UNIVERSIDAD TÉCNICA DE COTOPAXI

FACULTAD DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

CARRERA DE INGENIERÍA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES

PROYECTO DE INVESTIGACIÓN

"ANÁLISIS DE LA CIBERSEGURIDAD A LA INFRAESTRUCTURA TECNOLÓGICA DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI"

Proyecto de titulación presentado previo a la obtención del título de Ingenieros en Informática y Sistemas Computacionales.

AUTORES:
Alvarado Llano Washington Orlando
Changoluisa Pachacama Iván Santiago

TUTOR:
Ing. Mg. Manuel Villa Quishpe

Latacunga – Ecuador

Julio 2019

Universidad Técnica de Cotopaxi

Ingeniería Informatica Y Sistemas Computacionales

DECLARACIÓN DE AUTORÍA

Nosotros, **Alvarado Llano Washington Orlando y Changoluisa Pachacama Iván Santiago,** declaramos ser autores del presente proyecto de investigación **"ANÁLISIS DE LA CIBERSEGURIDAD A LA INFRAESTRUCTURA TECNOLÓGICA DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI",** siendo el Mg. Manuel Villa Quishpe tutor del presente trabajo, y absolvemos expresamente a la Universidad Técnica de Cotopaxi y sus representantes legales del posible reclamo o acción legal.

Además, certifico que las ideas, conceptos, procedimientos y resultados vertidos en el presente proyecto de investigación, son de mi exclusiva responsabilidad.

.....	.....
Washington Orlando Alvarado Llano	Changoluisa Pachacama Iván Santiago
CI. 0503370223	CI.1721652830

ii

Universidad Técnica de Cotopaxi

Ingeniería Informatica Y Sistemas Computacionales

AVAL DEL TUTOR DE PROYECTO DE TITULACIÓN

En calidad de Tutor del Trabajo de Investigación sobre el título: **"Análisis de la ciberseguridad a la infraestructura tecnológica de la Universidad Técnica de Cotopaxi"**, de **Alvarado Llano Washington Orlando y Changoluisa Pachacama Iván Santiago**, de la Carrera de Ingeniería en Informática y Sistemas Computacionales, considero que dicho Informe Investigativo cumple con los requerimientos metodológicos y aportes científico-técnicos suficientes para ser sometidos a la evaluación del Tribunal de Validación de Proyecto que el Consejo Directivo de la Facultad de Ciencias de la Ingeniería y Aplicadas de la Universidad Técnica de Cotopaxi designe, para su correspondiente estudio y calificación.

Latacunga, 24 de julio del 2019

.....

Ing. Mg. Manuel William Villa Quishpe

C.I.: 1803386950

Universidad Técnica de Cotopaxi

Ingeniería Informatica Y Sistemas Computacionales

APROBACIÓN DEL TRIBUNAL DE TITULACIÓN

En calidad de Tribunal de Lectores, aprueban el presente Informe de Investigación de acuerdo a las disposiciones reglamentarias emitidas por la Universidad Técnica de Cotopaxi, y por la FACULTAD de Ciencias de la Ingeniería y Aplicadas; por cuanto, los postulantes: **Alvarado Llano Washington Orlando y Changoluisa Pachacama Iván Santiago**, con el título de Proyecto de titulación: **"Análisis de la ciberseguridad a la infraestructura tecnológica de la Universidad Técnica de Cotopaxi"** han considerado las recomendaciones emitidas oportunamente y reúne los méritos suficientes para ser sometido al acto de Sustentación de Proyecto.

Por lo antes expuesto, se autoriza realizar los empastados correspondientes, según la normativa institucional.

Latacunga, 22 de julio del 2019.

Para constancia firman:

.....

Lector 1
Ing. MSc. Alex Llano
0502589864

.....

Lector 2
Ing. MSc. Corrales Segundo
CI. 0502409287

.....

Lector 3
Ing. MSc. Víctor Medina
CI. 0501373955

AGRADECIMIENTO

Quiero expresar mi gratitud a Dios, quien con su bendición me ha guiado para llegar a este triunfo en mi vida, por haberme permitido estar dónde me encuentro, y por lo que día a día pone en mi camino. A mi familia, por ser mi guía y acompañarme en el transcurso de mi vida, brindándome paciencia y sabiduría para culminar con éxito mis metas propuestas, pese a las adversidades e inconvenientes que se presentaron. A la Universidad Técnica de Cotopaxi, a la Carrera de Ciencias de la Ingeniería y Aplicadas, a los docentes por impartir sus conocimientos necesarios para poder culminar con éxito mis estudios. A mi Tutor de tesis Mg. Manuel Villa por su esfuerzo, dedicación, paciencia y por el apoyo y la confianza brindada, quien, con sus conocimientos, su experiencia nos supo guiar durante el desarrollo del proyecto de investigación.

WASHINGTON

AGRADECIMIENTO

A mis padres, abuelitos Gonzalo y María, Víctor y Anita quienes con su amor, paciencia y esfuerzo me han permitido llegar a cumplir hoy un sueño más, gracias por inculcar en mí el ejemplo de esfuerzo y valentía, de no temer las adversidades porque Dios está conmigo siempre.

IVÁN

DEDICATORIA

Dedico este trabajo principalmente a Dios, por haberme dado la vida y permitirme el haber llegado hasta este momento tan importante de mi formación profesional.

A mi esposa Carla quien ha estado en todo momento cuando más la necesitaba, por haberme dado su confianza, cariño y apoyo condicional para continuar con este proyecto, a mi hijo Martin quien es mi inspiración para poder seguir creciendo no solo como persona si no profesionalmente.

A mi madre Clemencia y a mi padre Fausto, por ser el pilar más importante y por demostrarme siempre su cariño y apoyo incondicional, por siempre ayudarme en las buenas y en las malas y en todo momento, siempre confiaron en mí y nunca me abandonaron. Gracias a todos.

WASHINGTON

DEDICATORIA

Quiero dedicar este proyecto. A mis hermanas Sonia y Linda Gabriela y especialmente a ti hermana desde cielo siempre me guías para termina mis sueños de ser alguien en la vida mi Linda Karina, por su cariño y apoyo incondicional, durante todo este proceso, por estar conmigo en todo momento gracias. A toda mi familia porque con sus oraciones, consejos y palabras de aliento hicieron de mí una mejor persona y de una u otra forma me acompañan en todos mis sueños y metas.

IVÁN

ÍNDICE GENERAL

INDICE DE TABLAS

ÍNDICE DE GRÀFICOS

UNIVERSIDAD TÉCNICA DE COTOPAXI

FACULTAD DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

TÍTULO: "ANÁLISIS DE LA CIBERSEGURIDAD A LA INFRAESTRUCTURA TECNOLÓGICA DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI"

AUTORES:
ALVARADO LLANO WASHINGTON ORLANDO
CHANGOLUISA PACHACAMA IVÁN SANTIAGO

RESUMEN

La ciberseguridad es un activo muy importante dentro de una empresa ya que trata principalmente del cuidado de los sistemas informáticos, es por ello que hoy en día en el Ecuador las empresas deciden implementar herramientas que puedan determinen el nivel de vulnerabilidad que existe dentro de su infraestructura tecnológicas, con el objetivo de prevenir posibles ataques cibernéticos o robos de información. En este sentido la presente investigación se desarrolló en torno al usó de entrevistas y encuestas al departamento de sistemas, docentes y alumnos, con la finalidad de tener una muestra de las falencias que tiene la institución en cuanto a ciberseguridad, además se obtuvo referencias bibliográficas en libros, internet y otros medios de comunicación para su familiarización en el presente tema.

En cuanto a los métodos de la investigación se ha orientado por el método Hipotético-Deductivo ya que permito conocer el origen del problema partiendo de lo más general a lo específico para mejor compresión del tema y cada uno de sus derivados. La presente investigación se basa en la norma ISO/IEC 27032/2012 un nuevo estándar de seguridad que resguarda la información de riesgos existentes en el ciberespacio, esto permitiéndonos a cumplir a cabalidad con los objetivos trazados y entregar posibles recomendaciones en conjunto con los resultados de los análisis realizados.

Palabras Claves: Seguridad informática, ciberseguridad, Linux., ataques informáticos, vulnerabilidades.

UNIVERSIDAD TÉCNICA DE COTOPAXI

FACULTAD DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

THEME: "ANALYSIS OF THE CIBERSECURITY TO THE TECHNOLOGICAL INFRASTRUCTURE OF THE TECHNICAL UNIVERSITY OF COTOPAXI"

AUTORE:

ALVARADO LLANO WASHINGTON ORLANDO
CHANGOLUISA PACHACAMA IVÁN SANTIAGO

ABSTRACT

Cybersecurity is a very important asset within a company because it deals mainly with the care of computer systems, that is why today in Ecuador companies decide to implement tools that can determine the level of vulnerability that exists within its technological infrastructure, with the aim of preventing possible cyber-attacks or information theft. In this sense, this research was developed around the use of interviews and surveys to the systems department, teachers and students, in order to have a sample of the shortcomings that the institution has in terms of Cybersecurity, also obtained bibliographic references were obtained in books, Internet and other media for familiarization in the present research.

As for the research methods, it has been guided by the Hypothetical-Deductive method since it allows us to know the origin of the problem, starting from the most general to the specific, for a better understanding of the subject and each one of its derivatives. This research was carried out based on the ISO/IEC 27032/2012 standard, a new safety standard that protects the information of existing risks in cyberspace, allowing us to fully comply with the objectives set and provide possible recommendations altogether with the results of the analysis performed.

Keywords: computer security, cybersecurity, Linux, computer attacks, vulnerabilities.

Universidad Técnica de Cotopaxi

CENTRO DE IDIOMAS

AVAL DE TRADUCCIÓN

En calidad de Docente del Idioma Inglés del Centro de Idiomas de la Universidad Técnica de Cotopaxi; en forma legal **CERTIFICO** que: La traducción del resumen del proyecto de investigación al Idioma Inglés presentado por los señores Egresados de la Carrera de **INGENIERÍA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES** de la **FACULTAD DE CIENCIAS DE LA INGENIERÍA Y APLICADAS, ALVARADO LLANO WASHINGTON ORLANDO** y **CHANGOLUISA PACHACAMA IVÁN SANTIAGO**, cuyo título versa **"ANÁLISIS DE LA CIBERSEGURIDAD A LA INFRAESTRUCTURA TECNOLÓGICA DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI"**, lo realizaron bajo mi supervisión y cumple con una correcta estructura gramatical del Idioma.

Es todo cuanto puedo certificar en honor a la verdad y autorizo a los peticionarios hacer uso del presente certificado de la manera ética que estimaren conveniente.

Latacunga, Julio 2019

Atentamente,

Lic. María Fernanda Aguaiza Iza
DOCENTE CENTRO DE IDIOMAS
C.C. 050345849-9

CENTRO DE IDIOMAS

1. INFORMACIÓN GENERAL

Título de proyecto: Análisis de la ciberseguridad a la infraestructura tecnológica de la UNIVERSIDAD TÉCNICA DE COTOPAXI

Fecha de inicio: Abril del 2019

Fecha de finalización: julio del 2019

Lugar de ejecución: Universidad Técnica de Cotopaxi

Unidad Académica que auspicia: Facultad de Ciencias de la Ingeniería y Aplicadas (CIYA)

Carrera que auspicia: Ingeniería en Informática y Sistemas Computacionales

Proyecto de investigación vinculación: Análisis de la Ciberseguridad a la Infraestructura Tecnológica dirigido a la Universidad Técnica de Cotopaxi

Equipo de trabajo:

TUTOR
Manuel William Villa Quisphe

AUTORES:
Alvarado Llano Washington Orlando
Changoluisa Pachacama Iván Santiago

Área de conocimiento

Línea de investigación: Tecnología de la información y comunicación.

Sub línea: Seguridad informática, ataques cibernéticos, vulnerabilidades

2. RESUMEN DEL PROYECTO

La ciberseguridad, también conocida como seguridad informática es aquella que se enfoca en la protección de la infraestructura computacionales, permitiendo dar a conocer los activos informáticos y sus vulnerabilidades y amenazas a los que se encuentran expuestos, así como su probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo a posibles ataques.

Teniendo en cuenta que las inseguridades de los sistemas informáticos podrían causar daños o pérdidas financieras o administrativas a instituciones públicas o privadas, nos hemos planteado como necesidad realizar un análisis a la infraestructura tecnológica de la Universidad Técnica de Cotopaxi, con el objetivo de estimar la magnitud del riesgo a que se encuentra expuesto su sistema informático de tal manera que permita determinar posibles brechas de seguridad.

Los objetivos fundamentales de la seguridad informática es contar con ejes principales en los que se enfoquen en la integridad, privacidad y disponibilidad de la información de cualquier sistema informático, esto solo podría lograrse contando con las herramientas necesarias y el personal debidamente capacitado para poder administrar todas las plataformas que sean asignadas.

En la actualidad la ciberseguridad es una rama de la informática en la cual se basa en proveer técnicas y herramientas necesarias para proteger la integridad de la información y que esta esté disponible cuando se la necesite. Hoy en día las personas que se dedican de lleno a cualquier campo de la informática y especialmente en el campo de la seguridad saben que cuentan con muchas herramientas para poder ser utilizadas y estar al tanto de las distintas amenazas que pudieran generarse dentro de una red corporativa.

Las herramientas de seguridad, escaneo de redes, auditoria o pentesting en la actualidad son muchas, y hoy por hoy gran parte de ellas son multiplataforma, de software libre e incluso de paga, cada una de ellas con alguna particularidad, pero lo rescatable de todo esto es que, así como se generan vulnerabilidades informáticas a diario también tenemos herramientas con las

cuales nos podemos defender y contrarrestar al máximo los problemas que estas brechas de seguridad nos podrían generar.

3. JUSTIFICACIÓN

En el Ecuador la ciberseguridad es un tema innovador, ya que en los últimos años un cierto porcentaje de empresas públicas y privadas han sufrido ataques cibernéticos a sus sistemas informáticos, poniendo en riesgos datos importantes de la empresa. Esto debido a que hay varias empresas que no tienen un sistema de seguridad, que controle la vulnerabilidad de sus equipos tecnológicos, haciéndolos más vulnerables a los ataques cibernéticos que existen en la actualidad.

El presente proyecto de investigación tiene como propósito realizar un análisis de factibilidad técnica y tecnológica a la infraestructura tecnológica de la Universidad Técnica de Cotopaxi, con la finalidad de mejorar la ciberseguridad de los recursos tecnológicos, para evitar amenazas que existe en el amplio mundo del internet por medio de procesos, planes y políticas de seguridad, la cual fortalecerá la parte intangible de la institución y evitar perdida de información.

El análisis se efectuará utilizando el sistema operativo Kali Linux GNU, el cual se instalará en los distintos equipos virtuales de una máquina física y de manera independiente a su sistema operativo nativo. El análisis se lo ejecutará de una parte interna o externa a la institución dónde se evaluará el proceso ejecutado y datos obtenidos durante el proceso.

4. BENEFICIARIOS DEL PROYECTO

- **Beneficiarios Directos**

Estudiantes, docentes, empleados y personal administrativo de la Universidad Técnica de Cotopaxi.

- **Beneficiarios Indirectos**

Población visitante de la Universidad Técnica de Cotopaxi.

5. PROBLEMA DE INVESTIGACIÓN

El avance tecnológico a nivel mundial ha transformado las operaciones de las empresas e instituciones y la forma en cómo interactúan las personas, pero a la vez han traído riesgos y dificultades en cuanto a la seguridad de la información. Según el informe sobre riesgos globales para 2016 del Foro Económico Mundial, los ataques cibernéticos se han considerado como uno de los principales riesgos globales entre los más probables de ocurrir y con mayores consecuencias, en los últimos años han aumentado rápidamente atacando a los negocios en todo tipo de sectores empresariales, para ello se necesitarán implementar nuevas herramientas que garanticen la seguridad minimizando los riesgos de ataques cibernéticos.

En la actualidad muchas organizaciones de cualquier sector, cuyos procesos críticos de negocio dependen de la tecnología, desconocen los riesgos a los que se exponen, producto de las posibles brechas de seguridad existentes en su plataforma tecnológica.

Gran parte de las empresas en el Ecuador son consideradas las más vulnerables a los ciberataques porque desconocen el impacto que pueden tener sobre su negocio. Esto lleva a que muchas no implementen las acciones necesarias para protegerse de manera efectiva, produciéndoles una pérdida de información que puede ser muy grande y recuperarse puede demandar mucho tiempo ya que los ciberataques pueden causar daño a la marca y pérdida de clientes.

5.1. Planteamiento del problema

¿Cómo mejorar la Ciberseguridad de la infraestructura tecnológica de la Universidad Técnica de Cotopaxi?

6. OBJETIVOS

6.1. OBJETIVO GENERAL

- Analizar la ciberseguridad a la infraestructura tecnológica de la UNIVERSIDAD TÉCNICA DE COTOPAXI, a través del sistema operativo Kali Linux, virtualizado en una maquina física para disminuir riesgos existentes a sus sistemas informáticos.

6.2. OBJETIVOS ESPECÍFICOS

- Detectar las brechas de seguridad que posee la plataforma tecnológica de la Institución por dónde un intruso o "hacker" podría acceder de forma no autorizada a sus activos de información.

- Presentar los riesgos asociados a las debilidades detectadas durante el análisis, detallando las consecuencias que podrían ocasionar a sus sistemas de información.

- Sugerir las alternativas que contribuyan a solventar o minimizar las vulnerabilidades detectadas durante el análisis, detallando los pasos a seguir para su protección.

7. ACTIVIDADES Y SISTEMA DE TAREAS EN RELACIÓN A LOS OBJETIVOS PLANTEADOS

Tabla 1: Actividades planificadas para darle cumplimiento a los objetivos

Objetivo	Actividad (Tareas)	Resultado de la actividad	Descripción de la actividad técnicas e instrumentos
Detectar las brechas de seguridad qu pose la plataforma tecnológica de Institución por dónde un intruso o "hacker" podría acceder de forma no autorizada a sus activos de información.	Inspección visual de los equipos tecnologícos de la Universidad Técnica de Cotopaxi	Fundamentación teórica del proyecto de investigación.	• Encuetas • Entrevistas • Investigación de campo.
Presentar los riesgos asociados a las debilidades detectadas durante el análisis, detallando las consecuencias que podrían ocasionar a los activos de información.	Elaboración de un informe sobre la vulnerabilidad de la infraestructura de la Universidad Técnica de Cotopaxi después de una exhaustiva Investigación,	Proyecto de investigación. Análisis de la ciberseguridad a la infraestructura tecnológica de la UTC.	• Aplicación Word
Sugerir las alternativas que contribuyan a solventar o minimizar las vulnerabilidades detectadas durante el análisis, detallando los pasos a seguir para su protección	Exposición de las alternativas para optimizar las infraestructura tecnológica de la Universidad Técnica de Cotopaxi	Proyecto de investigación.	• Investigación explicativa y descriptiva.

Fuente: Los autores

8. FUNDAMENTACIÓN CIENTÍFICO TÉCNICA

8.1. Antecedentes

A nivel mundial el concepto de seguridad informática ha ido incrementando su importancia, pese a que en algunos países aún sea un tema poco explorado. Pero lo realmente importante de esto es orientarse hacia esta rama de la informática y destacar que esta, hoy por hoy, deja de ser un recurso para convertirse en una necesidad, tanto para las empresas sin importar su tamaño, como para las personas.

Tanto es así, que en muchas organizaciones en las que la cultura informática está bien definida, la seguridad de la información ha pasado de ser un gasto a una necesidad. En la actualidad la seguridad informática ha adquirido tal nivel de relevancia debido a que es una manera de mantener y precautelar la integridad del activo más importante de una empresa: la información. Por lo tanto, es fundamental que aparezcan más personas capacitadas con un rol específico que tengan la capacidad de aplicar y hacer valer todos estos conceptos, a estos especialistas también se los puede llamar con el término de hacker ético.

Este individuo mira y analiza desde el punto de vista de un cracker y efectúa las técnicas conocidas dentro de un ambiente real como también dentro de uno simulado. Con el único objetivo de poder determinar las vulnerabilidades existentes y sus respectivas remediaciones, todo esto dentro del marco de la ética profesional. Esta persona posee el conocimiento necesario para aplicar cualquier técnica de penetración (pentesting) que pueda determinar alguna brecha de seguridad en sus distintos niveles.

La seguridad informática se basa principalmente en tres pilares fundamentales: integridad, disponibilidad y confidencialidad. Estos pilares deben de ser forjados mediante el uso de herramientas, la implementación de políticas y el cumplimiento de procesos. Es aquí dónde interviene el rol de un especialista en seguridad informática. Los especialistas de seguridad informática son los idóneos para determinar si un sistema o servicio es seguro y para ello se realizan una serie de análisis que ayudarán a determinar si el objeto de estudio cumple con los tres conceptos fundamentales.

De manera general lo primero es evaluar por ejemplo los tipos de ataques más comunes que podría sufrir la empresa. Considerando esto, se realizan una serie de pruebas de vulnerabilidad a los servicios o recursos que son considerados como los objetivos más básicos y comunes. En la actualidad la información sobre los diferentes tipos de ataques informáticos es muy amplia, puesto que se puede encontrar información acerca de todo tipo de ataques y a su vez, las posibles soluciones o recomendaciones para mitigar las vulnerabilidades ante un ataque eventual. Teniendo en cuenta esto, se dará a conocer los tipos de ataques más comunes y la forma como operan estos, de manera que se pueda reflejar el nivel de relevancia que adquiere la presente investigación tanto para la institución.

8.2. Ciberseguridad

La ciberseguridad también conocida como seguridad informática hace años atrás, ha modernizado el sistema de seguridad de las empresas ya que esta se ocupa del tratamiento de la información por medio de las computadoras y la integridad del sistema informático.

Se conoce como la seguridad tecnología de la información ya que engloba un gran número de técnicas y métodos para proteger nuestro sistema, así como otros dispositivos que son presas de ataques informáticos o cualquier robo de datos o identidad. En esta era digital debemos estar actualizados, por ello nuestro sistema debe estar dotado de la mejor seguridad y conocer a la perfección las nuevas herramientas, que van apareciendo para evitar estas amenazas. La ciberseguridad es importante a nivel mundial, puesto que los gobernantes de diferentes países inviertes millones de dólares en seguridad informática, la rápida transformación digital que estamos viviendo nos vuelve más vulnerables, el alto uso de dispositivos tecnológicos en la sociedad, facilitando actividades cotidianas, como comprar, estudiar, realizar actividades bancarias, etc. Por ese motivo se genera más riesgos de ser atacados por los famosos "hacker". Y es por ello que siempre hay que estar alerta, a posibles ataques informáticos (Vieites, 2013).

Actualmente existen un gran número de razones para aplicar y confiar en la ciberseguridad. En los sistemas informáticos actuales prácticamente no existe un concepto de ordenadores aislado como sucedía en ordenadores de generaciones anteriores a la actual, por lo que se observaría extraño ver un sistema informático que no esté dentro de una red de ordenadores para compartir recursos e información, así como acceso a internet, con las cuales las

amenazas les pueden llegar desde el interior o exterior, y al estar conectados en red un ataque a un equipo puede afectar a todo el conjunto (Vieites, 2013).

Se puede decir que es prácticamente imposible encontrar un sistema informático totalmente seguro, pero cuantas más y mejoras medidas de seguridad empleemos, mayor será la seguridad del sistema informático (Vieites, 2013).

8.3. Clasificación de ciberseguridad

Cuando hablamos de la seguridad en un sistema informático, podemos encontrar diversos tipos de seguridad, dependiendo de la naturaleza material de los elementos que utilicemos o de si se ocupan de evitar el ataque o incidentes o de recuperar el sistema una vez que este se haya producido.

8.4. Activa y pasiva

La ciberseguridad se divide en activa y pasiva, dependiendo de los elementos utilizados para la misma, así como de la actuación que van a tener en la seguridad de los mismos.

8.4.1. Activa

Se entiende por seguridad activa todas aquellas medidas que se utilizan para detectar las amenazas, y en caso de su detención generar los mecanismos adecuado para evitar los problemas.

Ejemplos de seguridad activa los podemos encontrar de contraseñas o claves de acceso, uso de antivirus, cortafuegos o firewall (Vieites, 2013).

8.4.2. Pasiva

Comprende todo el conjunto de medidas utilizadas para que una vez que se produzca el ataque o el fallo en la seguridad de nuestros sistemas, hacer que el impacto sea menor posible, y activar mecanismos de recuperación del mismo.

Ejemplo de seguridad pasiva son las copias de los datos de nuestro sistema (Vieites, 2013).

8.5. Fases de la ciberseguridad

Protegerse ante los peligros de la era actual implica llevar a cabo procesos de ciberseguridad que se sustenten sobre su efectividad y para hacerlo, hay que conocer las fases en las que aplicarlos.

Podemos dividir el proceso en tres fases concretas que suelen ser temario habitual del máster en seguridad empresarial: prevención, localización y reacción (Vieites, 2013).

8.5.1. Prevención

El primer paso siempre es la prevención, lo que reducirá en gran medida el margen de riesgo. Por ello, hay que actuar de forma temprana e informarnos de todo lo que puede ocurrirle a nuestro sistema. Determinar las posibles amenazas y cuáles serán las medidas de prevención y reacción en caso de vernos afectados por una de ellas, nos permitirá estar más preparados. Es primordial que los empleados del negocio tengan unos conocimientos básicos sobre ciberseguridad. Deben conocer las distintas herramientas que se utilizan y cómo garantizar su máximo nivel de seguridad para que no cometan errores que puedan abrir el camino a la entrada de los hackers (Vieites, 2013).

8.5.2. Localización

Después de prevenir, en el caso de haber sufrido algún tipo de problema, habrá que localizar dónde radica el problema. Para ello la mejor herramienta es disponer de un antivirus potente que nos ayude a detectar el ataque en tiempo real y concentrarnos en él de inmediato. Localizar el ataque o la infección no es tan fácil como pueda parecer, dado que los hackers son conscientes del uso de los antivirus y lo que hacen es trabajar de manera que sus ataques puedan pasar desapercibidos. En algunos casos, desde el momento en el que se produce el golpe hasta que la empresa lo detecta, pueden pasar más de 100 días. Para intentar reducir en la medida de lo posible este problema, hay que concentrarse en dos aspectos: gestionar las vulnerabilidades de nuestro sistema y por otro llevar a cabo una monitorización de forma continuada (Vieites, 2013).

8.5.3. Reacción

Una vez que hemos localizado la amenaza, tendremos que dar una respuesta técnica sobre la misma y para ello lo ideal es seguir cinco pasos. Comenzaremos desconectando los equipos de la red y seguidamente instalaremos un antivirus que pueda satisfacer las necesidades o actualizaremos el que ya teníamos. Después, llevaremos a cabo un análisis sobre el sistema y haremos cambios en todas las contraseñas. Para terminar, será crucial realizar una limpieza a fondo del sistema para comprobar que ya no existe ningún tipo de peligro. En el caso de que nos hayan robado datos o información confidencial, también deberemos proceder de la manera pertinente para comunicarlo a los usuarios afectados y elevar lo ocurrido a una situación de delito informático (Vieites, 2013).

8.6. Tipos de ataques

Para iniciar los tipos de ataques es importante primero mencionar que un ataque es iniciado desde una computadora con otra computadora o sitio web, con fin de comprometer la integridad, confidencialidad o disponibilidad del objetivo y la información almacenada en el ordenador. Es por ello que mencionaremos los tipos de ataques con sus respectivos objetivos.

8.6.1. Escaneo de puertos abiertos

Pese a que se puede clasificar a esta como una técnica también se la puede incluir dentro de los tipos de ataque sniffers. Puesto que, la finalidad de este es recopilar la información necesaria sobre los servicios se encuentran habilitados para la escucha de solicitudes a través de los diferentes puertos de red. Esto permitiría poder determinar a su vez la herramienta o el siguiente paso para realizar el ataque informático (CERT-MU, 2010).

8.6.2. Ataques de ramsonware

En el año 2017 el Ecuador fue parte de un ataque informático a escala mundial, dirigido hacia una multinacional que opera también en el país. Dicho ataque consistía en alterar el funcionamiento de equipos que cuenten con el sistema operativo Windows (Medina, 2017). El modus operandi de este, se basaba en tomar el control de la computadora y dejar casi sin efecto la manipulación por parte del usuario, posterior a esto el atacante exigía algún tipo de

desembolso monetario para el rescate o liberación del equipo. Este tipo de ataques son los conocidos como ataques de Ramsonware. De manera particular el ataque informático citado se realizó a través de un virus esparcido que se denominó wannacry (Check, 2018).

Este virus fue liberado en mayo del 2017 afectando a 15000 personas y 27 empresas alrededor del mundo. De acuerdo con el reporte realizado por CERT- MU (Computer Security Incident Response Team of Mauritius) equipo dedicado a investigar ataques informáticos alrededor del mundo (CERT-MU, 2017).

8.6.3. Ataques phishing

Otros de los ataques informáticos más conocidos es el ataque phising. Este ataque se funciona en base al envío de un correo falso solicitando o presentando información respecto a trámites bancarios suplantando la identidad de la institución. El objetivo principal de este cometido es persuadir a la víctima a registrar información confidencial del usuario, como credenciales de acceso a servicios de banca virtual, números y códigos de tarjetas de crédito o débito, estados de cuenta, estados financieros, entre otros (Vieites, 2013).

8.6.4. Ataques DoS

Sus siglas derivan de la frase "Denial of service" que significa denegación de servicio, el objetivo de este tipo de ataques es, como su nombre lo indica, negar a los usuarios el acceso a un servicio en específico o limitar el acceso al mismo alterando su funcionamiento. Los principales modos de identificar este tipo de ataque son, por ejemplo, descubrir un bajo rendimiento o rendimiento limitado de un servicio en un entorno de red. Otro de los síntomas que podrían presentarse es la no disponibilidad de acceso a sitios web que se monitorean como operativos, y por ende la restricción de acceso a servicios web (Vieites, 2013).

8.6.5. Ataques Man-In-The-Middle

Los ataques MITM tienen la finalidad de interceptar la comunicación entre dos sistemas por medio del uso de un software o entidad externa. Esto servirá como herramienta sniffer y podrá actuar como puente para los datos que se transmiten entre ambos sistemas. Gracias a esto, podrá recibir información confidencial e importante que se transmita, como credenciales de

acceso, documentos confidenciales, o incluso daría la posibilidad de modificar los paquetes recibidos y retransmitirlos con algún código malicioso que infecte al usuario receptor. Este tipo de ataques se lo puede realizar durante la navegación hacia sitios o servicios web, servicios o recursos de red, e incluso correos electrónicos (Vieites, 2013).

8.6.6. Ataques a redes wireless

Más allá del conocido ataque al protocolo WPA2 registrado en el año 2017, en el que se dio a conocer que el protocolo más seguro usado por los routers había sido vulnerado, existen sin duda otros tipos de ataques que no necesariamente atacan directamente a dicho protocolo.

Sino más bien que por medio de una base de datos trata de descifrar la clave que este router está usando para poder tener acceso a determinada rede wifi, estos son conocidos como los ataques de diccionarios de datos, en los cuales consiste poseer un diccionario con miles de claves y usuarios, esto ocurre que mediante un algoritmo se probará todas las combinaciones posibles y si se encuentra la clave dentro del diccionario pues lo indicará, esto mediante aplicativos que permiten conocer la mac address del ap que difunde el ssid así como también la de los dispositivos conectados, una vez conocido esto se envía una petición de des autenticación hacia el host una vez que el dispositivo se vuelva a conectar empezará el algoritmo a hacer su trabajo (Martinez, 2018).

8.6.7. Ataques inyección SQL

Estos tipos de ataques son conocidos por que se ejecutan a nivel web con la finalidad de obtener información directamente desde la base de datos, esto se puede lograr mediante las vulnerabilidades que se encuentran en la capa de back end, las consecuencias de este tipo de prácticas es poder acceder a información confidencial (Cebrian, 2014).

8.6.8. Cross-site request

Consiste en la falsificación de solicitudes entre sitios web o también conocido como ataques de un solo clic, lo novedoso de este tipo de ataques, consiste en llevar al usuario a ejecutar un tipo de exploit malicioso, mediante el cual se transmiten comandos no autorizados en páginas web que el propio usuario confía (Vieites, 2013).

8.6.9. Robo de cookies

Este tipo de ataques se realizan a nivel de desarrollo, en las cuales, mediante un script desarrollado en JavaScript por parte del cliente, hace que cuando el usuario accede a un enlace en internet, este automáticamente buscara las distintas cookies almacenados en la memoria de la computadora para posteriormente ser enviadas al atacante (Valero, 2014).

8.6.10. Normas Orientadas a la Ciberseguridad de Información

La normativa ISO 27032 es un nuevo estándar de ciberseguridad publicada en Julio de 2012 por La Organización Internacional de Normalización (ISO).

La Norma ISO/IEC 27032:2012 "Tecnologías de la información - Técnicas de seguridad - Directrices para la Ciberseguridad" ofrece unas líneas generales de orientación para fortalecer el estado de la Ciberseguridad en una empresa, utilizando los puntos técnicos y estratégicos más importantes para esa actividad y los que están relacionados con:

- La Seguridad en las redes
- Seguridad en internet
- Seguridad de la información
- Y la Seguridad de las aplicaciones

La Norma ISO/IEC 27032 pretende garantizar la seguridad en los intercambios de información en la Red para lograr hacer frente de una manera más efectiva al cibercrimen con más cooperación entre todos.

Con esta norma ISO/IEC 27032:2012 se ha creado un nuevo marco para mejorar la seguridad en internet. La norma ISO 27032 está totalmente orientada a intentar garantizar un entorno seguro a través de directrices de seguridad (ISO, 2019).

8.7. Virtualización mediante el uso de VMware

La virtualización inicialmente aparece en la década de los 60, pero oficialmente toma mucha fuerza desde los años 90 hacia la actualidad. El objetivo de la virtualización es que por medio de un software este tenga la capacidad de crear de forma virtual un ente informático, ya sea este considerado un hardware, software o un servicio. Dicho esto, la virtualización dentro del campo de la seguridad podrá facilitar el trabajo al momento de la realización de una prueba de penetración, ya que este hace uso de recursos virtuales que tienen la misma validez de un ambiente real.

La utilización de ambientes simulados en las pruebas de pentesting es de gran apoyo para el hacker ético ya que de esta forma se puede tener total control de las vulnerabilidades que se puedan encontrar a lo largo de este proceso. En la actualidad las herramientas de seguridad son muy versátiles, ya que estás vienen en distintas versiones, como aplicativos de escritorio, aplicativos web y sistemas operativos robusto y completos como es el caso de Kali Linux.

Uno de los softwares de virtualización más conocidos en el mundo de la informática es VM Ware, que como empresa tuvo sus inicios a finales de los años 90, en la ciudad de California en los Estados Unidos de América, este sistema posee gran cantidad de versiones de que se apegan dependiendo de las necesidades del usuario.

El ESXi no es otra cosa más que un hypervisor, que es el núcleo principal de la estructura vShepre, que se basa en una capa de virtualización que permite que se ejecuten varios sistemas operativos virtualizados sobre una misma máquina física. vSphere es conocido como la solución estelar para la virtualización de centros de datos, esto enfocado a un plano más profesional, ya que con esta herramienta de VMWare se permite agrupar muchos servidores virtualizados, no es otra cosa más que una granja de servidores virtual (Gomez, 2009).

8.7.1. Kali Linux

Es un sistema operativo de tipo de código abierto, distribución basada en Debian GNU/Linux el cual es exclusivo para auditorias informáticas, hacking ético o pentesting, que incluye una gran cantidad de herramientas para el trabajo diario orientado a la seguridad informática.

Este sistema operativo tuvo su lanzamiento oficial en el año 2013 y ha tenido como tarea principal ocupar el lugar de Backtrack y más allá de eso, la tarea principal satisfacer en gran manera a los usuarios. De manera general se puede considerar a Kali Linux como el sucesor de BackTrack. Esta distribución de Linux cuenta con alrededor de 600 herramientas instaladas para darle el uso adecuado acorde a nuestras necesidades.

Al igual que otras distribuciones de Linux, Kali cuenta con una arquitectura muy bien definida, basada en capas, que arranca desde su núcleo principal o Kernel, que es el encargado de comunicar toda la parte del software con el hardware.

Cuenta con capas de Shell Cli y Shell Grafico, que son las capas encargadas de poner en funcionamiento a los distintos aplicativos que se ejecutan en líneas de comando (CLI) así como también los que se encargan de ejecutar aplicativos con interfaz gráfica (GUI).
No está de más recalcar que esta distribución es una excelente herramienta para temas de ciberseguridad puesto que cuenta con la facilidad de ejecutar varios servicios a nivel grafico sin perder la esencia de Linux con su interfaz en líneas de comando.

Sin duda alguna este sistema operativo ha sido para los usuarios apasionados por la seguridad informática una herramienta de gran apoyo, puesto que una de las novedosas características de éste es la capacidad también de poder ejecutarse dentro de dispositivos con sistema operativo Android con privilegios de root (Caballero, 2018).

8.8. Ataques informáticos en el Ecuador

De acuerdo con Lubensky (2017), en el Ecuador, por ejemplo, son aproximadamente decenas de miles los ataques a redes o servicios tecnológicos a nivel nacional. Según una investigación realizada por un diario local del país (Expreso, 2011), al 2010 los delitos informáticos crecieron en un 360% en comparación con las estadísticas del año anterior a ese. Así también, a la misma fecha; las pérdidas económicas a causa de delitos o ataques informáticos Además de esto, según un estudio realizado por la empresa Deloitte entre los ataques más comunes detectados en el país se encuentran los ataques por malware, SQL injection, DoS Distribuido, IPV6, ataques internos, dispositivos móviles, análisis Logs entre otros.

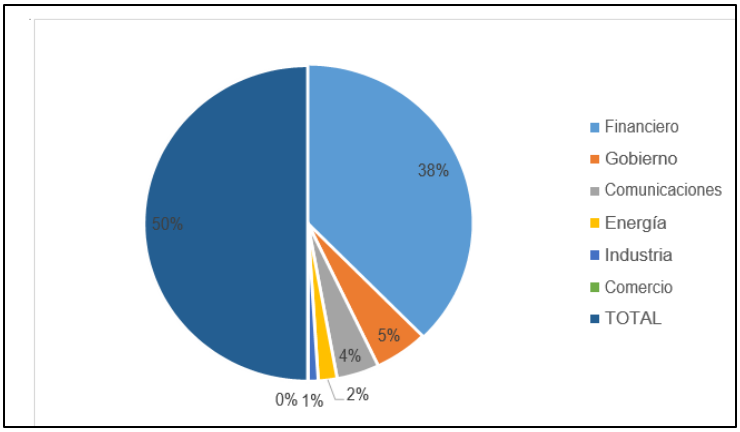
Tabla 2: Ataques más comunes en el país

SECTORES	ATAQUES POR DÍA	PORCENTAJE
Financiero	6600000	75.29%
Gobierno	925600	10.56%
Comunicaciones	737200	8.41%
Energía	325347	3.71%
Industria	173900	1.98%
Comercio	3600	0.04%
TOTAL	**8765647**	**100%**

Fuente: Ecuador, el cuarto país de la región que recibe más ataques cibernéticos (Doctor, 2012).
Elaborado: Los autores

Por su parte, la Fiscalía General del Estado, indicó que, en los primeros meses del año 2011, recibieron 1308 denuncias por delitos informáticos. De acuerdo con Xavier Almeida, experto en seguridad informática de la empresa GMS, el 90% de los ecuatorianos son propensos a sufrir un ataque de seguridad informática. Así lo corrobora también Karina Astudillo, de la empresa Elixircorp y docente de la maestría en Seguridad Informática de la Espol, quien mostró en cambio, cómo los portales que se manejan con JAVA (software que permite el uso de programas punteros, como herramientas, juegos y aplicaciones de negocios) son vulnerables a los ataques de hackers. Como parte de su exposición, hizo una demostración, que tardó menos de 15 minutos, de un "ataque de Phishing usando Metasploit en Backtrack Linux (Una versión anterior a Kali Linux)" (Expreso, Delitos Informaticos, 2011).

Gráfico Nº 1 Índice de ocurrencia de ataques informáticos en el país

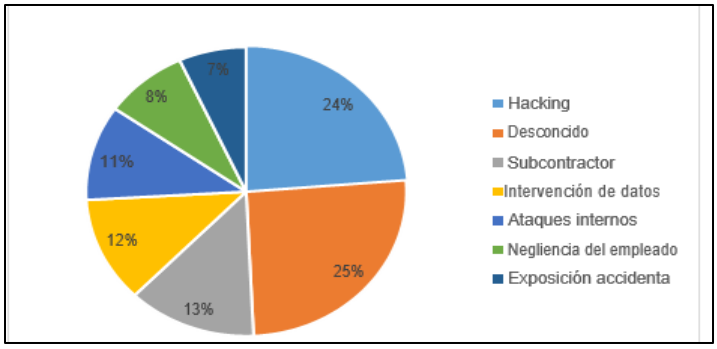


Fuente: Ecuador, el cuarto país que recibe más ataques cibernéticos.
Elaborado: Los autores

Vicente Lingan, de Kernel Panic, mostró cómo mediante el proceso de "ethical hacking" (simulación de ataques hostiles controlados para ver los huecos de vulnerabilidad de las redes) ha descubierto las fallas de muchos sitios webs públicos. Este método es utilizado y recomendado para los bancos para que detecten sus fallas de seguridad. "Para atrapar a un ladrón debes pensar como un ladrón", afirmó Lingan, quien además advirtió que "el Gobierno tiene que tener claro que no se trata de una película de ficción, sino de una realidad. Por lo tanto, hay que luchar y protegerse" (Expreso, 2011).

De acuerdo a otro estudio realizado por diario La Hora, periódico local comercializado a nivel nacional. El país es uno de los países más propensos a sufrir ataques informáticos. Tanto es así que ha sido catalogado como un blanco fácil para ataques de hackers (La Hora, 2011). Dato que se confirma también con el estudio que el reportaje que publicó Diario Expreso en el 2017, en dónde, se evidenció que Ecuador y al menos 100 países más a nivel mundial son los que más sufren ataques de seguridad informática de tipo extorsivo (Expreso, Ataques en el Ecuador, 2017).

Gráfico Nº 2 Índice de tipos de ataques de seguridad más comunes



Fuente: Ecuador, el cuarto país que recibe más ataques cibernéticos.
Elaborado: Los autores

Sin embargo, es necesario destacar que el país hace esfuerzos en la lucha contra este tipo de delitos mostrando al público formas de estar prevenido a través de campañas como las que hacen las instituciones financieras en las que se advierten sobre la difusión de información confidencial. Así también instituciones públicas como la policía nacional que, en su página web, enlista los tipos de ataques informáticos más comunes año a año. En este caso, por ejemplo, para el año 2018, en su artículo "Tendencias de la seguridad informática" (Policía Nacional del Ecuador, 2018).

El Ransomware: Sin duda, uno de las tendencias que más se repiten es el ransomware y según los expertos seguirá siendo una de las fuentes de negocio de los cibercriminales en 2018, debido a que "aún hay muchas organizaciones dispuestas a pagar grandes sumas de dinero por recuperar sus sistemas comprometidos, en lugar de contar con políticas de ciberseguridad que las mantengan protegidas ante cualquier amenaza".

Los dispositivos inteligentes inundan hogares y empresas. "A medida que aumentan las capacidades de la tecnología y se implementan nuevos sistemas disruptivos en las nuevas industrias, estos se convertirán en los objetivos principales para el cibercrimen y la actividad maliciosa". Tecnología CLOUD y la infraestructura que la soporta está en constante evolución, y con el creciente uso de los servicios de uso compartido de archivos en la nube, las fugas de datos seguirán siendo una gran preocupación para las organizaciones que se mueven en este entorno.

Criptomonedas: El Bitcoin y otras criptomonedas están experimentando un momento de crecimiento explosivo. Cada vez más gente está invirtiendo en divisas electrónicas cuyas cotizaciones no dejan de crecer, lo que provocará que los cibercriminales vean como mercado potencial que explotarán definitivamente en 2018.

Robo de datos personales y sensibles: 2017 ha sido un año productivo para los cibercriminales en cuanto a robo de datos personales, además, los expertos apuntan que los datos que robaban y que se han vendido tradicionalmente en la deep web, en 2018 se podrían consolidar nuevas formas como la extorsión, hasta ahora asociada mayoritariamente al ransomware.

Crimen Como Servicio (Crime-As-A-Service): En 2017 se experimentó un aumento considerable del cibercrimen debido a la oferta como servicio (CaaS), y esta tendencia continuará en los próximos meses. "En 2018, el CaaS permitirá que los cibercriminales, sin muchos conocimientos técnicos, compren herramientas y servicios para que puedan realizar ataques."

Amenazas Móviles: Los dispositivos móviles seguirán siendo uno de los principales vectores de ataque para los cibercriminales en 2018. A medida que las empresas sigan permitiendo a los empleados utilizar sus dispositivos móviles con fines corporativos, se hace fundamental

que exista un protocolo de seguridad para evitar el acceso no autorizado y garantizar que los datos confidenciales permanezcan seguros.

Así también en el mismo artículo se brinda a la ciudadanía, formas de estar prevenido ante eventuales ataques y cómo identificarlos. Por ejemplo, las conexiones a internet en redes públicas, de acuerdo a lo recomendado por la Policía Nacional si se requiere el uso de una red pública de internet tal como la red de un restaurante, hospital o aeropuerto, recomiendan no acceder a cuentas bancarias o información confidencial ya que puede estar en peligro. Únicamente utiliza para tareas sencillas tal y como revisar algún mensaje o correo electrónico.

Otra de las recomendaciones es el uso de contraseñas blindadas. Puesto que, si la extensión de la contraseña es corta o se utiliza una única para todos los dispositivos, debe estar alerta. La recomendación es que, una contraseña segura debe tener al menos ocho caracteres, es importante que contenga mayúsculas, minúsculas, números y signos especiales como el signo de #. Además, recomiendan que las contraseñas deben de ser modificadas al menos cada 6 meses.

Pese a esto, el 85% de los ataques informáticos ocurren por descuido o imprudencias del usuario. De acuerdo con un reportaje publicado por diario El Telégrafo (El Telégrafo, 2016), desde enero hasta mayo del 2016, se recibieron 530 denuncias por delitos informáticos de las cuales, aproximadamente el 70% de ellas, es decir 368 denuncias son debido al delito de "apropiación fraudulenta por medios electrónicos". En Guayas hubo 18 casos; Pichincha, 145; Manabí, 24; El Oro, 22; en el resto de provincias se registró una cantidad menor (Telegrafo, 2016).

Un estudio elaborado por la Policía Nacional, Interpol, el centro de respuesta a Incidentes Informáticos de Ecuador (Ecucert), con el soporte de organismos similares de América Latina, indica que el 85% de los ataques a los sistemas informáticos son causados por errores de los consumidores, quienes no toman precauciones al acceder a las redes sociales, utilizar el correo electrónico, y en el uso de usuario y contraseña. Las tácticas más comunes son los premios que se promocionan sin razón aparente, como viajes, loterías, boletos para Disneylandia, etc. advierte el experto. Una de las opciones temáticas de estafas que va en aumento en los últimos años son los videos sexuales de celebridades (Expreso, Ecuador Inmediato, 2017).

El 58% de personas deja sus teléfonos móviles que contienen información sensible, en sus vehículos o lugares de trabajo; el 60% utiliza la misma contraseña en dispositivos laborales y personales. El 35% ha hecho clics en correos recibidos por emisores desconocidos; el 59% almacena información de trabajo en la nube; y el 80% de amenazas en las redes sociales juega con la curiosidad de los usuarios que quieren saber quién o quiénes ven su perfil, anota el capitán Édgar Toapanta, oficial de Seguridad de la Información de la Policía (Expreso, Delitos Informaticos, 2011).

Tabla 3: Técnicas de ataque más utilizadas

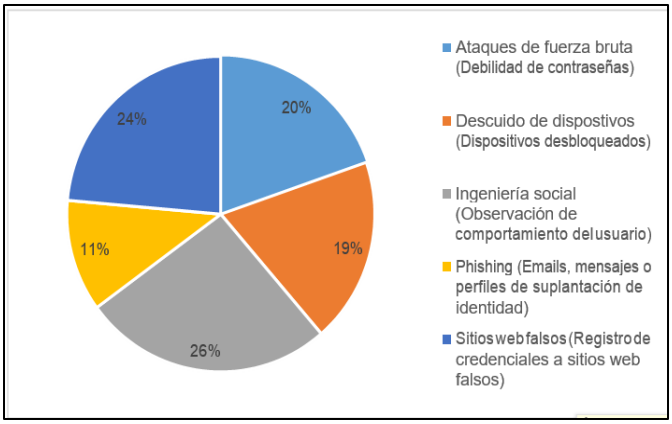
TÉCNICA DE ATAQUE	ÍNDICE DE EVENTUALIDAD
Ataques de fuerza bruta (Debilidad de contraseñas)	60%
Descuido de dispositivos (Dispositivos desbloqueados)	58%
Ingeniería social (Observación de comportamiento del usuario)	80%
Phishing (Emails, mensajes o perfiles de suplantación de identidad)	35%
Sitios web falsos (Registro de credenciales a sitios webs falsos)	72%

Fuente: Ecuador, el cuarto país de la región que recibe más ataques cibernéticos (Doctor Tecno, 2015)
Elaborado por: Los autores

"La investigación de los delitos informáticos necesariamente está revestida de un procedimiento técnico, como interceptación de comunicaciones, peritajes para establecer direcciones IP, para extraer información de memorias portátiles, para lo cual se requiere la participación de expertos en la materia", afirma el fiscal Wilson Toainga. La banca, comercio y entidades del Estado, entre otros sectores, recurren a los medios electrónicos para realizar su facturación como una manera de mejorar sus servicios y optimizar sus operaciones, lo que genera grandes oportunidades de crecimiento para Ecuador, señala Kerench Rodríguez,

gerente de la empresa informática D-Link. Pero esa situación también ha provocado riesgos, manifiesta el experto, ya que esa información sensible, si no cuenta con medidas de protección, puede quedar expuesta a los "intrusos informáticos", y llevar a más fraudes y robo de datos financieros para las empresas (Telegrafo, 2016).

Gráfico Nº 3 Técnicas de ataques más utilizadas



Fuente: Ecuador, el cuarto país que recibe más ataques cibernéticos
Elaborado: Los autores

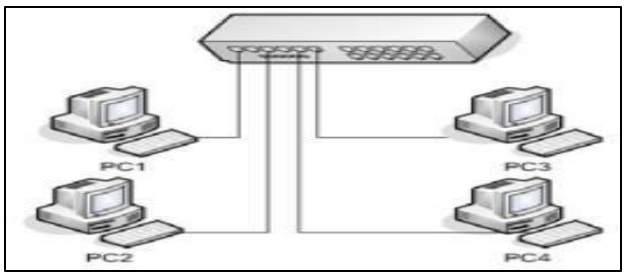
8.9. Laboratorios de seguridad informática

De acuerdo con iHackLabs, empresa de seguridad informática Londinense fundada en el 2016, la utilización de laboratorios de seguridad informática ayuda a que un especialista de seguridad o una empresa como tal, esté preparada ante eventuales ataques. Esto, teniendo en cuenta que, muchas veces solo se tiene una práctica de técnicas de defensa cuando ocurre un incidente o se evidencia el riesgo ante una vulnerabilidad encontrada por aun ataque. Por lo que, esta forma de ganar experiencia puede incurrir en grandes pérdidas para la compañía u organización. Por lo que, resulta importante tener un entorno adecuado en el que se puedan realizar constantes pruebas de vulnerabilidad a la infraestructura tecnológica de la empresa (iHackLabs, 2018).

Por otro lado, este tipo de implementaciones sirven no solo para la aplicación de técnicas de ataque y defensa sino también para la docencia. Es el caso del estudio realizado por Pagola et al. (2006), en el que se implementó un laboratorio de seguridad informática con herramientas de código abierto simulando un entorno de red real. En dicha implementación se simuló en un entorno de red utilizado por unos de los laboratorios de la facultad de Ingeniería de la Universidad de La Plata, montando cuatro equipos virtuales de los cuales tres operaban bajo

subredes diferentes mientras que el cuarto utilizaba un sistema operativo Linux para realizar pruebas de penetración a través de comandos vía terminal (iHackLabs, 2018)

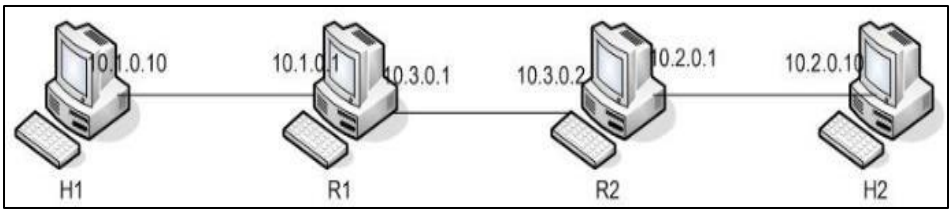
Gráfico Nº 4 infraestructura básica de un laboratorio



Fuente: Datos de la investigación
Elaborado por: Los autores

En este punto se puede observar el esquema básico de un laboratorio de seguridad informático, puesto que la idea principal, es como se lo ha mencionado previamente, simular un entorno de red real junto con los servicios o recursos que se utilicen. De esta manera, se podría llevar a cabo todo tipo de comandos o pruebas de vulnerabilidad, necesarias para violentar la seguridad de dicha red o de los servicios (iHackLabs, 2018).

Gráfico Nº 5 Arquitectura básica de un laboratorio virtualizado



Fuente: Datos de la investigación
Elaborado por: Los autores

8.10. Definiciones conceptuales

Es fundamental tener claro ciertos conceptos a los que se harán referencia a lo largo de la investigación como, pentesting, exploits, metasploits, entre otros. De esta manera se obtendrá una mejor comprensión del trabajo realizado (iHackLabs, 2018).

8.10.1. Pentesting

En la rama de la seguridad informática surge el termino en inglés denominado "pentesting" que en una hipotética traducción al español seria "test de penetración", estas pruebas no son más que un conjunto de prácticas, técnicas o ejercicios que se realizan a nivel tecnológico

debidamente aprobado por la entidad encargada de los servicios informáticos, para un análisis de las vulnerabilidades que podrían encontrarse dentro de una red corporativa o dentro de algún servicio tecnológico.

En esencia las técnicas de pentesting consisten en aplicar diversos métodos de ataque, de manera que se pueda explotar todas las brechas de seguridad que se denominan vulnerabilidades. Logrando esto se podrán definir las correcciones necesarias y los métodos de prevención a futuro para evitar nuevas vulnerabilidades. Esto se puede realizar tanto mediante la utilización de ambientes simulados dentro de una organización, así como también, desde un enfoque "ataque esperado" para determinar no solo las vulnerabilidades internas sino externas (Gonzáles, 2014)

8.10.2. Exploits

La palabra "exploit" es un término de descendencia inglesa el cual hace referencia a explotar o aprovechar exclusivamente los fallos o vulnerabilidades de un sistema informático esto de forma conceptual, sin embargo, desde un punto de vista técnico se lo podría catalogar como cualquier tipo de ejecutable o script que contiene comandos el cual tratará de vulnerar al máximo las seguridades de cualquier hardware o servicio tecnológico consiguiendo así que tome un comportamiento distinto al adecuado permitiendo el acceso no autorizado o el robo de algún tipo de información.

Como lo indica Josep Albors en su blog tecnológico, "Las definiciones habituales hablan de un programa o código que se aprovecha de un agujero de seguridad en una aplicación o sistema, de forma que un atacante podría usarla en su beneficio." (Oppleman, 2006).

8.10.3. Metasploit

Nombre del programa o framework de código abierto que permite la realización de ejecutables, scripts o comandos para la evaluación de vulnerabilidades. Este aplicativo viene ya instalado en la distribución de Kali, dado que sigue la política Kali Linux Network Service Policy no tiene habilitado los servicios de red, así como tampoco servicios de base de datos por lo tanto hay que realizar algunas configuraciones extras para poder hacer el uso correcto de este aplicativo que es de mucha ayuda para el hacker (Wilhelm, 2010).

8.10.4. Pentester

Se conoce como pentester a la persona con el conocimiento necesario debidamente certificada que posee la capacidad para realizar pruebas de penetración y vulnerabilidades en un entorno informático (Oppleman, 2006).

8.10.5. Target

En su traducción al español su significado es "objetivo" por lo tanto en informática se hace referencia al objetivo o al dispositivo informático al cual se va a escanear (Wilhelm, 2010).

8.10.6. Host

Se define como un host o anfitrión a todo equipo informático u ordenador que se toma como punto de inicio y fin en la transferencia de datos. Un host es todo dispositivo que cuenta con salida a internet y que cuenta con una dirección IP (Wilhelm, 2010).

8.10.7. Virtualización

Es la creación lógica de un servicio o hardware por medio de la utilización de un software. El cual permitirá la abstracción de los recursos de una computadora por medio de un programa (Gomez, 2009).

8.10.8. Nmap

Software de código abierto que sirve para el escaneo y recopilación de información de sistemas informáticos, así como el rastreo de puertos e identificación de servicios (Lyor, 2009).

8.10.9. Kali

Sistema operativo de código abierto basado en Debian GNU/Linux diseñado principalmente para las ramas de auditoria informática y seguridad informática (Caballero, 2018).

8.10.10. Seguridad informática

Rama de la informática que se encarga de proteger la infraestructura tecnológica y todo lo relacionado con ella.

8.10.11. VMware

Software de uso mediante licencia que permite la creación de recursos tecnológicos de forma virtualizada con la posibilidad de administrarlos de forma local o de forma remota (Gomez, 2009).

8.10.12. Terminal

Es una Interfaz que permite gestionar o administrar y acceder sistemas informáticos sin necesidad de una interfaz gráfica a través de líneas de comandos en texto plano. Este tipo de interfaces es común en sistemas Linux o Unix y es conocida como "Terminal", sin embargo, en sistemas de Microsoft es conocido como "CMD" que quiere decir "Comando".

8.10.13. SSH

Es un protocolo de red que permite el acceso a servidores de privados a través de la interfaz terminal o cmd, de forma segura y únicamente mediante línea de comandos, es decir no se hace uso de una interfaz gráfica.

8.10.14. Riesgo

De manera general el riesgo es el nivel o la probabilidad de que se produzca un incidente, y esto afecte a alguien o algo en específico. Trasladando este concepto al entorno de la informática, sería todo tipo de brecha de seguridad que podría utilizarse en contra de la empresa.

9. VALIDACIÓN DE LAS PREGUNTAS CIENTÍFICAS O HIPÓTESIS

9.1. HIPÓTESIS

Con el análisis de la ciberseguridad a la infraestructura tecnológica de la UNIVERSIDAD TÉCNICA DE COTOPAXI, utilizando el sistema operativo Kali Linux, virtualizado en una maquina física se podrá disminuir los riesgos existentes a sus sistemas informáticos.

10. METODOLOGÍA Y DISEÑO ESPERIMENTAL

10.1. Tipos de investigación

10.1.1. Investigación bibliográfica

La investigación bibliográfica es aquella etapa de la investigación científica dónde se explora qué se ha escrito en la comunidad científica sobre un determinado tema o problema, constituye una excelente introducción a todos los otros tipos de investigación.

Este tipo de investigación se utilizará para conocer antecedentes, versiones, características, ventajas, desventajas y demás aspectos que sean necesarios establecer a cerca de las vulnerabilidades que existen en el país.

10.1.2. Investigación de campo

La investigación de campo es el proceso que, utilizando el método científico, permite obtener nuevos conocimientos en el campo de la realidad social o bien estudiar una situación para diagnosticar necesidades y problemas a efectos de aplicar los conocimientos con fines prácticos.

Se realizará mediante visitas a la Universidad Técnica de Cotopaxi, que es dónde se realizara el análisis para verificar posibles vulnerabilidades.

10.1.3. Investigación experimental

La investigación experimental consiste en la manipulación de una variable experimental no comprobada, en condiciones rigurosamente controladas, con el fin de describir de qué modo o por qué causa se produce una situación o acontecimiento en particular.

Se utilizará la investigación experimental para comprobar las posibles brechas de seguridad y administración de los servidores.

10.2. Métodos de Investigación

10.2.1. Método Hipotético-Deductivo

Es el procedimiento o camino que sigue el investigador para hacer de su actividad una práctica científica. Por lo que es necesario utilizar este método en el proyecto ya que partimos de una hipótesis la misma que después será comprobada experimentalmente en base a la realidad.

10.2.2. Encuesta

"Es el procedimiento que consiste en preguntar, con ayuda o no de un cuestionario, a un buen número de personas sobre un tema determinado para averiguar la opinión dominante".

Esta técnica de investigación se aplicará a los ya que es necesario obtener la opinión de cada una de las personas que conforman en desarrollo de la institución.

10.2.3. Entrevista

"Es una técnica para obtener datos que consiste en un diálogo entre dos personas: el entrevistador (investigador) y el entrevistado; se realiza con el fin de obtener información de parte de este, que es por lo general, una persona entendida en a materia de la investigación".

Esta técnica se aplicará al Jefe de servicio informáticos de la universidad y Técnica de Cotopaxi.

11. ANÁLISIS Y DISCUSIÓN DE LOS RESULTADOS

PONDERACIONES DE VALIDACIÓN DE LA PROPUESTA

Para la validación de la investigación se optó por el criterio de la investigación de campo a través del método de encuestas realizadas a los Estudiantes y Profesionales de la Carrera Ing. en Sistemas Computacionales de la Universidad Técnica de Cotopaxi, en el periodo Marzo – Agosto del 2019, esto con la finalidad de evaluar conocimiento sobre la ciberseguridad.

En cuanto al desarrollo de las preguntas realizadas para las encuestas fue avalado por el Ing. Mg. Manuel Villa quien actualmente ocupa el cargo de Docente de Seguridad Informática en la Universidad Técnica de Cotopaxi. De esta manera, gracias a sus años de experiencia en el área de seguridad informática; formó parte del equipo de investigación el mismo que aportando con sus conocimientos. De manera que, queda certificado que todo el proceso que se ejecutó bajo los estándares y normativas de seguridad bajo las políticas de seguridad interna de la institución.

Por lo tanto, gracias a las encuestas realizadas a los estudiantes y profesionales de la Universidad Técnica de Cotopaxi. Nos permitió evaluar el conocimiento de los docentes, alumnos y profesionales del área tecnológica sobre la ciberseguridad.
Por ello se toma de un valor total de 500 personas entre alumnos, docentes y personal administrativo del área tecnológica.

Se toma como objetivo la muestra mediante la fórmula de población finita:

Para calcular el tamaño de la muestra se utiliza la siguiente fórmula:

$$n=(Z^2.n.p.q)/(e^2.(N-1)+〖(Z〗^2.n.p.q))$$

Dónde:

z= al nivel de confianza (tomado de la tabla de valores de confianza)
p= porcentaje de la población que tiene el atributo deseado
q= porcentaje de la población que no tiene el atributo deseado
N= tamaño del universo
e= error máximo de estimación aceptado
n= tamaño de la muestra

TABLA DE VALORES DE CONFIANZA PARA LA ELABORACIÓN DE LAS ENCUESTAS

Tabla 4: Valores de confianza

PORCENTAJES DE CONFIANZA	VALOR
95	1.96
90	1.65
91	1.7
92	1.76
93	1.81
94	1.89

Fuente: Los autores

Del cálculo realizado aplicando la fórmula de la muestra se obtuvo como resultado un dato de 217 encuestas a realizar

PROCESO DEL ANÁLISIS

Una vez realizado el tamaño de la muestra se realiza la encuesta a docentes, alumnos y personal administrativo del departamento de tecnología de la Universidad Técnica de Cotopaxi, con el objetivo principal de obtener la mayor evidencia posible sobre la ciberseguridad de la institución. A continuación, se muestran los resultados, por preguntas, obtenidos una vez realizadas las encuestas y tabulados los datos mediante un software de procesamiento de datos.

ÁREA DE LOS ENCUESTADOS

Tabla 5: Área de los encuestados

Opciones	Respuestas
Profesionales	83
Estudiantes	134
TOTAL	**217**

Fuente: Los autores

ENCUESTA PROFESIONALES

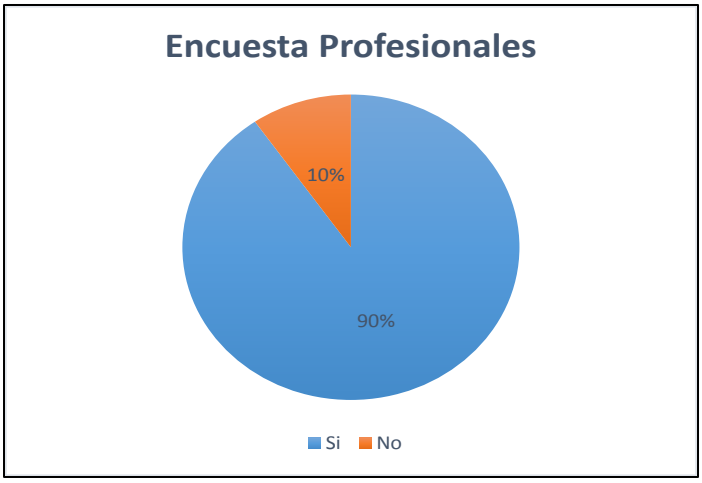
1. ¿Conoce usted que es la ciberseguridad?

Tabla 6: Ciberseguridad

ALTERNATIVAS	FRECUENCIA	PROMEDIO
Si	75	90%
No	8	10%
Total	83	100%

Fuente: Los autores

Gráfico Nº 6 Ciberseguridad



Fuente: Los autores

INTERPRETACIÓN: Los datos de la tabla 6 nos demuestra de un total 83, profesionales y pre profesionales de la Facultad de Ciencias de la Ingeniería y Aplicadas (CIYA), el 90% que corresponde a 75 personas encuestadas, detallan que, si conocen sobre la ciberseguridad, y el 10% que corresponde a 8 personas mencionan que no tiene conocimientos sobre la ciberseguridad.

CONCLUSIÓN: De acuerdo a los datos obtenidos se puede determinar que el personal docente y administrativo si dispone de los conocimientos sobre lo que es la ciberseguridad. Por lo que se recomienda que se siga impartiendo charlas sobre el tema ya que eso ayudara a estar prevenidos a posibles ataques cibernéticos.

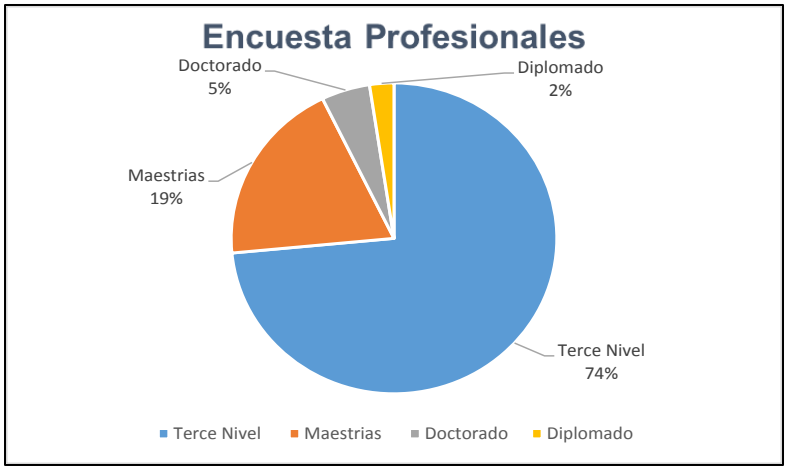
2. ¿Cuál es su nivel educativo?

Tabla 7: Nivel educativo

ALTERNATIVAS	FRECUENCIA	PROMEDIO
Tercer Nivel	61	74%
Maestrías	16	19%
Doctorado	4	5%
Diplomado	2	2%
Total	83	100%

Fuente: Los autores

Gráfico Nº 7 Nivel educativo



Fuente: Los autores

INTERPRETACIÓN: Los datos de la tabla 7 nos demuestra de un total 83, profesionales y pre profesionales de la Facultad de Ciencias de la Ingeniería y Aplicadas (CIYA), el 74% que corresponde a 61 personas encuestadas mencionan que tienen un título de tercer nivel, y el 19% que corresponde a 16 personas encuestadas tienen un título de posgrado, y el 5% que corresponde a 4 personas encuestadas disponen de un doctorado, y el 2% que corresponde a 2 personas tienen un diplomado.

CONCLUSIÓN: Podemos mencionar que el resultado más alto obtenido, son docentes y personal administrativo que constan con un título de cuarto nivel. Por lo que se recomienda que al resto de personal que no consta con un título de cuarto nivel se le de las ventajas para que se prepare y obtenga un título de cuarto nivel ya que eso ayuda al desarrollo de la institución.

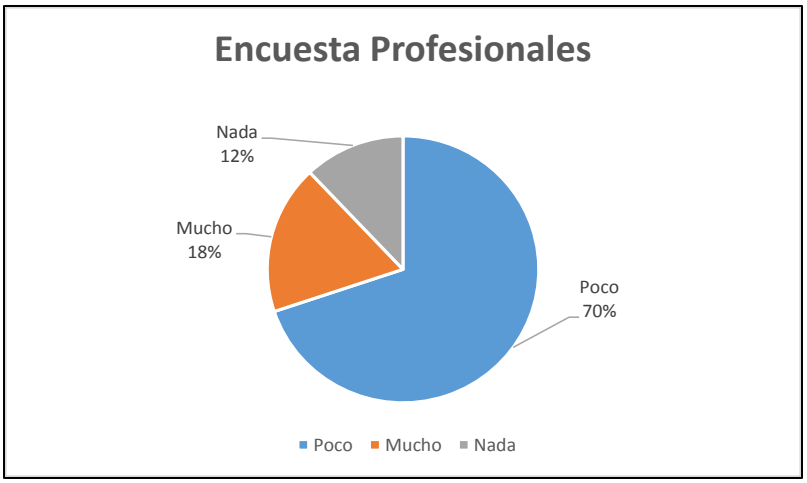
3. ¿Tiene usted conocimiento sobre la Ciberseguridad?

Tabla 8: Ciberseguridad

ALTERNATIVAS	FRECUENCIA	PROMEDIO
Poco	58	70%
Mucho	15	18%
Nada	10	12%
Total	83	100%

Fuente: Los Autores

Gráfico Nº 8 conocimientos



Fuente: Los autores

INTERPRETACIÓN: Los datos de la tabla 8 nos demuestra de un total 83, profesionales y pre profesionales de la Facultad de Ciencias de la Ingeniería y Aplicadas (CIYA), el 70% que corresponde a 58 personas tienen poco conocimiento sobre la ciberseguridad y el 18% que corresponde a 15 personas encuestas tienen mucho conocimiento sobre la ciberseguridad y el 12% que corresponde a 10 encuestados no tiene nada de conocimiento sobre la ciberseguridad.

CONCLUSIÓN: En los resultados se evidencian que el mayor porcentaje de los encuestados no dispone de conocimientos sobre la ciberseguridad. Por lo que se debería realizar más actividades que fortalezca los conocimientos sobre la ciberseguridad.

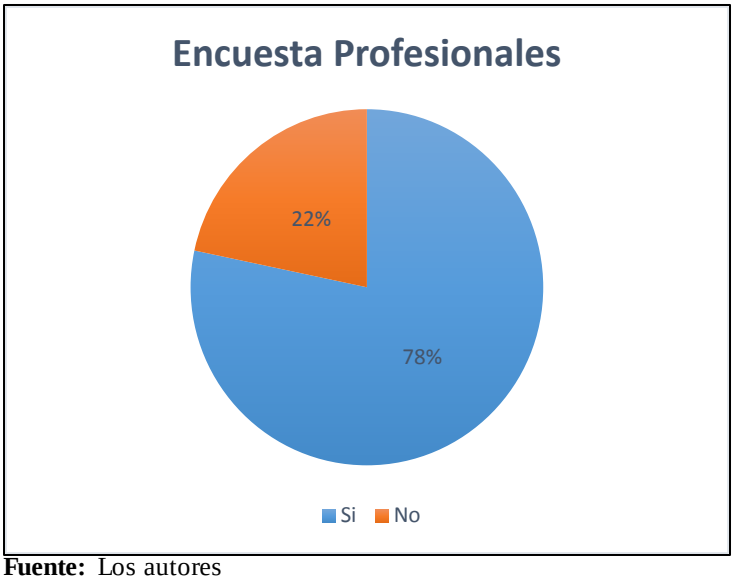
4. ¿Sabe usted que es Kali Linux?

Tabla 9: Kali Linux

ALTERNATIVAS	FRECUENCIA	PROMEDIO
Si	65	78%
No	18	22%
Total	83	100%

Fuente: los autores

Gráfico Nº 9 Kali Linux



Fuente: Los autores

INTERPRETACIÓN: Los datos de la tabla 9 nos demuestra de un total 83, profesionales y pre profesionales de la Facultad de Ciencias de la Ingeniería y Aplicadas (CIYA), el 78% que corresponde a 65 personas encuestadas mencionan que, si conocen sobre que es Kali Linux, y el 22% que corresponde a 18 personas no tiene conocimientos sobre lo que es Kali Linux.

CONCLUSIÓN: Podemos mencionar que el resultado más alto obtenido por parte de los profesionales se detalla que tienen un sólido conocimiento sobre lo que es Kali Linux, no obstante, los estudiantes, por lo que se recomienda que fortalezca más sobre el S.O. Linux.

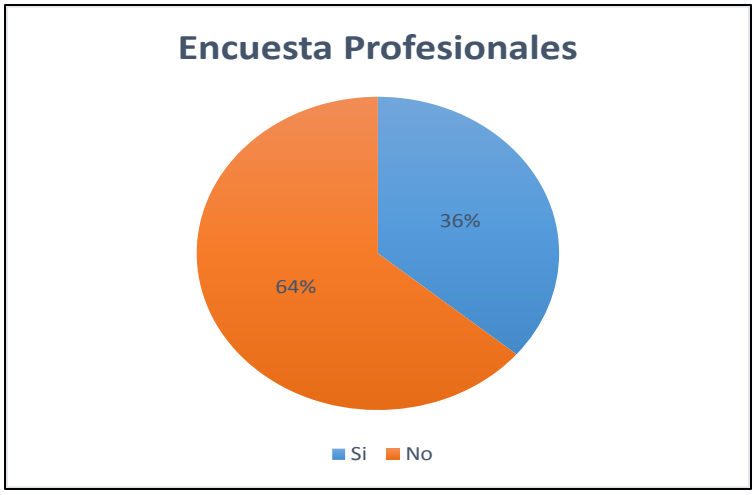
5. ¿Sabe usted qué tipo de Linux es Kali?

Tabla 10: Que tipo de Linux es Kali

ALTERNATIVAS	FRECUENCIA	PROMEDIO
Si	30	36%
No	53	64%
Total	83	100%

Fuente: Los autores

Gráfico Nº 10: Que tipo de Linux es Kali



Fuente: Los autores

INTERPRETACIÓN: Los datos de la tabla 10 nos demuestra de un total 83, profesionales y pre profesionales de la Facultad de Ciencias de la Ingeniería y Aplicadas (CIYA), el 64% que corresponde a 53 encuestados indican que si tiene conocimiento sobre qué tipos de Kali es Linux y el 64% que corresponde a 53 encuestados no tiene el conocimiento.

CONCLUSIÓN: Como se puede observar a través de los resultados obtenidos mediante esta pregunta un gran porcentaje de encuestados no tiene el conocimiento de que tipo de Linux es Kali, por lo que se recomendaría que se investigue más sobre los S.O basados en Linux.

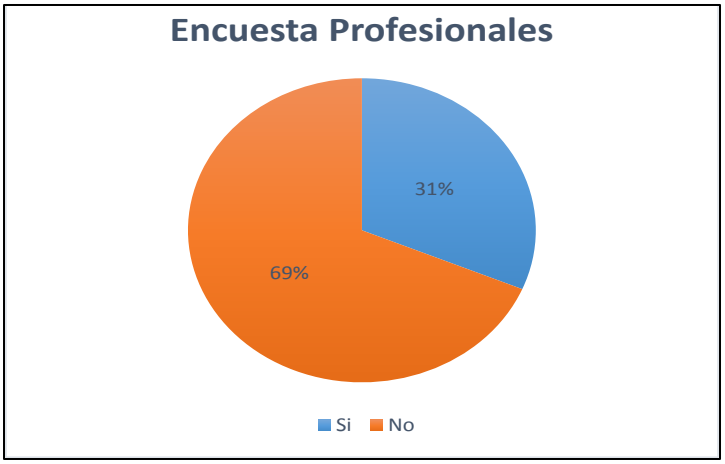
6. ¿Sabe usted cual es la función que cumple Metasploit Framework en Kali Linux?

Tabla 11: Metasploit Framework en Kali Linux

ALTERNATIVAS	FRECUENCIA	PROMEDIO
Si	26	31%
No	57	69%
Total	83	100%

Fuente: Los autores

Gráfico Nº 11: Metasploit Framework



Fuente: Los autores

INTERPRETACIÓN: Los datos de la tabla 11 nos demuestra de un total 83, profesionales y pre profesionales de la Facultad de Ciencias de la Ingeniería y Aplicadas (CIYA), el 31% corresponde a 26 encuestados los cuales mencionan que, si conocen sobre la función que cumple el Metasploit, y el 69% que corresponde a 57 encuestados no tiene el conocimiento sobre Metasploit.

CONCLUSIÓN: De acuerdo a los datos obtenidos de la encuesta se llega a la conclusión de que la mayor parte de profesionales no tiene el conocimiento sobre la función que cumple el Metasploit Framework. Por lo que se recomendaría se fomente cursos sobre dichas herramientas que permite visualizar las vulnerabilidades de sistemas informáticos.

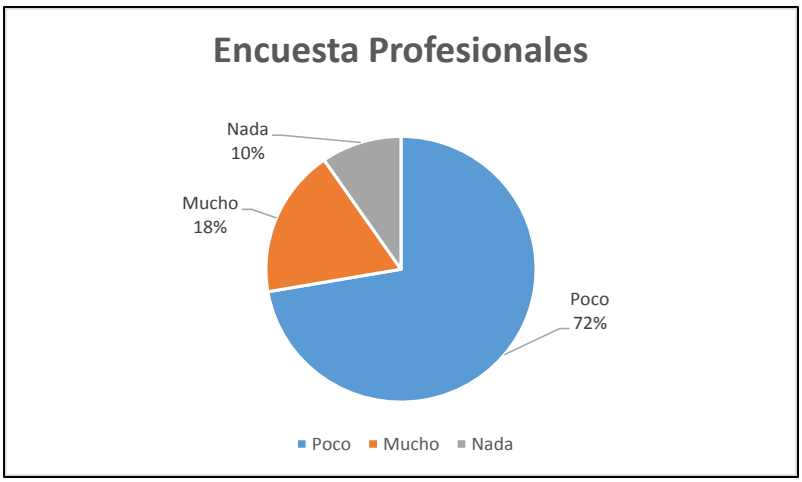
7. ¿Cuánto conoce usted sobre ataques phishing?

Tabla 12: Ataques phishing

ALTERNATIVAS	FRECUENCIA	PROMEDIO
Poco	60	72%
Mucho	15	18%
Nada	8	10%
Total	83	100%

Fuente: Los autores

Gráfico Nº 12 Ataques phishing



Fuente: Los autores

INTERPRETACIÓN: Los datos de la tabla 12 nos demuestra de un total 83, profesionales y pre profesionales de la Facultad de Ciencias de la Ingeniería y Aplicadas (CIYA), el 72% que corresponde a 60 personas tienen poco conocimiento sobre ataques phishing y el 18% que corresponde a 15 personas encuestadas. Tienen mucho conocimiento sobre los ataques phishing y el 10% que corresponde a 8 encuestadas no conocimiento sobre la pregunta planteada.

CONCLUSIÓN: En base a datos obtenidos respecto a los ataques phishing, se puede demostrar que el 72% de profesionales no considera la importancia de los ataques phishing que pueden ser realizados a través de la web, permitiéndoles exponerse a posibles riesgos y amenazas que se dan día a día.

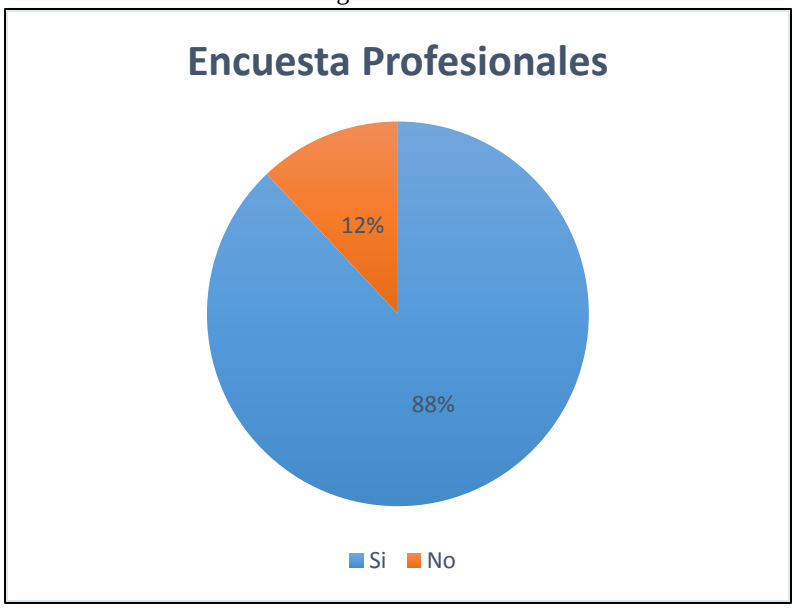
8. ¿Sabe usted cuales son los protocolos de Seguridad Informática?

Tabla 13: Protocolos de Seguridad Informática

ALTERNATIVAS	FRECUENCIA	PROMEDIO
Si	73	88%
No	10	12%
Total	83	100%

Fuente: Los autores

Gráfico Nº 13 Protocolos de seguridad informática



Fuente: Los autores

INTERPRETACIÓN: Lo datos de la tabla 13 nos demuestra de un total 83, profesionales y pre profesionales de la Facultad de Ciencias de la Ingeniería y Aplicadas (CIYA), el 88% que corresponde a 20 encuestados mencionan que, si conocen sobre los protocolos a seguir en la seguridad informática, y el 12% que corresponde a 10 personas encuestadas indican que no tiene conocimientos sobre la pregunta planteada.

CONCLUSIÓN: De acuerdo a datos obtenidos, durante la encuesta nos da como resultado que la mayor parte de profesionales dispone de conocimientos en cuanto a los protocolos de la seguridad informática.

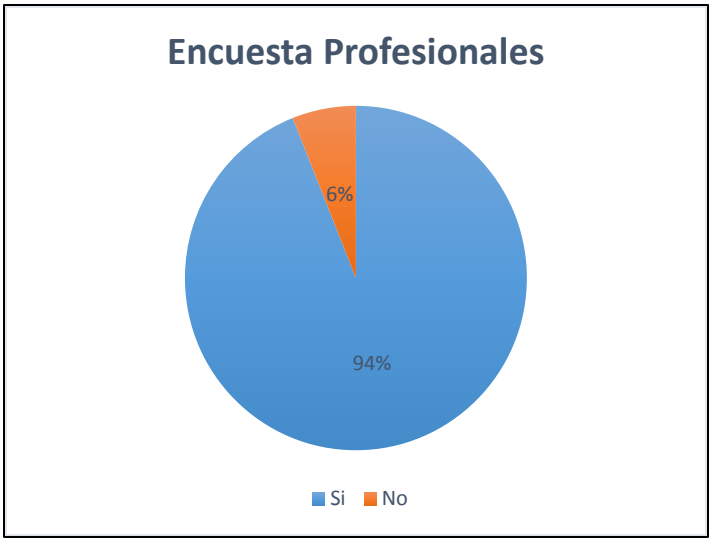
9. ¿Está usted informado acerca de las prevenciones que hay que tener para evitar el acceso de un hacker u otra amenaza a un sistema Informático?

Tabla 14: Prevenciones

ALTERNATIVAS	FRECUENCIA	PROMEDIO
Si	78	94%
No	5	6%
Total	83	100%

Fuente: Los autores

Gráfico Nº 14 : Prevenciones



Fuente: Los autores

INTERPRETACIÓN: Los datos de la tabla 14 nos demuestra de un total 83, profesionales y pre profesionales de la Facultad de Ciencias de la Ingeniería y Aplicadas (CIYA), el 94% que corresponde a 78 personas encuestadas conoce las prevenciones que se debe tener para evitar acceso de un hacker al sistema informático, y el 6% que corresponde a 5 personas no tiene conocimientos sobre la pregunta planteada.

CONCLUSIÓN: En base a los datos obtenidos se puede determinar que existen las respectivas prevenciones para evitar posible acceso no autorizado a los sistemas informáticos. Haciéndolos menos vulnerables para el resto de personas.

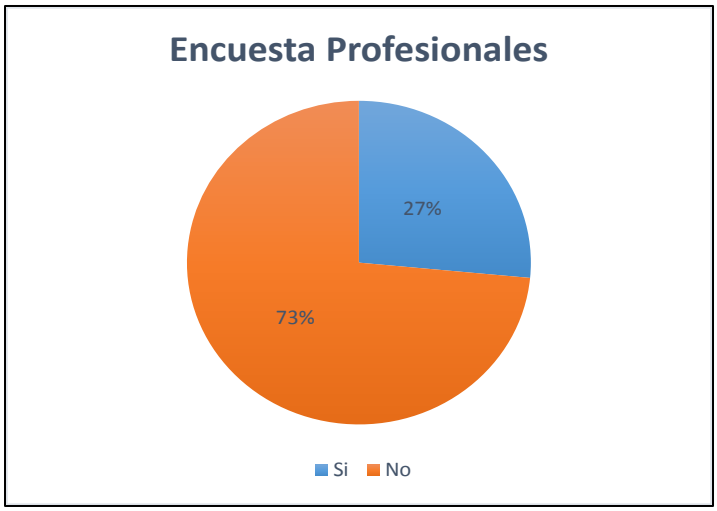
10. ¿Cree usted que los sistemas informáticos existentes en la Universidad Técnica de Cotopaxi son seguros?

Tabla 15: Sistemas seguros

ALTERNATIVAS	FRECUENCIA	PROMEDIO
Si	22	27%
No	61	73%
Total	83	100%

Fuente: Los autores

Gráfico Nº 15 Sistemas seguros



Fuente: Los autores

INTERPRETACIÓN: Los datos de la tabla 15 nos demuestra de un total 83, profesionales y pre profesionales de la Facultad de Ciencias de la Ingeniería y Aplicadas (CIYA), el 73% que corresponde a 61 personas encuestadas mencionan que no confían en el sistema informático de la UTC, y el 27% que corresponde a 22 personas confían en sistema informático de la UTC.

CONCLUSIÓN: De acuerdo a los datos obtenidos se puede visualizar que profesionales y pre profesionales no confían en el sistema de la Universidad Técnica de Cotopaxi. Por lo que se debe fortalecer el sistema de seguridad para obtener mayor confianza con los usuarios.

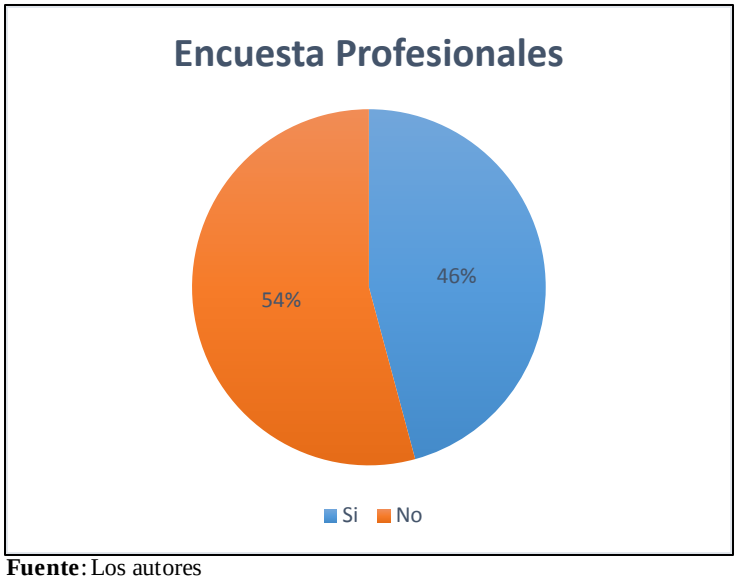
11. ¿Conoce usted que es un Sistema de Prevención (IDS)?

Tabla 16: Sistema de Prevención

ALTERNATIVAS	FRECUENCIA	PROMEDIO
Si	38	46%
No	45	54%
Total	83	100%

Fuente: Los autores

Gráfico Nº 16 Sistemas de prevención



Fuente: Los autores

INTERPRETACIÓN: Los datos de la tabla 16 nos demuestra de un total 83, profesionales y pre profesionales de la Facultad de Ciencias de la Ingeniería y Aplicadas (CIYA), el 54% que corresponde a 45 encuestados no tienen conocimientos sobre el sistema de IDS y el 46% que corresponde a 38 personas encuestadas sí disponen del conocimiento del sobre el sistema IDS.

CONCLUSIÓN: En los resultados obtenidos se puede evidenciar que un cierto porcentaje de profesionales y pre profesionales no disponen del conocimiento de la pregunta planteada, por lo que se podría recomendar se implemente más libros, revistas y artículos científicos sobre los sistemas IDS, y poder obtener más conocimientos sobre dicho tema.

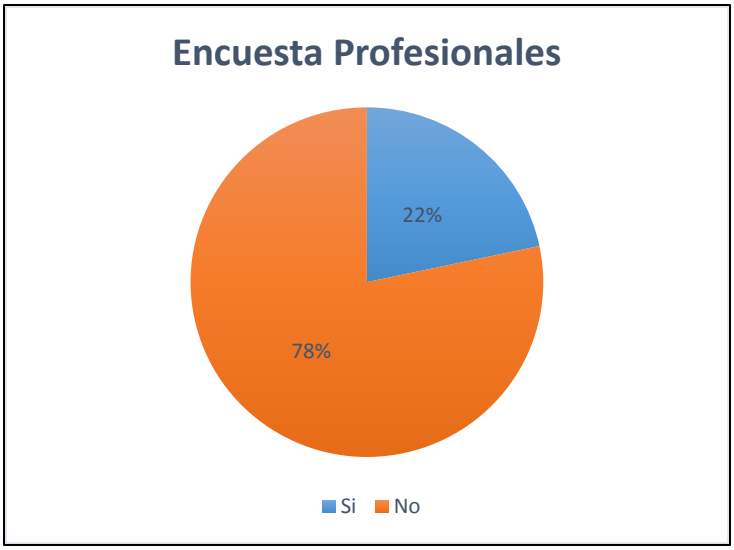
12. ¿Tiene usted conocimiento sobre la herramienta SqlMap en Kali Linux?

Tabla 17: Herramienta SqlMap

ALTERNATIVAS	FRECUENCIA	PROMEDIO
Si	18	22%
No	65	78%
Total	83	100%

Fuente: Los autores

Gráfico Nº 17 Herramienta SqlMap



Fuente: Los autores

INTERPRETACIÓN: Los datos de la tabla 17 nos demuestra de un total 83, profesionales y pre profesionales de la Facultad de Ciencias de la Ingeniería y Aplicadas (CIYA), el 78% que corresponde a 65 no tienen conocimientos sobre el SqlMap en Kali Linux y el 22% que corresponde a 18 personas encuestadas sí disponen del conocimiento de SqlMap.

CONCLUSIÓN: De acuerdo a los datos obtenidos se puede evidenciar que no existe el conocimiento so la herramienta SqlMap dentro del S.O Kali Linux. Por lo que se recomienda que sede más información sobre el tema.

ENCUESTAS ESTUDIANTES

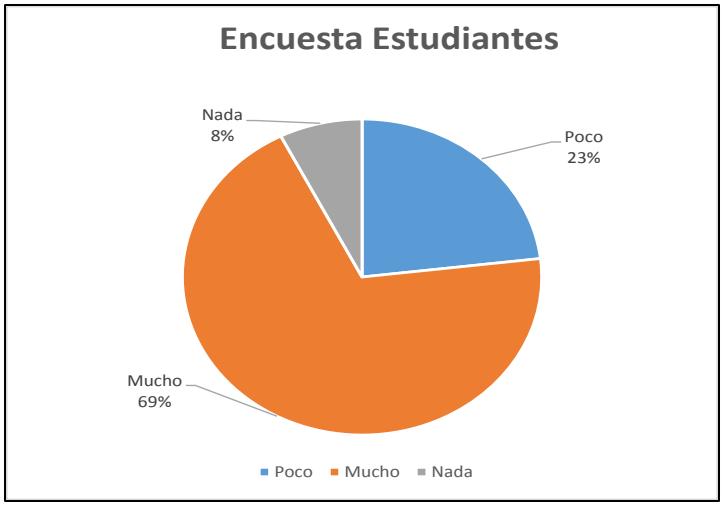
1. ¿Con que frecuencia usa usted el internet de la Universidad Técnica de Cotopaxi?

Tabla 18: Uso del internet

ALTERNATIVAS	FRECUENCIA	PROMEDIO
Poco	31	23%
Mucho	93	69%
Nada	10	7%
Total	134	100%

Fuente: Los autores

Gráfico Nº 18 Uso del internet



Fuente: Los autores

INTERPRETACIÓN: Los datos de la tabla 18 nos demuestra de un total 134, Estudiantes de la Facultad de Ciencias de la Ingeniería y Aplicadas (CIYA), el 23% que corresponde a 31 personas encuestadas, utilizan poco el internet de la UTC, y el 69% que corresponde a 93 personas encuestadas si utilizan el internet de la UTC, el 7% que corresponde a 10 encuestados no utilizan el servicio de internet de la institución

CONCLUSIÓN: Estos datos son de gran importancia para dar una idea más clara de la utilización de internet de la UTC por parte de los estudiantes, por lo tanto, se puede determinar que la herramienta del internet es fundamental para desarrollo del estúdiate en su formación.

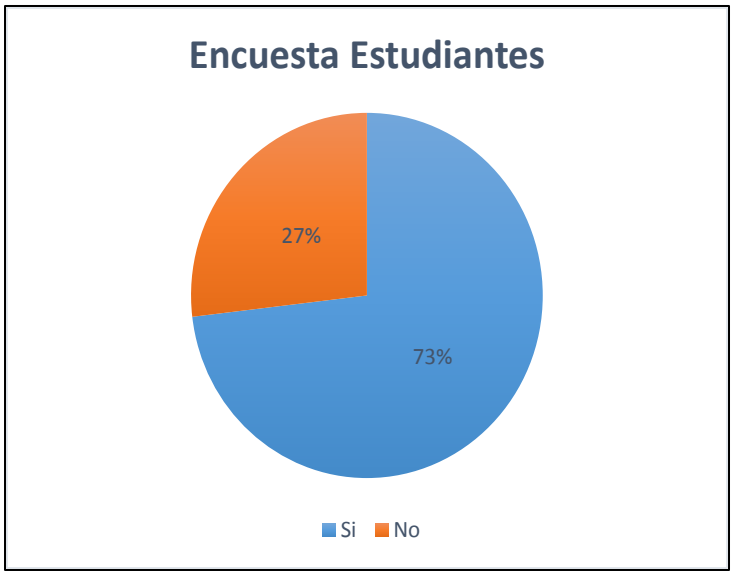
2. ¿Sabe usted que es un hacker?

Tabla 19: Que es un hacker

ALTERNATIVAS	FRECUENCIA	PROMEDIO
Si	98	73%
No	36	27%
Total	134	100%

Fuente: Los autores

Gráfico Nº 19 Que es un hacker



Fuente: Los autores

INTERPRETACIÓN: Los datos de la tabla 19 nos demuestra de un total 134, Estudiantes de la Facultad de Ciencias de la Ingeniería y Aplicadas (CIYA), el 73% que corresponde a 98 personas encuestadas tiene conocimiento sobre lo que es un hacker, y el 27% que corresponde a 36 personas encuestadas no dispone del conocimiento de lo que es un hacker.

CONCLUSIÓN: Se debería considera necesario leer libros y artículos tecnologías para poder tener conocimiento sobre lo que es un hacker, teniendo en cuenta que son personas que pueden robar datos informativos de un sistema.

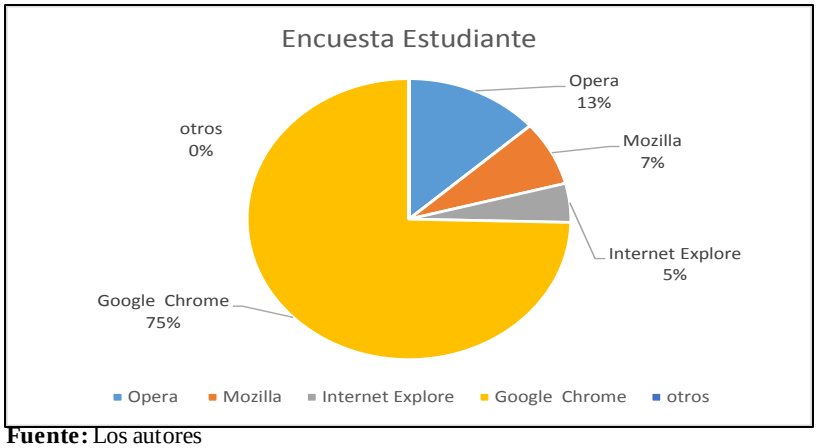
3. ¿Qué navegador web utiliza normalmente?

Tabla 20: Navegadores web

ALTERNATIVAS	FRECUENCIA	PROMEDIO
Opera	18	13%
Mozilla	10	7%
Internet Explore	6	4%
Google Chrome	100	75%
otros	0	0%
Total	134	100%

Fuente: Los autores

Gráfico Nº 20 Navegadores web



Fuente: Los autores

INTERPRETACIÓN: Los datos de la tabla 20 nos demuestra de un total 134, Estudiantes de la Facultad de Ciencias de la Ingeniería y Aplicadas (CIYA), el 13% que corresponde a 18 personas encuestadas utilizan el navegador opera, y el 7% que corresponde a 10 personas encuestadas utiliza el navegador Mozilla, el 4% que corresponde a 6 personas utilizan el navegador internet explore, el 75% que corresponde a 100 personas utiliza el navegador Google Chrome

CONCLUSIÓN: De acuerdo al dato obtenido se considera que el navegador más utilizado por parte de los estudiantes es Google Chrome, el cual lo toman como principal herramienta de búsqueda de información.

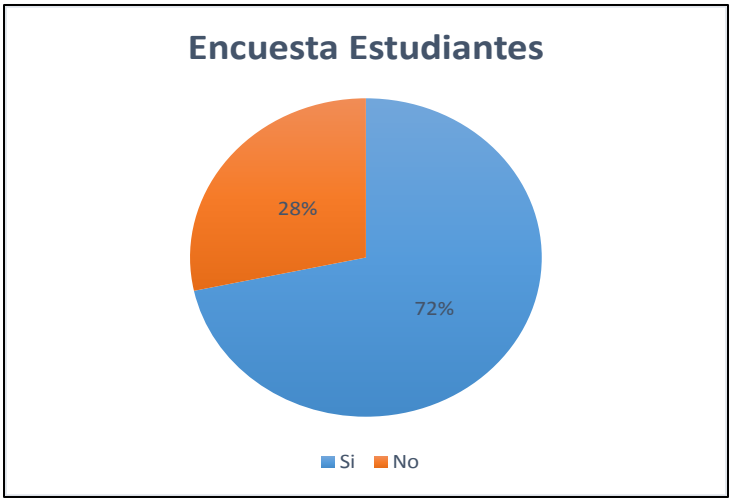
4. ¿Tiene usted algún software antivirus instalado en su computador?

Tabla 21: Antivirus

ALTERNATIVAS	FRECUENCIA	PROMEDIO
Si	96	72%
No	38	28%
Total	134	100%

Fuente: Los autores

Gráfico Nº 21 Antivirus



Fuente: Los autores

INTERPRETACIÓN: Los datos de la tabla 21 nos demuestra de un total 134, Estudiantes de la Facultad de Ciencias de la Ingeniería y Aplicadas (CIYA), el 72% que corresponde a 96 personas encuestadas utilizan un antivirus en su computador y 28% que corresponde a 38 personas encuestadas no tiene instalado un antivirus en su computador.

CONCLUSIÓN: De acuerdo a datos obtenidos los estudiantes de la UTC, no tiene conocimientos sobre los antivirus, por lo que sería necesario difundir información acerca del tema y todas las ventajas que brida la utilización de un Antivirus para su seguridad de su computador.

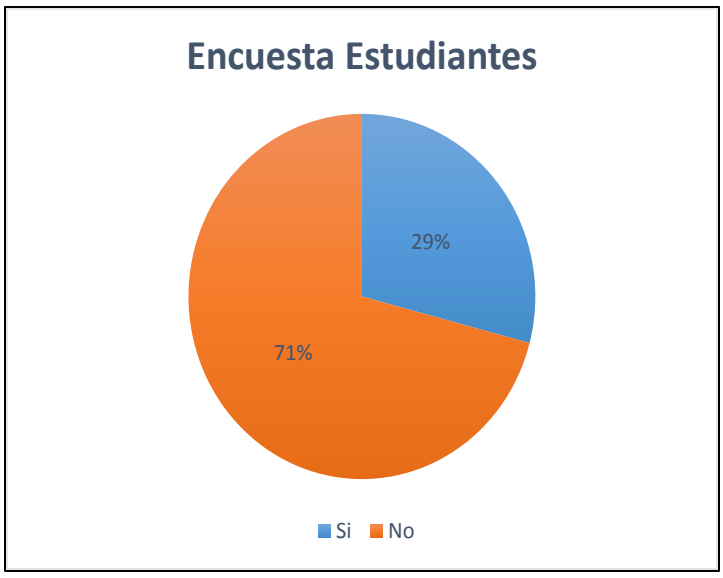
5. ¿Al navegar por la red wifi de la UTC considera que es seguro?

Tabla 22: Red wifi seguro

ALTERNATIVAS	FRECUENCIA	PROMEDIO
Si	39	29%
No	95	71%
Total	134	100%

Fuente: Los autores

Gráfico Nº 22 Red wifi seguro



Fuente: Los autores

INTERPRETACIÓN: Los datos de la tabla 22 nos demuestra de un total 134, Estudiantes de la Facultad de Ciencias de la Ingeniería y Aplicadas (CIYA), el 71% que corresponde a 95 personas encuestadas, consideran que no es seguro navegar por la red wifi de la UTC, y el 29% que corresponde a 39 personas confían en la red wifi de la institución.

CONCLUSIÓN: Podemos mencionar que el resultado más alto obtenido es la desconfianza del uso de la red wifi, por lo que el estudiante no se siente seguro al navegar por dicha red. Por tal razón se considera que se debería impartir más información sobre el tema de seguridad.

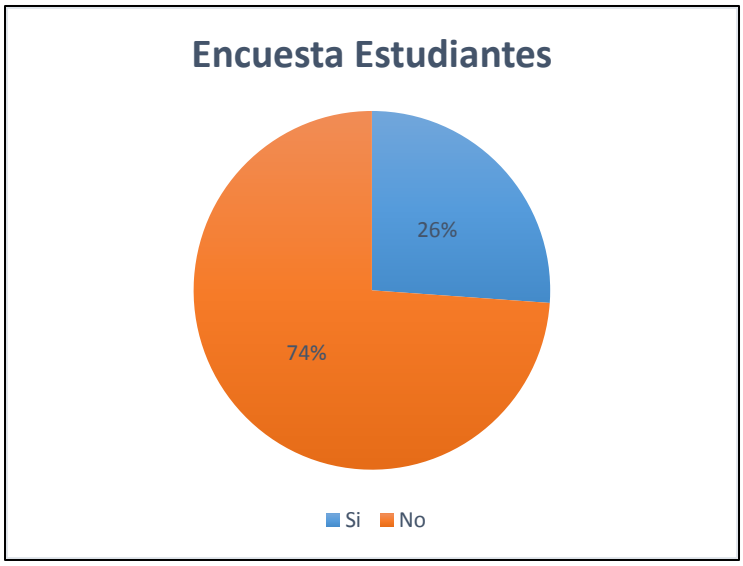
6. ¿Sabe usted sí la UTC ha sido blanco de algún ataque de cibernético?

Tabla 23: Ataque cibernético

ALTERNATIVAS	FRECUENCIA	PROMEDIO
Si	35	26%
No	99	74%
Total	134	100%

Fuente: Los autores

Gráfico Nº 23 Ataque cibernético



Fuente: Los autores

INTERPRETACIÓN: Los datos de la tabla 23 nos demuestran de un total 134, Estudiantes de la Facultad de Ciencias de la Ingeniería y Aplicadas (CIYA), el 74% que corresponde a 99 personas encuestadas consideran que no saben si la UTC ha sido blanco de un ataque cibernético, y el 26% que corresponde a 39 personas consideran que la UTC si ha sido blanco de un a taques cibernético.

CONCLUSIÓN: Con los resultados obtenidos podemos determinar que estudiantes de la institución determinan que no se ha sufrido ningún tipo de ataque dentro de la institución. Por lo que se podría recomendar es que se siga impartiendo conocimiento sobre el tema ya que todos estamos expuestos a ser víctimas de posibles ataques cibernéticos.

7. ¿Conoce usted de algún Ataque Cibernético que ha ocurrido en el País?

Tabla 24: Ataque Cibernético en el País

ALTERNATIVAS	FRECUENCIA	PROMEDIO
Si	66	49%
No	68	51%
Total	134	100%

Fuente: Los autores

Gráfico Nº 24 Ataque Cibernético en el País

Fuente: Los autores

INTERPRETACIÓN: Los datos de la tabla 24 nos demuestran de un total 134, Estudiantes de la Facultad de Ciencias de la Ingeniería y Aplicadas (CIYA), el 51% que corresponde a 68 personas encuestadas consideran que no saben sobre ataques sufridos dentro del país, y el 49% que corresponde a 66 personas encuestadas consideran que el país si ha sido blanco de ataques cibernéticos.

CONCLUSIÓN: Con datos obtenidos se puede determinar que el estudiante no tiene conocimiento sobre ataques sufridos en el país, por desinformación, por lo que se reitera la necesidad de dar más información a los estudiantes sobre posibles ataques cibernéticos dentro del país.

8. ¿Utiliza usted Algún software de firewall en tu Computador?

Tabla 25: Software de firewall

ALTERNATIVAS	FRECUENCIA	PROMEDIO
Si	38	28%
No	96	72%
Total	134	100%

Fuente: Los autores

Gráfico Nº 25 Software de firewall

Fuente: Los autores

INTERPRETACIÓN: Los datos de la tabla 29 nos demuestran de un total 134, Estudiantes de la Facultad de Ciencias de la Ingeniería y Aplicadas (CIYA), el 72% que corresponde a 96 personas encuestadas, mencionan que no tienen ningún software de firewall instalado en su computador, 28% que corresponde a 38 personas encuestas consideran que si tienen un software de firewall instalado en su computador.

CONCLUSIÓN: De acuerdo a los datos obtenidos se puede determinar que el estudiante no tiene conocimiento de un software de firewall, por lo que se reitera la necesidad de dar más información acerca del firewall.

UNIVERSIDAD TÉCNICA DE COTOPAXI

FACULTAD DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

CARRERA DE INGENIERÍA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES

PROYECTO DE INVESTIGACIÓN

INFORME TÉCNICO

"ANÁLISIS DE LA CIBERSEGURIDAD A LA INFRAESTRUCTURA TECNOLÓGICA DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI"

Latacunga – Ecuador

Julio – 2019

1. INTRODUCCIÓN

Dentro de una sociedad tan globalizada y con un entorno laboral como eje principal del desarrollo económico de los países, cada día que transcurre las empresas a nivel nacional y mundial poseen miles de servicios tecnológicos, los mismos que catapultan e intensifican la posesión de la marca dentro de cualquier mercado.

A nivel operacional cada compañía indistintamente al tipo de operación económica a la que esta se dedique los servicios informáticos que se implementan dentro de las empresas es el pilar fundamental para continuar con el desarrollo de sus operaciones.

Es importante mencionar que las empresas deben de contar con planes de contingencia a nivel tecnológico, que les permitan actuar de manera inmediata ante cualquier tipo de amenaza que pueda poner en riesgo la información que se maneja o la paralización de algún servicio en particular.

Dentro de los distintos planes de contingencia que cada empresa puede manejar, es importante destacar que no se puede estar totalmente seguro, pero si se puede minimizar de gran forma los impactos que pudieran producirse con algún tipo de amenaza que atente contra nuestros servicios informáticos.

También es fundamental destacar que, a nivel departamental en todas las empresas e instituciones grandes, así como ocurre en la Universidad Técnica de Cotopaxi, el departamento de sistemas informáticos está sujeto a auditorias informáticas, en las cuales se realiza distintas observaciones a nivel de procesos y procedimientos y en los cuales es importante ir disminuyendo este tipo de observaciones.

2. ANTECEDENTES

En la Universidad Técnica de Cotopaxi específicamente dentro del departamento de Tecnología de la Información, en su objetivo de ofrecer siempre la disponibilidad absoluta de sus servicios informáticos y preocupándose por la información que maneja cada uno de los usuarios surge la necesidad de realizar un Análisis a su infraestructura tecnológica para de esa manera evaluar sus posibles brechas de seguridad que dispone su infraestructura.

3. OBJETIVO

El objetivo principal de este proyecto de investigación es dar a conocer sus posibles vulnerabilidades informáticas, y dar posibles recomendaciones, con la finalidad de estar preparados y en constante vigilancia de las posibles amenazas que pudieran presentarse a futuro.

4. ANTECEDENTES

El análisis fue realizado desde una parte interna a la institución con el objetivo de validar la seguridad de sus sistemas informáticos, permitiéndonos obtener como resultados una muestra de las falencias que tiene la institución en cuanto a Ciberseguridad.

5. ANÁLISIS A LA INFRAESTRUCTURA TECNOLÓGICA DE LA UTC

El análisis fue realizado desde una parte interna a la institución con el objetivo de validar la seguridad de sus sistemas informáticos, permitiéndonos obtener como resultados una muestra de las falencias que tiene la institución en cuanto a Ciberseguridad.

5.1. SOFTWARE UTILIZADOS

- Kali Linux 64 Bit versión 2019.2
- VMware WorkStation versión 15.0.4
- Nmap
- OWAspzap 2.8.0

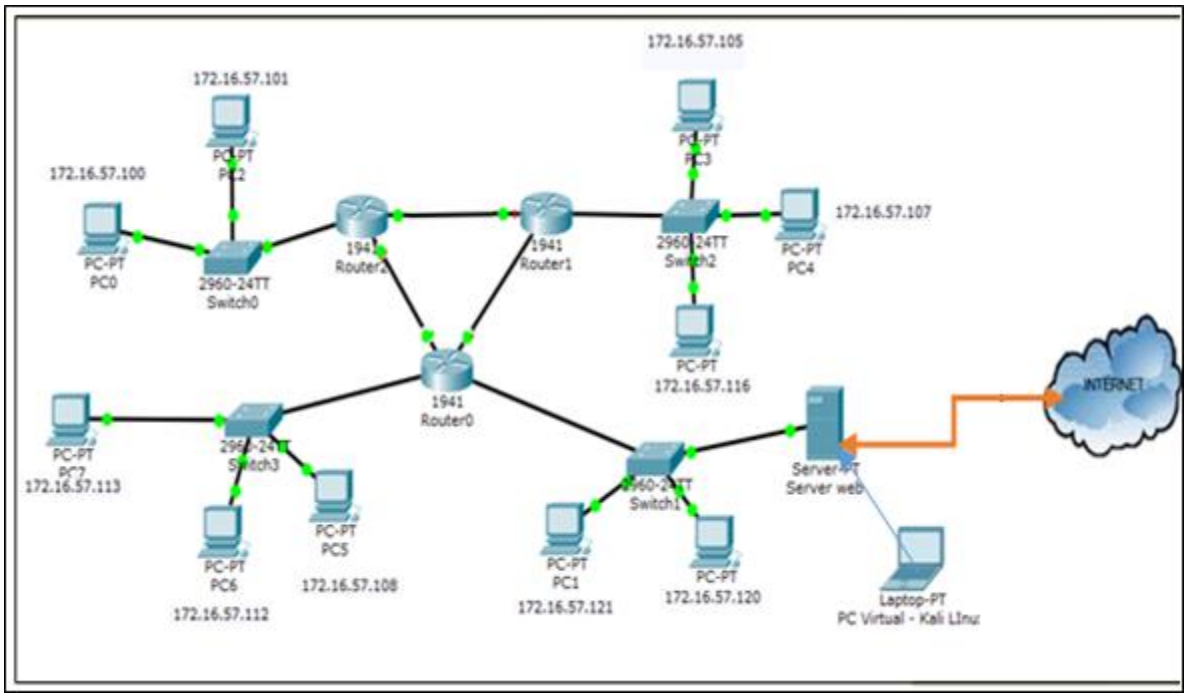
6. INFORME DE PRUEBAS REALIZADAS

6.1. Recolección de Información, escaneo de red y puertos

En esta primera prueba se hace uso de los aplicativos NMAP y OWAspzap los mismos que sirven para un análisis de red y escaneo de puertos abiertos, este tipo de programas son muy útiles para recopilación de información los mismos que en un hipotético riesgo sirvan para

determinar si hay algún tipo de host no identificado por nuestro equipo de seguridad dentro de nuestra de red, esto se debe ya que al hacer un scan de la red, particularmente NMAP muestra los nombres de los equipos que tuvieron cualquier tipo de conexión dentro de sus servidores, en este caso de la Universidad Técnica de Cotopaxi hemos seleccionado un puerto como objetivos en el cual detallamos su vulnerabilidad.

Esquema de topología de red para análisis de vulnerabilidad



6.2. Funciones de sus elementos:

Router

También conocido como enrutador, es el encargado de interconectar las computadoras para que funcionen en un marco de una red como muestra en la topología del análisis.

Switch o Conmutador

Es un dispositivo de interconexión que se utiliza para conectar los dispositivos dentro de una red formando lo que se conoce como una red de área local.

Ip

Número que identifica de manera lógica y jerárquica una interfaz en red (Elemento de comunicación / conexión)

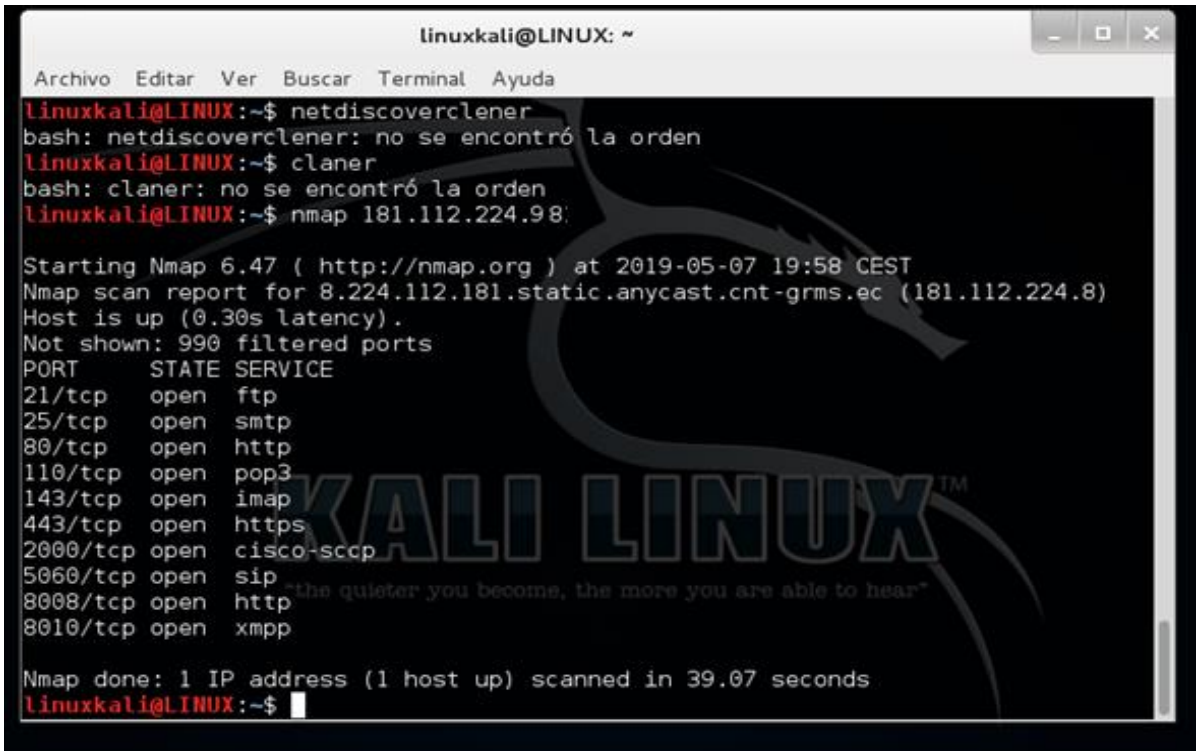
Servidor

Es una aplicación en ejecución capaz de entender las peticiones de un cliente y devolverle una respuesta en concordancia

6.3. Comandos utilizados nmap

Sintaxis: nmap [tipo_de_escaneo] [opciones] {red | puerto_obejtivo_ FTP}
nmap –sS 181.112.224.98
nmap –sN 181.112.224.98
nmap www.utc.edu.ec–vv nmap –sS 192.168.5.0/24
nmap –sT –O www.utc.edu.ec nmap –sA 181.112.224.98
nmap –sT 181.112.224.98
nmap –sU 181.112.224.98
nmap –sF 181.112.224.98
nmap –sX 181.112.224.98
nmap –sV 181.112.224.98
nmap –T 181.112.224.98
nmap –v 181.112.224.98
nmap –p 1-65535 –T4 –A –v www.utc.edu.ec

Resultados



nmap – 181.112.224.98 Los parámetros que indican en el gráfico de la capturada del escaneo se puede visualizar los puertos abiertos.

6.4. ANÁLISIS DE PUERTOS ABIERTOS Y SUS VULNERABILIDADES

A continuación, detallaremos sus referencias de vulnerabilidades que posee cada uno de sus puertos abiertos con sus respectivos riesgos asociados. La idea de este análisis es hacer conciencia para determinar de forma rápida y fácil los diferentes ataques que puedes sufrir en caso que tengas algunos de estos puertos abiertos.

7. Puertos abiertos y sus posibles ataques

7.1. Puerto 21 ftp

- Buffer Overflow
- Denegación de servicio (DoS)

7.2. Puerto 25 smtp

- Denegación de Servicio (DoS)
- Recogida de Información

7.3. Puerto 80 http

- Denegación de servicio (DoS)
- Recogida de Información
- Posibilidades de sniffer
- Ataque CGI

7.4. Puerto 110 pop3

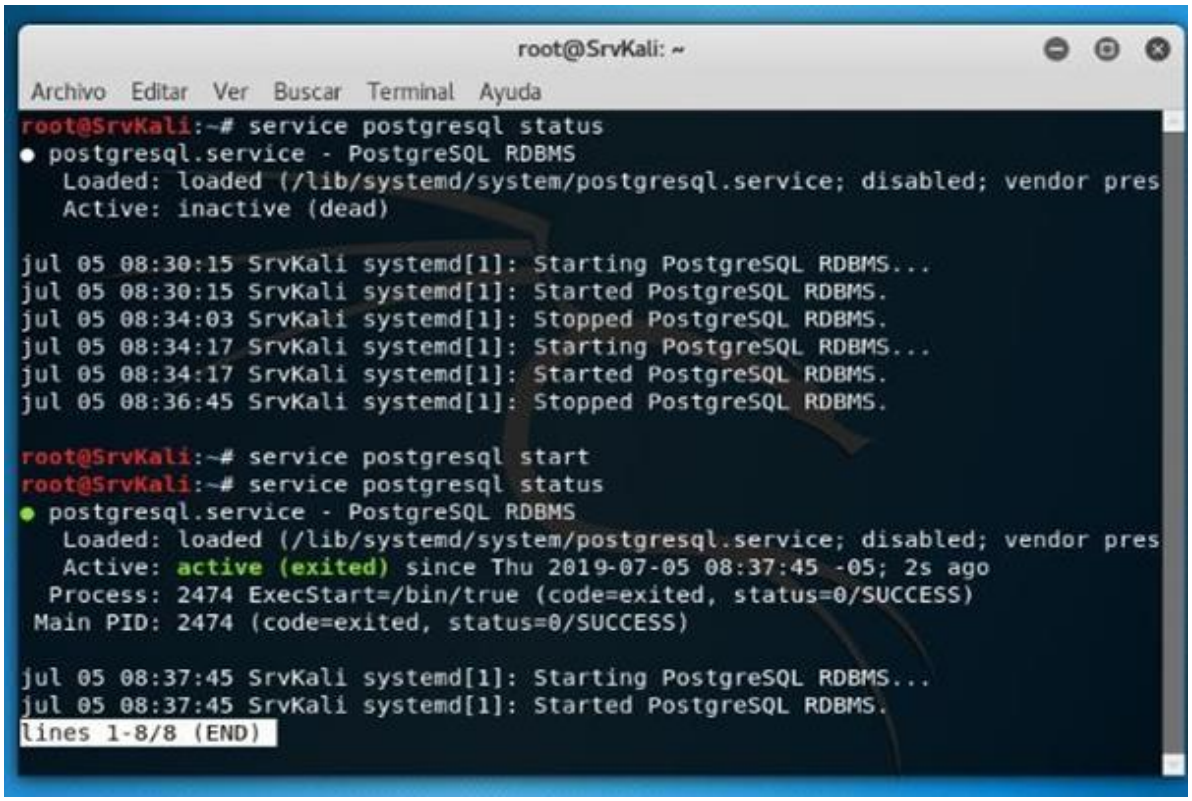
- Buffer Overflow
- Denegacion de Servicio (DoS)
- Ataque de Fuerza Bruta

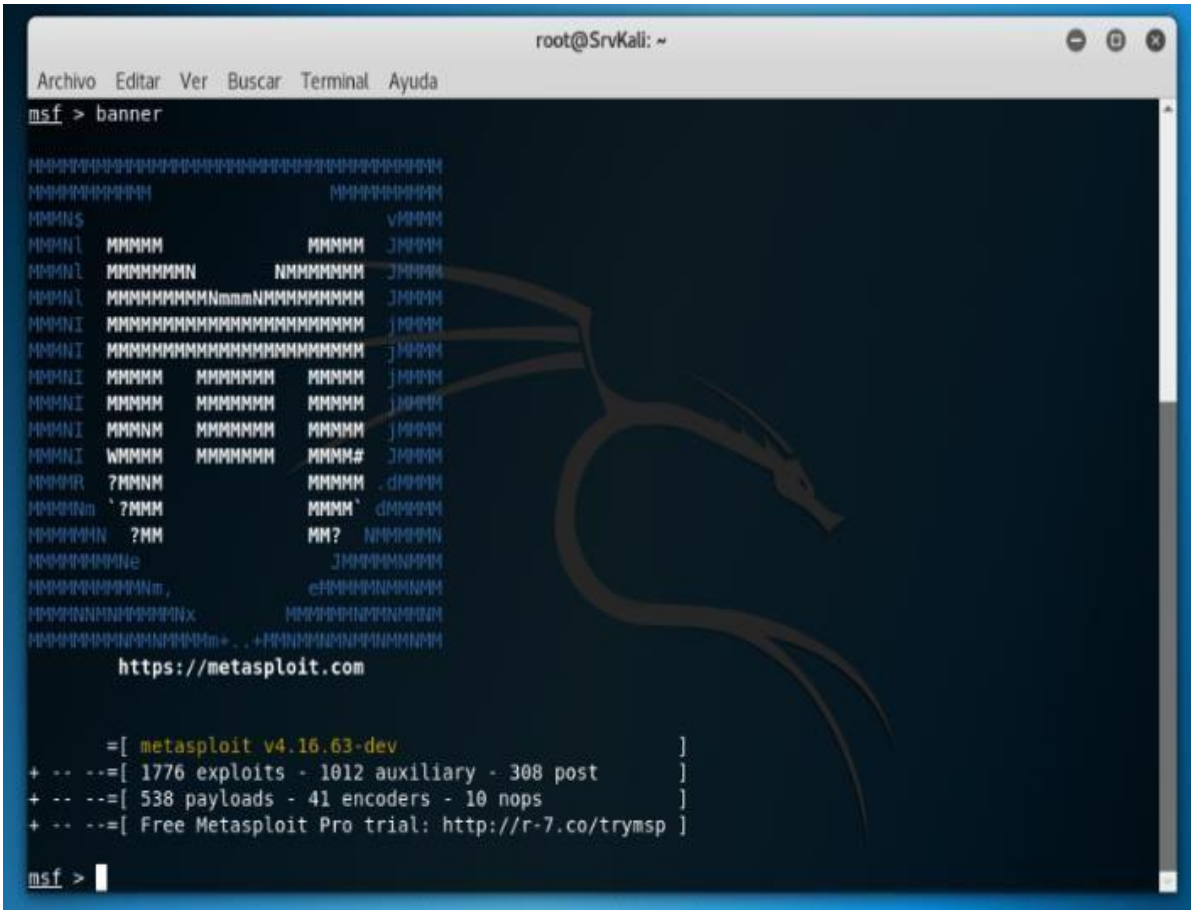
De acuerdo a lo detallado se recomienda bloquear todos aquellos puertos que no son utilizados, e incluso cuando esté convencido de que dichos puertos están siendo bloqueados, aún debería supervisarlos de cerca para detectar intentos de algún intruso.

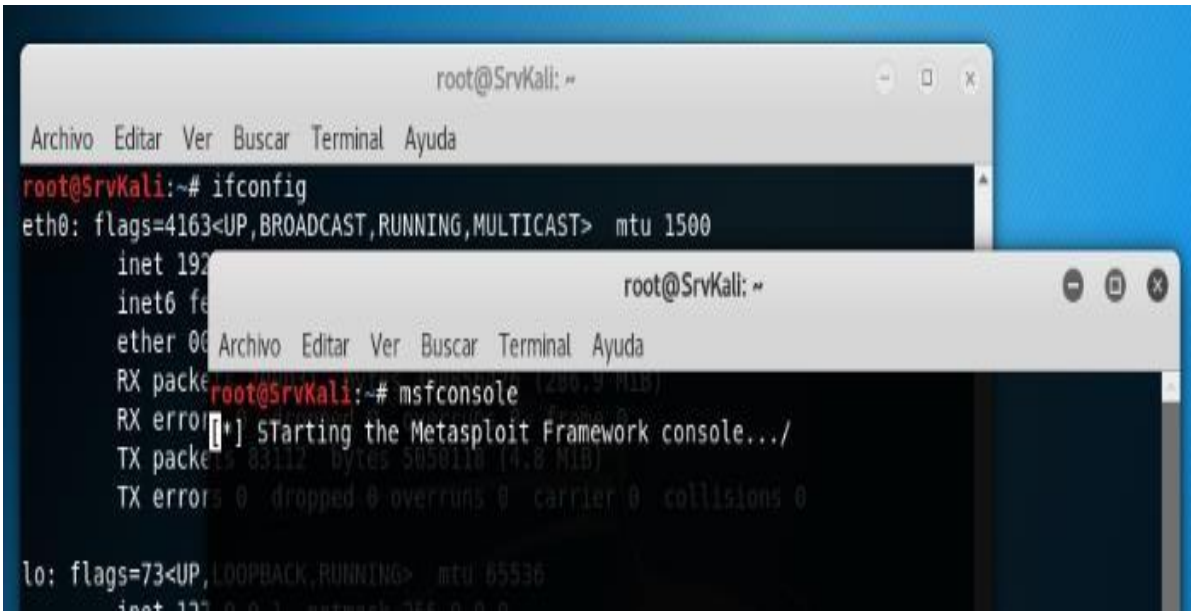
8. CREACIÓN DE EXPLOIT

Para esta oportunidad se ha hecho uso de la herramienta Metasploit, el mismo que es un framework que sirve para proveer información acerca de las vulnerabilidades que pudiera tener algún dispositivo. Este software es una gran herramienta que sirve para el desarrollo y posterior ejecución de Exploits que pueden ejecutarse en un equipo remoto, mediante la creación de pequeñas secuencias de códigos o comandos, mismo que pueden tomar la forma de un ejecutable para cualquier sistema operativo, ya sea Windows, Mac OS, e incluso el conocido sistema operativo de dispositivos móviles Android, todo esto es posible mediante esta herramienta, cabe destacar que todos estos tipos de ataque pueden realizarse dentro de la LAN corporativa e incluso desde fuera de ella.

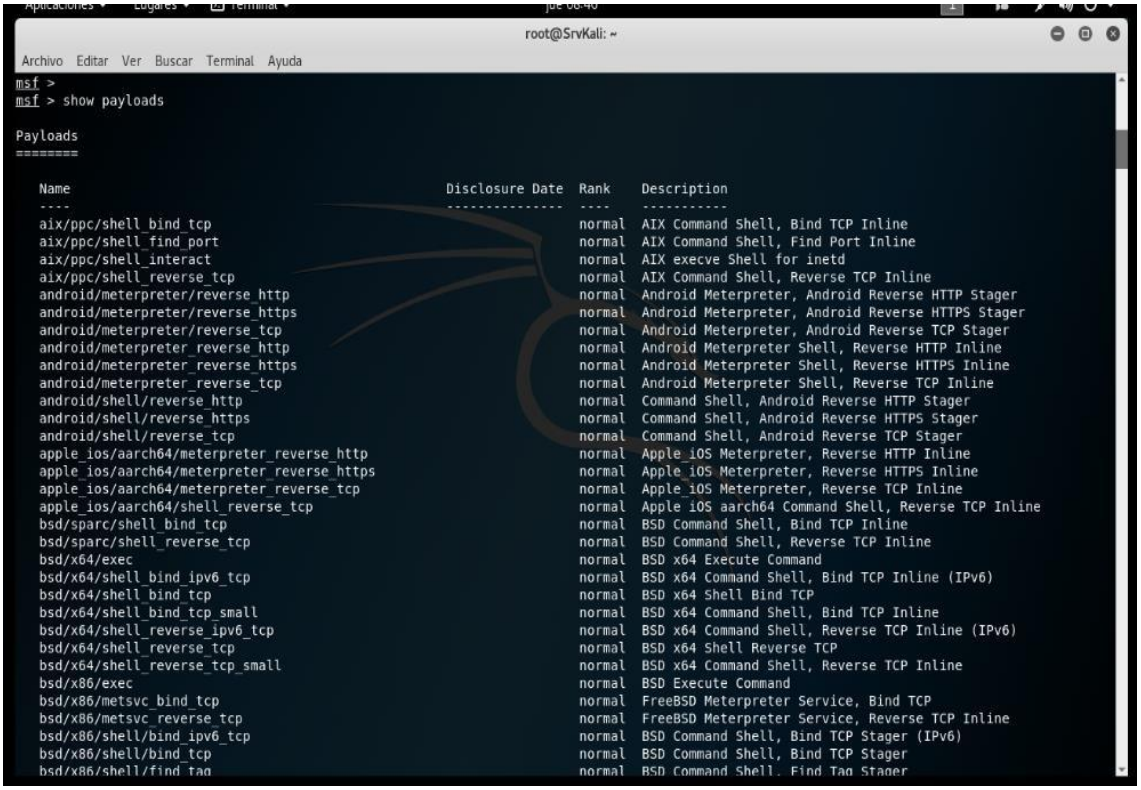
Iniciar servicios de base de datos postgresql



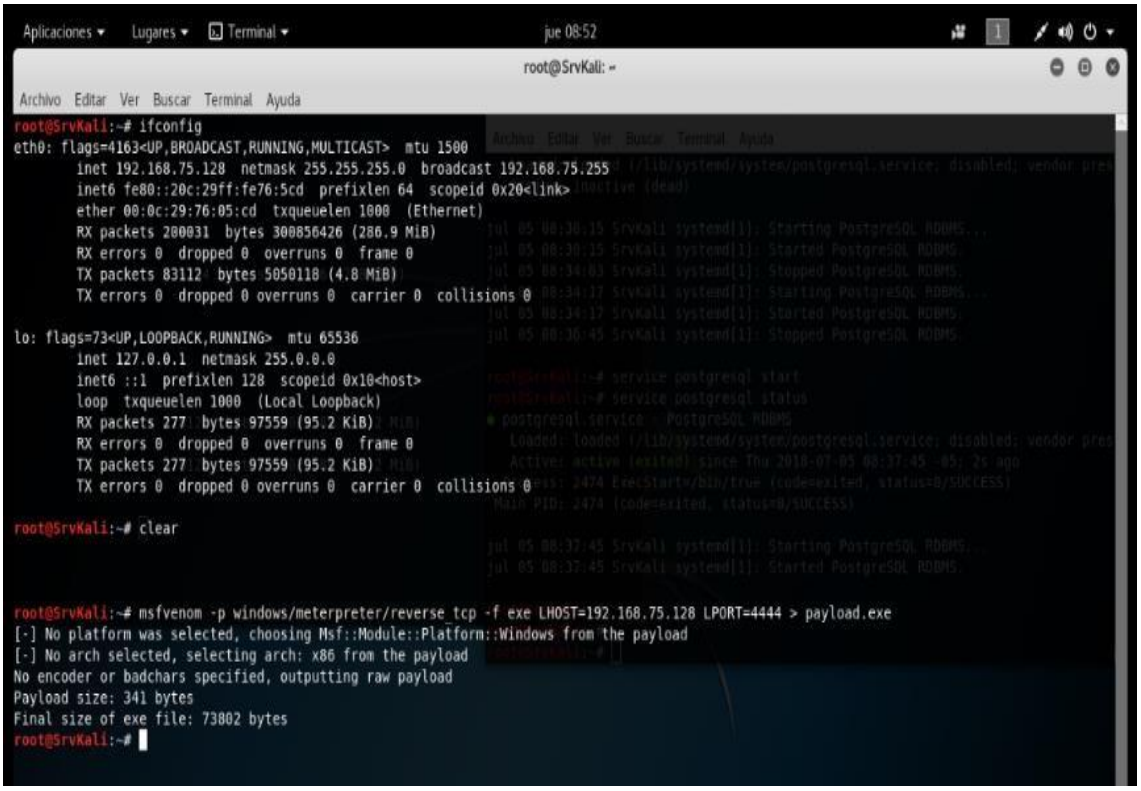




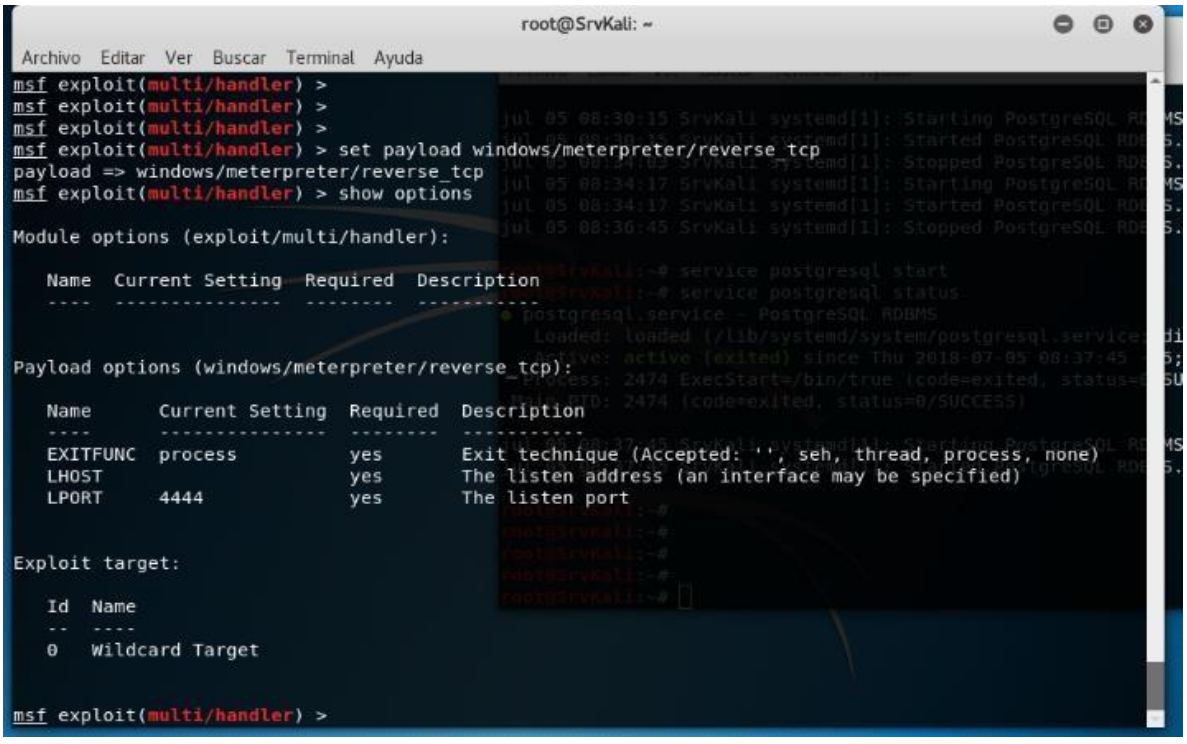
Mostrar payloads disponibles en la herramienta



Creación del Payload



Configuración del puerto



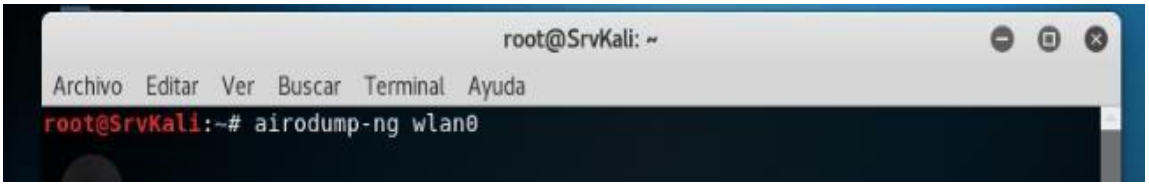
9. Vulnerabilidades en redes Wifi

Para las vulnerabilidades Wireless hay distintos aplicativos dentro del sistema operativo Kali Linux, entre ellos son las distintas herramientas de la suite de aircrack, las cuales nos pueden ayudar a determinar el tráfico que se maneja dentro de la red, si bien es cierto este tipo de herramientas no atacan directamente al protocolo de autenticación que usa una red Wireless sino más bien se basan en diccionarios de datos que atacan directamente a la clave que se usa para poder autenticarse dentro de la red, esto se consigue mediante algoritmos basados en diccionarios de datos que tratan de descifrar todas las posibles combinaciones de las palabras agregadas en el diccionario de datos.

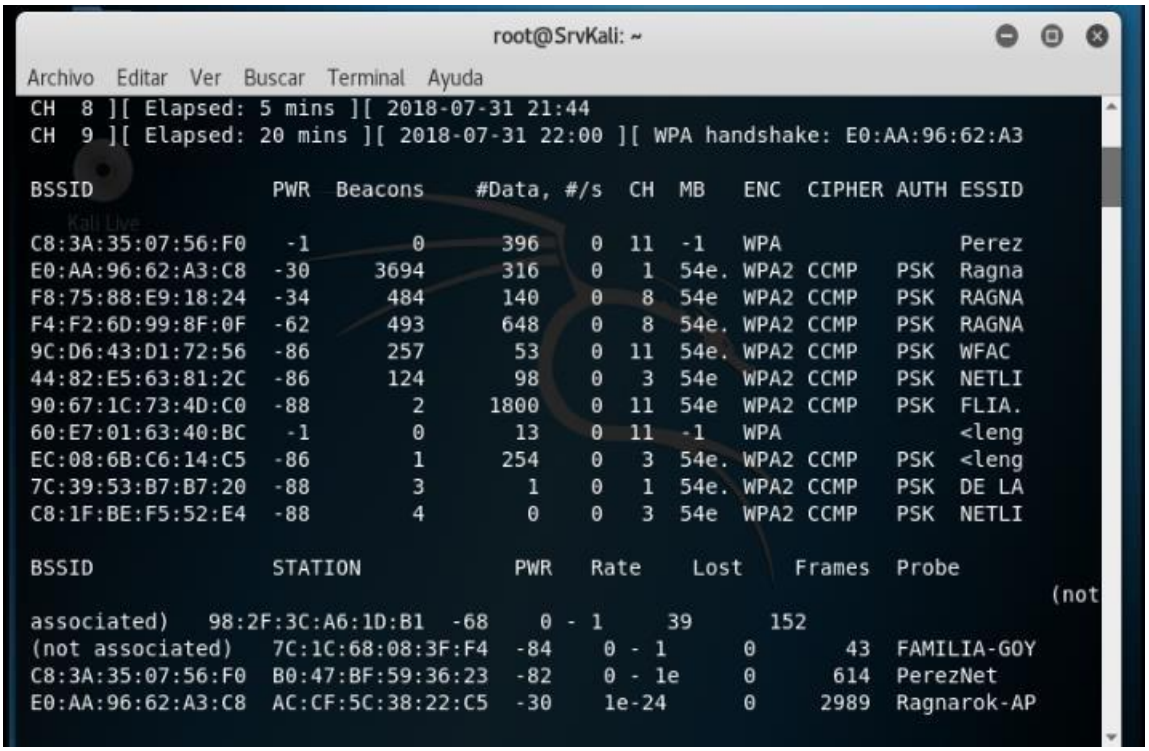
9.1. Comandos utilizados

iwconfig
Matar procesos
airmon-ng check kill airmon-ng check kill
Iniciar tarjeta en modo monitor airodump-ng wlan0mon airmon-ng start wlan0 Escanear redes
airodump-ng wlan0mon
airodump-ng –c 1 –w capture –bssid e0:aa:96:62:a3:c8 wlan0mon
Enviar a des autenticar a un host conectado en la red
aireplay-ng --deauth 10–a e0:aa:96:62:a3:c8–c ac:cf:5c:38:22:c5 wlan0mon
Des encriptar la clave de la red Wireless con el archivo .cap
Crunch 1010–t%%%%%%%%1234567890|aircrack-ng–w–capture-01.cap –o wifi-ti

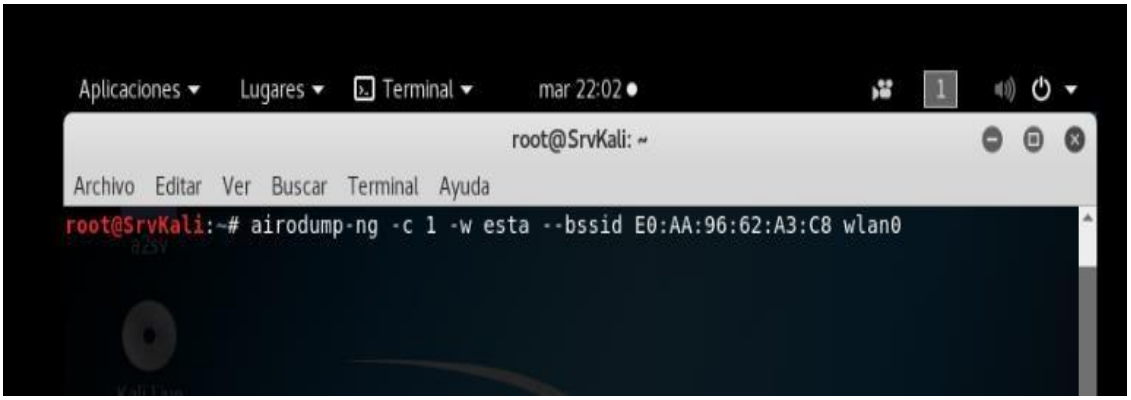
Escaneo de redes Wireless disponibles



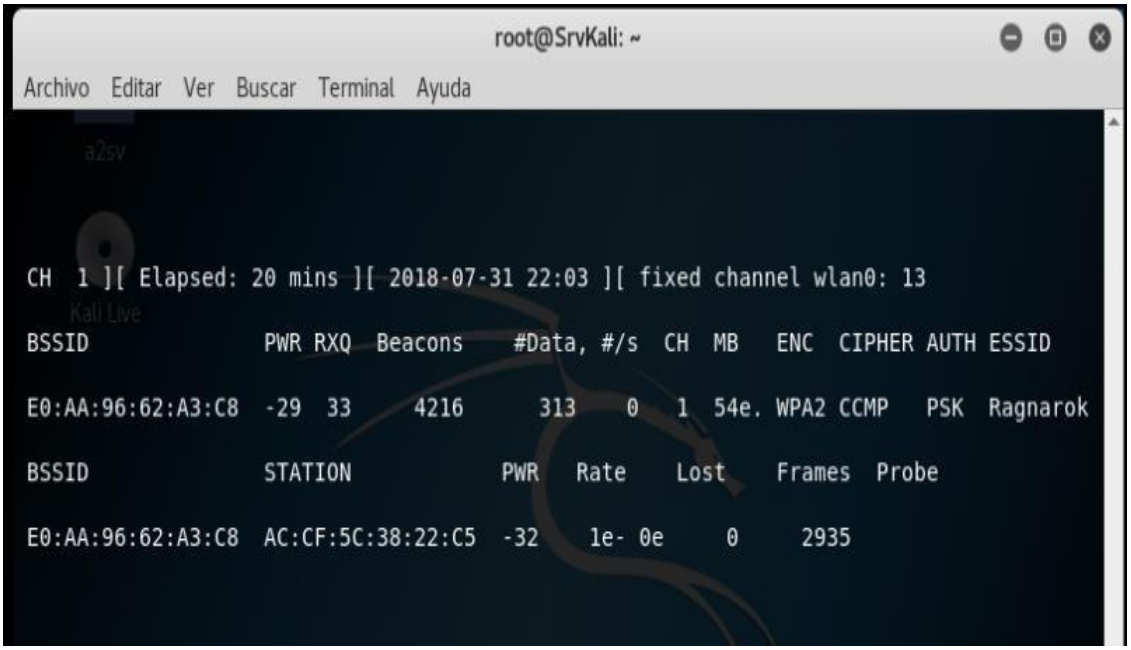
Redes Wireless encontradas



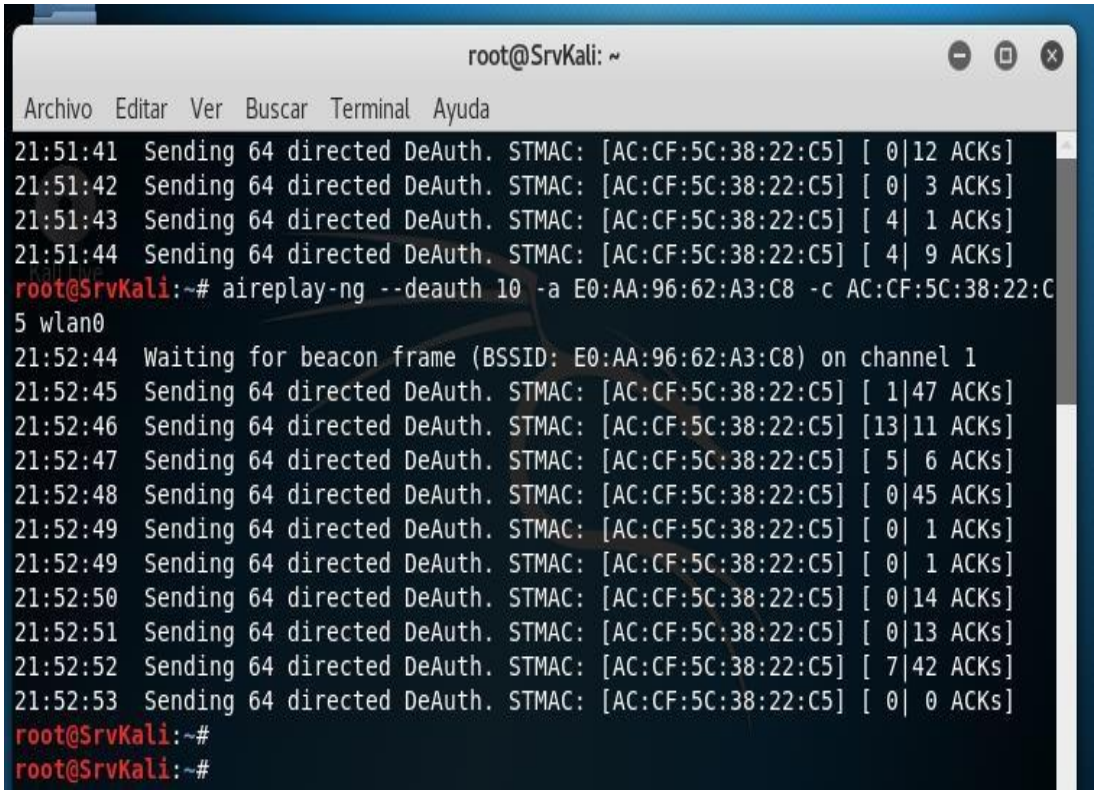
Selección del SSID a vulnerar



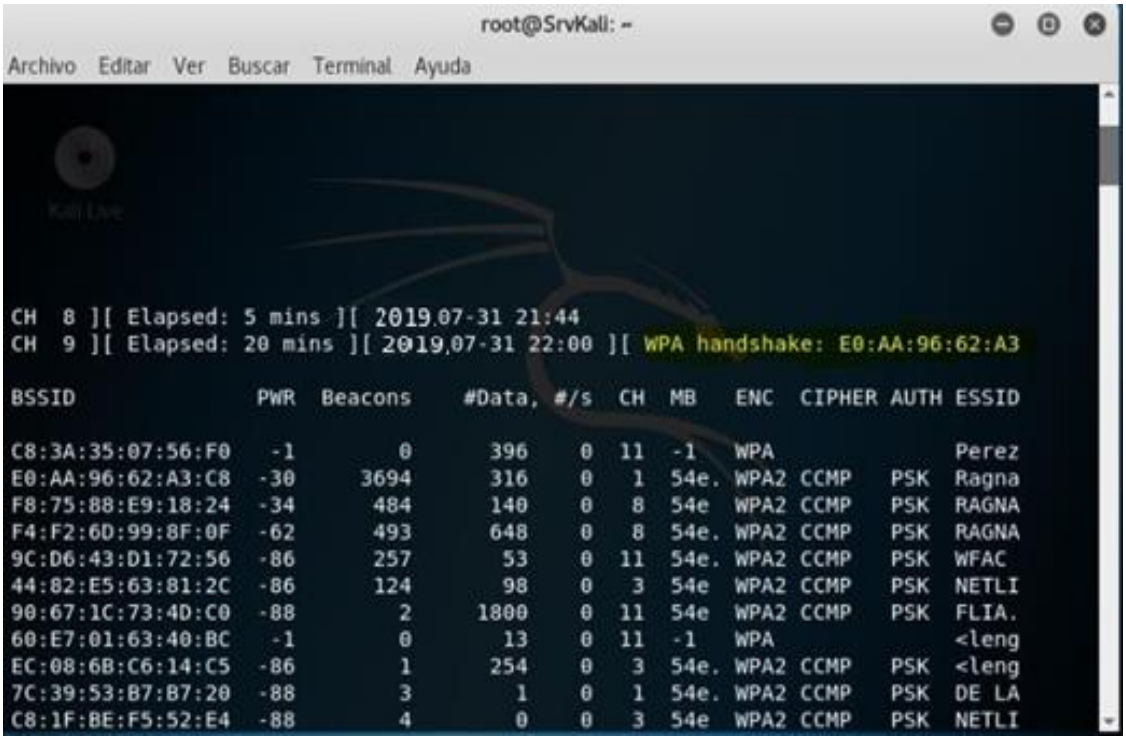
SSID con los hosts conectados a dicho punto de acceso



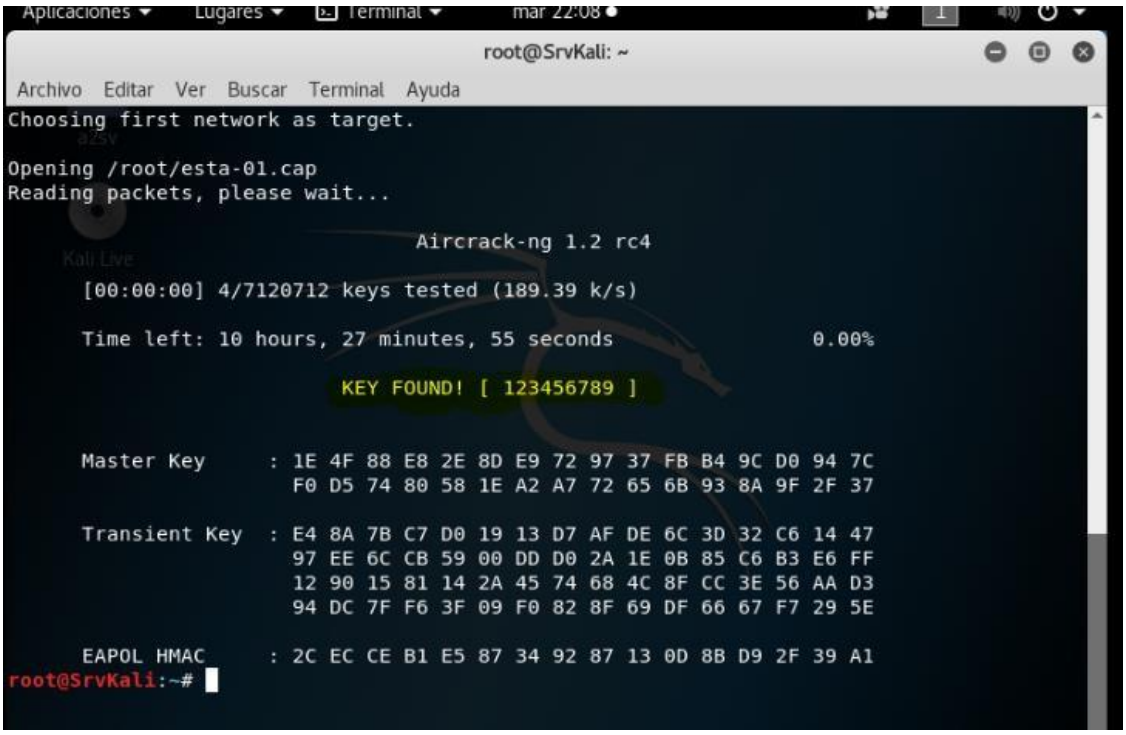
Enviar peticiones de des autenticación al host seleccionado



Captura de la clave, una vez desconectado el dispositivo se vuelve a autenticar a la red y se crea el handshake



Se ha encontrado la clave con la cual se autentica en el punto de acceso, todo esto mediante el



10. Fuerza Bruta

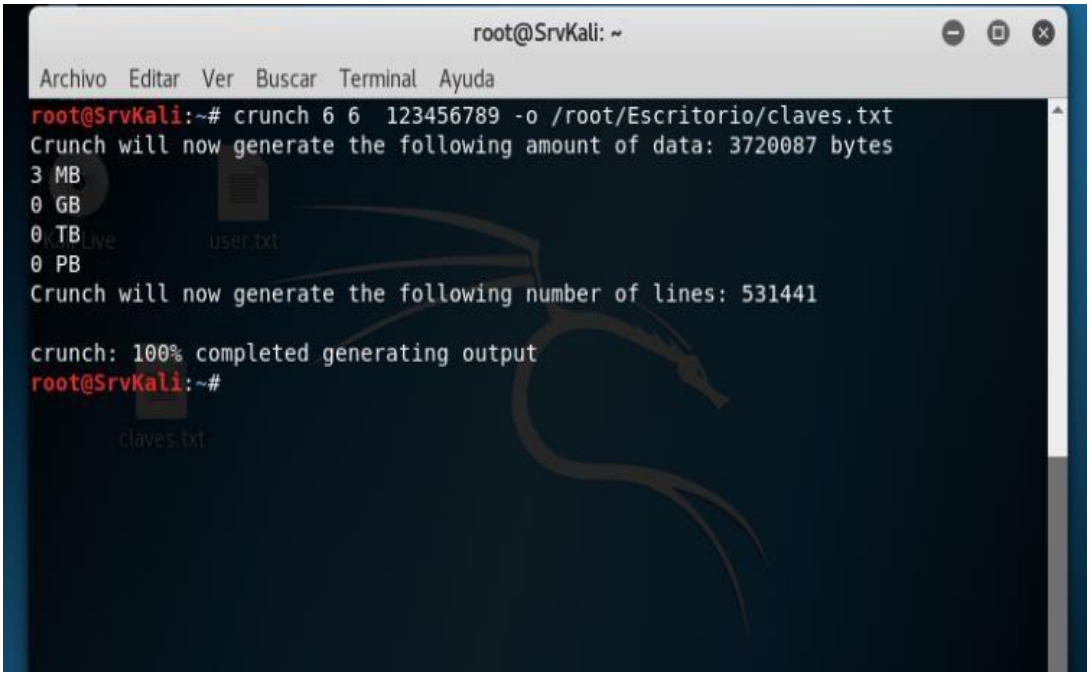
Los ataques de fuerza bruta, no es más que atacar a un servicio por medio de un puerto, lo que permitirá saber la contraseña con la que se autentica dicho administrador del servicio, todo esto realizado mediante los ya conocidos diccionarios de datos, que consisten en probar las combinaciones posibles para poder acceder al control total de un servicio de red.

En esta prueba se ha realizado ataques de fuerza bruta a un servicio ftp, el cual mediante la creación de un diccionario de datos se trata de descifrar la clave con la que se autentica al servidor.

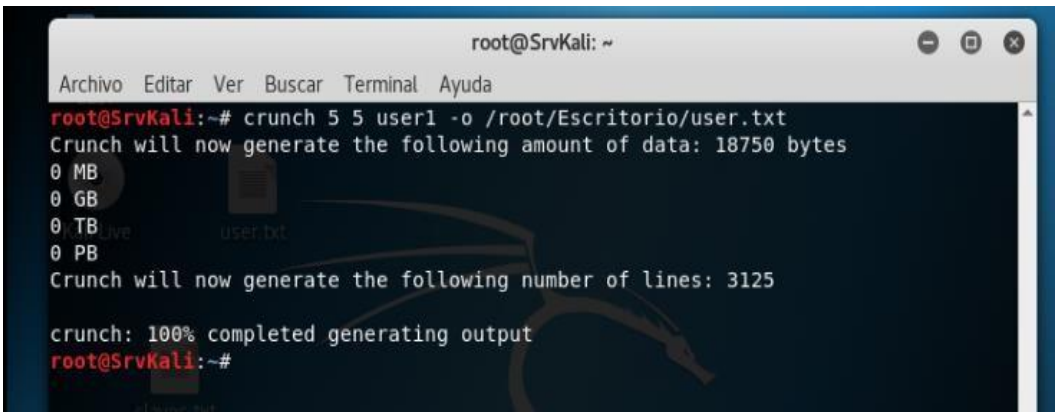
10.1. Comandos utilizados Creación de diccionarios

crunch 5 5 user1 –o /root/Escritorio/diccionaro1.txt
crunch 6 6 123456789 –o /root/Escritorio/diccionario2.txt
Descifrando contraseña del servicio FTP
hydra–L/root/Escritorio/diccionario1.txt –P
/root/Escritorio/diccionario2.txt 192.168.100.86 ftp
Los diccionarios de datos se pueden crear a nuestra conveniencia o usar los que vienen dentro de Kali.

Creación de un diccionario exclusivo para los usuarios.



Creación de un diccionario de claves



11. VULNERABILIDADES WEB

Para el escáner de vulnerabilidades web, se ha hecho uso de 3 aplicativos los cuales, son de ayuda para mostrar desde direcciones ip o puertos disponibles, hasta vulnerabilidades que se presentan por protocolos de navegación, exploradores e incluso técnicas de desarrollo.

11.1. Comandos utilizados

NMAP: http://www.utc.edu.ec

nmap –sV 181.112.224.98

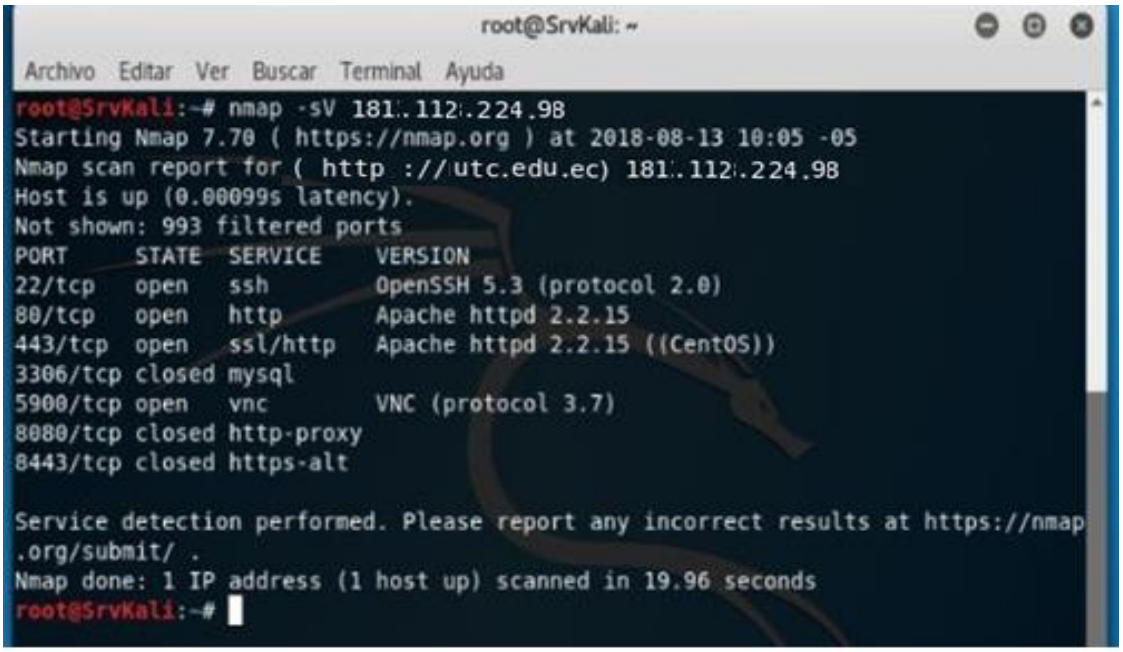
A2SV

Instalar A2SV

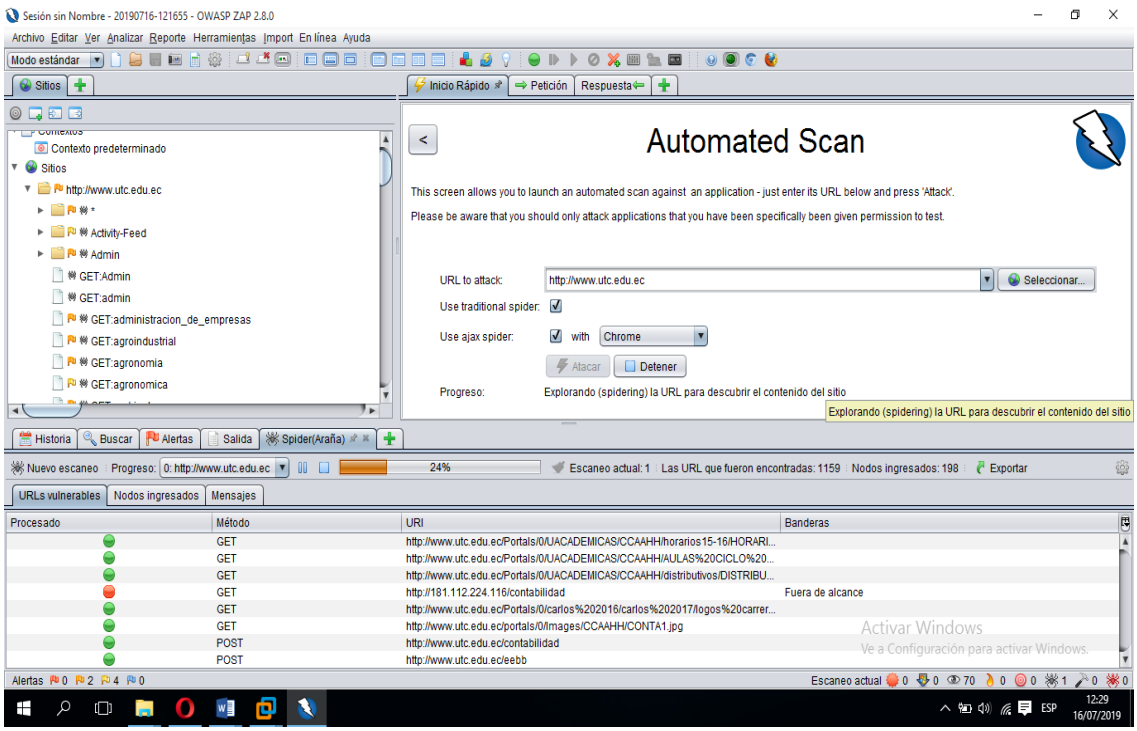
cd Documemtos/

Documentos# git clone https://github.com/hahwul/a2sv.git Documentos# cd a2sv/ Documentos/a2sv# chmod +x install.sh Documentos/a2sv# ./install.sh Documentos/a2sv# python a2sv.py Escanear con A2SVDocumentos/a2sv# python a2sv.py –t www.utc.edu.ec

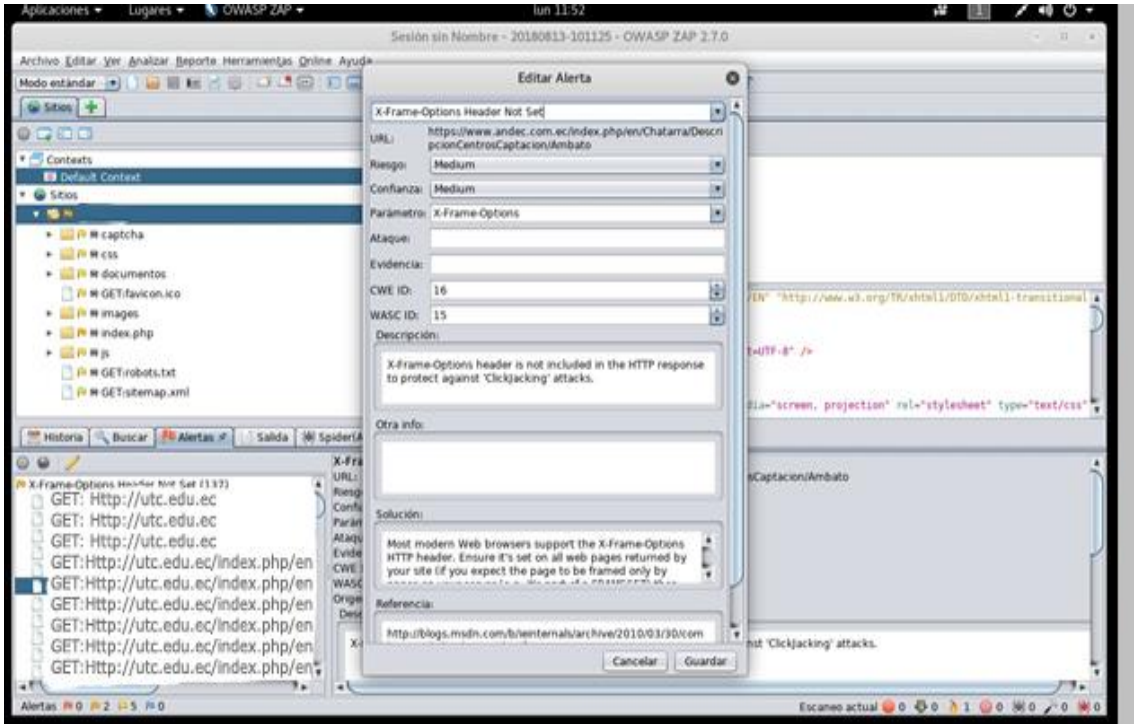
Información valiosa acerca del objetivo con NMAP



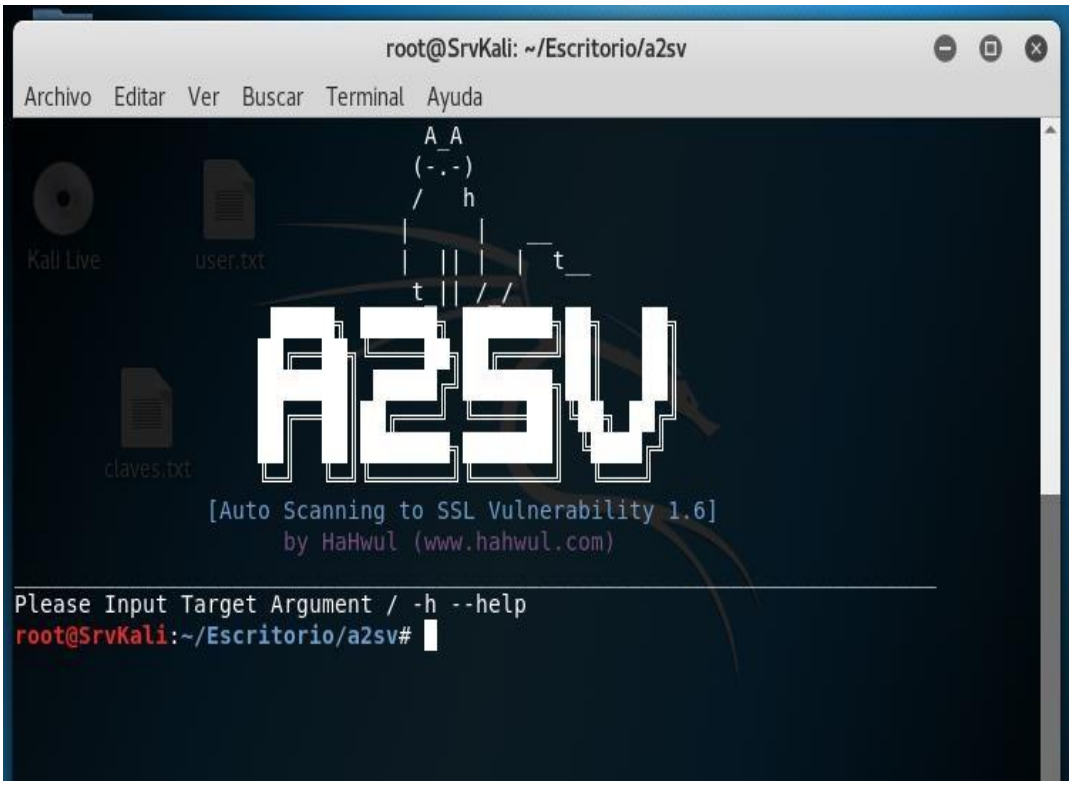
OWAspzap escáner web clase por clase a nivel de desarrollo

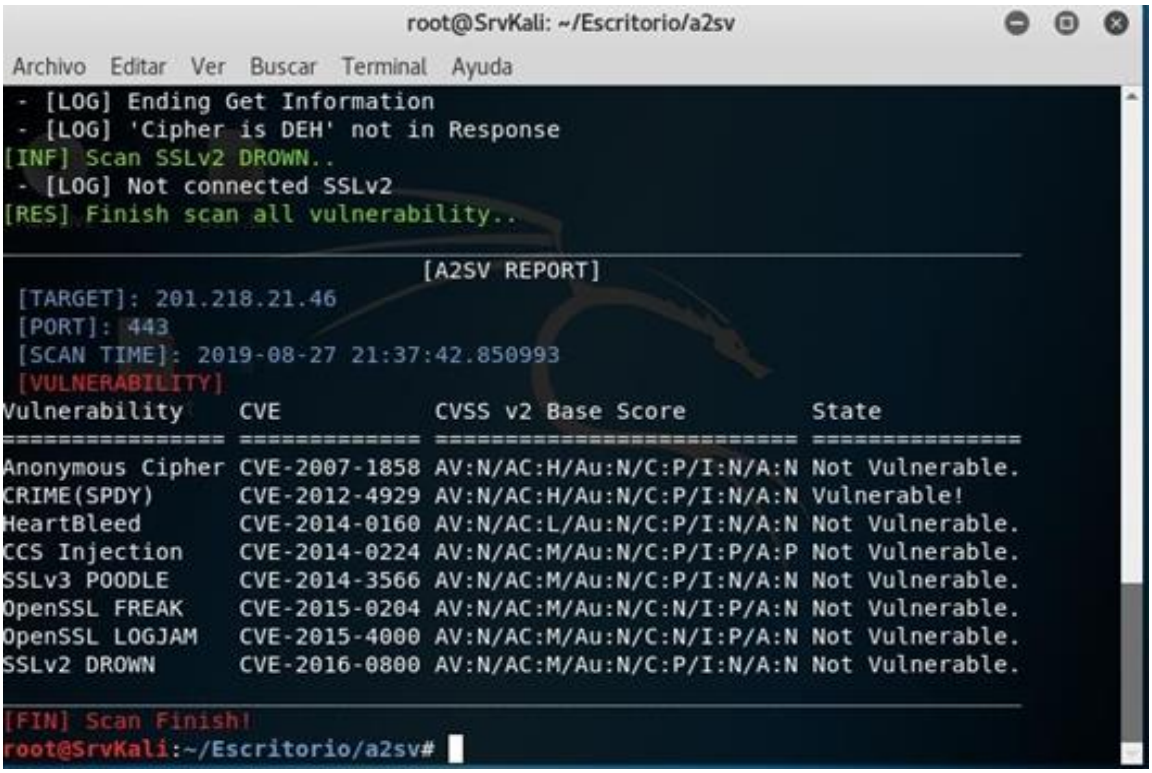


Información sobre aleras encontradas



Escáner SSL con A2SV





Resultado del escáner con A2SV

Dentro de los resultados encontrados con las herramientas utilizadas para estas pruebas es importante destacar que con NMAP hemos podido observar los puertos abiertos con los que cuenta el servidor dónde está alojado dicho aplicativo web, en temas de OWASP nos permite ver las clase del desarrollo de la página web, por lo tanto hemos observado algunas alertas de tipo medianas en cuanto al desarrollo y la generación de cookies que en algún momento podrían representar algún tipo de riegos, por otra parte el aplicativo A2SV nos muestra vulnerabilidades de tipo de protocolos de comunicación, en la que nos indica que la web de la UTC es vulnerable al protocolo CRIME (SPDY) en las que representa un riesgo al momento de que los cookies recuperan contenidos sobre la información mostrada, por lo tanto en algún momento puede guardar sesiones que pueden ser punto vital para desencadenar otro tipo de ataques.

12. RECOMENDACIONES

- Tomar en consideración los puertos abiertos o que escuchan algún tipo de servicio, es

importante habilitar solo los puertos necesarios, tales como los puertos 80 que se utiliza para permitir la navegación por internet mediante el protocolo HTTP y el puerto 25 que queden ser asignado al protocolo de correo SMTP, puerto 21 que se lo utiliza para las conexiones FTP, estos puestos pueden ser filtrarlos con algún tipo de herramienta, como un firewall.

- Es importante que la consola de administración de antivirus mantenga la firma de base de datos actualizada con un BitDefender que permita bloquear los keylogging y otros malware.

- En cuanto a las redes Wireless, su autenticación y tráfico generado, se recomienda que al menos al SSID exclusivo del departamento de T.I. sea blindado con algún otro tipo de seguridad como puede ser un filtrado mac.

- Para el caso de las vulnerabilidades web, es importante hacer un recorrido más extenso sobre las alarmas encontradas, si bien es cierto no son críticas, pero es importante tomar en cuenta las recomendaciones dadas por las herramientas utilizadas.

12. IMPACTOS

12.1. IMPACTO TÉCNICO

Durante el análisis a la infraestructura Tecnológica de la Universidad Técnica de Cotopaxi se puedo visualizar su nivel de vulnerabilidad que posee su sistema informático, de modo que en los tiempos actuales las nuevas herramientas tecnologías permiten realizar un análisis más detallado permitiéndonos verificar sus posibles brechas de seguridad y de esa manera dar futuras recomendaciones para evitar ser atacados por los hackers.

12.2. IMPACTO SOCIAL

La tecnología no es un término nuevo, sin embargo, gracias a los nuevos procesos tecnológicos que se vienen evolucionando se ha potenciado, en que muchas empresas desearían obtener una herramienta que valore el nivel de vulnerabilidad y la seguridad de sus sistemas informáticos, permitiéndoles obtener un informe más detallado sobre el nivel de

riesgos que posee sus sistemas de información de las entidades laborales, se acogen a herramientas que facilitan y aseguran los procesos que realizan en sus respectivos entornos de trabajo.

12.3. IMPACTO ECONÓMICOS

Si bien es cierto en esta oportunidad el proyecto de investigación no genera ningún costo de implementación para la institución, puesto que se lo realiza con herramientas de software libre el cual están a disposición en el internet. Esta herramienta de software libre nos da oportunidad de realizar nuestros propios análisis de vulnerabilidades para evaluar los estándares de seguridad de los sistemas informáticos.

13. PRESUPUESTOS PARA LA ELABORACIÓN DEL PROYECTO

13.1. Gastos directos

Tabla 26: Gastos Directos

Descripción	Cantidad:	Valor Unitario ($):	Valor Total ($):
Hojas de papel Bond	1 Resmas	4	4,00
Impresiones a blanco y negro	70	0,05	3,50
Impresiones a color	30	0,25	7,50
Copias	80	0,05	4,00
Esferos	1	0,50	0,50
Anillados	3	5,00	15,00
Conexión Internet	4 Meses	20,00	80,00
USB/Flash	1	8,00	8,00
Computador	1	Uso diario	50,00
Total Gastos Directos:		$ 28,85	**$ 172,50**

Fuente: Los autores

13.2. Gatos indirectos

Tabla 27: Gastos Indirectos

Descripción:	**Valor:**
Movilidad	$ 50,00
Total:	**$ 50,00**

Fuente: Los autores

13.3. Gastos totales del proyecto

Tabla 28: Presupuesto Total del Proyecto

Gastos:	**Total:**
Gastos Directos	$ 172,50
Gastos Indirectos	$ 50,00
10% de Imprevistos	$ 20,00
Total Presupuesto:	**$ 242,50**

Fuente: Los autores

14. CONCLUSIONES Y RECOMENDACIONES

14.1. CONCLUSIONES

- De manera general, el análisis a la infraestructura tecnológica de la universidad Técnica de Cotopaxi se lo realizo en base a una virtualización del sistema operativo Kali Linux instalado en una maquina física. Esto permitiéndonos visualizar sus brechas de seguridad y dándonos el acceso a gran parte de la infraestructura para poder realizar las pruebas necesarias.

- Los resultados de las pruebas de seguridad informática que se hizo al personal de sistemas informáticos. nos permitió conocer la falta de conocimiento que tiene en cuanto a la ciberseguridad. Dejando así a la institución vulnerable a todos los riesgos cibernéticos de información vital y privada de la misma.

- Con la finalización de nuestro trabajo de investigación se desea promover y motivar a la institución en temas de la seguridad informática y a la vez al departamento de sistemas tome conciencia sobre posibles riegos que puede sufrir la infraestructura tecnológica de la institución.

14.2. RECOMENDACIONES

- Tomar en consideración los puertos abiertos o que escuchan algún tipo de servicio, es importante habilitar solo los puertos necesarios, tales como los puertos 80 que se utiliza para permitir la navegación por internet mediante el protocolo HTTP y el puerto 25 que queden ser asignado al protocolo de correo SMTP, puerto 21 que se lo utiliza para las conexiones FTP, estos puestos pueden ser filtrarlos con algún tipo de herramienta, como un firewall.

- Es importante que la consola de administración de antivirus mantenga la firma de base de datos actualizada con un BitDefender que permita bloquear los keylogging y otros malware.

- En cuanto a las redes Wireless, su autenticación y tráfico generado, se recomienda que al menos al SSID exclusivo del departamento de T.I. sea blindado con algún otro tipo de seguridad como puede ser un filtrado mac.

- Para el caso de las vulnerabilidades web, es importante hacer un recorrido más extenso sobre las alarmas encontradas, si bien es cierto no son críticas, pero es importante tomar en cuenta las recomendaciones dadas por las herramientas utilizadas.

15. BIBLIOGRAFÍA

Caballero, E. (2018). *kali linux gias practicas.* Lima-peru.

Cebrian, m. (2014). *Ataques de base de datos injection.* Mexico: PID00191663.

Cert, L. (2019). *Defenza frente a las ciberamenazas*. Obtenido de https://www.ccn-cert.cni.es/gestion-de-incidentes/lucia.html: https://www.ccn-cert.cni.es/gl/gestion-de-incidentes/lucia/23-noticias/297-publicada-isoiec-27013.html

CERT-MU. (2010). *The wannacry ramsonware. República de Mauricio: CERT-MU.* Obtenido de The wannacry ramsonware. República de Mauricio: CERT-MU.: http://cert-mu.govmu.org/English/Documents/White%20Papers/White%20Paper%20-%20The%20WannaCry%20Ransomware%20Attack.pdf

Check, P. (2018). *Cyber Attack.* Israel: Software Technologies LTD.

Consultores, G. A. (2019). *NORMA ISO 27032 "GESTIÓN DE LA CIBERSEGURIDAD.* Obtenido de https://www.grupoacms.com/norma-iso-27032: https://www.grupoacms.com/norma-iso-27032

Doctor, T. (2012). *Ecuador, el cuarto pais de la region que resive mas ataques ciberneticos*. Obtenido de Ecuador, el cuarto pais de la region que resive mas ataques ciberneticos: http://www.doctortecno.com/noticia/ecuador-cuarto-pais-region-que-recibe-mas-ataques-ciberneticos

Expreso. (20 de 08 de 2011). Delitos Informaticos. *Deletitos Informaticos Ecuador*, pág. 15.

Expreso. (17 de 05 de 2017). Ataques en el Ecuador. *Ecuador sufre ciber ataques extorsivos*, pág. 20.

Expreso. (20 de 05 de 2017). *Ecuador Inmediato.* Obtenido de Ecuador Inmediato: http://www.ecuadorinmediato.com/index.php?module=Noticias&func=news_user_view&id=156133

Gomez. (17 de 11 de 2009). *Dviops.net*. Obtenido de Dviops.net: https://www.duiops.net/manuales/vmware/vmwarebasico.htm

Gonzáles, P. (2014). *Pentesting con Kali.* Mexico: word.

Gordillo, D. (5 de 12 de 2012). *Los destructives.* Obtenido de Los dectructives: https://losindestructibles.wordpress.com/2012/09/24/robo-de-sesiones-por-medio-de-cookies/

iHackLabs. (21 de 8 de 2018). *iHackLabs*. Obtenido de Concienciat.gva.es/wp-content/uploads/2018/03/infor_nmap6_listado_de_comandos.pdf

ISO, 2. (15 de 07 de 2019). *DEFENSA FRONTE ÁS CIBERAMEAZAS.* Obtenido de https://www.ccn-cert.cni.es/

Lyor, g. (2009). *NMAP Network Scanning.* Mexico.

Martinez, D. (2018). *Ataques a redes wireless.* Catalunya.

Oppleman, V. (2006). *Extreme Exploits Hackers Y Seguridad.* España: Anaya Multimedia.

Robles, m. (2016). *Virtualizacion con Vmware.* Vmware.

Semanat, A. (2010). *1Estrategia de seguridad contra ataques internos en redes locales.* Cuba: 1815-5928, 29(3), 26-34.

TechnologiesAcces. (2016). vulnerabilidad Cross Site. *acens*, 1.

Telegrafo. (16 de 08 de 2016). *El telegrafo.* Obtenido de delitos informáticos: https://www.eltelegrafo.com.ec/noticias/judicial/1/en-ecuador-el-85-de-los-delitos-informaticos-ocurre-por-descuido-del-usuario

Valero, D. (10 de 24 de 2014). *Las cookies, el arma de los hackers para suplantar la identidad.* Obtenido de ADSLZONE: https://www.adslzone.net/2014/10/24/consejos-de-seguridad-para-evitar-riesgos-al-activar-las-cookies-de-internet/

Verdejo, G. (2017). *Denegación de servicio: DOS / DDOS.* Mexico.

Vieites, Á. G. (2013). Auditoría de seguridad informática. En Á. G. Vieites, *Auditoría de seguridad informática* (pág. 11). Mexico: RA-MA.

Wilhelm, T. (2010). *Professional Penetration.* San Fransico: Jan Kanclirz Jr.

ANEXOS

ENCUESTAS

Tema de investigación: "Análisis de la Ciberseguridad a la Infraestructura Tecnológica de la Universidad Técnica De Cotopaxi"

Dirigido a:

Profesionales y Pre-Profesionales de la UTC

Cuestionario sobre la Ciberseguridad Tecnológica de la UTC

Objetivo: Recopilar la información mediante el cuestionario a los docentes y alumnos Pre Profesionales para determina la seguridad de la infraestructura tecnológica de la Universidad Técnica de Cotopaxi.

Datos Generales:			
1. Instituciones, categoría, materia, sexo, provincia,			
Institución:	**Sector de ubicación:**	**Categoría:**	**Grado:**
	Urbana ☐	**Fiscal** ☐	
	Rural ☐	**Particular** ☐	
	Sexo:	**Edad:**	**Conocimiento**
UTC	**Masculino** ☐		**sobre**
	Femenino ☐		**Ciberseguridad**
			Si ☐
			No ☐
conocimientos sobre la Ciberseguridad Informática			

Instrucciones: (por favor marque con una X en la(s) que corresponda)

2. ¿Cuál es su nivel educativo?
Título Terminado (Tercer Nivel) ☐ **Posgrado(Maestría)** ☐ **Diplomado** ☐ **Doctorado** ☐
3. ¿Tiene usted conocimiento sobre la Ciberseguridad?
Nada ☐ **Poco** ☐ **Mucho** ☐

4. ¿Sabe usted que es Kali Linux?

Sí ☐ **No** ☐

5. ¿Sabe usted qué tipo de Linux es Kali?

Sí ☐ **No** ☐

6. ¿Sabe usted cual es la función que cumple Metasploit Framework en Kali Linux?

Sí ☐ **No** ☐

7. ¿Cuánto conoce usted sobre ataques phishing?

Nada ☐ **Poco** ☐ **Mucho** ☐

8. ¿Sabe usted cuales son los protocolos de Seguridad Informática?

Sí ☐ **No** ☐

9. ¿Está usted informado acerca de las prevenciones que hay que tener para evitar el acceso de un hacker u otra amenaza a un sistema Informático?

Sí ☐ **No** ☐

10. ¿Cree usted que los sistemas informáticos existentes en la Universidad Técnica de Cotopaxi son seguros?

Sí ☐ **No** ☐

11. ¿Conoce usted que es un Sistema de Prevención (IDS)?

Sí ☐ **No** ☐

12. ¿Conoce usted Cuál es la función de un Firewall

Sí ☐ **No** ☐

13. ¿Tiene usted conocimiento sobre la herramienta SqlMap en Kali Linux?

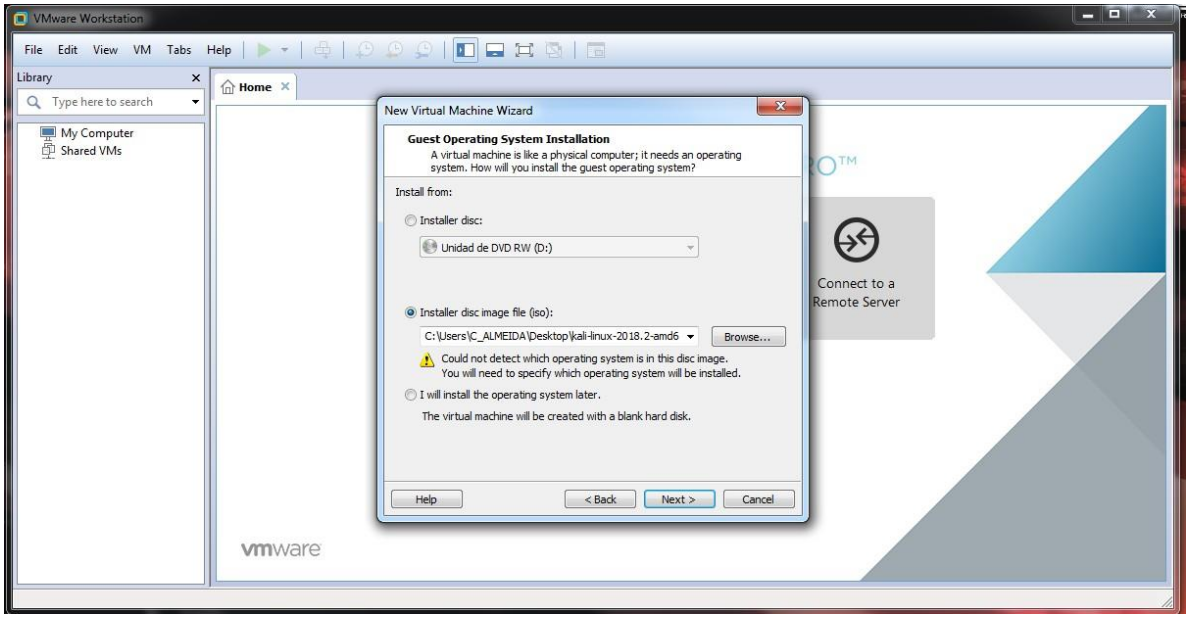
Sí ☐ **No** ☐

Fecha:

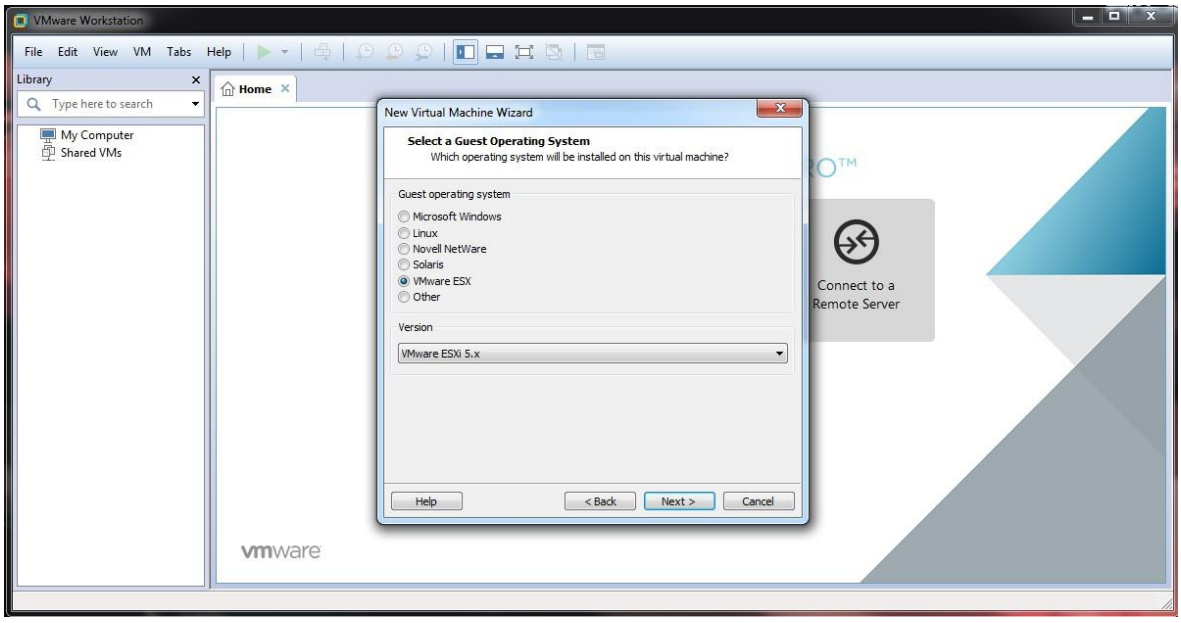
……

MANUAL DE INSTALACIÓN KALI LINUX

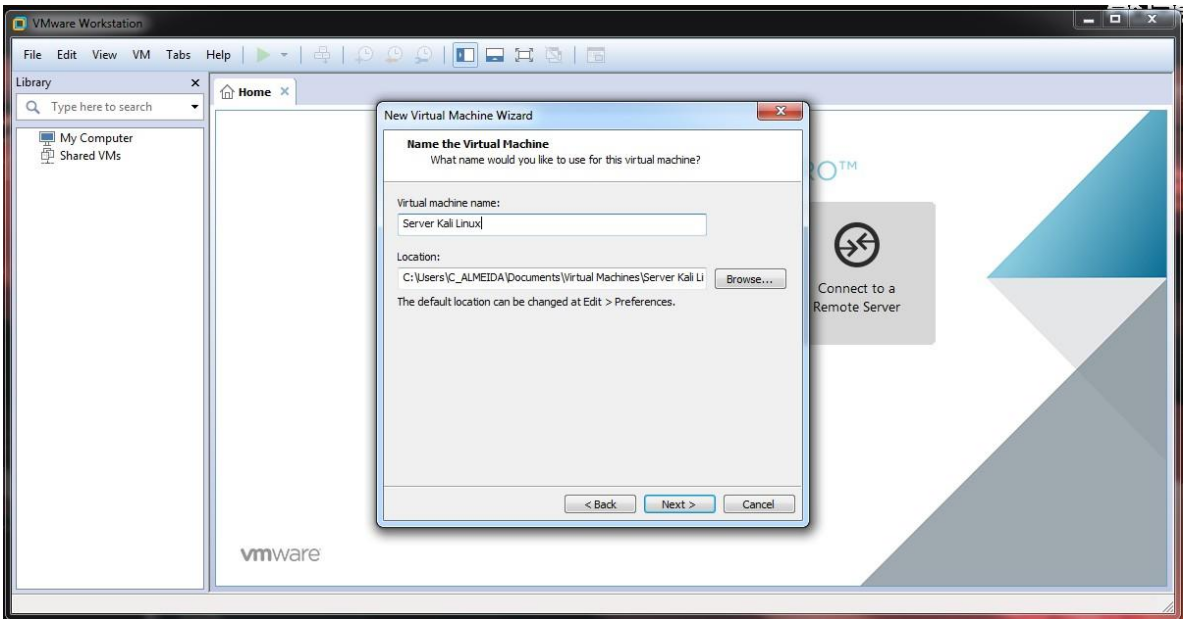
1. Seleccionar la imagen ISO la cual se contiene dentro de la maquina física (PC)



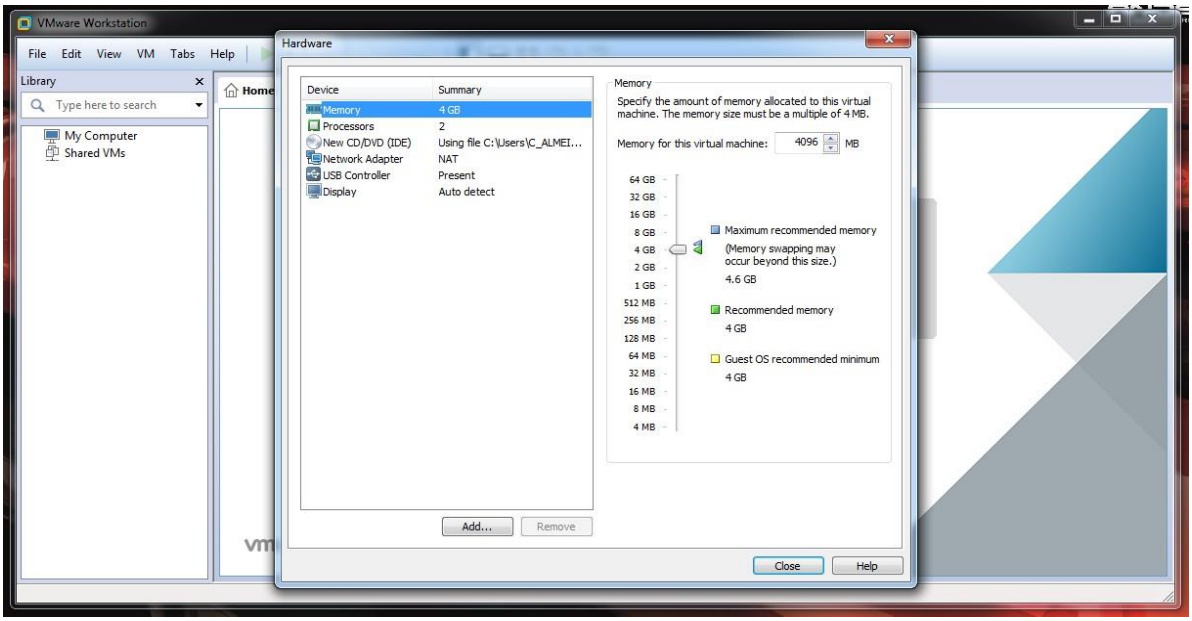
2. Seleccionar compatibilidad con sistemas operativos Linux, esto con la finalidad de que la instalación de la herramienta Kali cuente con una infraestructura compatible.



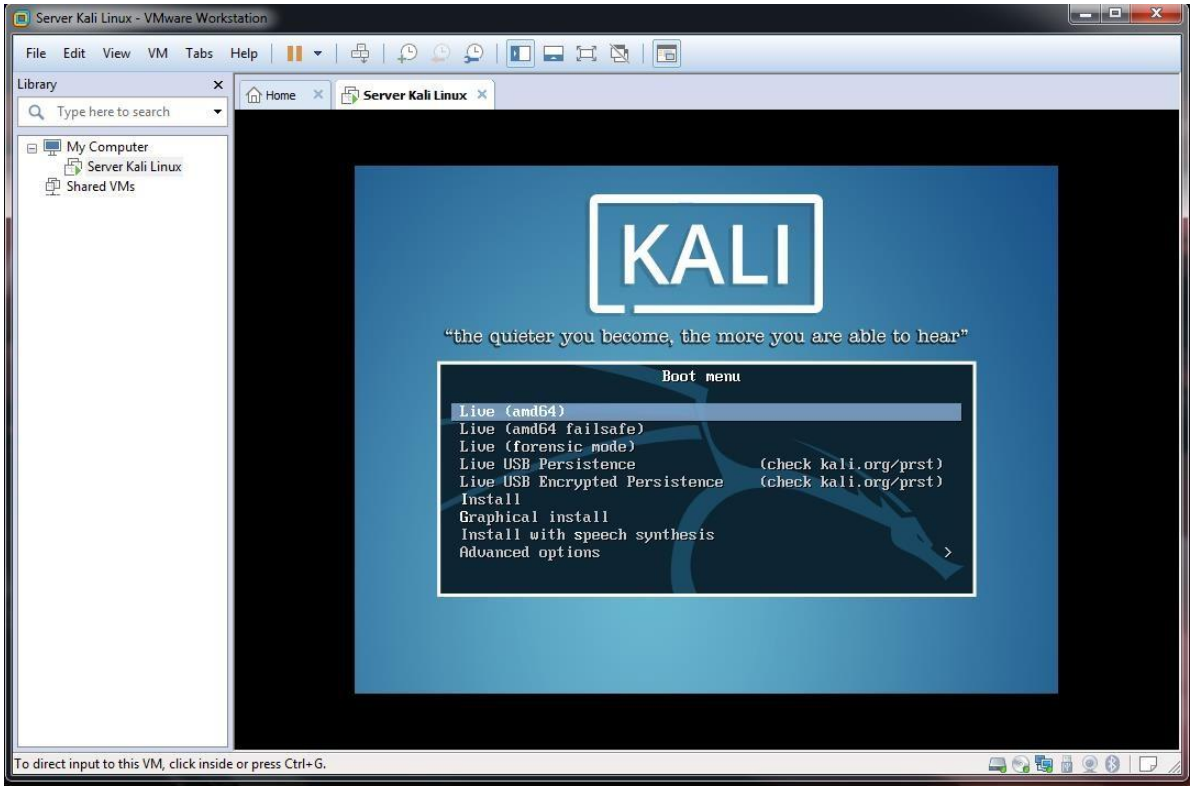
3. Asignar nombre Kali Linux.



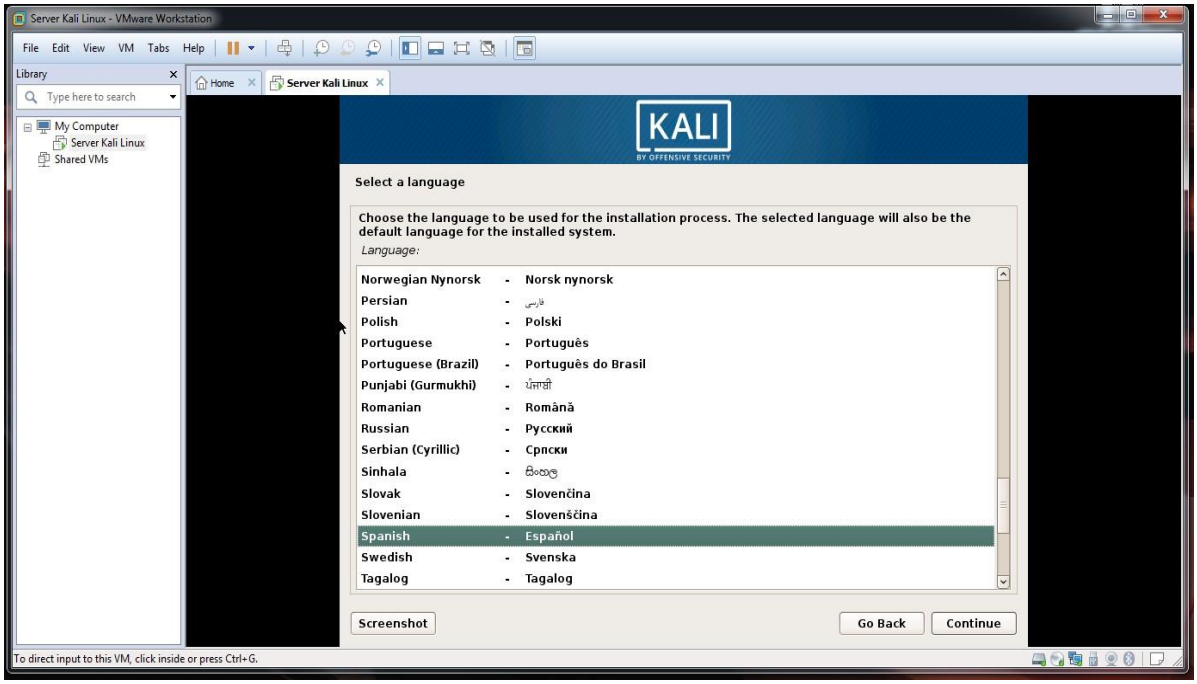
4. Asignación de recursos físicos de la memoria RAM



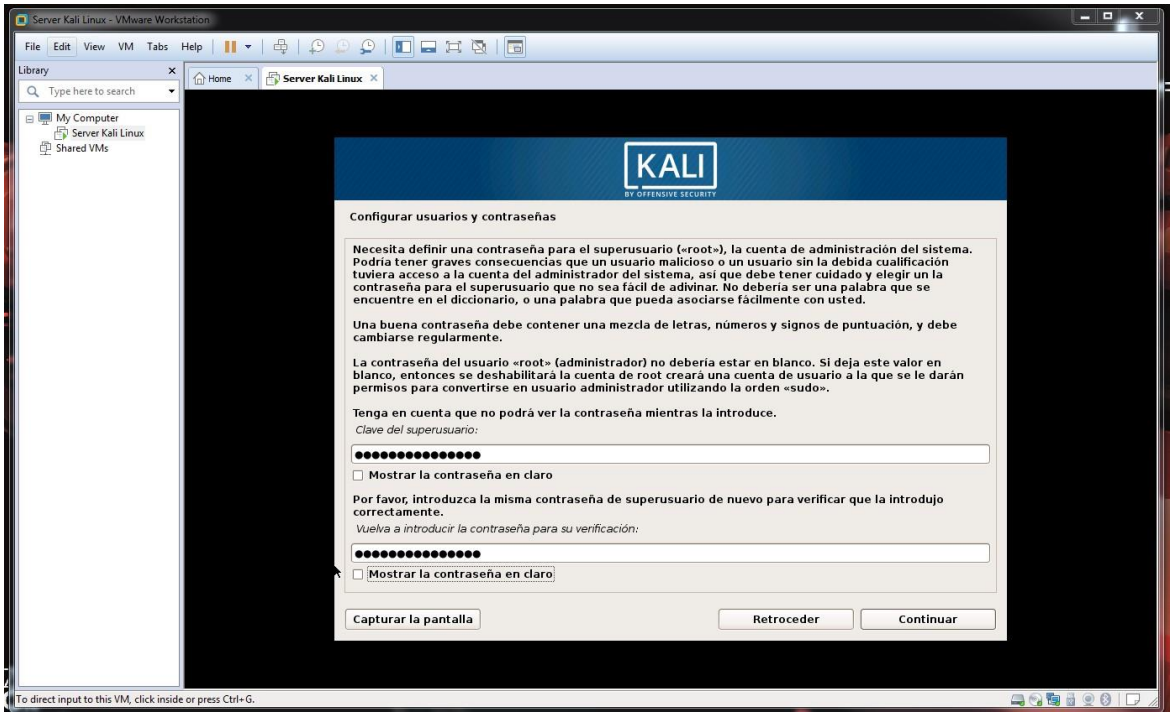
5. Instalación de Kali Linux



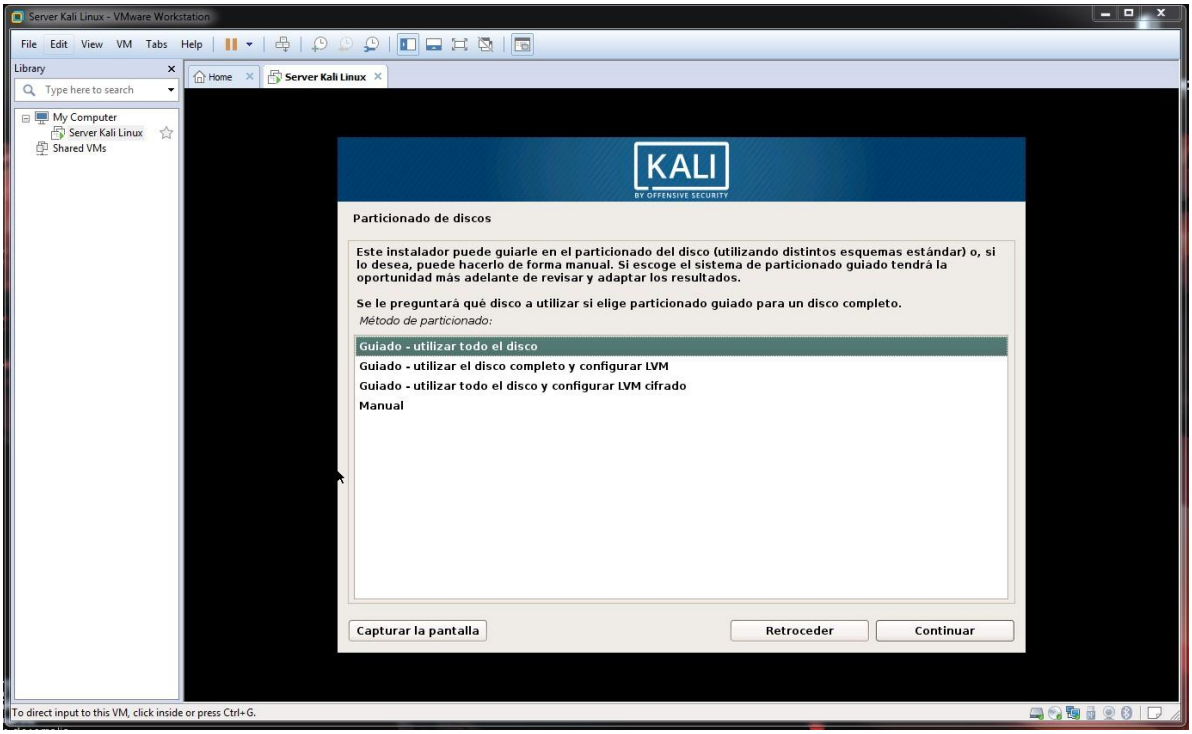
6. Seleccionar el idioma español a instalar



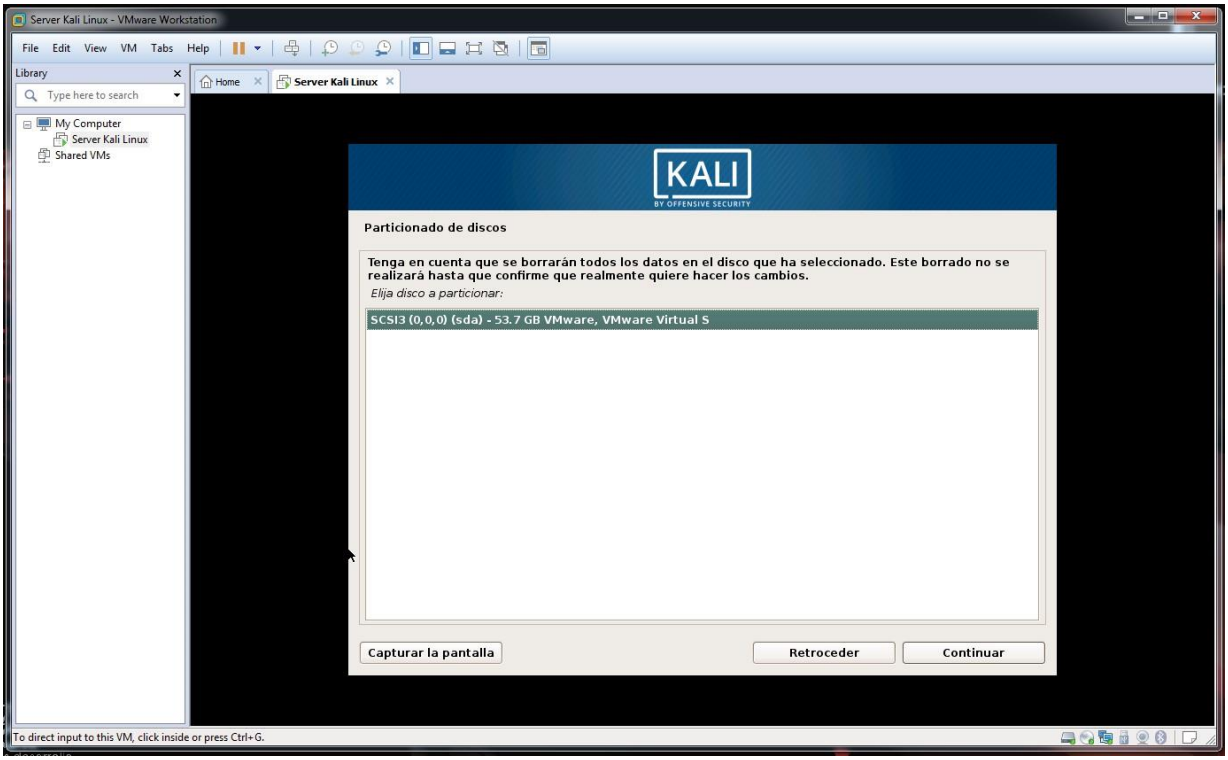
7. Configuración de usuario y password



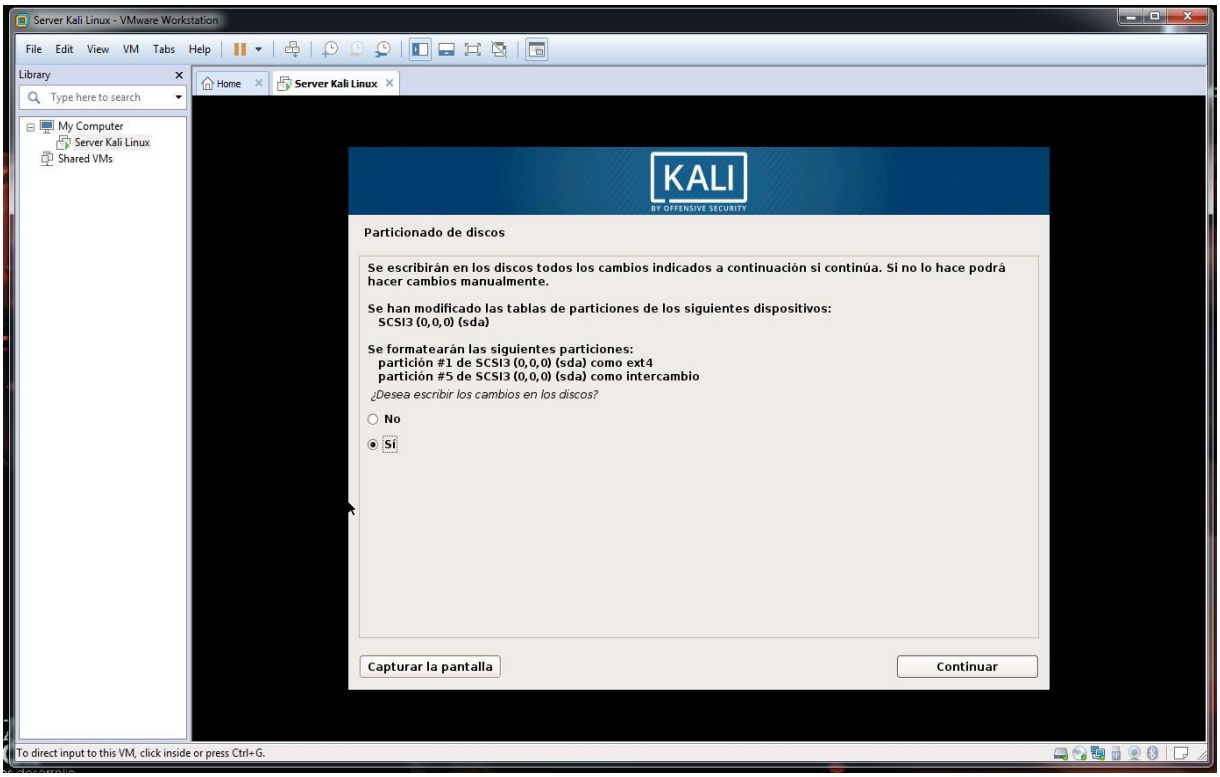
8. Compartir disco virtual dónde se instalará la versión del sistema operativo



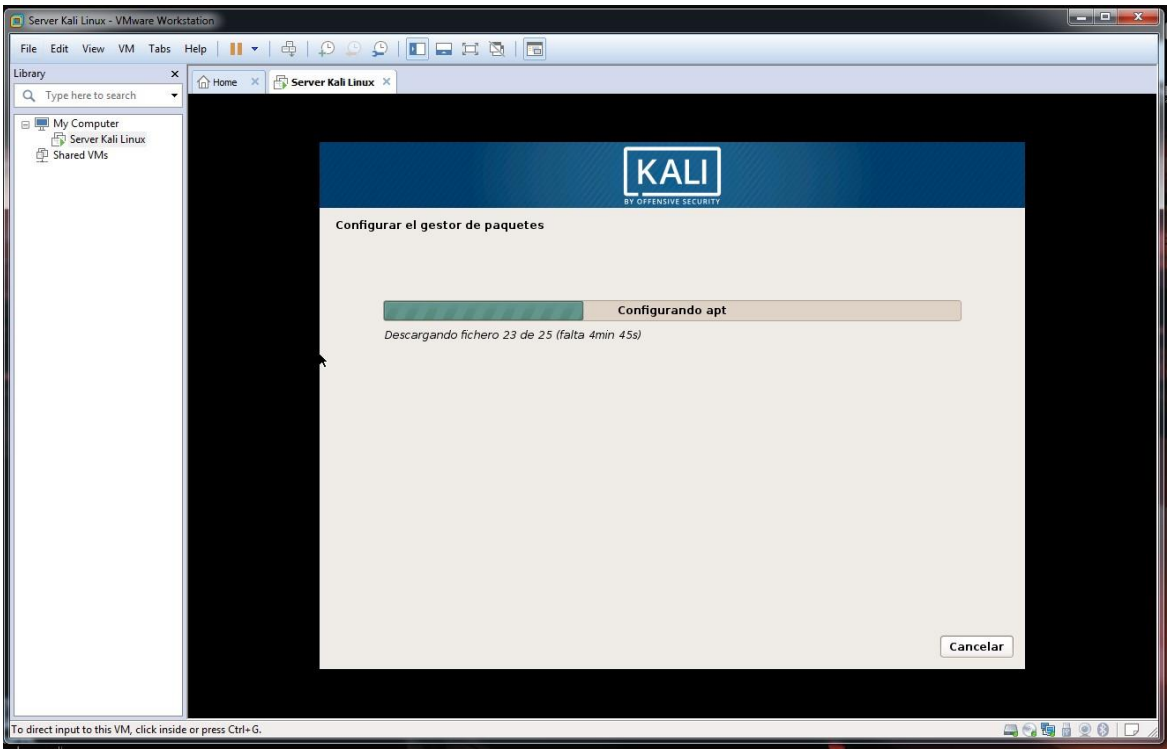
9. Selección del disco virtual



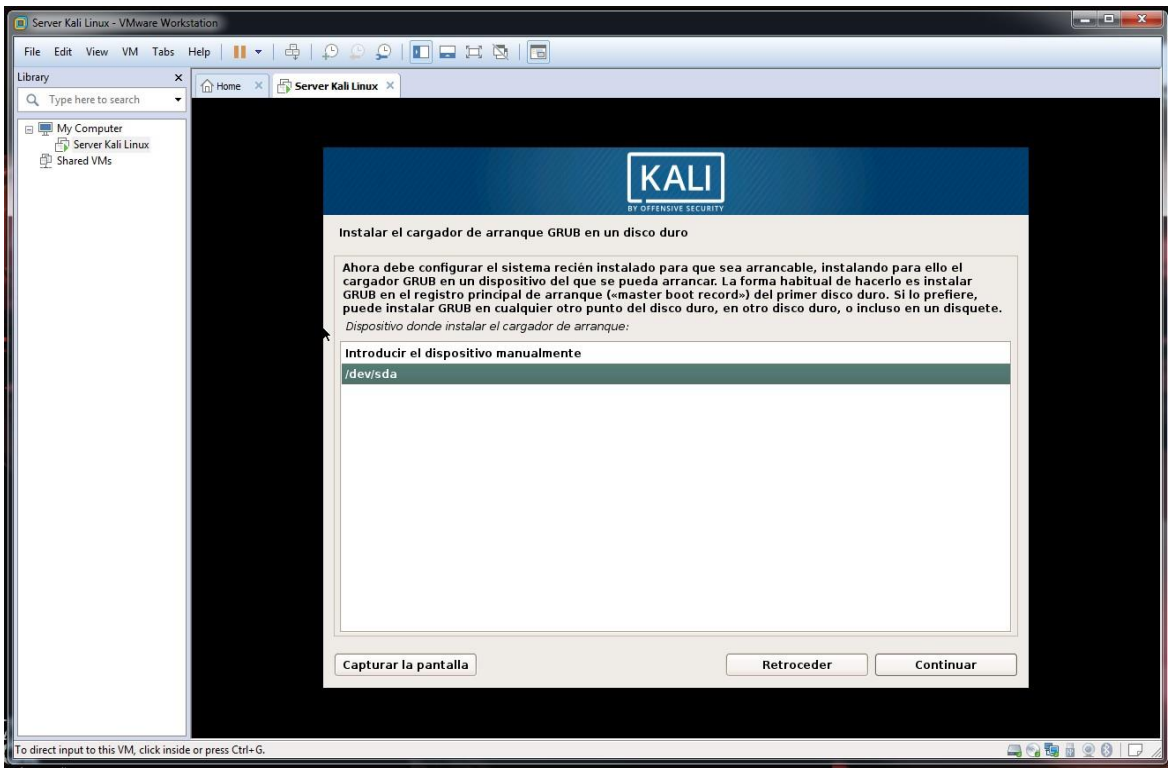
10. Aplicar configuraciones del disco virtual



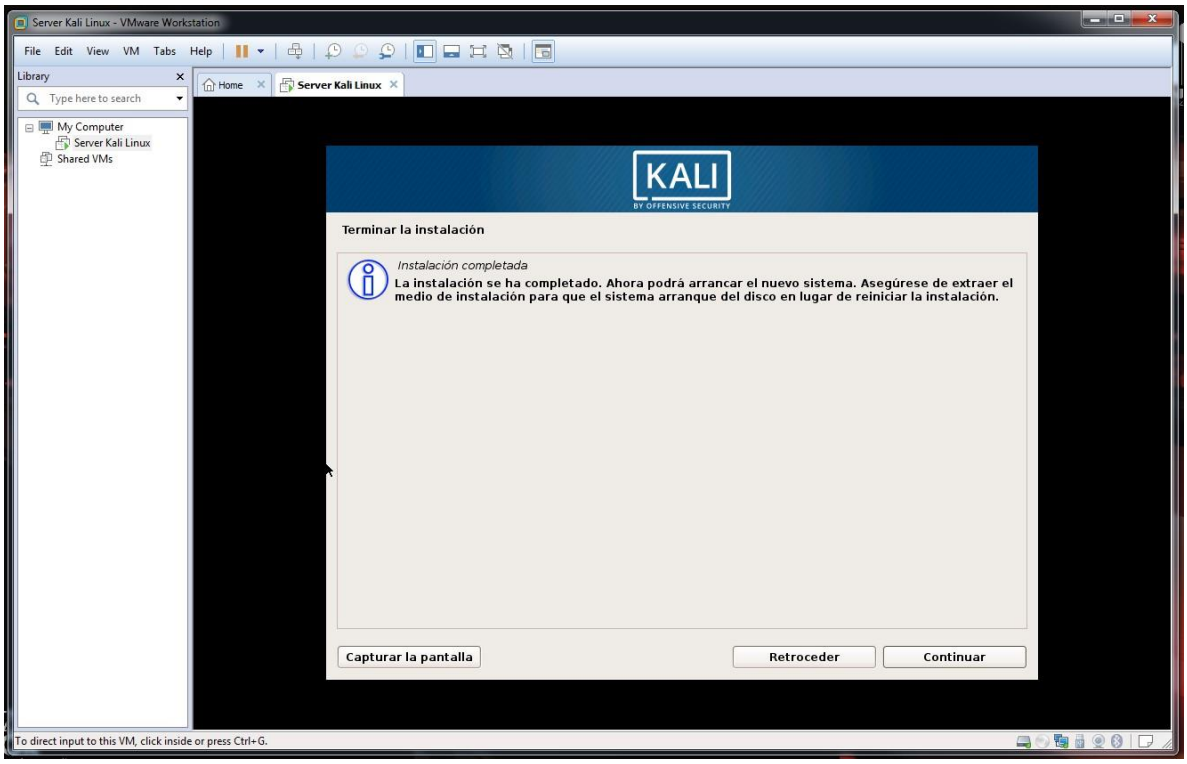
11. Instalación del sistema operativo Kali Linux



12. Seleccionar el cargador de arranque que contendrá los archivos de configuración.



13. Finalización de instalación



14. Inicio del sistema operativo