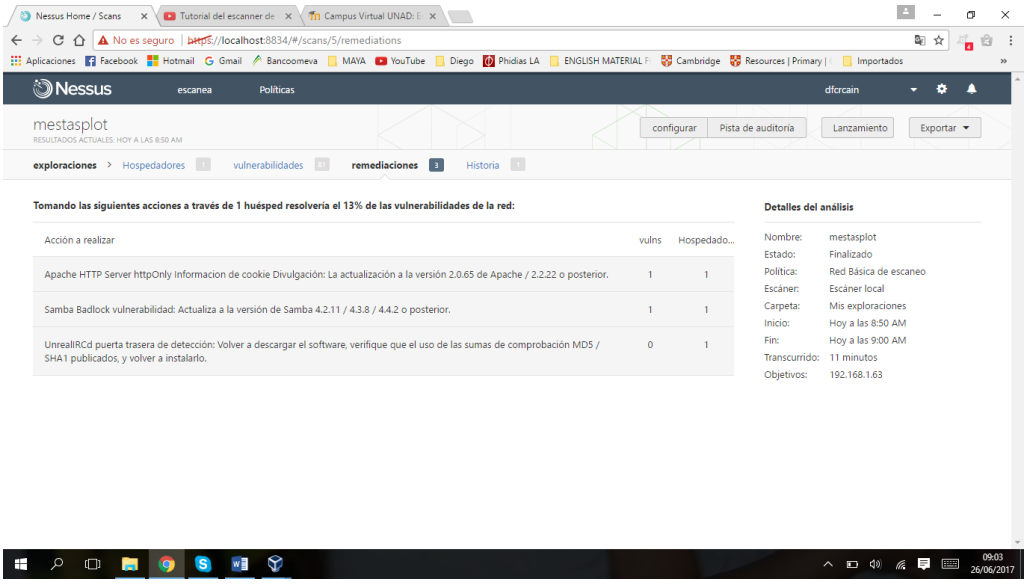
Ilustración 62. Posible solución para la vulnerabilidad



Fuente: el autor

Aquí vemos otro ejemplo donde para todas las vulnerabilidades q nos encuentra nos va a dar la misma información

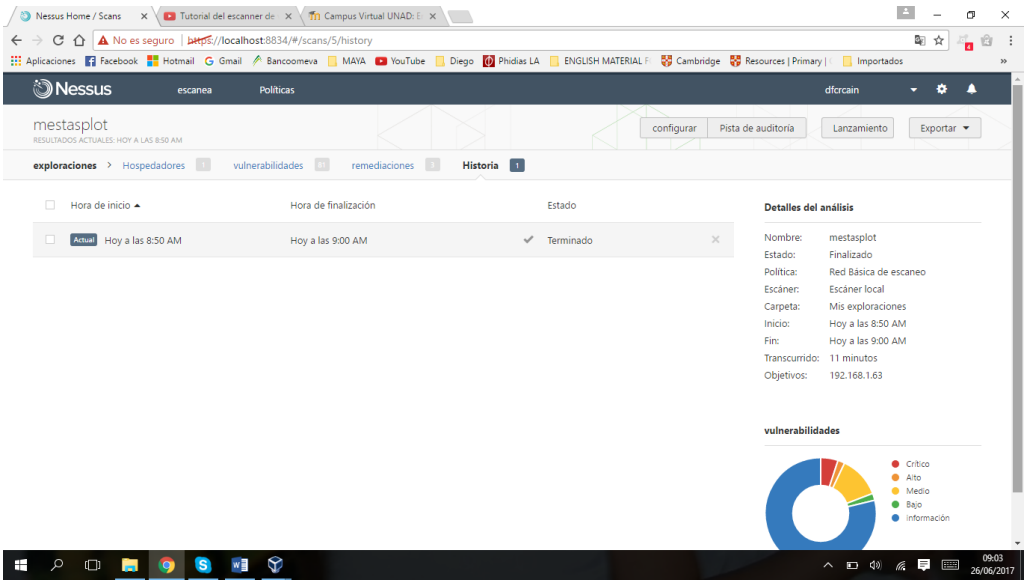
Ilustración 63. Otra vulnerabilidad



Fuente: el autor

También en otra pestaña Nessus nos da como una recomendación a hacer para resolver gran parte de los problemas de las vulnerabilidades.

Ilustración 64. Otra opción para resolver las vulnerabilidades



Fuente: el autor

En la última pantalla que nos muestra es un historial de las veces que se han hecho el escaneo.