UNIVERSIDAD CATÓLICA LOS ÁNGELES DE CHIMBOTE

FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

IMPLEMENTACIÓN DE HACKING ÉTICO PARA LA DETECCIÓN Y EVALUACIÓN DE VULNERABILIDADES DE RED EN LA EMPRESA COMPLEX DEL PERÚ S.A.C.-TUMBES; 2017.

TESIS PARA OPTAR EL GRADO ACADÉMICO DE MAESTRO EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIÓN

AUTOR:
BACH. JEAN CARLOS BERMEO OYOLA

ASESOR:
MGTR. EDY JAVIER GARCÍA CORDOVA

TUMBES - PERÚ

2017

JURADO EVALUADOR DE TESIS Y ASESOR

DR. ING. VÍCTOR ÁNGEL ANCAJIMA MIÑÁN
PRESIDENTE

MGTR. ING. MARLENY SERNAQUE BARRANTES
MIEMBRO

MGTR. ING. OSWALDO CORONADO ZULOETA
MIEMBRO

MGTR. ING. EDY JAVIER GARCÍA CORDOVA
ASESOR

DEDICATORIA

A Dios, por darme la vida y la oportunidad de crecer, por darme salud, fortaleza y la sabiduría para poder logra mis objetivos.

A mis padres y familiares, por haberme brindado el apoyo incondicional dándome sus concejos y los buenos deseos de superación e inculcándome valores morales y creando una disciplina para mi desarrollo personal y profesional de manera responsable.

A María Lucila, persona, muy importante en mi vida, gracias a su apoyo incondicional y todos sus deseos, que me da para seguir siempre adelante, la satisfacción y felicidad que me hace sentir su sonrisa angelical siempre que logro un objetivo, a cada uno de mis compañeros de la universidad que compartieron los trabajos grupales, su valioso tiempo y por su amistad durante el desarrollo de formación académica.

A cada uno de los docentes que supieron entender las condiciones personales y me brindaron el apoyo profesional académico con su amistad durante mis años de estudio.

AGRADECIMIENTO

A mis padres y familiares, los cuales me brindaron el apoyo incondicional ciclo tras ciclo académico y la motivación para poder llegar a cumplir cada meta propuesta.

Agradezco a los docentes que tuvieron a cargo el curso taller de tesis por brindar sus conocimientos y sabiduría en la redacción, diseño e implementación para nuestro proyecto final.

A mi asesor, apoyarme al momento de realizar la presente tesis bajo su dirección guiando mis ideas para poder logar un buen resultado.

Al Gerente de la Empresa Complex del Perú, por facilitar y darme la oportunidad de continuar con los estudios y lograr cumplir con mi objetivo de poder terminar mi carrera profesional.

RESUMEN

La inseguridad y perdida de información en organizaciones y empresas en los últimos años, es consecuencia de su falta de preocupación respecto a la seguridad de la información en los servicios que estas ofrecen, lo que da lugar a vulnerabilidades que requieren ser descubiertas por personal y servicios especializados en Hacking Ético. El presente informe de Tesis está desarrollado de acuerdo la línea de investigación en Implementación de las Tecnologías de la Información y Comunicación, de la Escuela profesional de Ingeniería de Sistemas de la Universidad Los Ángeles de Chimbote (ULADECH CATÓLICA). El objetivo principal es realizar la Implementación de Hacking Ético, en la Empresa Complex del Perú S.A.C; para ayudar en la detección y evaluación de vulnerabilidades de Red, de acuerdo a las características, la investigación fue cuantitativa, de diseño no experimental, tipo descriptiva y de corte transversal; la cual tiene una población que está constituida por 24 trabajadores, donde se tomó una muestra similar a la cantidad de la población, es decir 24 trabajadores; convirtiéndose esta en una población muestral. En la investigación se obtuvo que el 96.00% de los trabajadores encuestados están insatisfechos con las circunstancias actuales y por lo tanto el 100% de los encuestados revelaron una necesidad de implementación de hacking ético; para mejorar la seguridad de la información y detectar ataques de red, en beneficio de la Empresa en especial de su información.

Se logró realizar la Implementación de Hacking Ético en la Empresa. Aplicándose el análisis con las herramientas tecnológicas de seguridad, de la actual red de datos en la empresa. Así mismo, se ha formulado una propuesta tecnológica de seguridad, que permita establecer políticas de comunicación oportuna al detectarse posibles vulnerabilidades y/o penetraciones en la red de datos de la empresa Complex del Perú S.A.C – Tumbes

Palabras clave: Hacking ético, Implementación, Seguridad informática, Vulnerabilidad.

ABSTRACT

The insecurity and loss of information in organizations and companies in recent years, is a consequence of their lack of concern about the security of information in the services they offer, which leads to vulnerabilities that need to be discovered by staff and services Specialized in Ethical Hacking. This thesis report is developed according to the line of research in Implementation of Information and Communication Technologies, of the Professional School of Systems Engineering of the Los Angeles University of Chimbote (ULADECH CATÓLICA). The main objective is to carry out the Implementation of Ethical Hacking, in the Complex Company of Peru S.A.C; to assist in the detection and evaluation of network vulnerabilities, according to the characteristics, the research was quantitative, non-experimental design, descriptive and cross-sectional type; which has a population that is constituted by 24 workers, where a sample similar to the amount of the population was taken, that is 24 workers; becoming a sample population. The research found that 96.00% of the surveyed workers are dissatisfied with the current circumstances and therefore 100% of the respondents revealed a need to implement ethical hacking; to improve information security and detect network attacks, for the benefit of the Company especially its information.

The Implementation of Ethical Hacking in the Company was achieved. Applying the analysis with security technology tools, the current data network in the company. Likewise, a security technology proposal has been formulated, which allows to establish timely communication policies when detecting possible vulnerabilities and / or penetrations in the data network of the company Complex del Perú S.A.C – Tumbes

Keywords: Ethical hacking, Implementation, Information security, Vulnerability.

ÍNDICE DE CONTENIDO

JURADO EVALUADOR DE TESIS Y ASESOR ii
DEDICATORIA iii
AGRADECIMIENTO iv
RESUMEN v
ABSTRACT vi
ÍNDICE DE CONTENIDO vii
ÍNDICE DE TABLAS x
ÍNDICE DE GRÁFICOS xi
I. INTRODUCCIÓN 1
II. REVISIÓN DE LA LITERATURA 5
2.1. Antecedentes 5
2.1.1. Antecedentes a nivel internacional 5
2.1.2. Antecedentes a nivel nacional 7
2.1.3. Antecedentes a nivel local 9
2.2. Bases teóricas 10
2.2.1. Empresa Investigada 10
2.2.2. Seguridad de la Información 11
2.2.3. Delito Informático 13
2.2.4. Sistema de Gestión de Seguridad de la Información (SGSI 14
2.2.5. ISO/IEC 27001 16
2.2.6. ISO/IEC 27002 17
2.2.6.1. Objetivo 1 18
2.2.6.2. Objetivo 2 20
2.2.6.3. Objetivo 3 22
2.2.6.4. Objetivo 4 24
2.2.7. Hacking Ético 27
2.2.8. Fases del Hacking Ético 27
2.2.8.1. Reconocimiento 27
2.2.8.2. Escaneo 28
2.2.8.3. Explotación 29

2.2.8.4. Mantener el Acceso 29
2.2.8.5. Borrado de Huellas 30
2.2.8.6. Caso Cracka 31
2.3. HIPÓTESIS 34
III. METODOLOGÍA 35
3.1. Diseño de la investigación 35
3.2. Población y Muestra 36
3.3. Técnicas e instrumentos 37
3.3.1. Técnica 37
3.3.2. Instrumentos 37
3.4. Definición operacional de las variables en estudio 38
3.5. Procedimiento de recolección de datos 39
3.6. Plan de análisis 39
3.7. Matriz de Consistencia 40
3.8. Principios Éticos 41
IV. RESULTADOS 42
4.1. Resultados 42
4.1.1. Dimensión 01: Nivel de satisfacción de las circunstancias Actuales ... 42
4.1.2. Dimensión 02: Necesidad de Implementación de hacking ético 54
4.2. Análisis de Resultados 66
4.3. Propuesta de mejora 68
4.3.1. Antecedentes 68
4.3.2. Procedimiento 69
4.3.3. Documentos del SGSI 70
V. CONCLUSIONES 93
REFERENCIAS BIBLIOGRÁFICAS 95
ANEXO Nº 1: CRONOGRAMA DE ACTIVIDADES 97
ANEXO Nº 2: PRESUPUESTO 98
ANEXO Nº 3: CUESTIONARIO 99
ANEXO Nº4: VALIDACIÓN DEL INSTRUMENTO 101

ÍNDICE DE TABLAS

Tabla Nro. 1: Matriz de Operacionalización de Variables 38
Tabla Nro. 2: Matriz de consistencia 40
Tabla Nro. 3: Conocimiento hacking ético 42
Tabla Nro. 4: Personal Capacitado 43
Tabla Nro. 5: Conocimiento hacking ético 44
Tabla Nro. 6: Información Jaqueada 45
Tabla Nro. 7: Beneficios de hacking ético 46
Tabla Nro. 8: Vulnerabilidad de Red 47
Tabla Nro. 9: Capacitación de trabajadores 48
Tabla Nro. 10: Seguridad de Información 49
Tabla Nro. 11: Inseguridad de Información 50
Tabla Nro. 12: Instalación de hacking ético 51
Tabla Nro. 13: Nivel de Satisfacción de las circunstancias actuales 52
Tabla Nro. 14: Solución a la vulnerabilidad de red 54
Tabla Nro. 15: Empresas con hacking ético 55
Tabla Nro. 16: Ahorrar tiempo y dinero 56
Tabla Nro. 17: Implementación de hacking ético 57
Tabla Nro. 18: Manejo del hacking ético 58
Tabla Nro. 19: Clientes beneficiados 59
Tabla Nro. 20: Presentación de hacking ético 60
Tabla Nro. 21: Alternativa correcta 61
Tabla Nro. 22: Hacking ético para la seguridad 62
Tabla Nro. 23: Beneficios a la empresa 63
Tabla Nro. 24: Necesidad de la Implementación hacking ético 64
Tabla Nro. 25: Resumen General por Dimensiones 65
Tabla Nro. 26: Resultados de vulnerabilidad 91
Tabla Nro. 27: Escaneos de Vulnerabilidad 92

ÍNDICE DE GRÁFICOS

Gráfico Nro. 1: Seguridad de la Información 12
Gráfico Nro. 2: Políticas de Seguridad 15
Gráfico Nro. 3: Protección a la Información 16
Gráfico Nro. 4: Nivel Satisfacción de las circunstancias actuales..... 53
Gráfico Nro. 5: Resumen general de dimensiones 66
Gráfico Nro. 6: Evaluación de la empresa Complex del Perú S.A.C 70
Gráfico Nro. 7: Reporte de dominio por netcraft - parte 1 71
Gráfico Nro. 8: Reporte de dominio por netcraft - parte 2 72
Gráfico Nro. 9: Reporte de dominio por Whois - parte 1 72
Gráfico Nro. 10: Reporte de dominio por Whois - parte 2 73
Gráfico Nro. 11: Búsqueda en Google, Bing y recopilar información 73
Gráfico Nro. 12: consulta whois al dominio www.complex.com.pe..... 74
Gráfico Nro. 13: Dig: Para extraer información de los servidores DNS 75
Gráfico Nro. 14: DNSENUM 76
Gráfico Nro. 15: Metagoofil 77
Gráfico Nro. 16: DMITRY 78
Gráfico Nro. 17: WhatWeb..... 79
Gráfico Nro. 18: Ping Barridos de red..... 79
Gráfico Nro. 19: Consulta ping al servidor de BD 80
Gráfico Nro. 20: Fping.....81
Gráfico Nro. 21: NSLOOKUP.....82
Gráfico Nro. 22: Nmap 83
Gráfico Nro. 23: Consulta de NMAP a un rango de direcciones IP 84
Gráfico Nro. 24: Escaneo de Puertos Abiertos..... 70
Gráfico Nro. 25: Escaneo de a una dirección IP 86
Gráfico Nro. 26: Escaneo de Puertos TCP y UDP 87
Gráfico Nro. 27: Fierce..... 88
Gráfico Nro. 28: Escaneo de Vulnerabilidades 89
Gráfico Nro. 29: Entorno de Configuración escaneo de puertos..... 90
Gráfico Nro. 30: NESSUS - Herramienta de análisis de vulnerabilidades..... 91

Gráfico Nro. 31: Configuración para realizar un escaneo NESSUS 92

I. INTRODUCCIÓN

La generalización y expansión del uso de las tecnologías, telecomunicaciones e informática en los diferentes contextos empresariales, académicos, personales y públicos, hacen de las TIC una base común para todas nuestras actividades En muchas generaciones se ha venido evolucionando el uso de TIC en diferentes ámbitos empresariales, personales, públicos, es una base en la vida del ser humano. Así mismo se mantiene en pie, por lo tanto debe ser protegida con la finalidad de no ser utilizados de manera incorrecta [1].

Se interpreta como seguridad informática las plataformas utilizadas en el mercado, el uso que le dan y con qué propósito. Así mismo es tener cuidado a la vulnerabilidad, riesgos y manipulaciones. Por lo tanto, se recomienda mantener y conocer las reglas de seguridad.

En los últimos tiempos las cosas buenas siempre van cerca de las malas. Según estudios realizados referentes a estos temas se explica que los expertos realizan auditorías planeadas a los sistemas mediante metodologías y así detectan la vulnerabilidad de la red [2].

Las personas dedicadas al hacker ético son dedicadas a esos temas, pueden realizar cosas a favor como también en contra, por lo tanto, esta investigación permite encontrar la vulnerabilidad de la red.

En los últimos tiempos aumentado el porcentaje de delitos informáticos de impactos grandes, como consecuencia ha permitido también el aumento de profesionales especializados en estos temas, con conocimientos penetrados y profundizados. En el caso de las Empresas y organizaciones han tenido la obligación de buscar soluciones a estos problemas presentados [3].

Contar con especialistas en seguridad informática significa afrontar los problemas actuales de seguridad informática y mitigar las posibles amenazas, así como

reducir las vulnerabilidades de la propia organización. Con este curso el alumno comprenderá el contexto de los ataques informáticos y la metodología en un panorama general utilizado en pruebas de penetración. Entenderá entonces las técnicas y los métodos empleados en ambientes reales para la disminución de las vulnerabilidades. De esta forma podrá establecerse una metodología para la auditoría tecnológica en los sistemas o las redes de una organización, con una postura sobre la evaluación de la seguridad de la información.

La Empresa Complex Del Perú S.A.C.- Tumbes recibe ataques informáticos a sus sistemas, ocasionan pérdidas de dinero, clientes, imagen, robo de información confidencial y prestigio. Por lo tanto, investigamos sobre esta situación, realizamos un análisis de la opinión de los trabajadores sobre la incomodidad que sienten al ser perjudicados por el hacking con el fin de proteger la reputación y continuidad de la empresa.

No cuenta con controles de seguridad informática la empresa y es incómodo tener un conocimiento para tomar decisiones pro-activas frente a un ataque cibernético. La inversión que realiza la empresa con la implementación de un hacking ético permite minimizar la pérdida de dinero y maximizar las ganancias, aun cuando ocurren ataques cibernéticos. Aumentará su imagen, prestigio, fidelidad porque protegerá la información confidencial y la relación con clientes, inversores, proveedores.

Partiendo de la realidad del problema, se propone el enunciado del problema: ¿De qué manera la implementación de Hacking, ayuda en la detección y evaluación de vulnerabilidades de Red en la Empresa Complex del Perú S.A.C – Tumbes; 2017?

Con el motivo de dar un desenlace a esta realidad problemática se determinó el siguiente objetivo general: Realizar la Implementación de Hacking Ético, en la Empresa Complex del Perú S.A.C; como medio de ayuda en la detección y evaluación de vulnerabilidades de Red.

En relación al objetivo general se definen los objetivos específicos:

1. Realizar el análisis de la actual red de datos en la Empresa Complex del Perú S.A.C – Tumbes; 2017, para evaluar los problemas de vulnerabilidad.

2. Formular una propuesta tecnológica que permita establecer un medio de comunicación oportuna al detectarse vulnerabilidades o penetraciones en la red de la Empresa Complex del Perú S.A.C – Tumbes.

Los riesgos que atacan a las redes son actos que inculca a buscar soluciones de seguridad. Estas infracciones realizadas con la utilización de programas hacker pueden ser detenidas siempre y cuando las organizaciones conozcan la descripción de dichos programas, y busquen soluciones guiados de las normas regidas a la seguridad.

Mayormente las Empresas pequeñas carecen de conocimiento sobre estos temas de vulnerabilidad de red, por lo tanto, les afecta con más frecuencias por no contar con expertos en el tema. El proyecto propuesto busca, mediante la investigación de herramientas hacker; dar a conocer de manera holística a la empresa descripción de cada una de las herramientas, para que así puedan prevenir ataques.

La presente investigación tiene su justificación académica basada en conocimientos logrados a través de los años de estudio en la Universidad Católica los Ángeles de Chimbote, los utilizo para realizar la investigación en la empresa Complex del Perú S.A.C referente al hacking ético por la vulnerabilidad de la red.

Asimismo, se justifica operativamente porque La Empresa Complex del Perú S.A.C cuenta con personal especializado en TIC (Tecnologías de Información y Comunicación), redes; por lo tanto, lo indispensable sería una capacitación referente al tema de investigación, así podrá monitorear el hacking ético implementado.

Su justificación económica se basa en la implementación del hacking ético

permitirá ahorrar tiempo y dinero en la empresa, además se evalúa el punto financiero de la empresa que cuenta con la facultad de asumir los costos necesarios de la implementación de hacking ético para la detección y evaluación de vulnerabilidades de red.

Su justificación tecnológica se basa en la idea de la implementación de hacking ético en la empresa se origina en base a la inseguridad que proporciona la red. Por lo tanto, la propuesta planteada ayudará a lograr la seguridad de la información y datos, en beneficio a todos los usuarios (trabajadores, clientes, administrativos).

Como justificación institucional, se basa en la realización de la presente investigación ayuda a mejorar el desarrollo de los procesos internos y externos de la empresa, llevar un control adecuado de las áreas administrativas y tener una imagen empresarial intachable frente al público en general.

La presente investigación se desarrolla en la ciudad de Tumbes, en la empresa Complex del Perú S.A.C. Engloba el estudio y análisis para la implementación del hacking ético, los dispositivos físicos y la tecnología actual.

II. REVISIÓN DE LA LITERATURA

2.1. Antecedentes

2.1.1. Antecedentes a nivel internacional

Ortiz B. [4], en el año 2015 realizó su investigación titulada: Hacking ético para detectar fallas en la seguridad informática de la intranet del gobierno provincial de Imbabura e implementar un sistema de gestión de seguridad de la información (SGSI), basado en la norma ISO/IEC 27001: 2005. El presente proyecto aborda la seguridad de la información de los elementos involucrados en el procesamiento, almacenamiento o transporte de la información en el Gobierno Provincial de Imbabura. La norma ISO/IEC 27001:2005 ha sido seleccionada como guía para el desarrollo de las actividades descritas en este documento con el objetivo de implementar un sistema de gestión de seguridad de la información. La norma ISO/IEC 27001:2005 establece tres requisitos previos para el análisis del diseño del sistema de gestión de seguridad de la información, el primero de ellos es un inventario de activos de información del Gobierno Provincial de Imbabura, para lo cual se ha tomado énfasis en la data center como centro de operaciones y procesamiento de la información. La detección de las vulnerabilidades es realizada en base a técnicas de hacking ético desde una perspectiva black-box (caja negra), es decir existe un desconocimiento inicial de los sistemas a evaluar y paulatinamente mediante varios procesos descubrir las características del equipo y las respectivas vulnerabilidades. De esta forma se pretende imitar un ataque hacker desde cualquier parte del mundo con intenciones maliciosas. Una vez se ha identificado los problemas se procede a seleccionar los controles recomendados por la norma ISO/IEC 27001:2005 para el tratamiento del riesgo de los activos de la información, finalizando con

la implementación de los controles seleccionados entre ellos la política de seguridad de la información.

Méndez D. [5], en el año 2014 desarrolló su investigación titulada: Investigación y elaboración de un instructivo sobre las herramientas hacker más utilizadas en el ámbito informático. La seguridad informática comprende software, bases de datos, metadatos, archivos y todo lo que la organización valore y signifique un riesgo si ésta llega a manos de otras personas. Este tipo de información se conoce como información privilegiada o confidencial. A lo largo del tiempo, el avance de los medios tecnológicos y de comunicación ha provocado el surgimiento de nuevos medios de ataques y de nuevas modalidades delictivas. Cada día se descubren nuevos puntos débiles, Bajo esta escenografía donde los principales actores son las organizaciones de cualquier magnitud y rubro, los sistemas de información, el dinero y delincuentes informáticos; se torna realmente necesario y fundamental idear estrategias de seguridad que permitan establecer barreras defensivas orientadas a mitigar efectivamente ataques tanto externos como internos. Pero para lograr atenuar de manera eficaz el impacto provocado por los ataques informáticos, es de esencial importancia conocer de qué manera atacan y cuáles son los puntos débiles de un sistema comúnmente explotado en los que se deben enfocar los esfuerzos de seguridad. Por lo tanto, el presente trabajo de tesis pretende ofrecer un instructivo de las herramientas hacker más utilizadas en el ámbito informático. Palabras Claves: herramientas hacker, seguridad informática.

Acosta A. [6], en el año 2014 realizó su tesis titulada: Hacking, Cracking y otras conductas ilícitas cometidas a través de Internet. Uno de los mayores inconvenientes a que se enfrentan los operadores jurídicos a la hora de analizar y actuar respecto del mundo de la informática, es el poco conocimiento que en esta área se posee, principalmente debido a que, en general, se considera a éste un entorno

más propio de las ingenierías y las matemáticas que de las humanidades que es el ámbito natural donde el hombre de derecho está acostumbrado a desenvolverse. Expresión de lo anterior la encontramos en el hecho de que, en la mayoría de la bibliografía especializada consultada en el curso de esta investigación, en general se le dediquen líneas muy breves y escuetas al tratamiento de los diferentes aspectos y caracterizaciones de los delitos informáticos, centrándose la mayoría de las veces el análisis en los aspectos netamente jurídicos de los mismos, y en particular en su consagración legal, sin adentrarse más a fondo en lo que este nuevo ámbito del conocimiento significa, en sus particularidades, en sus antecedentes y explicaciones no sólo jurídicas, sino que también sociales, culturales e incluso filosóficas, puesto que de lo que hablamos no sólo es de la regulación de un sector más del acontecer social, sino que hablamos de todo un mundo nuevo, esencialmente dinámico, revolucionario, con sus propios rasgos distintivos de interacción y comportamiento; un espacio esencialmente globalizado, en el cual se han demostrado insuficientes los intentos meramente nacionales por regularlo, y en el que se hace imprescindible una acción conjunta de los diferentes países para darle un estatuto jurídico verdaderamente aplicable, real, eficiente y eficaz, que responda a sus propias particularidades, puesto que ya desde antaño se ha constatado que no es el derecho el capaz de transformar, por sí solo, las realidades sociales, sino que éste debe adecuarse a ellas, cuestión que tratándose de Internet es aún un desafío a cumplir.

2.1.2. Antecedentes a nivel nacional

Muñoz D. [7], en el año 2015 realizó una investigación titulada: Implementación de una solución de hacking ético para mejorar la seguridad en la infraestructura informática de la caja municipal de Sullana -agencia Chimbote. El presente trabajo de investigación se realizó en la Caja Municipal de Sullana - Agencia Chimbote, cuya

actividad principal es el rubro financiero principalmente para la micro y pequeña empresa. La empresa tiene algunos años en la provincia del Santa, tiempo en el cual ha logrado posicionarse y competir con otras entidades financieras. Presenta como principales características sus bajos intereses, atención personalizada y enlace a nivel nacional. Los sistemas que utilizan, así como las aplicaciones, manejan gran cantidad de información de los clientes de carácter confidencial o riesgoso, la misma que tiene· que ser transmitida a través de la red informática con la mayor seguridad, reduciendo al mínimo los riesgos informáticos. Como solución al problema de la seguridad se implementó una solución de hacking ·' •\ ético en la infraestructura informática de la Caja Municipal de Sullana - Agencia Chimbote, con lo cual se mejoró la seguridad en la transferencia de datos.

Mamani T. [8], desarrolló en el 2014 su trabajo titulado: Modelo de sistema criptográfico de seguridad para las redes de comunicaciones en la región puno-2012, debido a que cuando se requiere compartir datos e informaciones en las redes, estas son expuestos a riesgos como denegación de servicios, observación y modificación no autorizada, la cual trae consecuencias en las transacciones. Para ello se planteó como objetivo fundamental "Modelar el sistema criptográfico de seguridad para las redes de comunicaciones" para proteger y tomar medidas de seguridad restringiendo los datos, cumpliendo con las políticas de seguridad, mecanismos consistentes y prácticas que regulan. Por tal razón se considera justificable la elaboración del modelo. La metodología utilizada es la investigación científica, exploratoria, descriptiva y explicativa, para el diseño se utilizó la herramienta técnica UML con los procedimientos científicos de la ingeniería de software. La implementación del modelo de seguridad se realizó a través de la aplicación del sistema de seguridad criptográfico asimétrico estándar corporativo determinando mecanismos y niveles de protección de datos, para las transacciones en redes, utilizando protocolo SSL con

autenticación certificada, con esta se cifran los datos para intercambiar entre el servidor y el cliente mediante el algoritmo de criptografía asimétrica. Se ha demostrado que la aplicación de sistema seguridad con SSL VeriSign con tecnología web mejora de manera continua en seguridad e integridad de datos, asegurando el tráfico de HTTP, que lo convierte en HTTPS que garantiza que las transacciones sean seguras entre terminales distintas en redes, de esta manera disminuye vulnerabilidades y riesgos.

Ortega J. [9], desarrolló su trabajo de investigación titulado: Diseño de red de comunicación de datos para la Institución Educativa Privada Emilio Soyer Cabero ubicada en el Distrito de Chorrillos, Lima, Perú, en primer lugar, se aborda la realidad problemática observada relacionada con la importancia y necesidad de diseñar una red de comunicación de datos con el fin de dotar a la institución educativa privada Emilio soyer cabero de un sistema de transmisión de información mediante la comunicación de todos los dispositivos de red que ésta maneje para ventaja de los trabajadores, docentes y alumnos. la estructura que hemos seguido en este proyecto se compone de 3 capítulos. el primer capítulo comprende el planteamiento del problema, el segundo capítulo el desarrollo del marco teórico y el tercer capítulo corresponde al desarrollo del diseño.

2.1.3. Antecedentes a nivel local

Muñoz C. [10], en el año 2014 investigó su proyecto titulado: Diseño de una red de telecomunicaciones de banda ancha para la región Tumbes. La presente tesis consiste en el diseño de una red de telecomunicaciones de banda ancha para la Región Tumbes y tiene como objetivo la conectividad regional, integrando todos los distritos de la región con redes de alta capacidad de transmisión que permita atender las necesidades de comunicaciones de banda ancha, además de

la conectividad integral a la red de banda ancha nacional. El proyecto se plantea como fin el ser un instrumento que contribuya al desarrollo socioeconómico y el mejoramiento de calidad de vida de la población de la región, Para tal propósito se realiza un análisis demográfico y socioeconómico de la región que permitirá proyectar la demanda de los servicios de telecomunicaciones en un periodo de 10 años; con lo cual se podrá estimar la capacidad de la red. El proyecto se basa en el uso de infraestructura de redes eléctricas de alta y media tensión existente en la región; sobre dicha infraestructura se soportará cable de fibra óptica tipo ADSS, totalmente dieléctrico y flexible. A partir de dicha red se tendrán los nodos de transporte, se definirá el trazado de la ruta de fibra óptica, tecnologías y capacidades a ser empleadas en la red. Además, se presentará el análisis económico del proyecto, donde se evaluará la sostenibilidad y rentabilidad en el tiempo. Al final del presente trabajo, se podrá identificar las consideraciones necesarias que se deben tomar en cuenta para realizar el despliegue e implementación de la red de banda ancha propuesta para la región Tumbes.

2.2. Bases teóricas

2.2.1. Empresa Investigada

Dirección

Av. Juan Velasco Alvarado Mz. B LT1, 4ta.Etapa AAHH La Curva - Aguas Verdes, Zarumilla – Tumbes

Historia

Esta empresa, comienza su función en el año 2005 en la ciudad de Aguas Verdes, Tumbes. El servicio que brindaba era de almacén temporal a todos dedicados al comercio de la frontera.

Por supuesto sigue en relación con el desarrollo económico de nuestra frontera, con la finalidad de lograr correctas operaciones de importación y exportación de los que trabajan con nosotros. Incluye diferentes productos como comercio, pesca, agricultura, minería, etc. El personal de nuestra identidad está en constante capacitación para brindar un servicio eficaz y correcto.

Visión

Ser un Depósito Temporal de clase internacional, posicionada como la mejor en la frontera norte del Perú.

Misión

Mejorar constantemente el nivel de atención en los lugares donde trabajemos, ayudando a nuestros clientes a optimizar su cadena de suministro.

2.2.2. Seguridad de la Información

La seguridad de la información como conjunto de medidas de protección hacia las instituciones, organizaciones, logrando el éxito, integridad y confidencialidad en su sistema. Todos los datos que mantienen en su institución como clientes, trabajadores se registraban manualmente con muchas dificultades y problemas.

Los sistemas primero te ayudan con ahorrar tiempo, espacio y hasta dinero, logrando realizar sus procesos de gestiones en menor tiempo y con correcto destinatario, mejora la organización mucho [11].

En toda institución, organización su información es la herramienta fundamental y de mucha importancia por lo tanto necesidad una buena

protección. Contar con seguridad informática permite que este con gran seguridad bajo cuidado de amenazas. Como se tiene conocimiento la información está distribuida en correos, usb, impresa, almacenes, y archivos [12].

A continuación, los principios de la seguridad de la información:

- Confidencialidad
- Integridad
- Disponibilidad

Gráfico Nro. 1: Seguridad de la Información

Fuente: Mifsud [11].

Ventajas

1. Prevalece la integridad de la información.
2. Protege correctamente y evita daños [13].

3. Su protección esta mediante normas.
4. Brinda conocimientos al personal de alrededor.

2.2.3. Delito Informático

El delito informático implica actividades criminales que en un primer momento los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robos o hurto, fraudes, falsificaciones, perjuicios, estafa, sabotaje, etc. Sin embargo, debe destacarse que el uso de las técnicas informáticas ha creado nuevas posibilidades del uso indebido de las computadoras, lo que ha propiciado a su vez la necesidad de regulación por parte del Derecho [14].

Partiendo de esta compleja situación y tomando como referencia el "Convenio de Ciberdelincuencia del Consejo de Europa", podemos definir los delitos informáticos como: "los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos" [15].

Tipos de Delitos Informáticos

La Organización de Naciones Unidas (ONU) manifiesta los siguiente [16]:

1. Estafa realizada en utilización de computadora.

- Manipulación de los datos de entrada
- Manejo erróneo de programas.
- Manipulación de los datos de salida
- Trampa cometida por adulterar datos.

2. Perjuicios o cambios de software

- Manipulación informática
- Acceso denegado a sistemas informáticos.
- Entrar o difundir programas de uso privado.

Ellas son:

- "Fraude en el campo de la informática.
- Falsificación en materia informática.
- Sabotaje informático y daños a datos computarizados o programas informáticos.
- Acceso no autorizado.
- Intercepción sin autorización.
- Reproducción no autorizada de un programa informático protegido.
- Espionaje informático.
- Uso no autorizado de una computadora.
- Tráfico de claves informáticas obtenidas por medio ilícito.
- Distribución de virus o programas delictivos."

2.2.4. Sistema de Gestión de Seguridad de la Información (SGSI)

SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de Information Security Management System [17].

La información, junto a los procesos y sistemas que hacen uso de ella, son activos muy importantes de una organización. La confidencialidad,

integridad y disponibilidad de información sensible pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial necesarios para lograr los objetivos de la organización y asegurar beneficios económicos.

Las organizaciones y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo. Los virus informáticos, el "hacking" o los ataques de denegación de servicio son algunos ejemplos comunes y conocidos, pero también se deben considerar los riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente desde dentro de la propia organización o aquellos provocados accidentalmente por catástrofes naturales y fallos técnicos [17].

Gráfico Nro. 2: Políticas de Seguridad

Fuente: Procedimientos en relación [17].

Fundamentos:

El SGSI para proteger y brindar seguridad para la información, se brinda aspectos confidentes [18]:

- Confidencialidad: la información está totalmente protegida ante todos, siempre y cuando sean personas u organizaciones autorizadas.
- Integridad: la información está totalmente exacta como de origen.
- Disponibilidad: quien esté autorizado puede localizar y acceder y mantener la información infinidad de veces.

2.2.5. ISO/IEC 27001

La ISO 27001 es el resultado de muchas evoluciones de estándares con relación a seguridad informática [19].

Gráfico Nro. 3: Protección a la Información

Fuente: Organization [19].

La Plataforma Tecnológica ISOTools optimiza las dificultades de la implementación y mantenimiento de SGSI en base a la norma ISO 27001 y por lo tanto permite el cumplimiento de la norma ISO 27002 [19].

¿Cuáles son los beneficios de la Gestión de Seguridad de la Información ISO/IEC 27001?

- Identifique los riesgos y coloque controles en el sitio para gestionarlos o eliminarlos [20]
- Flexibilidad para adaptar controles a todas las áreas o áreas seleccionadas de su organización
- Gane la confianza de los interesados y de los clientes de que sus datos están protegidos
- Demuestre cumplimiento y gane estatus como proveedor preferido
- Satisfaga más expectativas de licitaciones al demostrar cumplimiento

2.2.6. ISO/IEC 27002

La ISO/IEC 27002:2005 es una norma, un estándar, que brinda guiar hacia las buenas prácticas, logrando control apto en la seguridad de la información [21].

Control de Accesos

El objetivo es controlar el acceso por medio de un sistema de restricciones y excepciones a la información como base de todo sistema de seguridad informática.

Para impedir el acceso no autorizado a los sistemas de información se deberían implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas de información, bases de datos y servicios de información, y estos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento.

Los procedimientos comprenden todas las etapas del ciclo de vida de los accesos de los usuarios de todos los niveles, desde el registro inicial de nuevos usuarios hasta la privación final de derechos de los usuarios que ya no requieren el acceso.

La cooperación de los usuarios es esencial para la eficacia de la seguridad, por lo tanto, es necesario concientizar a los mismos acerca de sus responsabilidades por el mantenimiento de controles de acceso eficaces, en particular aquellos relacionados con el uso de contraseñas y la seguridad del equipamiento.

El Control de Accesos está basado en cuatro Objetivos:

2.2.6.1. Objetivo 1

El objetivo es controlar los accesos a la información y las instalaciones utilizadas para su procesamiento.

Requisitos de negocio para el control de accesos

Se deben controlar los accesos a la información, los recursos de tratamiento de la información y los procesos de negocio en base a las necesidades de seguridad y de negocio de la Organización.

Las regulaciones para el control de los accesos deberían considerar las políticas de distribución de la información y de autorizaciones.

Los propietarios de activos de información que son responsables ante la dirección de la protección "sus" activos deberían tener la capacidad de definir y/o aprobar las reglas de control de acceso y otros controles de seguridad. Asegúrese de que se les

responsabiliza de incumplimientos, no conformidades y otros incidentes.

Actividades de Control del riesgo

- **Política de control de accesos:** Se debería establecer, documentar y revisar una política de control de accesos en base a las necesidades de seguridad y de negocio de la Organización.
- **Control de acceso a las redes y servicios asociados:** Se debería proveer a los usuarios de los accesos a redes y los servicios de red para los que han sido expresamente autorizados a utilizar.

Métricas Asociadas

Porcentaje de sistemas y aplicaciones corporativas para los que los "propietarios" adecuados han: (a) sido identificados, (b) aceptado formalmente sus responsabilidades, (c) llevado a cabo -o encargado- revisiones de accesos y seguridad de aplicaciones, basadas en riesgo y (d) definido las reglas de control de acceso basadas en roles.

Enlaces a Soluciones Recomendadas

- **OpenNAC:** Solución de código abierto para el control de acceso de red en entornos LAN/WAN corporativos y compatible con diversos fabricantes de tecnología de red. Permite la autenticación, autorización y auditoría basada en las políticas de acceso a la red.
- **Packetfence:** Solución de código abierto para el control de acceso de red que se puede utilizar para asegurar de

manera eficaz desde las redes pequeñas a grandes redes heterogéneas.

- **Seguridad en Intranet:** Monografía sobre la seguridad en las redes corporativas en base a las políticas de control de acceso.

2.2.6.2. Objetivo 2

El objetivo es el de garantizar el acceso a los usuarios autorizados e impedir los accesos no autorizados a los sistemas de información y servicios.

Gestión de Acceso de Usuario

Se deberían establecer procedimientos formales para controlar la asignación de los permisos de acceso a los sistemas y servicios de información.

Los procedimientos deberían cubrir todas las etapas del ciclo de vida del acceso de los usuarios, desde del registro inicial de los nuevos usuarios hasta su baja cuando ya no sea necesario su acceso a los sistemas y servicios de información.

Se debería prestar especial atención, si fuera oportuno, a la necesidad de controlar la asignación de permisos de acceso con privilegios que se salten y anulen la eficacia de los controles del sistema.

Actividades de Control de Riesgo

- **Gestión de altas/bajas en el registro de usuarios:** Debería existir un procedimiento formal de alta y baja de

usuarios con objeto de habilitar la asignación de derechos de acceso.

- **Gestión de los derechos de acceso asignados a usuarios:** Se debería de implantar un proceso formal de aprovisionamiento de accesos a los usuarios para asignar o revocar derechos de acceso a todos los tipos de usuarios y para todos los sistemas y servicios.
- **Gestión de los derechos de acceso con privilegios especiales:** La asignación y uso de derechos de acceso con privilegios especiales debería ser restringido y controlado.
- **Gestión de información confidencial de autenticación de usuarios:** La asignación de información confidencial para la autenticación debería ser controlada mediante un proceso de gestión controlado.
- **Revisión de los derechos de acceso de los usuarios:** Los propietarios de los activos deberían revisar con regularidad los derechos de acceso de los usuarios.
- **Retirada o adaptación de los derechos de acceso:** Se deberían retirar los derechos de acceso para todos los empleados, contratistas o usuarios de terceros a la información y a las instalaciones del procesamiento de información a la finalización del empleo, contrato o acuerdo, o ser revisados en caso de cambio.

Métricas Asociadas

Tiempo medio transcurrido entre la solicitud y la realización de peticiones de cambio de accesos y número de solicitudes de cambio de acceso cursadas en el mes anterior (con análisis de tendencias y comentarios acerca de cualquier pico / valle (p. ej., "Implantada nueva aplicación financiera este mes").

Enlaces a Soluciones Recomendadas

- **DBAudit:** DB Audit es una completa solución out of the box de seguridad para bases de datos y auditoría para Oracle, Sybase, MySQL, DB2 y MS SQL Server.
- **Manage Engine:** Solución web (free trial 30 days) que permite realizar las tareas más comunes, como las altas y bajas de usuarios y la aplicación de políticas de grupo, a través de un interfaz intuitivo y fácil de aprender. A través de sus informes detallados, ofrece visibilidad completa sobre todos los objetivos en el Directorio Activo.
- **Pangolín:** Pangolín es una herramienta automática de pruebas de penetración de inyección SQL desarrollado por NOSEC. Su objetivo es detectar y aprovechar las vulnerabilidades de inyección SQL en aplicaciones web.
- **UserLock:** Permite proteger el acceso a las redes de Windows®, impidiendo las conexiones simultáneas, al dar la posibilidad de limitar las conexiones de los usuarios y proporcionando a los administradores el control remoto de las sesiones, de las funcionalidades de alerta, de informes y análisis sobre todas las conexiones/desconexiones efectuadas en sus redes.

2.2.6.3. Objetivo 3

El objetivo es hacer que los usuarios sean responsables de la protección de la información para su identificación.

Responsabilidades del Usuario

- La cooperación de los usuarios autorizados es esencial para una seguridad efectiva.

- Los usuarios deberían ser conscientes de sus responsabilidades en el mantenimiento de controles de acceso eficaces, en particular respecto al uso de contraseñas y seguridad en los equipos puestos a su disposición.

- Se debería implantar una política para mantener mesas de escritorio y monitores libres de cualquier información con objeto de reducir el riesgo de accesos no autorizados o el deterioro de documentos, medios y recursos para el tratamiento de la información.

- Asegúrese de que se establecen las responsabilidades de seguridad y que son entendidas por el personal afectado. Una buena estrategia es definir y documentar claramente las responsabilidades relativas a seguridad de la información en las descripciones o perfiles de los puestos de trabajo.

- Son imprescindibles las revisiones periódicas para incluir cualquier cambio. Comunique regularmente a los empleados los perfiles de sus puestos (p. ej., en la revisión anual de objetivos), para recordarles sus responsabilidades y recoger cualquier cambio.

Actividades de Control de Riesgo

Uso de información confidencial para la autenticación: Se debería exigir a los usuarios el uso de las buenas prácticas de seguridad de la organización en el uso de información confidencial para la autenticación.

Métricas Asociadas

Porcentaje de descripciones de puesto de trabajo que incluyen responsabilidades en seguridad de la información (a) totalmente documentadas y (b) formalmente aceptadas.

Enlaces a Soluciones Recomendadas

KEEPASS: KeePass es una aplicación free open source para la gestión de contraseñas que sirve de ayuda para gestionar las contraseñas de un modo seguro. Puedes almacenar todas las contraseñas en una única base de datos, la cual permanece accesible mediante una única clave maestra o fichero. Por tanto, sólo se tiene que recordar una única contraseña o seleccionar el fichero clave para acceder a la base de datos cifrada mediante algoritmo robusto (AES y Twofish).

2.2.6.4. Objetivo 4

Control de acceso a sistemas y aplicaciones
Los medios deberían ser controlados y físicamente protegidos.

Se deberían establecer los procedimientos operativos adecuados para proteger los documentos, medios informáticos (discos, cintas, etc.), datos de entrada o salida y documentación del sistema contra la divulgación, modificación, retirada o destrucción de activos no autorizadas.

Asegure los soportes y la información en tránsito no solo físico sino electrónico (a través de las redes). Cifre todos los datos sensibles o valiosos antes de ser transportados.

Actividades de Control de Riesgo

- **Restricción del acceso a la información:** Se debería restringir el acceso de los usuarios y el personal de mantenimiento a la información y funciones de los sistemas de aplicaciones, en relación a la política de control de accesos definida.

- **Procedimientos seguros de inicio de sesión:** Cuando sea requerido por la política de control de accesos se debería controlar el acceso a los sistemas y aplicaciones mediante un procedimiento seguro de log-on

- **Gestión de contraseñas de usuario:** Los sistemas de gestión de contraseñas deberían ser interactivos y asegurar contraseñas de calidad.

- **Uso de herramientas de administración de sistemas:** El uso de utilidades software que podrían ser capaces de anular o evitar controles en aplicaciones y sistemas deberían estar restringidos y estrechamente controlados.

- **Control de acceso al código fuente de los programas:** Se debería restringir el acceso al código fuente de las aplicaciones software.

Métricas Asociadas

Porcentaje de soportes de backup o archivo que están totalmente encriptados.

Enlaces Recomendados

- **0PHCRACK:** Utilidad para verificar la fortaleza de las contraseñas en uso y determinar políticas y frecuencias en la renovación de las contraseñas.

- **JOHN THE RIPPER:** Utilidad para verificar la fortaleza de las contraseñas en uso y determinar políticas y frecuencias en la renovación de las contraseñas.

- **KEEPASS:** KeePass es una aplicación free open source para la gestión de contraseñas que sirve de ayuda para gestionar las contraseñas de un modo seguro. Puedes almacenar todas las contraseñas en una única base de datos, la cual permanece accesible mediante una única clave maestra o fichero. Por tanto, sólo se tiene que recordar una única contraseña o seleccionar el fichero clave para acceder a la base de datos cifrada mediante algoritmo robusto (AES y Twofish).

- **OXID:** Utilidad para verificar la fortaleza de las contraseñas en uso y determinar políticas y frecuencias en la renovación de las contraseñas.

- **PASSWORD GENERATOR:** Generador on-line de contraseñas.

- **RANDOW PASSWORD GENERATOR:** Generador de contraseñas seguras.

2.2.7. Hacking Ético

Su función principal y fundamental es analizar los programas informáticos, con el propósito de evaluar el estado actual y real de la seguridad de información. Por supuesto para poder realizar un hacking ético primeramente es contar con la autorización de la empresa, institución u organización, y detallar un contrato que cumpla derechos de la empresa y normas. El resultado obtenido será entregado [22].

La principal función del hacking ético es que les facilita a las empresas las claves para protección de los ciberataques.

2.2.8. Fases del Hacking Ético

Las 5 Fases del Hacking o también conocido como el Circulo del Hacking, es el proceso que utilizan los hackers maliciosos para hackear y obtener el completo acceso a un sistema vulnerable. [23]

Los hackers éticos también siguen de una forma similar este proceso que utilizan los hackers maliciosos, solo que los hackers éticos no siguen todas las fases del Circulo del Hacking, su trabajo de los hackers éticos recién termina en la Fase 3 del Circulo Hacking.

2.2.8.1. Reconocimiento

Es la fase en la cual se busca recolectar toda información esencial del objetivo mediante el uso de varias técnicas y herramientas.

Existen dos Tipos de Reconocimientos:

Pasivo.

El reconocimiento pasivo implica la adquisición de información, sin la interacción directa con el objetivo.

Ejemplo:

- Dumpster Diving (Buscar en la basura)
- Búsqueda de información en los buscadores como google
- Buscar en la base de datos de Internet (Whois)
- Buscar país y ciudad donde residen los servidores
- Buscar nombres de dominios
- Buscar información de contacto
- Buscar toda la información que se pueda extraer de los DNS (Domain Name Server)

Activo.

Implica la adquisición de información, con la interacción directa con el objetivo.

- Ingeniería Social
- Port Scanning
- Usar herramientas de software para hacer un escaneo de la red.
- Descubrir el rango de direcciones IPs
- Identificar Sistemas Operativos
- Identificar Nombres de Equipos
- Identificar las Cuentas de Usuarios
- Buscar donde están localizados los Routers

2.2.8.2. Escaneo

Esta es la fase que el hacker realiza antes de lanzar un ataque a la red (network), en la Fase de Escaneo el hacker utiliza toda la información que recolecto en la Fase de Reconocimiento para identificar vulnerabilidades específicas.

Ejemplo:

Si en la Fase 1 el hacker descubrió que su objetivo utiliza un sistema operativo Windows XP entonces el hacker buscara vulnerabilidades específicas que funcionen en ese sistema operativo para saber por dónde atacarlo.

Se puede utilizar cualquier herramienta automatizada para escanear toda red, cuentas de usuarios, hosts, servicios y vulnerabilidades que permitan el acceso al sistema vulnerable.

2.2.8.3. Explotación

Esta es una de las fases más importantes para el hacker porque es la fase de penetración al sistema vulnerable, en esta fase el hacker explota las vulnerabilidades que encontró en la Fase de Escaneo.

La explotación puede ocurrir de forma:

- LAN (Local Área Network)
- Offline (sin estar conectado)
- Internet

2.2.8.4. Mantener el Acceso

La Fase de Mantener Acceso se realiza una vez finalizada con éxito la Fase de Obtener Acceso del sistema vulnerable, en esta fase la prioridad del hacker es mantener el acceso al sistema vulnerable.

En esta fase el hacker puede utilizar el sistema vulnerable como plataforma para el lanzamiento de nuevos ataques, el hacker utiliza sus propios recursos y recursos del sistema vulnerable para escanear y explotar vulnerabilidades de otros sistemas que quiere atacar que se encuentren dentro o fuera de la red, el hacker

también utiliza otras herramientas llamados Sniffers para capturar todo el tráfico de la red, incluyendo sesiones de Telnet y FTP (File Transfer Protocol).

En esta fase el hacker puede tener la habilidad de subir o bajar cualquier tipo de archivo del sistema, puede alterar el funcionamiento de las aplicaciones que tiene el sistema y modificar cualquier tipo de archivos o información que se encuentre en el sistema, el hacker suele fortalecer y parchar todas las vulnerabilidades del sistema vulnerable para que otros hackers no puedan tener ningún tipo de acceso.
Si el hacker quiere permanecer indetectable y tener acceso al sistema en cualquier momento, va a tener que usar algunas herramientas como el:

- Backdoor (Puertas Traseras)
- Trojans (Troyanos)
- Shell o Shell Inversa
- Cuentas de altos privilegios como cuentas de Administrador o de System.
- También puede utilizar otras herramientas como el Tunneling, RootKits, Keyloggers, Spyware.

2.2.8.5. Borrado de Huellas

Esta fase es donde el hacker trata de descubrir y destruir toda la evidencia de su presencia y de sus actividades ilícitas y lo hace por varias razones entre ellas seguir manteniendo el acceso al sistema comprometido ya que si borra sus huellas los administradores de redes no tendrán evidencias ni pistas claras sobre la intrusión al sistema, además borrando sus huellas evita ser detectado y ser atrapado por la policía informática.

Herramientas y técnicas que utiliza el Hacker para ocultar sus huellas:

- Troyanos
- Steganography
- Tunneling
- RootKits
- ELSave
- WinZapper
- Navegación Anónima: Tor, Proxys Anónimos, VPN, etc.
- Alteración de los Log Files (Archivos donde se almacenan todos los eventos ocurridos en un sistema informático y permite obtener información detallada sobre los hábitos de los usuarios).
- Eliminar todos los registros del sistema que indiquen que el hacker tuvo acceso al sistema.
- Eliminar todas las cuentas de usuario que se creó y se utilizó para la intrusión al sistema.
- Eliminar los archivos del IDS (Sistema de Detención de Intrusos).
- Ocultar todos los ficheros ADS Stream.

2.2.8.6. Caso Cracka

El misterioso adolescente británico que hackeó al director de la CIA.

El último ciberdelincuente en llamar la atención de la prensa internacional es un joven británico que a sus 16 años consiguió

hackear los correos personales del Director de la CIA, el director del FBI y el Director de Inteligencia Nacional. Además, hackeó las cuentas de teléfono de este último y reveló la identidad de 31.000 agentes del gobierno de Estados Unidos: CIA, Seguridad Nacional, FBI…

La verdadera identidad de este joven no se ha desvelado, pero sabemos que se hace llamar "Cracka" y asegura ser miembro de un grupo de hackers llamado "Crackas with Attitude" que actúa en defensa del Movimiento Palestino. "Cracka" fue detenido el mes pasado en el sureste de Inglaterra.

Terminología

Crackers: es un individuo que crea y modifica software y hardware de computadoras, para desarrollar nuevas funciones o adaptar las antiguas, sin que estas modificaciones sean dañinas para el usuario del mismo [24].

Ethical Hacking: es un profesional que cuenta con conocimientos de seguridad e vulnerabilidades en diversas plataformas y aplicaciones. Su objetivo es identificar y validar las vulnerabilidades que las comprometan [25].

Hacker: es un experto tecnológico cuyos conocimientos en materia de seguridad, sistemas operativos y/o programación, sobrepasan no solamente los conocimientos medios de cualquier usuario final, sino también los de muchos profesionales de estos sectores [26].

Red de Datos: aquellas infraestructuras o redes de comunicación que se ha diseñado específicamente a la Transmisión de información mediante el intercambio de datos [27].

Virus informáticos: son sencillamente programas maliciosos (malware) que “infectan” a otros archivos del sistema con la intención de modificarlo o dañarlo [28].

Vulnerabilidad: es una debilidad del sistema informático que puede ser utilizada para causar un daño. Las debilidades pueden aparecer en cualquiera de los elementos de una computadora, tanto en el hardware, el sistema operativo, cómo en el software [29].

2.3. HIPÓTESIS

Realizar la Implementación de Hacking Ético para mejorar la detección y evaluación de vulnerabilidades de Red en la Empresa Complex del Perú S.A.C – Tumbes; 2017.

III. METODOLOGÍA

3.1. Diseño de la investigación

TIPO DE ESTUDIO:

Esta investigación es una investigación cuantitativa, por lo tanto, Fernández, P. y Díaz, P. [30], define que trata de determinar la fuerza de asociación o correlación entre variables, la generalización y objetivación de los resultados a través de una muestra para hacer inferencia a una población de la cual toda muestra procede.

NIVEL DE LA INVESTIGACIÓN:

Basado en la naturaleza del estudio de la investigación, reúne por su nivel, las características de un estudio descriptivo. Según Tamayo y Tamayo M. [31], en su libro Proceso de Investigación Científica, la investigación descriptiva "comprende la descripción, registro, análisis e interpretación de la naturaleza actual, y la composición o proceso de los fenómenos. El enfoque se hace sobre conclusiones dominantes o sobre grupo de personas, grupo o cosas, se conduce o funciona en presente".

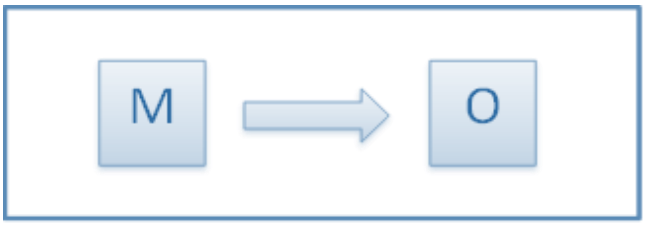
Según Sabino [32], "La investigación de tipo descriptiva trabaja sobre realidades de hechos, y su característica fundamental es la de presentar una interpretación correcta. Para la investigación descriptiva, su preocupación primordial radica en descubrir algunas características fundamentales de conjuntos homogéneos de fenómenos, utilizando criterios sistemáticos que permitan poner de manifiesto su estructura o comportamiento. De esta forma se pueden obtener las notas que caracterizan a la realidad estudiada".

DISEÑO DE LA INVESTIGACIÓN:

Dzul [33], define que la investigación no experimental es aquel que se realiza sin manipular deliberadamente variables. Se basa fundamentalmente en la observación de fenómenos tal y como se dan en su contexto natural para después analizarlos.

Seehorn [34], La investigación de corte transversal implica la recogida de datos una vez durante una cantidad de tiempo limitada. La investigación transversal suele ser descriptiva más que experimental. Estos tipos de estudios son útiles para describir un efecto particular en una población en particular en un momento determinado en el tiempo.

El diseño de la investigación se gráfica de la siguiente manera:



Dónde:

M = Muestra

O = Observación

3.2. Población y Muestra

La población de la presente investigación está definida en 24 trabajadores, que tienen relación directa con el tema de investigación sobre el manejo de la red.

La muestra se ha tomado la misma cantidad de la población que es 24 trabajadores, por lo tanto, no se ha realizado ninguna técnica de selección de muestreo.

3.3. Técnicas e instrumentos

3.3.1. Técnica

En la investigación se utilizó la encuesta como técnica y el cuestionario como instrumento de tipo cerrado dicotómico, que quiere decir solo de dos opciones; si o no.

La encuesta:

Según Andrés [35], la encuesta es un método de investigación y recopilación de datos utilizados para obtener información de personas sobre diversos temas. Las encuestas tienen una variedad de propósitos y se pueden llevar a cabo de muchas maneras dependiendo de la metodología elegida y los objetivos que se deseen alcanzar.

3.3.2. Instrumentos

Cuestionario:

De acuerdo con Galán [36], define que el cuestionario es un conjunto de preguntas diseñadas para generar los datos necesarios para alcanzar los objetivos propuestos del proyecto de investigación. El cuestionario permite estandarizar e integrar el proceso de recopilación de datos. Un diseño mal construido e inadecuado conlleva a recoger información incompleta, datos no precisos de esta manera genera información nada confiable. Por esta razón el cuestionario es en definitiva un conjunto de preguntas respecto a una o más variables que se van a medir.

3.4. Definición operacional de las variables en estudio

Tabla Nro. 1: Matriz de Operacionalización de Variables

Variable	**Definición Conceptual**	**Dimensiones**	**Indicadores**	**Definición Operacional**
Implementación de un hacking ético	Hacking Ético: analiza los sistemas y programas informáticos corporativos, asumiendo el rol de un ciberdelincuente y simulando ataques a la empresa con el objetivo de evaluar el estado real de si seguridad TI [22].	− Satisfacción de la seguridad de información − Identificación de problemas	− Incomodidad − Satisfacción − Seguridad − Nivel	Si No
		− Necesidad de implementación de hacking ético	− Nueva implementación − Necesidad de instalación SGSI	

Fuente: Elaboración propia.

3.5. Procedimiento de recolección de datos.

Se seleccionó al personal indicado para aplicar la encuesta y se le entregó su respectivo material impreso. También se considera evitar tecnicismos ofreciendo así una mejor oportunidad para transmitir las ideas, completa y puntual, entre el encuestador y encuestado, finalmente se procedió a brindar y orientar al encuestado en todo momento que él lo requiera.

3.6. Plan de análisis

Finalmente se rescató los datos obtenidos de las encuestas, se empezó la tabulación de los resultados de cada pregunta en el programa Microsoft Excel versión 2013.

3.7. Matriz de Consistencia

Tabla Nro. 2: Matriz de consistencia

ENUNCIADO PROBLEMA	OBJETIVO GENERAL DE LA INVESTIGACIÓN	OBJETIVOS ESPECÍFICOS	METODOLOGÍA
¿De qué manera la implementación de Hacking, ayuda en la detección y evaluación de vulnerabilidades de Red en la Empresa Complex del Perú S.A.C – Tumbes; 2017?	Realizar la implementación de Hacking Ético, en la Empresa Complex del Perú S.A.C; como medio de ayuda en la detección y evaluación de vulnerabilidades de Red.	1. Realizar el análisis de la actual red de datos en la empresa Complex del Perú S.A.C – Tumbes; 2017, para evaluar los problemas de vulnerabilidad. 2. Formular una propuesta tecnológica que permita establecer un medio de comunicación oportuna al detectarse vulnerabilidades o penetraciones en la red de la empresa Complex del Perú S.A.C – Tumbes.	Tipo de la investigación: Cuantitativa Nivel de la investigación: Descriptiva. Diseño de la investigación: No Experimental y de Corte Transversal

Fuente: Elaboración propia.

3.8. Principios Éticos

En el desarrollo de esta investigación denominada Implementación de Hacking Ético para la detección y evaluación de vulnerabilidades de red en la Empresa Complex del Perú S.A.C.-Tumbes; 2017, se estima considerar de manera óptima la práctica de principios éticos. Asimismo, se ha cumplido los derechos de propiedad de los libros y de fuentes electrónicas, indispensables para el cumplimiento de la teoría.

Además, se han cogido datos de ambiente público, pero sin hacer ningún tipo de cambios o modificaciones, se pueden consultar para corroborar lo escrito. Como también se tomó datos exactos provenidos de encuestas para cumplir con la parte de la metodología, en el ítem de análisis de la investigación. Por lo tanto, se cree conveniente reservar la identidad personal del encuestado.

IV. RESULTADOS

4.1. Resultados

4.1.1. Dimensión 01: Nivel de satisfacción de las circunstancias Actuales

Tabla Nro. 3: Conocimiento hacking ético

Distribución de las frecuencias y respuestas relacionadas con conocimiento sobre hacking ético; respecto a la Implementación de Hacking Ético para la Detección y Evaluación de Vulnerabilidades de Red en la Empresa Complex del Perú S.A.C.-Tumbes; 2017.

Alternativas	n	%
Si	2	8.00
No	22	92.00
Total	24	100.00

Fuente: Cuestionario aplicado al personal de la Empresa Complex del Perú S.A.C.-Tumbes; 2017.; para alegar a la interrogante: ¿Usted tiene conocimiento sobre hacking ético?

Aplicado por: Bermeo, J.; 2017.

Mediante la Tabla Nro. 3 podemos visualizar que el 92.00% de los encuestados revelaron que NO tienen conocimientos sobre hacking ético, por lo tanto, el 8.00% de los trabajadores encuestados indicó que sí.

Tabla Nro. 4: Personal Capacitado

Distribución de las frecuencias y respuestas relacionadas con personal capacitado sobre temas de informática; respecto a la Implementación de Hacking Ético para la Detección y Evaluación de Vulnerabilidades de Red en la Empresa Complex del Perú S.A.C.-Tumbes; 2017.

Alternativas	n	%
Si	1	4.00
No	23	96.00
Total	24	100.00

Fuente: Cuestionario aplicado al personal de la Empresa Complex del Perú S.A.C.-Tumbes; 2017.; para alegar a la interrogante: ¿Cree usted que la empresa cuenta con personal capacitado sobre temas de informática?

Aplicado por: Bermeo, J.; 2017.

Mediante la Tabla Nro. 4 podemos visualizar que el 96.00% de los encuestados revelaron que NO cuentan con personal capacitado sobre temas de informática, por lo tanto, el 4.00% de los trabajadores encuestados indicó que sí.

Tabla Nro. 5: Conocimiento hacking ético

Distribución de las frecuencias y respuestas relacionadas con tener hacking ético en la empresa; respecto a la Implementación de Hacking Ético para la Detección y Evaluación de Vulnerabilidades de Red en la Empresa Complex del Perú S.A.C.-Tumbes; 2017.

Alternativas	n	%
Si	--	--
No	24	100.00
Total	24	100.00

Fuente: Cuestionario aplicado al personal de la Empresa Complex del Perú S.A.C.-Tumbes; 2017.; para alegar a la interrogante: ¿La empresa cuenta con un hacking ético?

Aplicado por: Bermeo, J.; 2017.

Mediante la Tabla Nro. 5 podemos visualizar que el 100.00% de encuestados revelaron que NO cuenta con hacking ético la empresa.

Tabla Nro. 6: Información Jaqueada

Distribución de las frecuencias y respuestas relacionadas a la información que puede ser jaqueada; respecto a la Implementación de Hacking Ético para la Detección y Evaluación de Vulnerabilidades de Red en la Empresa Complex del Perú S.A.C.-Tumbes; 2017.

Alternativas	n	%
Si	4	7.00
No	20	83.00
Total	24	100.00

Fuente: Cuestionario aplicado al personal de la Empresa Complex del Perú S.A.C.-Tumbes; 2017.; para alegar a la interrogante: ¿Usted como trabajador piensa que su información puede ser jaqueada?

Aplicado por: Bermeo, J.; 2017.

Mediante la Tabla Nro. 6 podemos visualizar que el 83.00% de encuestados revelaron que NO creen que su información puede ser jaqueada, por lo tanto, el 7.00% de los trabajadores encuestados indicó que sí.

Tabla Nro. 7: Beneficios de hacking ético

Distribución de las frecuencias y respuestas relacionadas con conocimiento sobre beneficios de hacking ético; respecto a la Implementación de Hacking Ético para la Detección y Evaluación de Vulnerabilidades de Red en la Empresa Complex del Perú S.A.C.-Tumbes; 2017.

Alternativas	n	%
Si	3	12.00
No	21	88.00
Total	24	100.00

Fuente: Cuestionario aplicado al personal de la Empresa Complex del Perú S.A.C.-Tumbes; 2017.; para alegar a la interrogante: ¿Conoce usted los beneficios que el hacking ético?

Aplicado por: Bermeo, J.; 2017.

Mediante la Tabla Nro. 7 podemos visualizar que el 88.00% de encuestados revelaron que NO conocen los beneficios de hacking ético, por lo tanto, el 12.00% de los trabajadores encuestados indicó que sí.

Tabla Nro. 8: Vulnerabilidad de Red

Distribución de las frecuencias y respuestas relacionadas con conocimiento sobre vulnerabilidad de la red; respecto a la Implementación de Hacking Ético para la Detección y Evaluación de Vulnerabilidades de Red en la Empresa Complex del Perú S.A.C.-Tumbes; 2017.

Alternativas	n	%
Si	1	4.00
No	23	96.00
Total	24	100.00

Fuente: Cuestionario aplicado a los trabajadores la Empresa Complex del Perú S.A.C.-Tumbes; 2017.; para alegar a la interrogante: ¿Usted tiene conocimiento sobre la vulnerabilidad de la red?

Aplicado por: Bermeo, J.; 2017.

Mediante la Tabla Nro. 8 podemos visualizar que el 96.00% de encuestados revelaron que NO tienen conocimiento sobre vulnerabilidad de la red, por lo tanto, el 4.00% de los trabajadores encuestados indicó que sí.

Tabla Nro. 9: Capacitación de trabajadores

Distribución de las frecuencias y respuestas relacionadas con capacitación a los trabajadores sobre el tema de investigación; respecto a la Implementación de Hacking Ético para la Detección y Evaluación de Vulnerabilidades de Red en la Empresa Complex del Perú S.A.C.-Tumbes; 2017.

Alternativas	n	%
Si	2	8.00
No	22	92.00
Total	24	100.00

Fuente: Cuestionario aplicado a los trabajadores la Empresa Complex del Perú S.A.C.-Tumbes; 2017.; para alegar a la interrogante: ¿Se ha capacitado alguna vez a los trabajadores sobre el tema hacker?

Aplicado por: Bermeo, J.; 2017.

Mediante la Tabla Nro. 9 podemos visualizar que el 92.00% de encuestados revelaron que NO han capacitado a los trabajadores sobre el tema hacker, por lo tanto, el 8.00% de los trabajadores encuestados indicó que sí.

Tabla Nro. 10: Seguridad de Información

Distribución de las frecuencias y respuestas relacionadas con la satisfacción de la seguridad de información de la empresa; respecto a la Implementación de Hacking Ético para la Detección y Evaluación de Vulnerabilidades de Red en la Empresa Complex del Perú S.A.C.-Tumbes; 2017.

Alternativas	n	%
Si	1	4.00
No	23	96.00
Total	24	100.00

Fuente: Cuestionario aplicado a los trabajadores la Empresa Complex del Perú S.A.C.-Tumbes; 2017.; para alegar a la interrogante: ¿Está satisfecho con la seguridad de la información actual que cuenta la empresa?

Aplicado por: Bermeo, J.; 2017.

Mediante la Tabla Nro. 10 podemos visualizar que el 96.00% de encuestados revelaron que NO están satisfechos con la seguridad de la información actual que cuenta la empresa, por lo tanto, el 4.00% de los trabajadores encuestados indicó que sí.

Tabla Nro. 11: Inseguridad de Información

Distribución de las frecuencias y respuestas relacionadas con la inseguridad de información en la empresa; respecto a la Implementación de Hacking Ético para la Detección y Evaluación de Vulnerabilidades de Red en la Empresa Complex del Perú S.A.C.-Tumbes; 2017.

Alternativas	n	%
Si	3	12.00
No	21	88.00
Total	24	100.00

Fuente: Cuestionario aplicado a los trabajadores la Empresa Complex del Perú S.A.C.-Tumbes; 2017.; para alegar a la interrogante: ¿Usted teme por la seguridad de la información de la empresa que sea jaqueada?

Aplicado por: Bermeo, J.; 2017.

Mediante la Tabla Nro. 11 podemos visualizar que el 88.00% de encuestados revelaron que NO temen por la seguridad de la información ser jaqueada en la empresa, por lo tanto, el 12.00% de los trabajadores encuestados indicó que sí.

Tabla Nro. 12: Instalación de hacking ético

Distribución de las frecuencias y respuestas relacionadas con la instalación de Hacking Ético; respecto a la Implementación de Hacking Ético para la Detección y Evaluación de Vulnerabilidades de Red en la Empresa Complex del Perú S.A.C.-Tumbes; 2017.

Alternativas	n	%
Si	--	--
No	24	100.00
Total	24	100.00

Fuente: Cuestionario aplicado a los trabajadores la Empresa Complex del Perú S.A.C.-Tumbes; 2017.; para alegar a la interrogante: ¿Usted alguna vez ha visto la instalación de un hacking ético?

Aplicado por: Bermeo, J.; 2017.

Mediante la Tabla Nro. 12 podemos visualizar que el 100.00% de encuestados revelaron que NO han visto ninguna vez sobre instalación de hacking ético.

Resumen de 1° Dimensión

Tabla Nro. 13: Nivel de Satisfacción de las circunstancias actuales

Nivel de Satisfacción de las circunstancias actuales; respecto a la Implementación de Hacking Ético para la Detección y Evaluación de Vulnerabilidades de Red en la Empresa Complex del Perú S.A.C.-Tumbes; 2017.

Alternativas	n	%
Si	1	4.00
No	23	96.00
Total	24	100.00

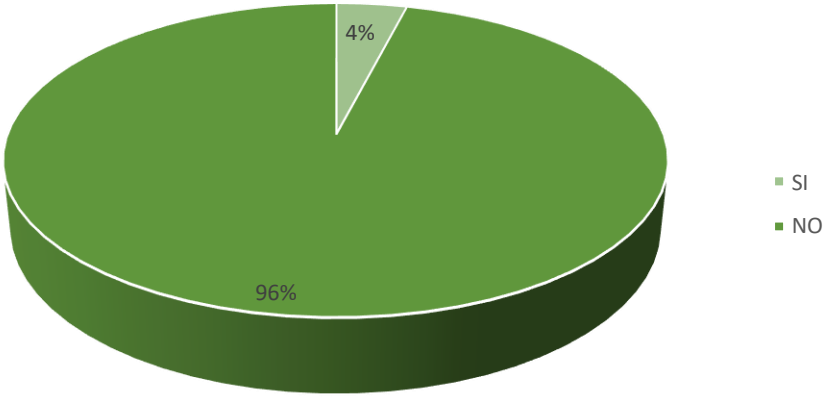
Fuente: Aplicación del Cuestionario para medir la Dimensión: Nivel de Satisfacción de las circunstancias actuales, basado en diez interrogantes aplicadas al personal de la Empresa Complex del Perú S.A.C.-Tumbes; 2017.

Aplicado por: Bermeo, J.; 2017.

Mediante la Tabla Nro. 13 podemos visualizar que el 96.00% de encuestados revelaron que NO están satisfechos con las circunstancias actuales en la empresa, por lo tanto, el 4.00% de los trabajadores encuestados indicó que sí.

Gráfico Nro. 4: Nivel Satisfacción de las circunstancias actuales

Nivel de Satisfacción de las circunstancias actuales; respecto a la Implementación de Hacking Ético para la Detección y Evaluación de Vulnerabilidades de Red en la Empresa Complex del Perú S.A.C.- Tumbes; 2017.



Fuente: Tabla Nro. 13.

4.1.2. Dimensión 02: Necesidad de Implementación de hacking ético

Tabla Nro. 14: Solución a la vulnerabilidad de red

Distribución de las frecuencias y respuestas relacionadas sobre el hacking ético ayudará a solucionar la vulnerabilidad de la red; respecto a la Implementación de Hacking Ético para la Detección y Evaluación de Vulnerabilidades de Red en la Empresa Complex del Perú S.A.C.-Tumbes; 2017.

Alternativas	n	%
SI	23	96.00
NO	1	4.00
Total	24	100.00

Fuente: Cuestionario aplicado al personal de la Empresa Complex del Perú S.A.C.-Tumbes; 2017.; para alegar a la interrogante: ¿Cree usted que el hacking ético solucionará la vulnerabilidad de la red?

Aplicado por: Bermeo, J.; 2017.

Mediante la Tabla Nro. 14 podemos visualizar que el 96.00% de encuestados revelaron que, SI creen que el hacking ético solucionará la vulnerabilidad de la red, por lo tanto, el 4.00% de los trabajadores encuestados indicó que no.

Tabla Nro. 15: Empresas con hacking ético

Distribución de las frecuencias y respuestas relacionadas sobre las demás empresas si cuentan con hacking ético; respecto a la Implementación de Hacking Ético para la Detección y Evaluación de Vulnerabilidades de Red en la Empresa Complex del Perú S.A.C.-Tumbes; 2017.

Alternativas	n	%
SI	19	79.00
NO	5	21.00
Total	24	100.00

Fuente: Cuestionario aplicado al personal de la Empresa Complex del Perú S.A.C.-Tumbes; 2017.; para alegar a la interrogante: ¿Cree Usted que las demás empresas cuentan con un hacking ético?

Aplicado por: Bermeo, J.; 2017.

Mediante la Tabla Nro. 15 podemos visualizar que el 79.00% de encuestados revelaron que, SI creen que las demás empresas cuentan con un hacking ético, por lo tanto, el 21.00% de los trabajadores encuestados indicó que no.

Tabla Nro. 16: Ahorrar tiempo y dinero

Distribución de las frecuencias y respuestas relacionadas sobre el hacking ético permitirá ahorrar tiempo; respecto a la Implementación de Hacking Ético para la Detección y Evaluación de Vulnerabilidades de Red en la Empresa Complex del Perú S.A.C.-Tumbes; 2017.

Alternativas	n	%
SI	24	100.00
NO	--	--
Total	24	100.00

Fuente: Cuestionario aplicado al personal de la Empresa Complex del Perú S.A.C.-Tumbes; 2017.; para alegar a la interrogante: ¿Usted cree que hacking ético permitirá ahorrar tiempo y dinero en la empresa?

Aplicado por: Bermeo, J.; 2017.

Mediante la Tabla Nro. 16 podemos visualizar que el 100.00% de encuestados revelaron que SI creen que el hacking ético permitirá ahorrar tiempo y dinero en la empresa.

Tabla Nro. 17: Implementación de hacking ético

Distribución de las frecuencias y respuestas relacionadas sobre la implementación de hacking ético en la empresa; respecto a la Implementación de Hacking Ético para la Detección y Evaluación de Vulnerabilidades de Red en la Empresa Complex del Perú S.A.C.-Tumbes; 2017.

Alternativas	n	%
SI	24	100.00
NO	--	--
Total	24	100.00

Fuente: Cuestionario aplicado al personal de la Empresa Complex del Perú S.A.C.-Tumbes; 2017.; para alegar a la interrogante: ¿Usted está de acuerdo con la implementación de hacking ético en la empresa?

Aplicado por: Bermeo, J.; 2017.

Mediante la Tabla Nro. 17 podemos visualizar que el 100.00% de encuestados revelaron que SI están de acuerdo con la implementación de hacking ético en la empresa.

Tabla Nro. 18: Manejo del hacking ético

Distribución de las frecuencias y respuestas relacionadas sobre el manejo factible del hacking ético ayudará a solucionar la vulnerabilidad de la red; respecto a la Implementación de Hacking Ético para la Detección y Evaluación de Vulnerabilidades de Red en la Empresa Complex del Perú S.A.C.-Tumbes; 2017.

Alternativas	n	%
SI	22	92.00
NO	2	8.00
Total	24	100.00

Fuente: Cuestionario aplicado al personal de la Empresa Complex del Perú S.A.C.-Tumbes; 2017.; para alegar a la interrogante: ¿Usted considera factible el manejo de hacking ético?

Aplicado por: Bermeo, J.; 2017.

Mediante la Tabla Nro. 18 podemos visualizar que el 92.00% de encuestados revelaron que, SI consideran factible el manejo del hacking ético, por lo tanto, el 8.00% de los trabajadores encuestados indicó que no.

Tabla Nro. 19: Clientes beneficiados

Distribución de las frecuencias y respuestas relacionadas sobre el hacking ético en beneficio a los clientes; respecto a la Implementación de Hacking Ético para la Detección y Evaluación de Vulnerabilidades de Red en la Empresa Complex del Perú S.A.C.-Tumbes; 2017.

Alternativas	n	%
SI	24	100.00
NO	--	--
Total	24	100.00

Fuente: Cuestionario aplicado al personal de la Empresa Complex del Perú S.A.C.-Tumbes; 2017.; para alegar a la interrogante: ¿De acuerdo a su opinión, los clientes serán beneficiados con la implementación del hacking ético?

Aplicado por: Bermeo, J.; 2017.

Mediante la Tabla Nro. 19 podemos visualizar que el 100.00% de encuestados revelaron que SI serán beneficiados los clientes con la implementación del hacking ético.

Tabla Nro. 20: Presentación de hacking ético

Distribución de las frecuencias y respuestas relacionadas sobre la presentación de hacking ético; respecto a la Implementación de Hacking Ético para la Detección y Evaluación de Vulnerabilidades de Red en la Empresa Complex del Perú S.A.C.-Tumbes; 2017.

Alternativas	n	%
SI	24	100.00
NO	--	--
Total	24	100.00

Fuente: Cuestionario aplicado al personal de la Empresa Complex del Perú S.A.C.-Tumbes; 2017.; para alegar a la interrogante: ¿Estaría de acuerdo que hacking ético tenga presentación activa y fascinante?

Aplicado por: Bermeo, J.; 2017.

Mediante la Tabla Nro. 20 podemos visualizar que el 100.00% de encuestados revelaron que SI están de acuerdo que el hacking ético tenga presentación activa y fascinante.

Tabla Nro. 21: Alternativa correcta

Distribución de las frecuencias y respuestas relacionadas sobre los trabajadores que estén de acuerdo con la implementación de hacking ético; respecto a la Implementación de Hacking Ético para la Detección y Evaluación de Vulnerabilidades de Red en la Empresa Complex del Perú S.A.C.-Tumbes; 2017.

Alternativas	n	%
SI	23	96.00
NO	1	4.00
Total	24	100.00

Fuente: Cuestionario aplicado al personal de la Empresa Complex del Perú S.A.C.-Tumbes; 2017.; para alegar a la interrogante: ¿Considera usted que todos los trabajadores estarán de acuerdo con la implementación de hacking ético?

Aplicado por: Bermeo, J.; 2017.

Mediante la Tabla Nro. 21 podemos visualizar que el 96.00% de encuestados revelaron que, SI están de acuerdo los trabajadores con la implementación de hacking ético, por lo tanto, el 4.00% de los trabajadores encuestados indicó que no.

Tabla Nro. 22: Hacking ético para la seguridad

Distribución de las frecuencias y respuestas relacionadas sobre el hacking ético recomendarlo a otras empresas para la seguridad; respecto a la Implementación de Hacking Ético para la Detección y Evaluación de Vulnerabilidades de Red en la Empresa Complex del Perú S.A.C.-Tumbes; 2017.

Alternativas	n	%
SI	24	100.00
NO	--	--
Total	24	100.00

Fuente: Cuestionario aplicado al personal de la Empresa Complex del Perú S.A.C.-Tumbes; 2017.; para alegar a la interrogante: ¿Recomendaría a otras empresas utilizar hacking ético para la seguridad?

Aplicado por: Bermeo, J.; 2017.

Mediante la Tabla Nro. 22 podemos visualizar que el 100.00% de encuestados revelaron que SI recomendarían a otras empresas la implementación de hacking ético para obtener seguridad en la información.

Tabla Nro. 23: Beneficios a la empresa

Distribución de las frecuencias y respuestas relacionadas sobre el hacking ético que presenta diversos beneficios en la empresa; respecto a la Implementación de Hacking Ético para la Detección y Evaluación de Vulnerabilidades de Red en la Empresa Complex del Perú S.A.C.-Tumbes; 2017.

Alternativas	n	%
SI	22	92.00
NO	2	8.00
Total	24	100.00

Fuente: Cuestionario aplicado al personal de la Empresa Complex del Perú S.A.C.-Tumbes; 2017.; para alegar a la interrogante: ¿Cree usted que la propuesta presentará gratos beneficios a la empresa?

Aplicado por: Bermeo, J.; 2017.

Mediante la Tabla Nro. 23 podemos visualizar que el 92.00% de encuestados revelaron que, SI creen que la propuesta planteada presentará gratos beneficios a la empresa, por lo tanto, el 8.00% de los trabajadores encuestados indicó que no.

Resumen de 2° Dimensión

Tabla Nro. 24: Necesidad de la Implementación hacking ético

Necesidad de la Implementación hacking ético, respecto a la Implementación de Hacking Ético para la Detección y Evaluación de Vulnerabilidades de Red en la Empresa Complex del Perú S.A.C.-Tumbes; 2017.

Alternativas	n	%
SI	24	100.00
NO	--	--
Total	24	100.00

Fuente: Aplicación del cuestionario para medir la Dimensión: Necesidad de la Implementación hacking ético, basado en diez interrogantes aplicadas al personal de la Empresa Complex del Perú S.A.C.-Tumbes; 2017.

Aplicado por: Bermeo, J.; 2017.

Mediante la Tabla Nro. 24 podemos visualizar que el 100.00% de encuestados revelaron que SI necesitan de la implementación de hacking ético para la seguridad de información en la empresa.

Tabla Nro. 25: Resumen General por Dimensiones

Nivel de satisfacción y necesidad de la implementación de hacking ético, respecto a la Implementación de Hacking Ético para la Detección y Evaluación de Vulnerabilidades de Red en la Empresa Complex del Perú S.A.C.-Tumbes; 2017.

DIMENSIONES	ALTERNATIVAS DE RESPUESTAS				TOTAL MUESTRA	
	SI	%	NO	%	n	%
Satisfacción de las circunstancias actuales	1	4.00	23	96.00	24	100.00
Necesidad de la implementación de hacking ético	24	100.00	--	--	24	100.00

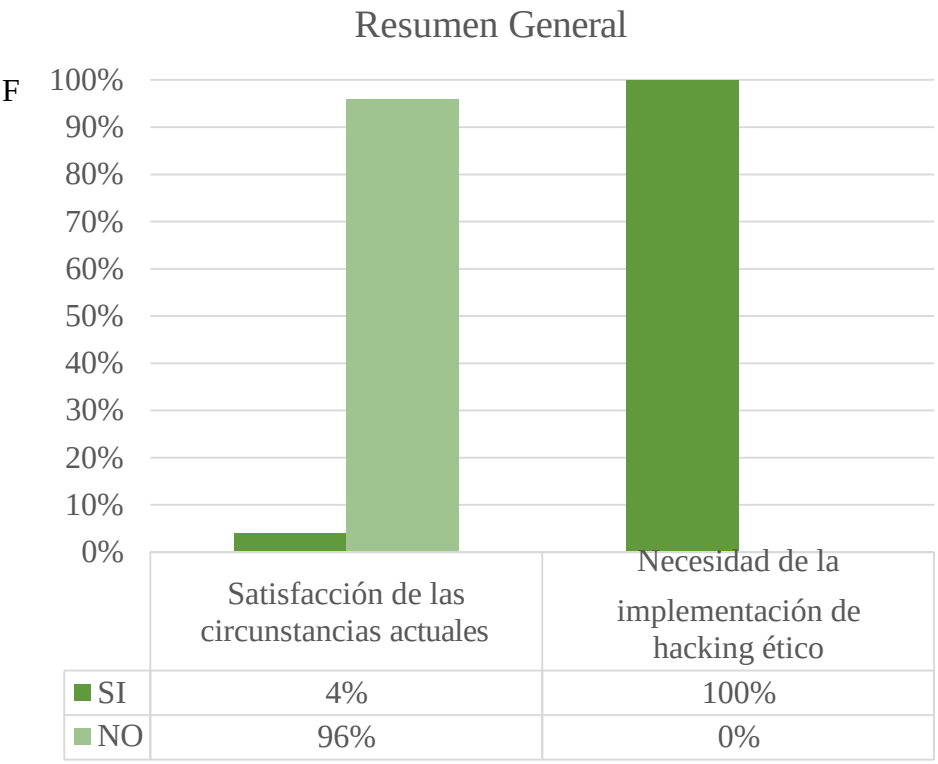
Fuente: Aplicación del cuestionario sobre las dos dimensiones: satisfacción de las circunstancias actuales y necesidad de implementación de hacking ético, basado en diez preguntas aplicadas al personal de la Empresa Complex del Perú S.A.C.-Tumbes; 2017.

Aplicado por: Bermeo, J.; 2017.

Mediante la Tabla Nro. 25 podemos visualizar que en la primera dimensión el 96.00% de los encuestados no están satisfechos con las circunstancias actuales, en la segunda dimensión el 100.00% de los encuestados expresaron que SI necesitan la propuesta de la implementación de hacking ético para seguridad en la empresa.

Gráfico Nro. 5: Resumen general de dimensiones

Nivel de satisfacción y necesidad de la implementación de hacking ético, respecto a la Implementación de Hacking Ético para la Detección y Evaluación de Vulnerabilidades de Red en la Empresa Complex del Perú S.A.C.-Tumbes; 2017.



Fuente: Tabla Nro. 25.

4.2. Análisis de Resultados

Se cumplió con la encuesta y el instrumento (cuestionario), lo cual nos ha brindado resultados por parte de los usuarios. Se da a conocer el respectivo análisis de resultados:

1. En la 1° dimensión: Satisfacción de las circunstancias Actuales en la empresa en la Tabla Nro. 25 podemos apreciar que el visualizar y descifrar que el 96.00% de los trabajadores de la Empresa Complex del Perú S.A.C.-Tumbes, concluyeron que las circunstancias actuales son insatisfactorias e inadecuadas, no brindan seguridad a la empresa

como a sus trabajadores, por lo tanto, se determinó la opción de implementación de hacking ético; así mismo el 4 % de los encuestados manifestaron que SI. Este desenlace tiene similitud con las siguientes investigaciones desarrolladas por Muñoz D. [7], además por Mamani T. [8], en relación por sus proyectos y por dimensión coincidente manifiestan completa insatisfacción los usuarios de sus determinaciones diarias en sus instituciones. El tema en relación es sobre hacking ético para evaluación de la vulnerabilidad de la red.

2. En la 2° dimensión: Necesidad de Implementación de hacking ético, mediante la Tabla Nro. 25 apreciamos el resultado que el 100.00% de los empleados de la Empresa Complex del Perú S.A.C.-Tumbes, concluyeron que SI requieren y necesitan la implementación de hacking ético Este desenlace tiene similitud con las siguientes investigaciones desarrolladas por Muñoz D. [7], además por Mamani T. [8], en relación por sus proyectos y por dimensión coincidente remarcaron la alternativa con alto porcentaje de la necesidad de implementación sobre hacking ético en sus instituciones. Es fundamental mantener un orden establecido en sus procesos desarrollados usualmente y corroborar con la protección de información externa e interna por la vulnerabilidad existente de la red en la empresa.

4.3. Propuesta de mejora

Se propone implementación de un SGSI, en base a la norma ISO/IEC 27001:2005 se redacta la documentación de los diseños aplicados y la práctica aplicada.

El cual nos brindara los procedimientos y lineamientos necesarios para identificar y evaluar los riesgos, las amenazas, las vulnerabilidades de los activos de información.

Realizar y plasmar las políticas de seguridad que se respalden en las bases de la seguridad, continuando de las normas y procesos que aplican en detalles técnicos, finalmente todo el desarrollo con modificaciones incluidas en el SGSI quedara plasmado como evidencia del cumplimiento total en el que se incluye:

1. Definición y comunicación de las políticas de seguridad del SGI.
2. Monitoreo de la Base de Datos para la administración de activos de información.
3. Implementación de herramientas tecnológicas con una adecuada configuración de firewall, VPN, etc.
4. Configuración de Directorios Activos para restringir la instalación de programas, entre otros.

4.3.1. Antecedentes

Los correctos procesos de la información de la Empresa Complex del Perú S.A.C – Tumbes cumplen con los aspectos de seguridad estableciendo confidencialidad e integridad de la información, respetando estándares y políticas de la empresa.

La política de seguridad de la información brinda sus aspectos de cumplimiento para la correcta implementación del SGSI. Ninguna

norma o proceso es superior sobre la política de seguridad de la información.

4.3.2. Procedimiento

Para la seguridad informática esta apta la norma ISO/IEC 27001:2005. Realizar los procesos respetándolos principios de seguridad marcados en su política, como lo siguiente:

- **Organización de la seguridad de la información:** marca los puntos para la gestión de seguridad de información externo e interno de la empresa.
- **Gestión de activos de información:** realiza la identificación, evaluación y modificación de la inseguridad de la información.
- **Seguridad del Recurso Humano:** Se establecen reglas para el personal laboral en relación a la seguridad de la información.
- **Seguridad Física y Ambiental:** Cumplir con la instalación correcta de hardware y el funcionamiento de ellos.
- **Gestión de comunicaciones y operaciones:** Especifica los procedimientos operacionales para la protección de la información en su transporte, modificación y almacenamiento tomando medidas de seguridad como antivirus, respaldo, almacenamiento, intercambio de información, gestión de redes entre otras.
- **Control de acceso:** Establecen rigidez para la manipulación de la información, de acuerdo al cargo que manejas se te otorgara la información necesaria.
- **Gestión de continuidad del negocio:** Mantener con firmeza su puesto de trabajo y cumplir con seguridad y en caso contrario de presentar inconvenientes dar solución de inmediata a ello.
- **Cumplimiento:** Asegurar que las políticas de seguridad de información sean cumplidas correctamente como o indican la norma antes mencionada.

4.3.3. Documentos del SGSI

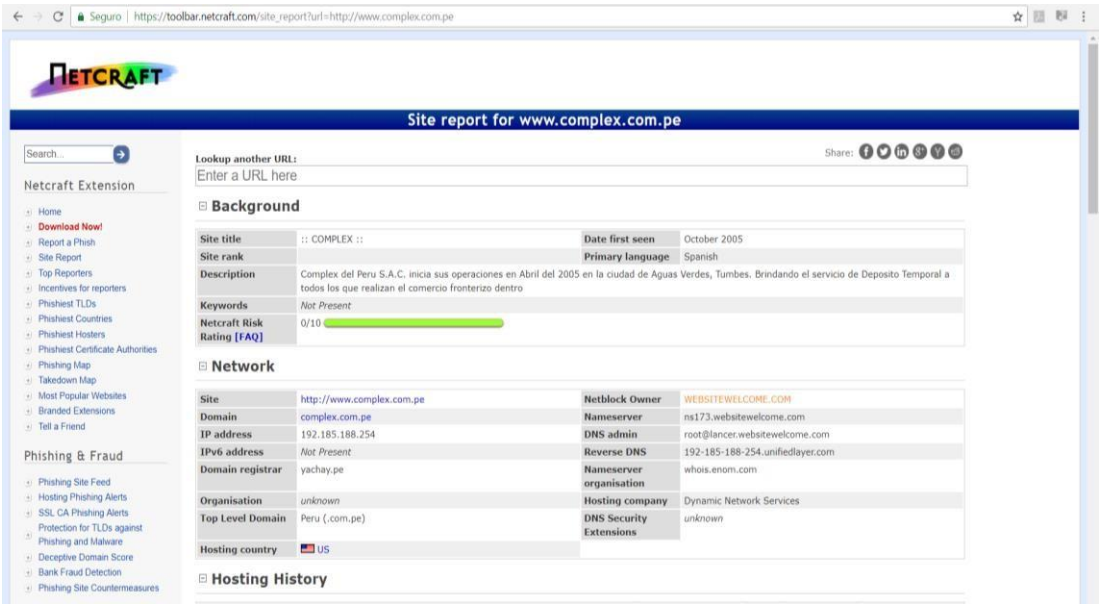
La implementación del SGSI está basado en el cumplimiento por la Norma ISO/IEC 27001:2005. Primeramente, las políticas de seguridad indican cumplir los lineamientos para la elaboración de los siguientes documentos de la implementación. Se detalla a continuación:

- Política de la seguridad de la información
- Normas y procesos de seguridad informática.
- Estándares.
- Registros de seguridad

Gráfico Nro. 6: Evaluación de la empresa Complex del Perú S.A.C

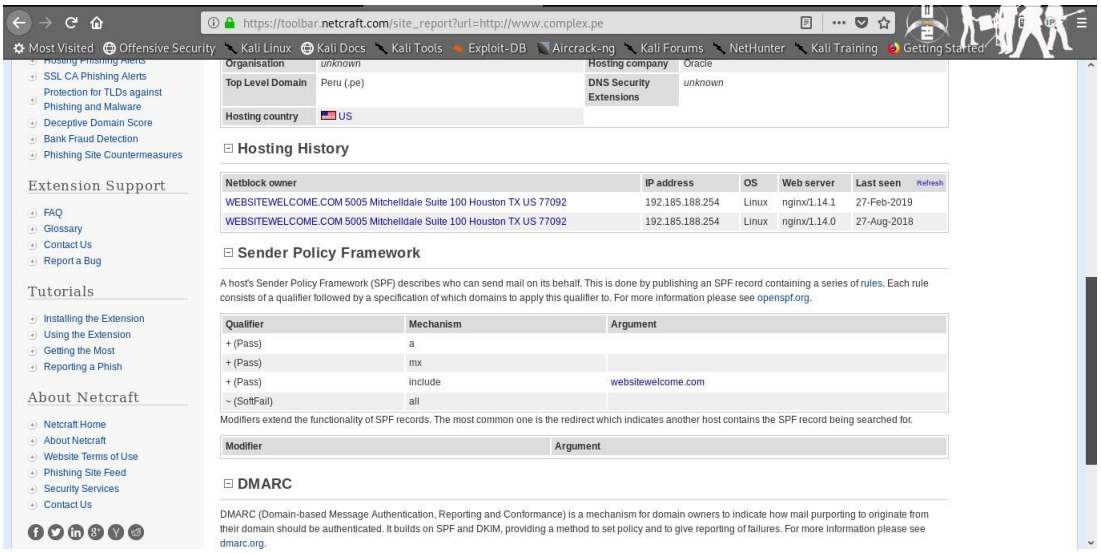
Fuente: Elaboración propia.

Gráfico Nro. 7: Reporte de dominio por netcraft - parte 1



Fuente: Elaboración propia.

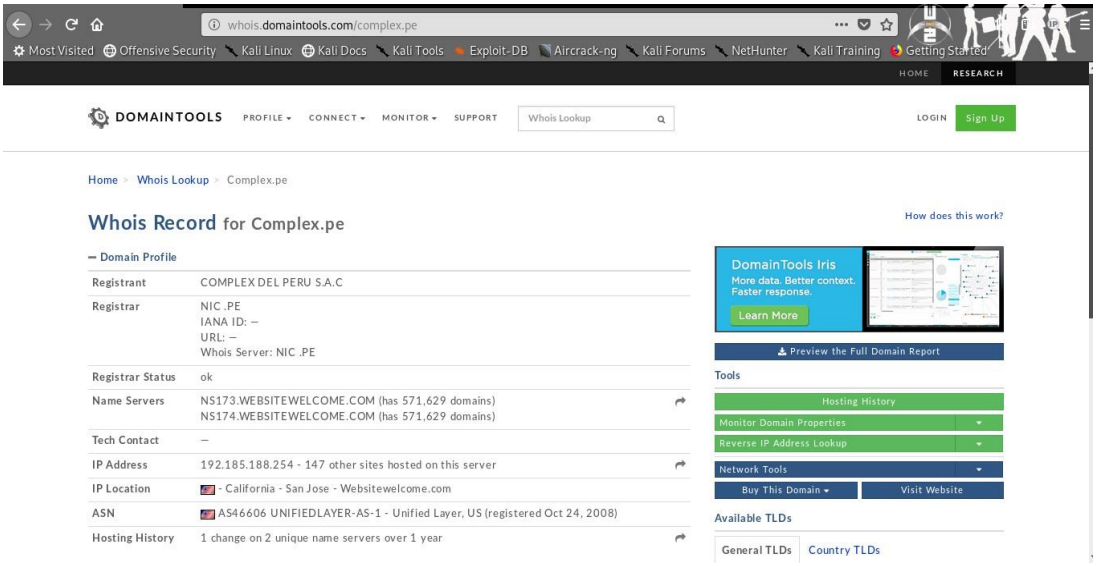
Gráfico Nro. 8: Reporte de dominio por netcraft - parte 2



Fuente: Elaboración propia.

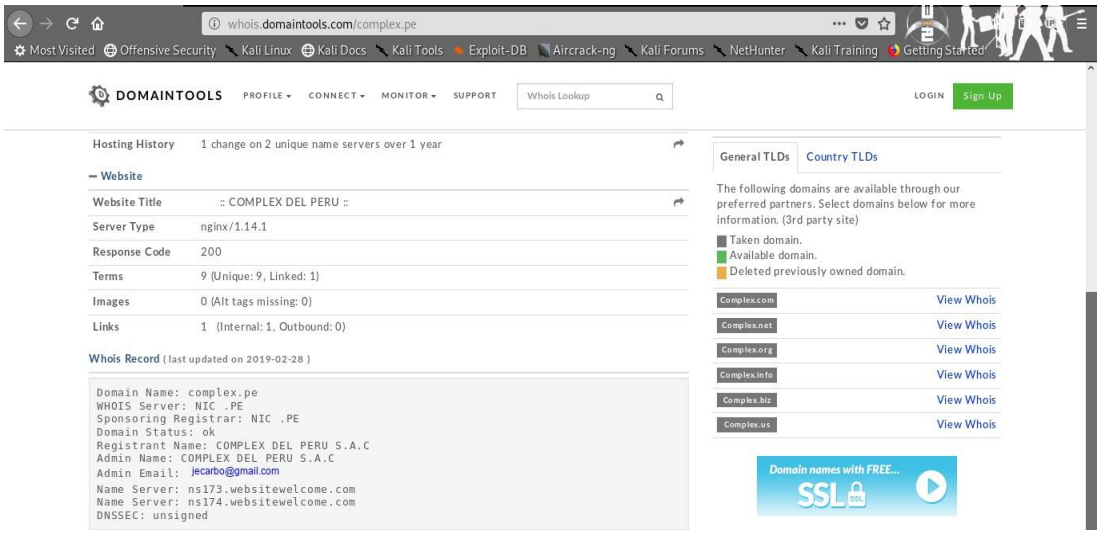
SITIO	DOMINIO	DIRECCION IP	SISTEMA OPERATIVO	SERVIDOR WEB
www.complex.com.pe	www.complex.com.pe	192.185.188.254	linux	nginx

Gráfico Nro. 9: Reporte de dominio por Whois - parte 1



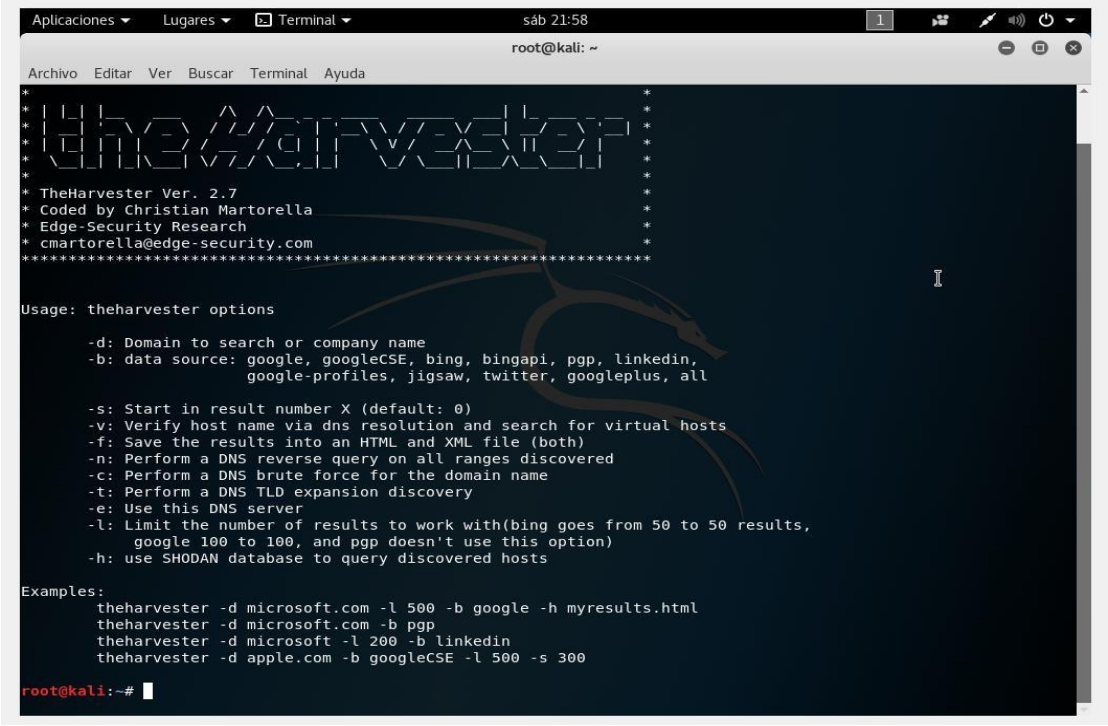
Fuente: Elaboración propia.

Gráfico Nro. 10: Reporte de dominio por Whois - parte 2



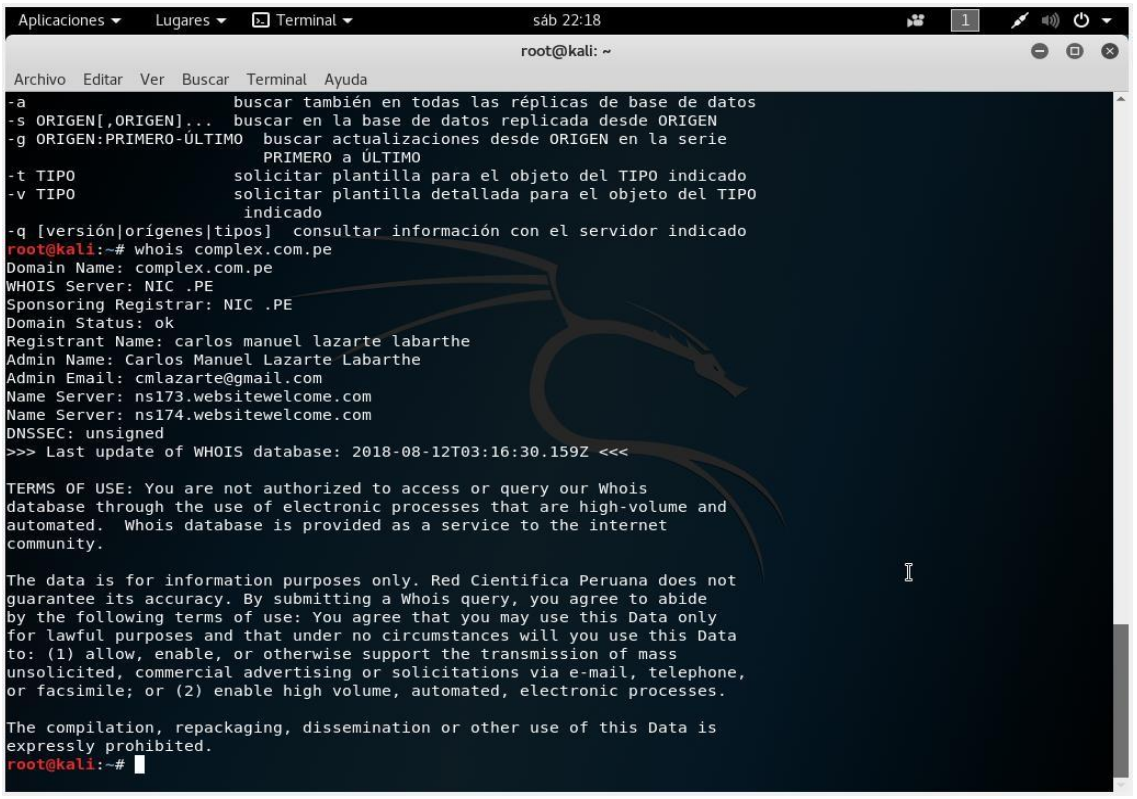
Fuente: Elaboración propia.

Gráfico Nro. 11: Búsqueda en Google, Bing y recopilar información



Fuente: Elaboración propia.

Gráfico Nro. 12: consulta whois al dominio www.complex.com.pe

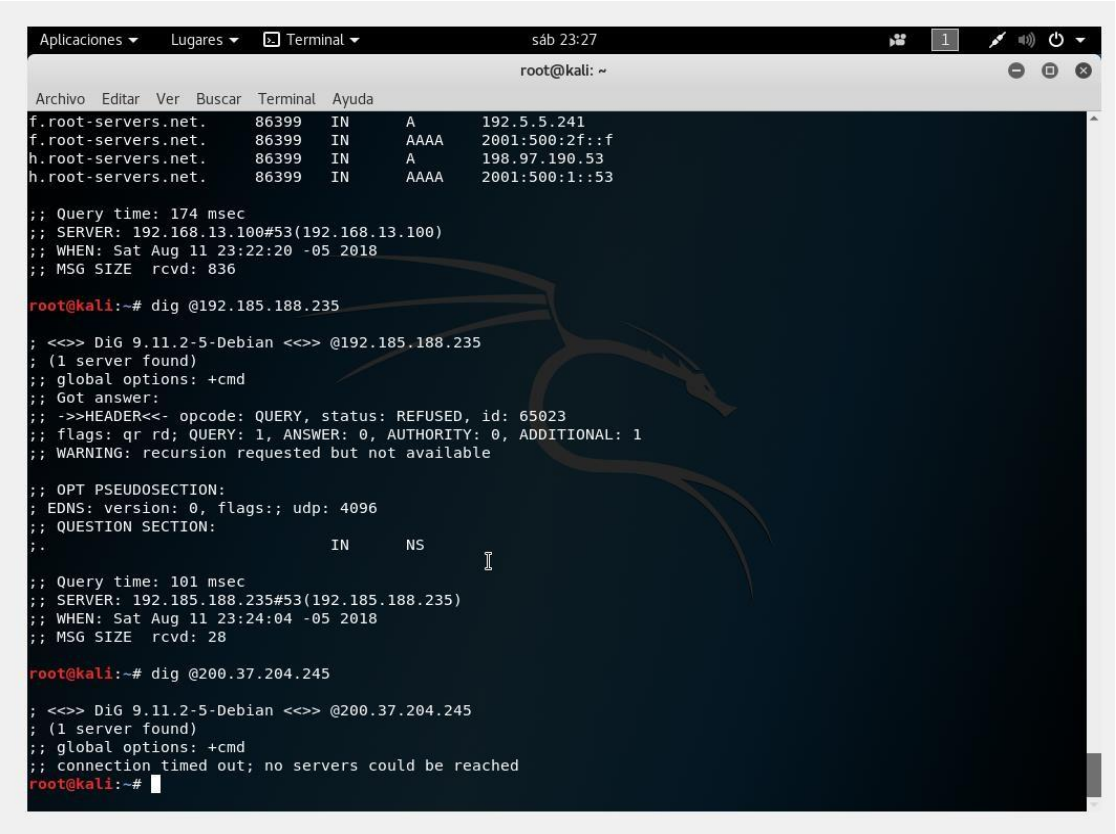


Fuente: Elaboración propia.

Se recopilación de datos:

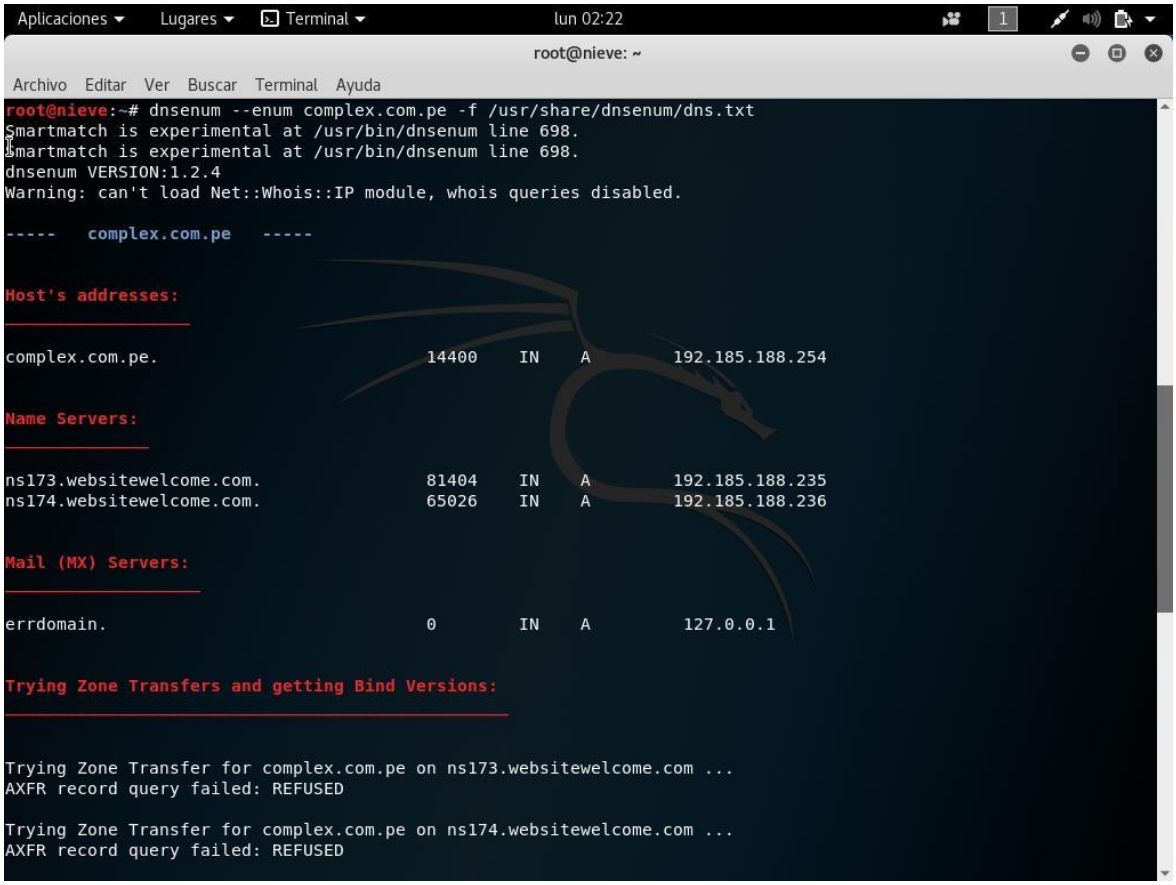
- Nombre de la persona que registro el dominio
- Correo de la persona que registro el dominio
- Nombres de DNS

Gráfico Nro. 13: Dig: Para extraer información de los servidores DNS



Fuente: Elaboración propia.

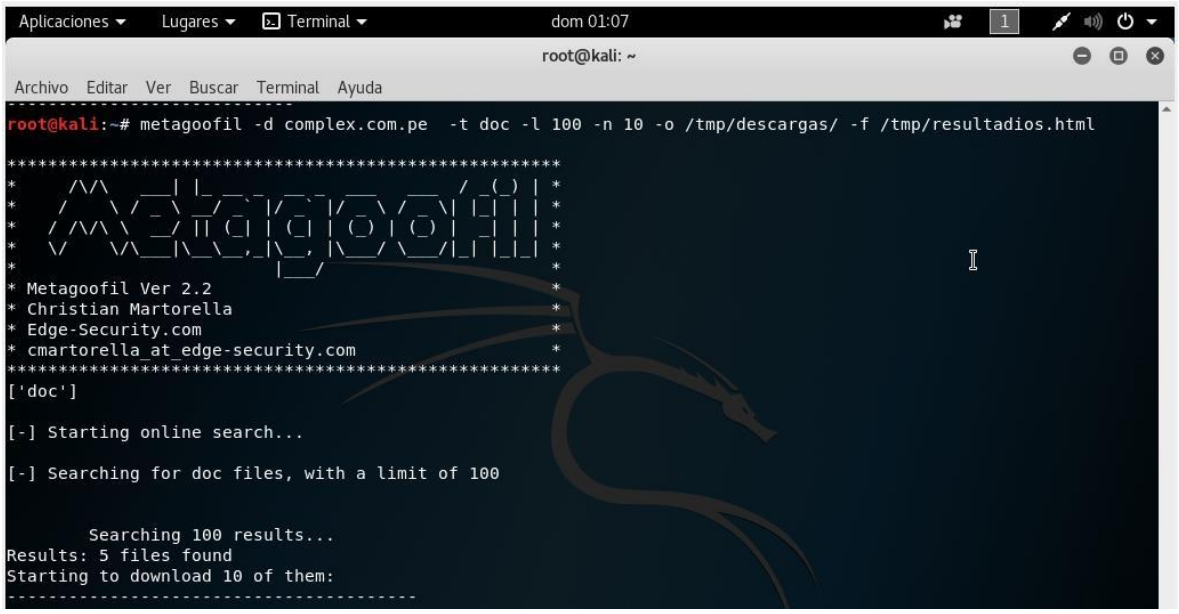
Gráfico Nro. 14: DNSENUM



Fuente: Elaboración propia.

Utilizado para realizar una consulta de subdominios atraves de fuerza bruta, en las imágenes se logra aprecar los resultados que se obtuvieron, ips, servidor de correo, ftp, dns

Gráfico Nro. 15: Metagoofil

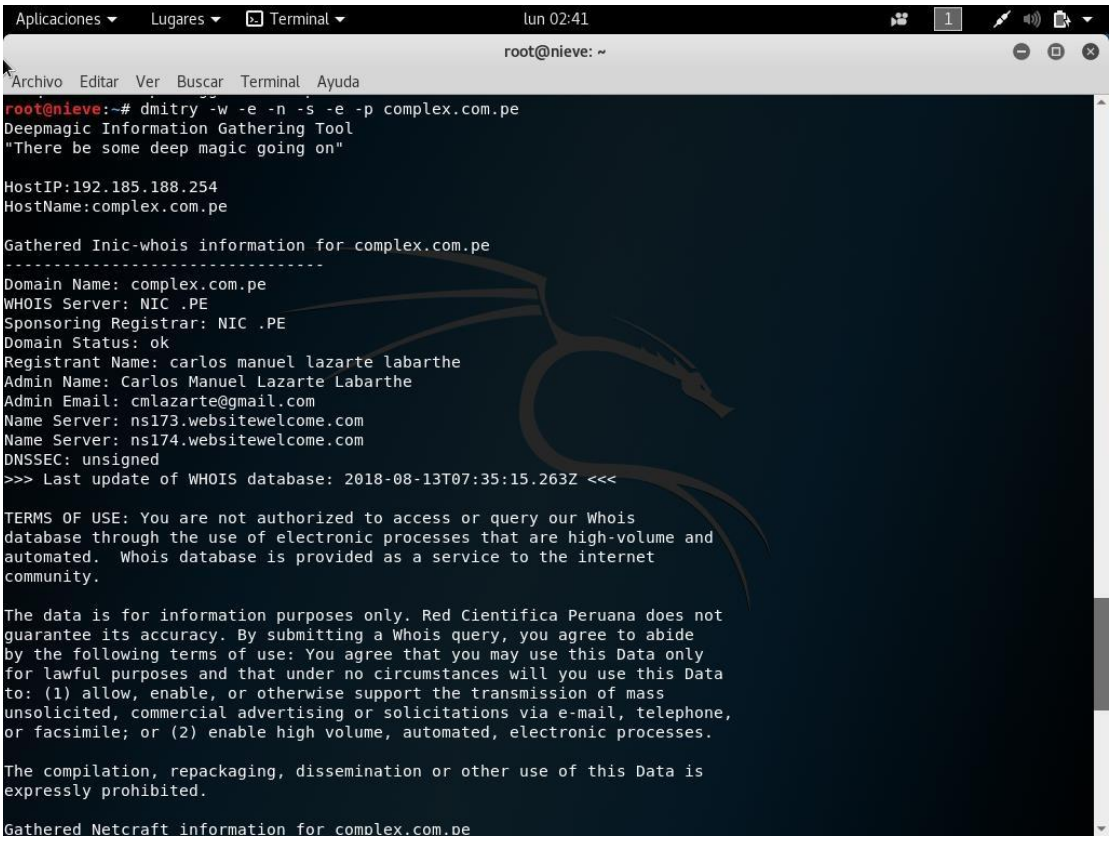


Fuente: Elaboración propia.

Se logra extraer Meta-Data (Datos sobre los Datos), de ciertos ficheros accesibles en los websites de nuestro “objetivo”.

Los ficheros que utiliza son los clásicos utilizados en ofimática PDF,PPT,DOC,XLS y MDB; del Meta-Data obtenido nos interesa sólo ciertos campos.

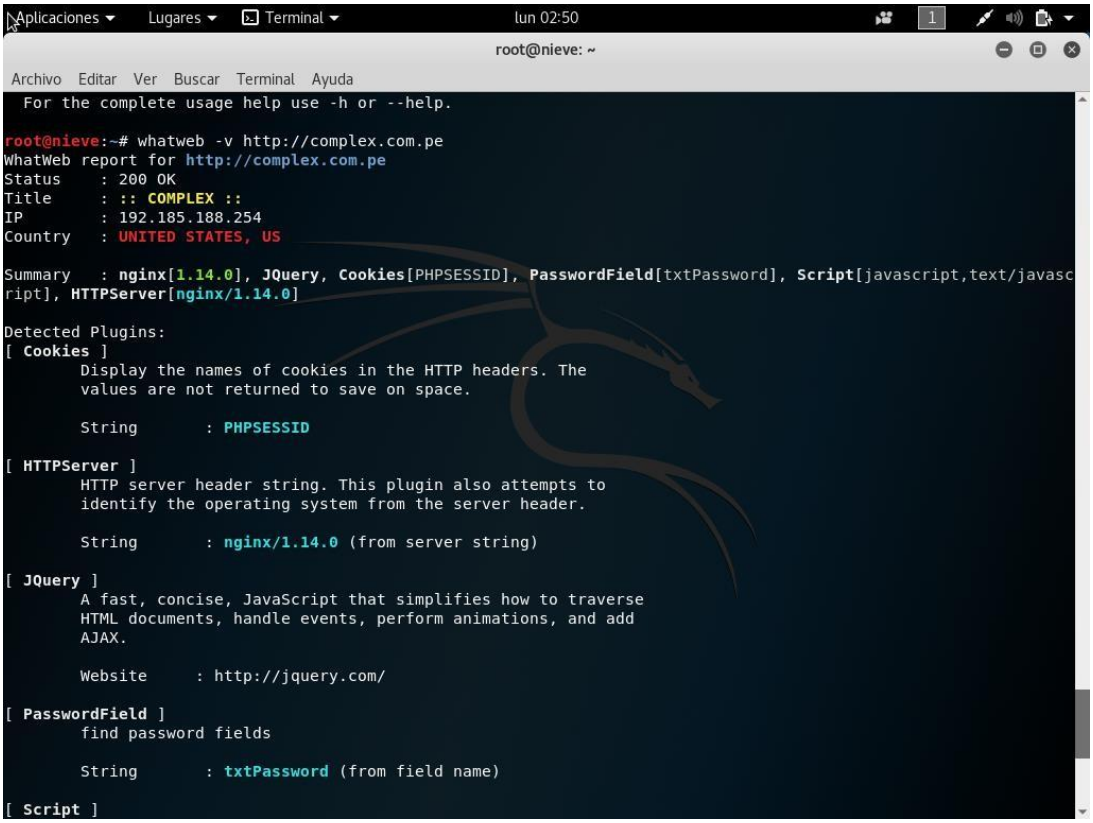
Gráfico Nro. 16: DMITRY



Fuente: Elaboración propia.

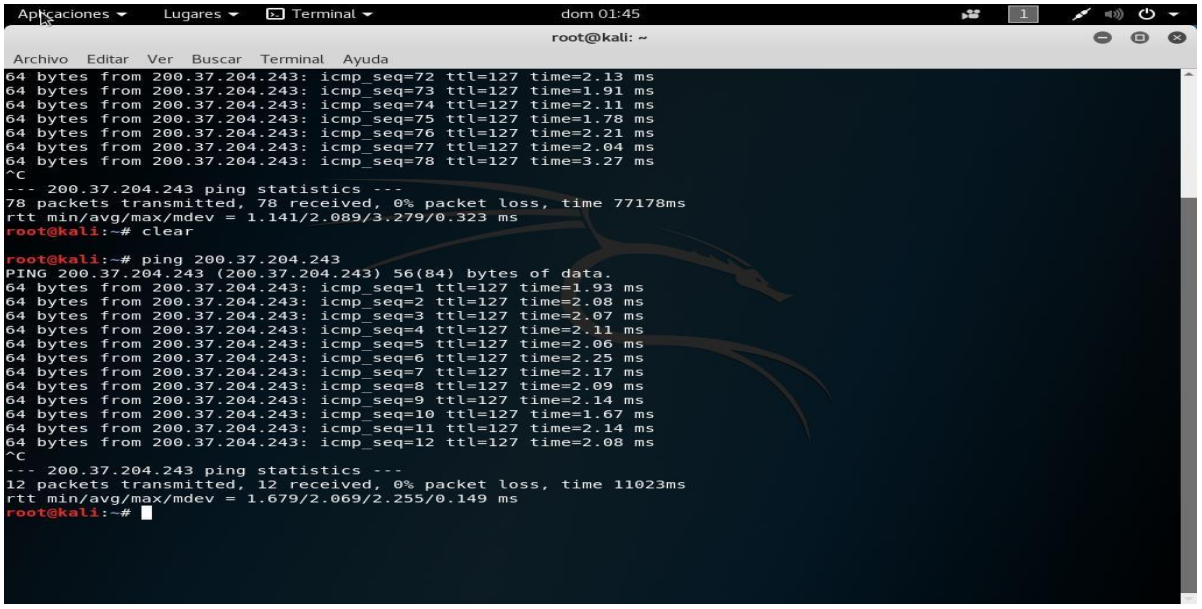
Herramienta que tiene la capacidad de recopilar informacion del objetivo, nos muestra un reporte de los datos del domino, ip y puertos abiertos.

Gráfico Nro. 17: WhatWeb



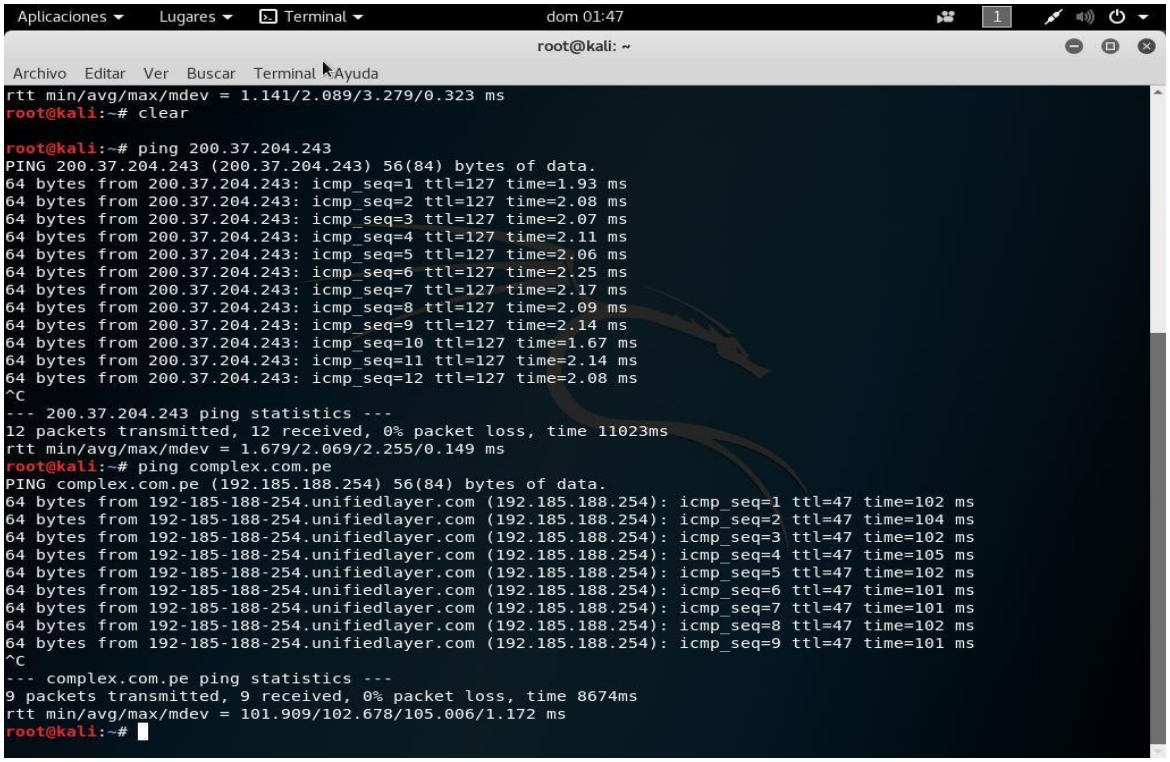
Fuente: Elaboración propia.

Gráfico Nro. 18: Ping Barridos de red



Fuente: Elaboración propia.

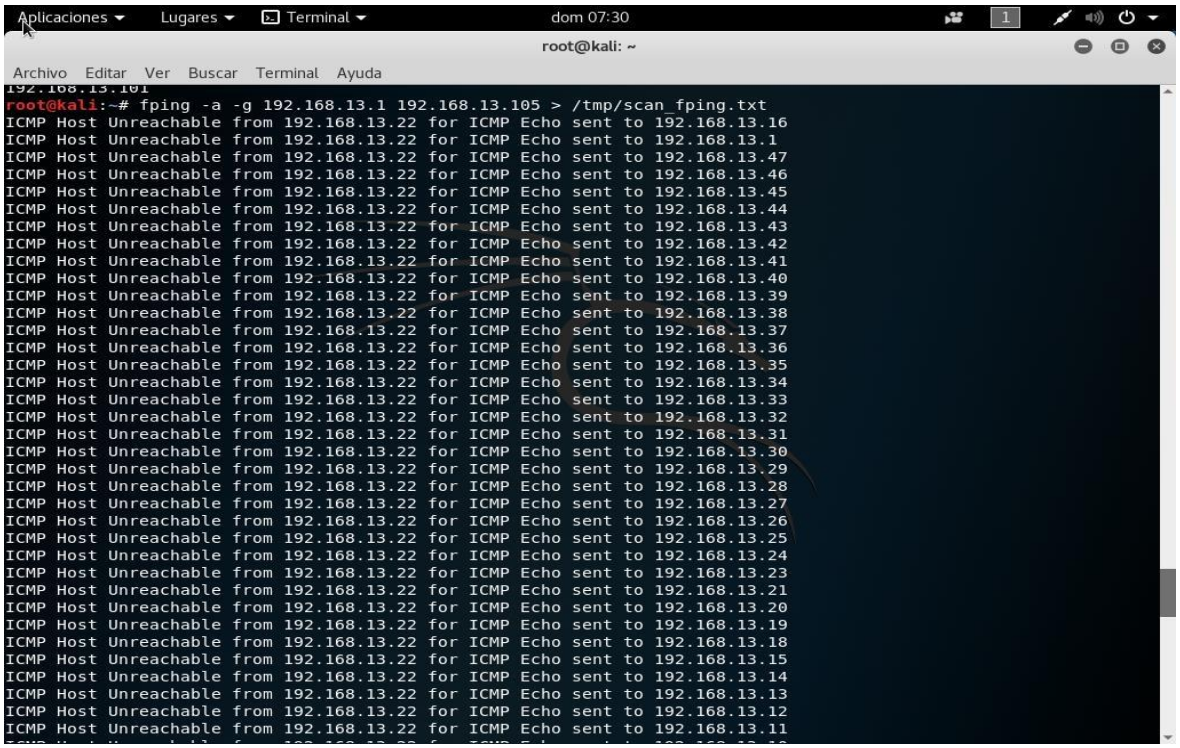
Gráfico Nro. 19: Consulta ping al servidor de BD



Fuente: Elaboración propia.

Consulta ping al dominio www.complex.com.pe

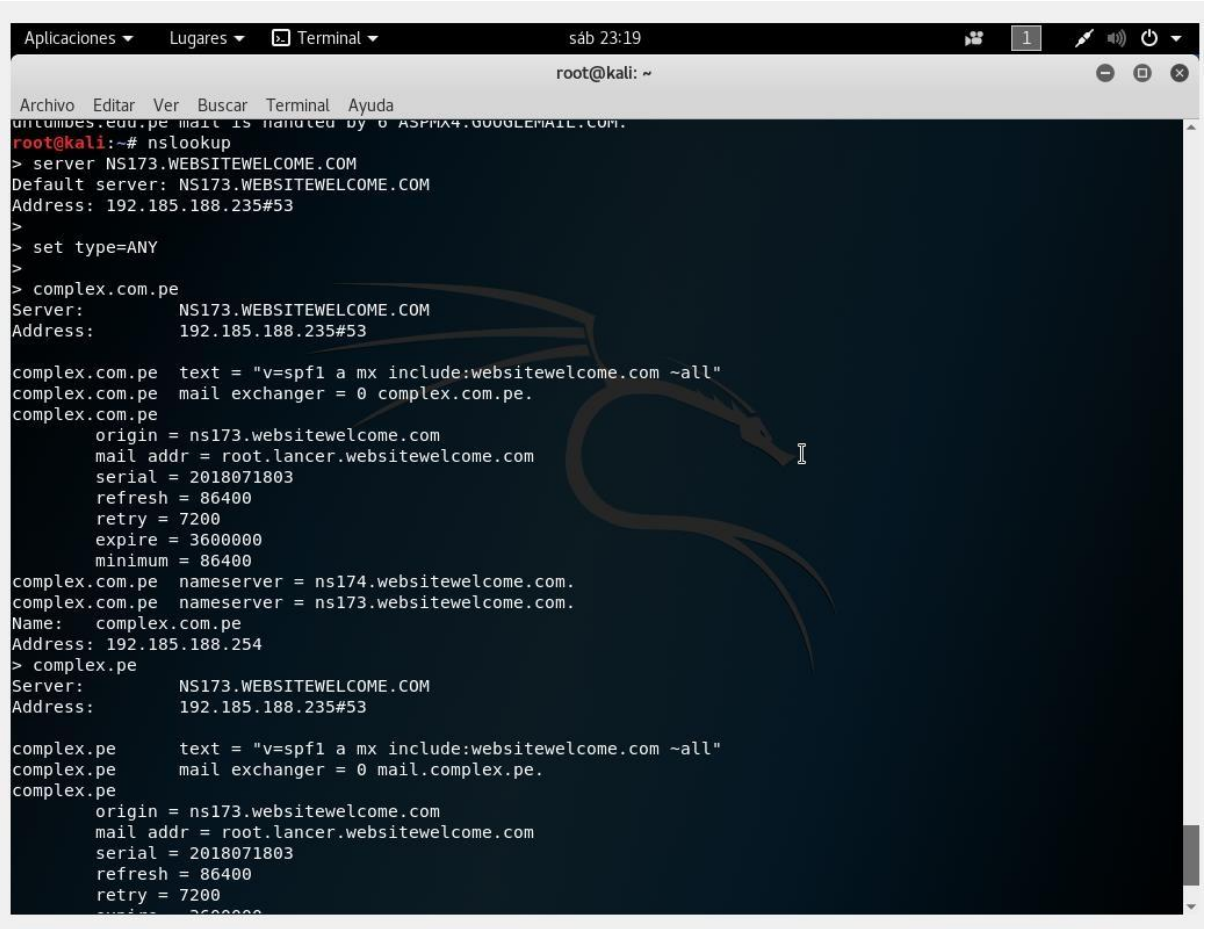
Gráfico Nro. 20: Fping



Fuente: Elaboración propia.

Para determinar si un objetivo responde. fping difiere de ping en la especificación de cualquier número de objetivos en la línea de comando, o especificar un archivo conteniendo una lista de objetivos a los cuales hacer ping.

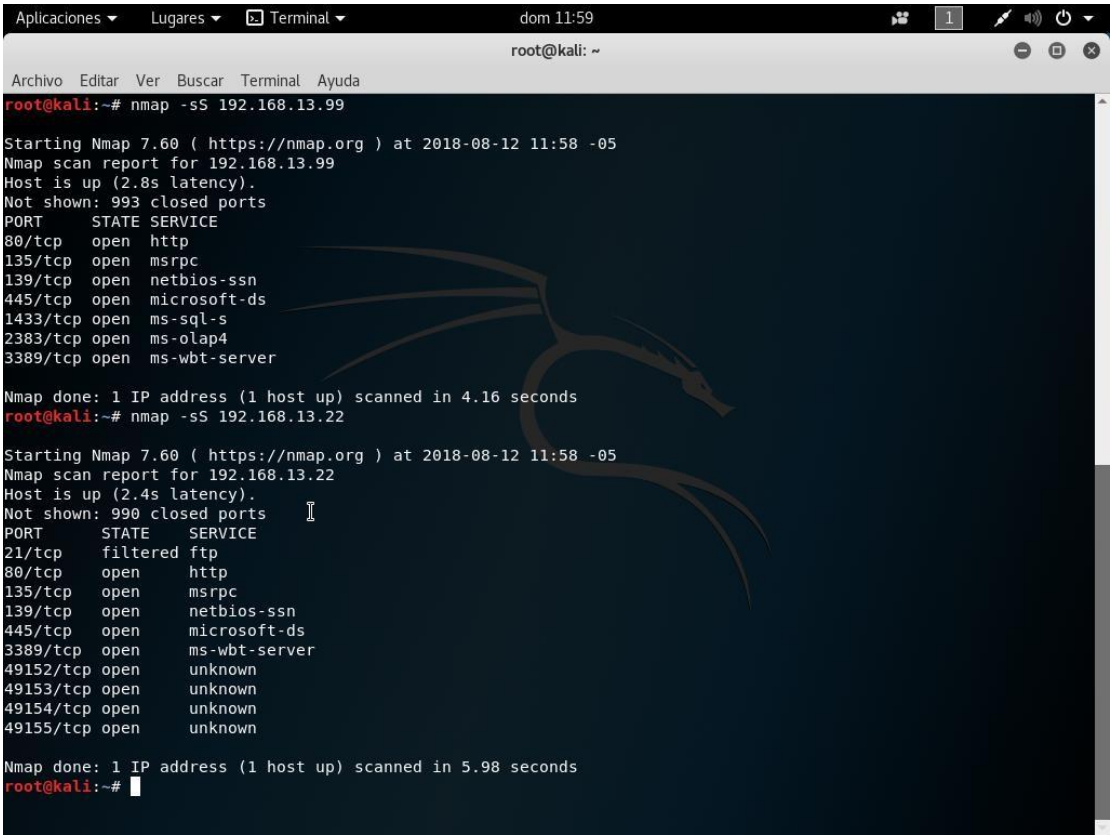
Gráfico Nro. 21: NSLOOKUP



Fuente: Elaboración propia.

Permite consultar un servidor de nombre y obtener informacion, acerca del domino, en la imagen apreciamos los resultados obtenidos

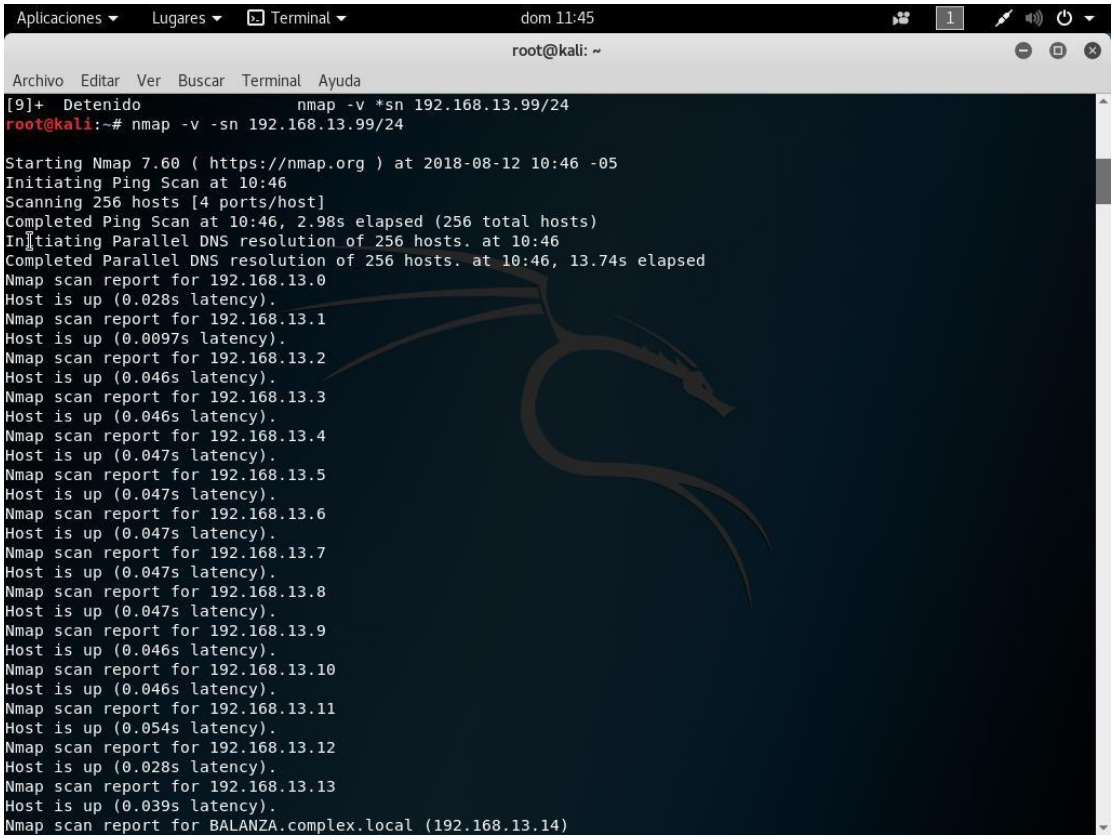
Gráfico Nro. 22: Nmap



Fuente: Elaboración propia.

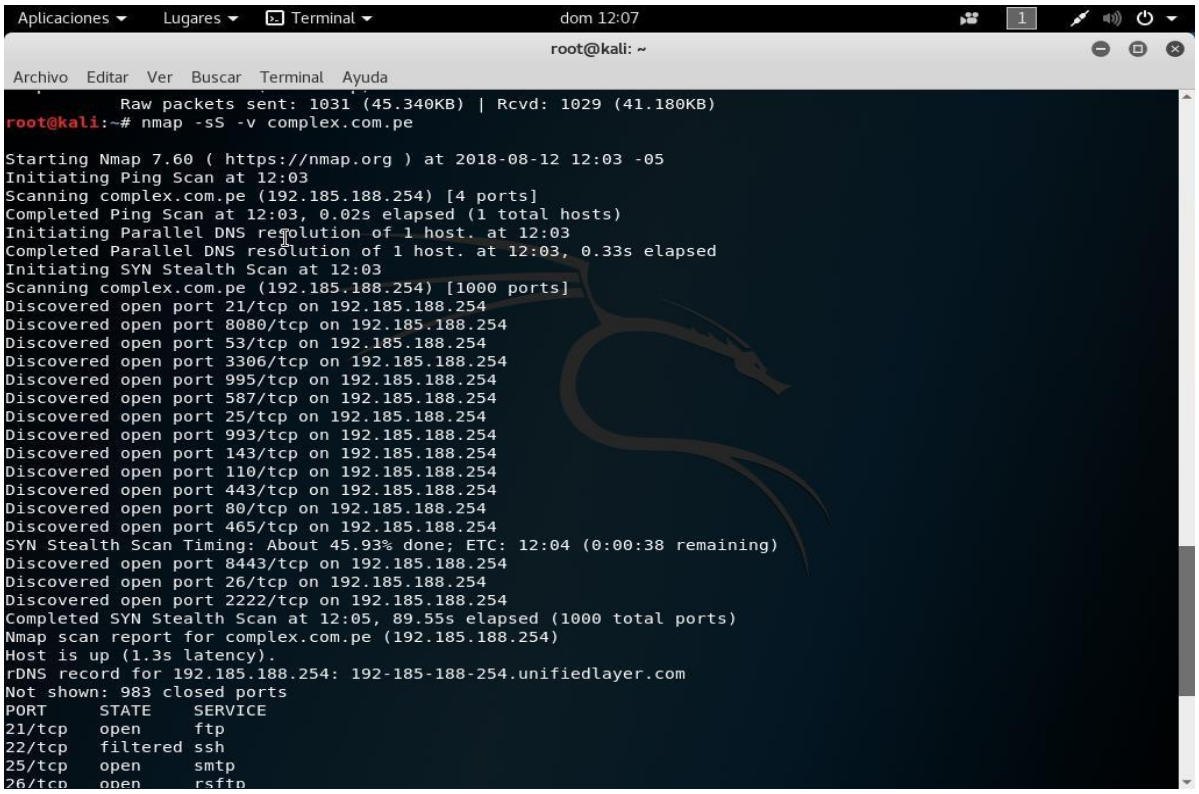
Para efectuar rastreo de puerto, escaneamos la siguiente direccion IP, y nos muestra la lista de los puertos que se encuentran abiertos.

Gráfico Nro. 23: Consulta de NMAP a un rango de direcciones IP



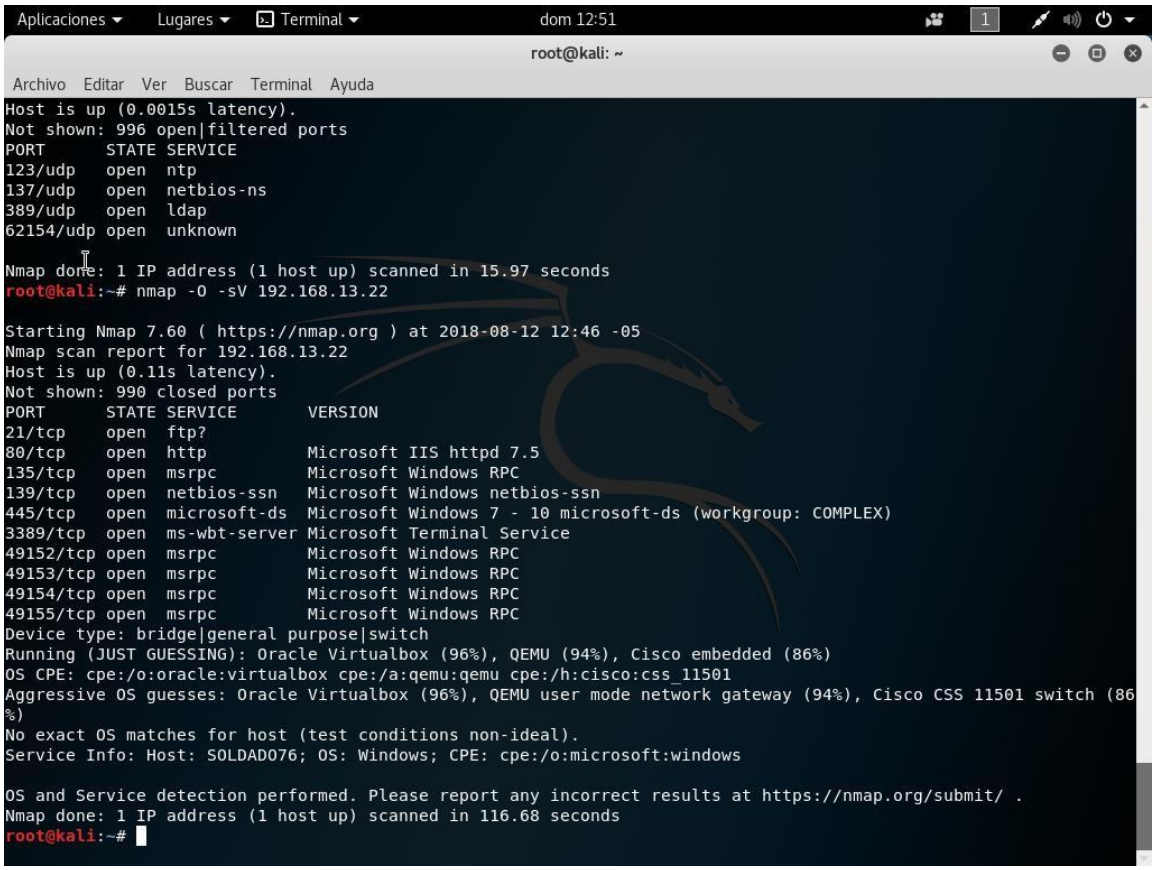
Fuente: Elaboración propia.

Gráfico Nro. 24: Escaneo de Puertos Abiertos



Fuente: Elaboración propia.

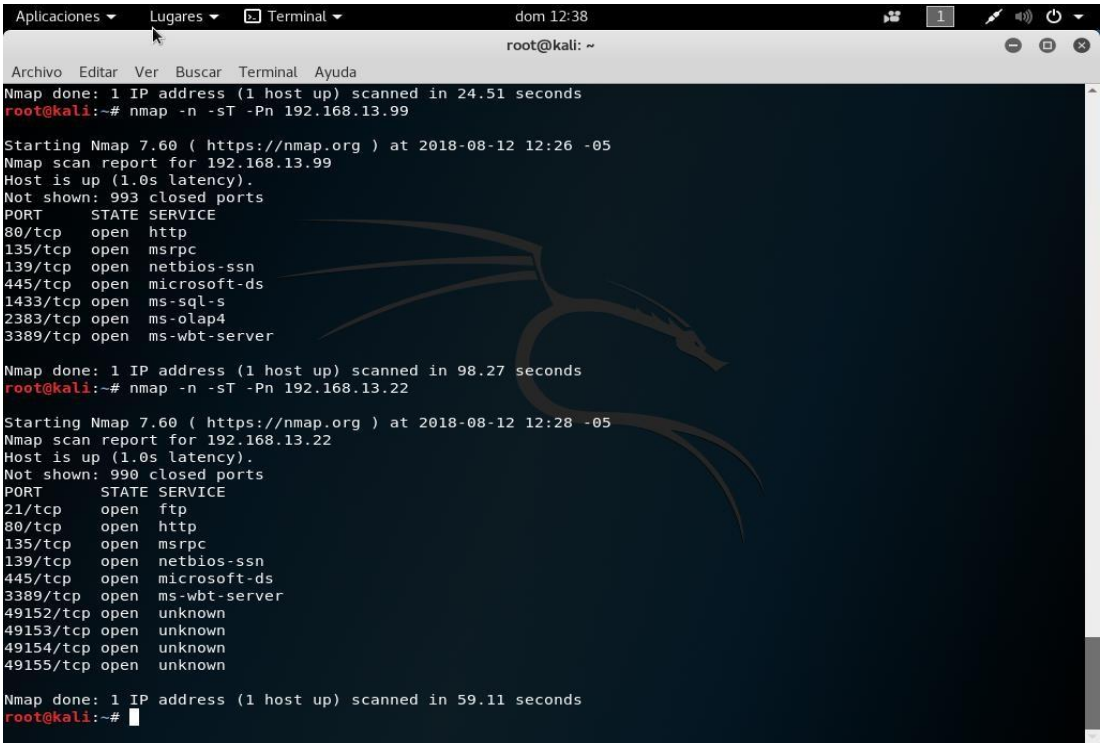
Gráfico Nro. 25: Escaneo de una dirección IP



Fuente: Elaboración propia.

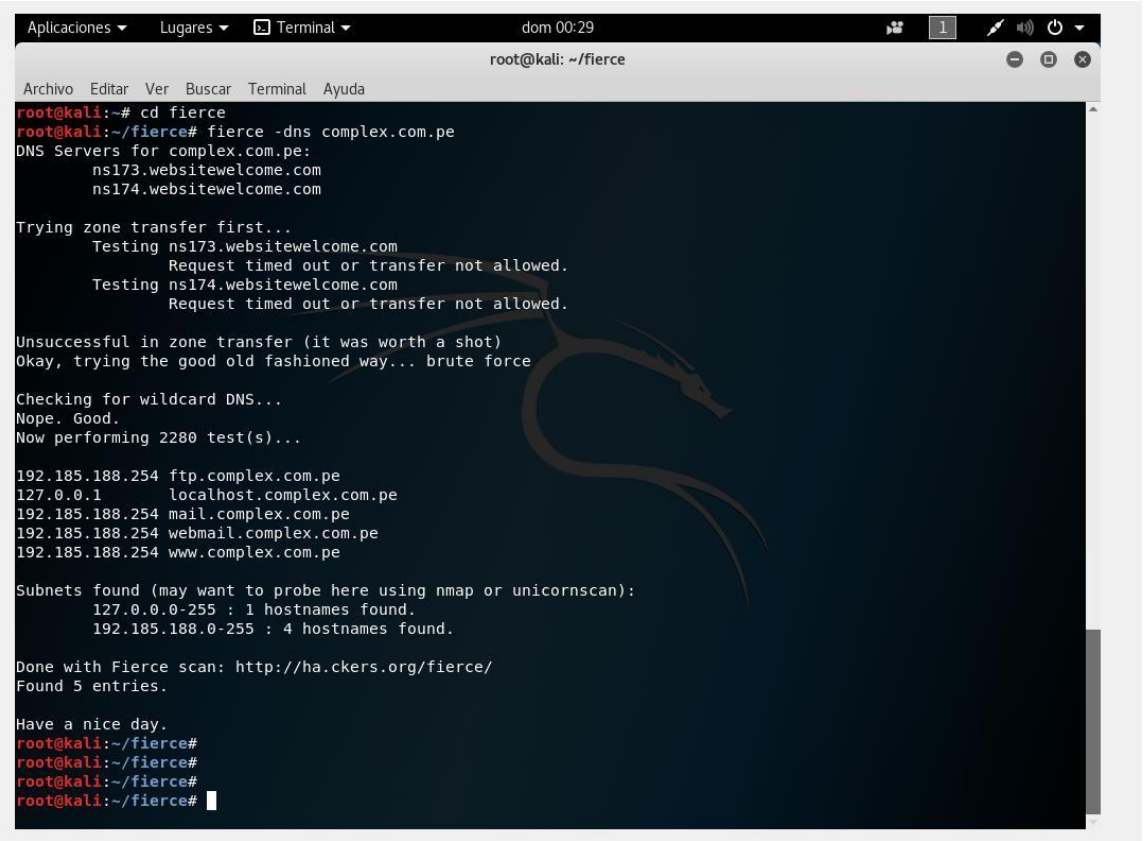
La cual nos muestra los puertos abiertos y el sistema operativo que está usando.

Gráfico Nro. 26: Escaneo de Puertos TCP y UDP



Fuente: Elaboración propia.

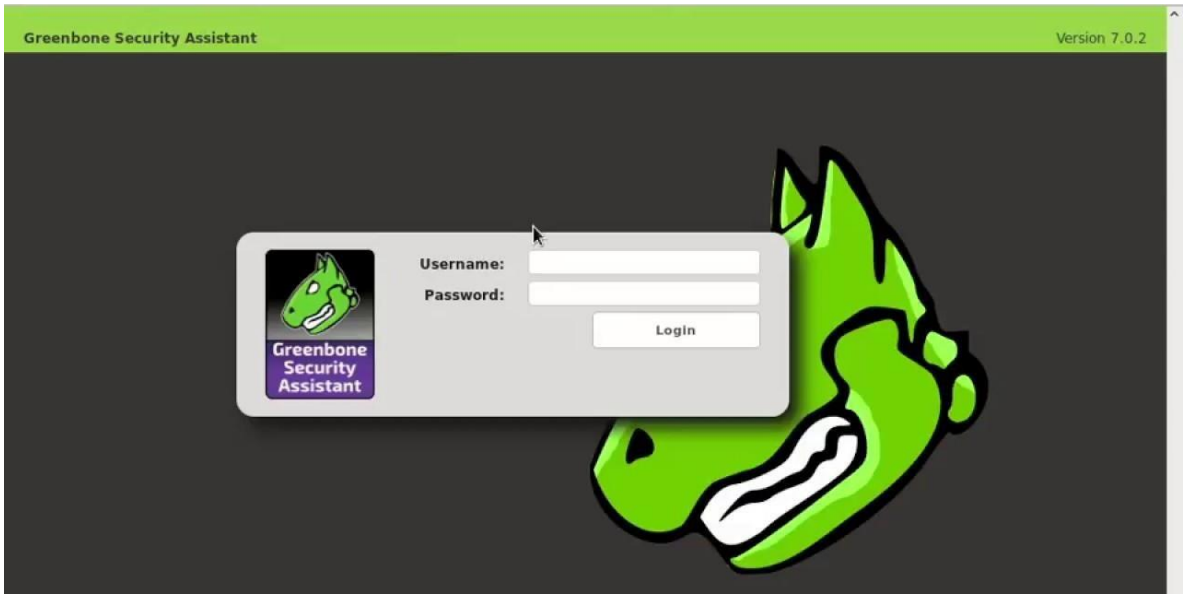
Gráfico Nro. 27: Fierce



Fuente: Elaboración propia.

Consulta de dominio usando fierce, se logra obtener direcciones ip, dominio, dns, servidor de correo y ftp.

Gráfico Nro. 28: Escaneo de Vulnerabilidades



Fuente: Elaboración propia.

Open Vas

Pantalla de inicio de openvas

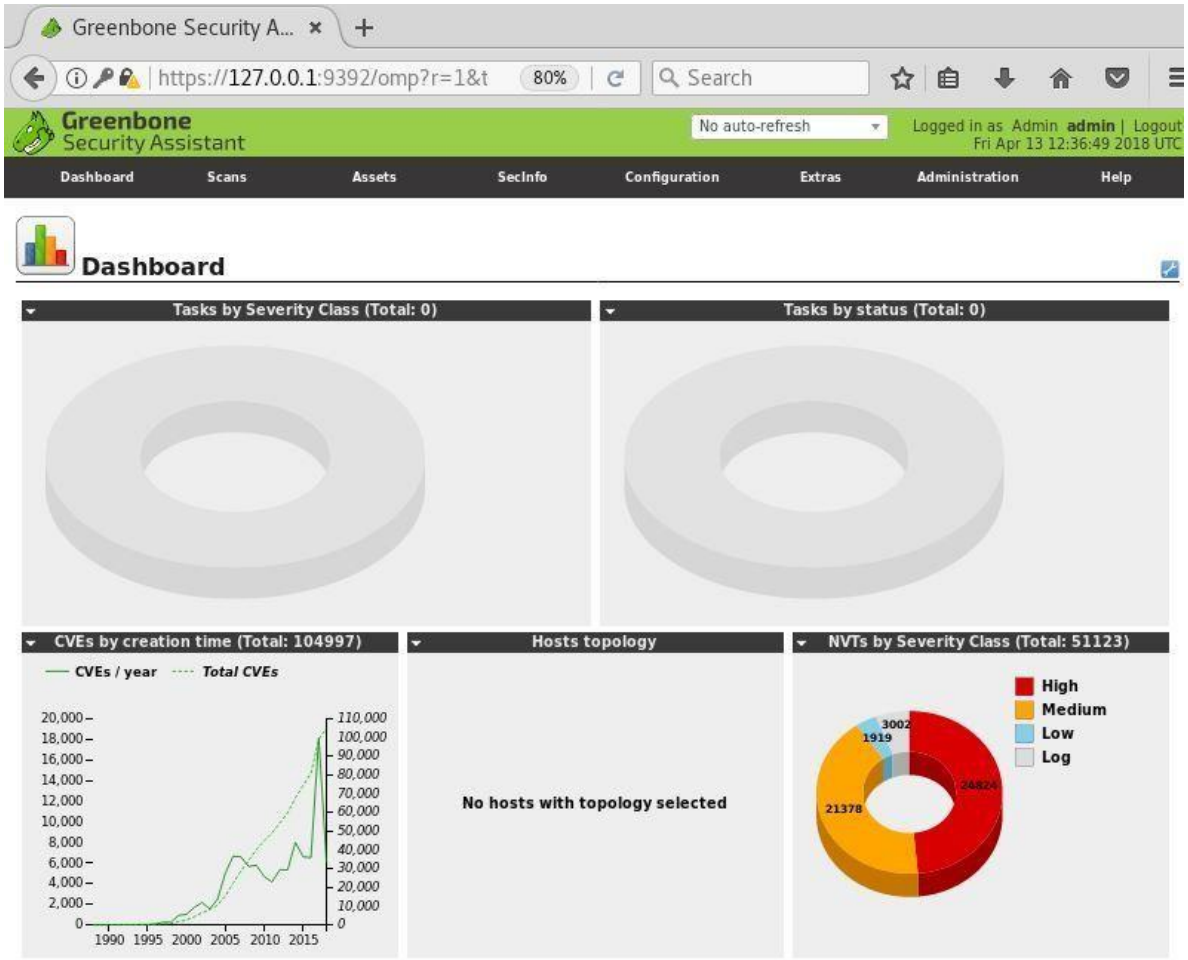


Gráfico Nro. 29: Entorno de Configuración escaneo de puertos

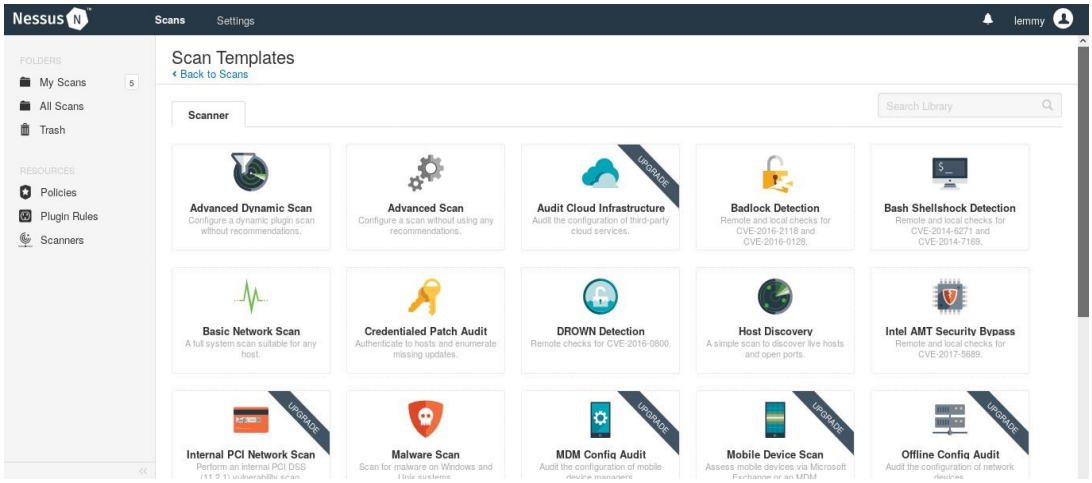
Fuente: Elaboración propia.

Tabla Nro. 26: Resultados de vulnerabilidad

HOST	RESULTADOS DEL ESCANEO DE VULNERABILIDADES			
	ALTO	MEDIO	BAJO	LOGS
192.168.13.13	1	1	0	0
192.168.13.15	1	2	1	0
192.168.13.17	0	4	1	0
192.168.13.18	1	1	1	0
192.168.13.19	0	4	1	0
192.168.13.21	1	1	1	0
192.168.13.23	1	1	1	0
192.168.13.28	1	2	1	0
192.168.13.30	0	0	0	0
192.168.13.31	0	0	0	0
192.168.13.32	0	0	0	0
192.168.13.36	0	0	0	0
192.168.13.90	0	0	0	0
192.168.13.94	0	0	0	0
192.168.13.98	0	3	1	0
192.168.13.99	0	2	1	0
192.168.13.100	0	1	1	0

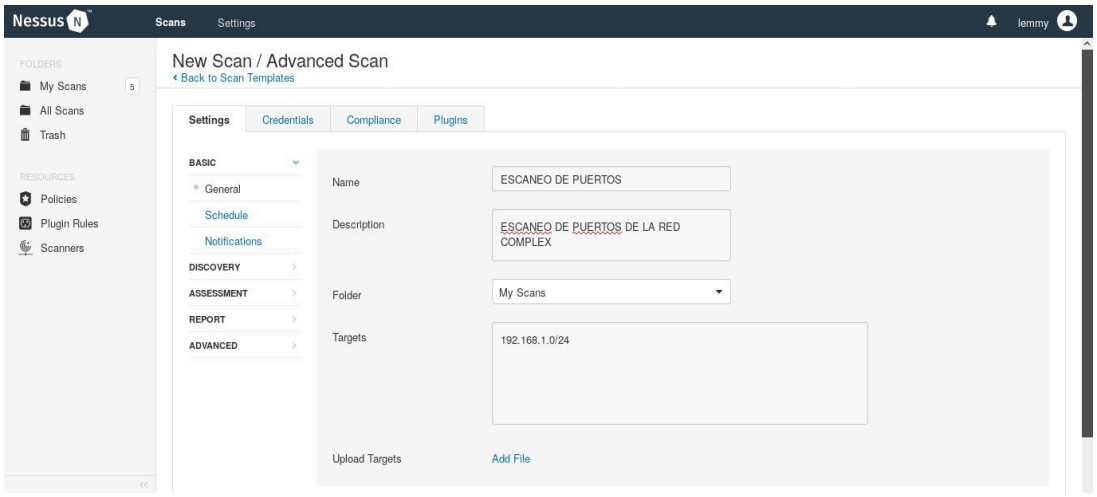
Fuente: Elaboración propia.

Gráfico Nro. 30: NESSUS - Herramienta de análisis de vulnerabilidades



Fuente: Elaboración propia.

Gráfico Nro. 31: Configuración para realizar un escaneo NESSUS



Fuente: Elaboración propia.

Tabla Nro. 27: Escaneos de Vulnerabilidad

HOST	RESULTADOS DEL ESCANEO DE VULNERABILIDADES				
	CRITICO	ALTO	MEDIO	BAJO	INFO
192.168.13.13	0	0	8	3	48
192.168.13.15	0	0	8	3	49
192.168.13.17	0	0	8	3	73
192.168.13.18	0	0	0	0	35
192.168.13.19	0	0	1	0	41
192.168.13.21	2	0	0	0	35
192.168.13.23	0	0	8	3	47
192.168.13.28	0	0	17	6	0
192.168.13.30	4	0	2	0	24
192.168.13.31	0	0	8	2	61
192.168.13.32	0	0	0	0	26
192.168.13.36	0	0	0	0	4
192.168.13.90	0	0	0	0	17
192.168.13.94	0	0	0	0	27
192.168.13.98	0	0	8	3	50
192.168.13.99	0	0	10	0	70
192.168.13.100	0	0	6	0	77

Fuente: Elaboración propia.

V. CONCLUSIONES

1. Se ha logrado realizar la Implementación de Hacking Ético, en la Empresa Complex del Perú S.A.C – Tumbes; 2017; como medio de ayuda en la detección y evaluación de vulnerabilidades de Red.

2. Se ha realizado el análisis, utilizando herramientas tecnológicas de seguridad, de la actual red de datos en la empresa Complex del Perú S.A.C – Tumbes; por lo que se ha evaluado los problemas de vulnerabilidad a los que se encuentra expuesta la red.

3. Así mismo, se ha formulado una propuesta tecnológica de seguridad, que permita establecer políticas de comunicación oportuna al detectarse posibles vulnerabilidades y/o penetraciones en la red de datos de la empresa Complex del Perú S.A.C – Tumbes.

RECOMENDACIONES

1. La norma ISO/IEC 27001:2005, exige cumplir con monitorear las actividades en medidas adoptadas con relación a la seguridad de la información, en base a los resultados debe corregir o actualizar cambios dependiendo de la revisión.

2. Es importante documentar los procesos establecidos para la implementación de SGSI, para brindar información requerida al personal de la Empresa.

3. Por lo tanto, se estima conveniente asignar una directiva encargada de la seguridad informática de la empresa para evitar pequeños inconvenientes.

4. Se recomienda capacitar a su personal de trabajo en especial a los del cargo de la seguridad informática, así mismo estarán aptos para intervenir y brindar soluciones.

5. Se sugiere al personal capacitado para la seguridad informática su mayor cuidado y protección, ya que el incidente está en la manipulación del ser humano.

REFERENCIAS BIBLIOGRÁFICAS

[1] c. p. i. s. c. d. v. y. m. Certifícate en Hacking Ético. Implementa un sistema de seguridad, *Experto Universitario en Hackin ético (ETHICAL HACKING)*, 2017.

[2] A. Guevara Soriano, *Hacking ético: Mitos y Realidades*, 2017.

[3] Seguridad Informática, «Introducción al hacking ético,» México, 2017.

[4] B. F. Ortiz Beltrán, «Hacking ético para detectar fallas en la seguridad informática de la intranet del gobierno provincial de Imbabura e implementar un sistema de gestión de seguridad de la información (SGSI), basado en la norma ISO/IEC 27001: 2005.,» Ibarra - Ecuador, 2015.

[5] D. L. Méndez Ávila, «Investigación y elaboración de un instructivo sobre las herramientas hacker más utilizadas en el ámbito informático.,» Ecuador, 2014.

[6] A. Acosta Patroni, «Hacking, Cracking y otras conductas ilícitas cometidas a través de Internet,» Chile, 2014.

[7] D. C. Muñoz Casanova, «Implementación de una solución de hacking ético para mejorar la seguridad en la infraestructura informática de la caja municipal de Sullana -agencia Chimbote.,» Chimbote, 2015.

[8] T. Mamani Ttito, «Modelo de sistema criptográfico de seguridad para las redes de comunicaciones en la región puno-2012,» Puno, 2014.

[9] J. R. Ortega Cubas, «Diseño de red de comunicación de datos para la Institución Educativa Privada Emilio Soyer Cabero ubicada en el Distrito de Chorrillos, Lima, Perú,» Lima, 2014.

[10] C. C. Muñoz Ramirez, «Diseño de una red de telecomunicaciones de banda ancha para la región Tumbes,» Tumbes, 2014.

[11] E. Mifsud , «Seguridad de la información / Seguridad informática,» 2016.

[12] «Indecopi,» [En línea]. Available: https://www.indecopi.gob.pe/principios-de-la-seguridad-de-la-informacion. [Último acceso: 20 setiembre 2017].

[13] v. carrasquilla, «Ventajas y Desventajas De La Seguridad Informatica,» 2015.

[14] M. Estrada Garavilla, «Delitos Informáticos,» 2016.

[15] G. d. C. I. 9001:2008, *Definición de delito Informático*, 2015.

[16] . H. D. Carrion, «Presupuestos para la Punibilidad del Hacking,» 2017.

[17] *Sistema de Gestión de la Seguridad de la Información*, 2015.

[18] C. Perdomo, *Sistemas de Gestión de Seguridad de la Información*, 2014.

[19] I. O. f. Standardization, «ISO 27001. Origen e historia.,» 2016.

[20] «Gestión de Seguridad de la Información ISO/IEC 27001,» [En línea]. Available: https://www.bsigroup.com/es-MX/seguridad-dela-informacion-ISOIEC-27001/. [Último acceso: 10 setiembre 2017].

[21] I. 27002.ES, «EL PORTAL ISO 27002 EN ESPAÑOL,» 2012. [En línea]. Available: http://www.iso27000.es/iso27002_9.html#home. [Último acceso: 11 03 2019].

[22] S. Informática, *¿Qué es el Hacking Ético y para qué sirve?*, 2016.

[23] HECTORPEDRAZA10, «Fases del Haking Etico,» [En línea]. Available: https://hectorpedraza10.wordpress.com/2014/11/21/fases-del-haking-etico/. [Último acceso: 11 03 2019].

[24] Por Paul Estrella, *¿Qué es un Ethical Hacker?*, 2017.

[25] I. d. I. Eléctrica, *Redes de datos*, 2014.

[26] *Aprender Informatica*, 2016.

[27] M. Rivero, *¿Qué son los virus informáticos?*, 2015.

[28] Eduardo Álvarez, *cracker, hackers, seguridad informática*, 2016.

[29] Julian Lasso, *Seguridad Informática: ¿Qué es una vulnerabilidad, una amenaza y un riesgo?*, 2015.

[30] Fernández, P. y Díaz, P. , *investigación cuantitativa*, 2014.

[31] T. Tamayo, *Metodologia de la Investigacion*, 2014.

[32] Sabino, *La investigación de tipo descriptiva trabaja sobre realidades de hechos, y su característica fundamental es la de presentar una interpretación correcta*, 2015.

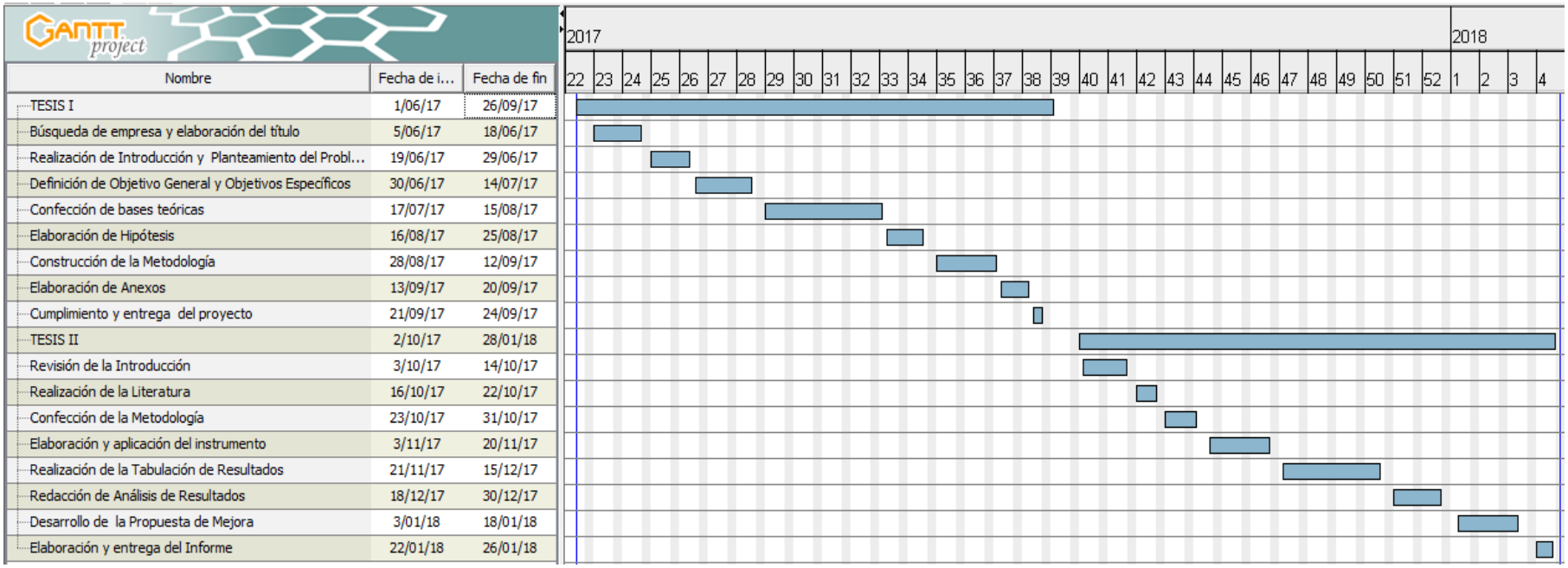
[33] M. Dzul Escamilla, *Diseño No experimental*, 2015.

[34] Ashley Seehorn, *Métodos de investigación de corte transversal*, 2014.

[35] QuestionPro, *Definición de encuesta*, 2016.

[36] M. Galán Amador, *El cuestionario aplicado a la investigación*, 2015.

ANEXO Nº 1: CRONOGRAMA DE ACTIVIDADES



Nombre	Fecha de i...	Fecha de fin
TESIS I	1/06/17	26/09/17
Búsqueda de empresa y elaboración del título	5/06/17	18/06/17
Realización de Introducción y Planteamiento del Probl...	19/06/17	29/06/17
Definición de Objetivo General y Objetivos Específicos	30/06/17	14/07/17
Confección de bases teóricas	17/07/17	15/08/17
Elaboración de Hipótesis	16/08/17	25/08/17
Construcción de la Metodología	28/08/17	12/09/17
Elaboración de Anexos	13/09/17	20/09/17
Cumplimiento y entrega del proyecto	21/09/17	24/09/17
TESIS II	2/10/17	28/01/18
Revisión de la Introducción	3/10/17	14/10/17
Realización de la Literatura	16/10/17	22/10/17
Confección de la Metodología	23/10/17	31/10/17
Elaboración y aplicación del instrumento	3/11/17	20/11/17
Realización de la Tabulación de Resultados	21/11/17	15/12/17
Redacción de Análisis de Resultados	18/12/17	30/12/17
Desarrollo de la Propuesta de Mejora	3/01/18	18/01/18
Elaboración y entrega del Informe	22/01/18	26/01/18

Fuente: Elaboración propia.

ANEXO Nº 2: PRESUPUESTO

PROYECTO: IMPLEMENTACIÓN DE HACKING ÉTICO PARA LA DETECCIÓN Y EVALUACIÓN DE VULNERABILIDADES DE RED EN LA EMPRESA COMPLEX DEL PERÚ S.A.C.-TUMBES; 2017.

TESISTA: BACH. JEAN CARLOS BERMEO OYOLA

INVERSIÓN: S/. 1,236.00

Descripción	**Cantidad**	**Precio Unidad (S/.)**	**Monto (S/.)**
Pasajes locales	30	10.00	300.00
Almuerzos	10	10.00	100.00
Lapiceros	30	1.00	30.00
hojas	1	28.00	28.00
Lápiz	25	1.00	25.00
Grapas	1	3.00	3.00
Alquiler de internet	60	1	60.00
copias	400	0.10	40.00
Impresión	400	0.5	200.00
Movilidad	30	15.00	450.00
		TOTAL S/.	1,236.00

Fuente: Elaboración propia.

ANEXO Nº 3: CUESTIONARIO

PROYECTO: IMPLEMENTACIÓN DE HACKING ÉTICO PARA LA DETECCIÓN Y EVALUACIÓN DE VULNERABILIDADES DE RED EN LA EMPRESA COMPLEX DEL PERÚ S.A.C.- TUMBES; 2017.

TESISTA: BACH. JEAN CARLOS BERMEO OYOLA

Primera Dimensión: Satisfacción de circunstancias actuales			
N°	Pregunta	SI	NO
01	¿Usted tiene conocimiento sobre hacking ético?		
02	¿Cree usted que la empresa cuenta con personal capacitado sobre temas de informática?		
03	¿La empresa cuenta con un hacking ético?		
04	¿Usted como trabajador piensa que su información puede ser jaqueada?		
05	¿Conoce usted los beneficios que el hacking ético?		
06	¿Usted tiene conocimiento sobre la vulnerabilidad de la red?		
07	¿Se ha capacitado alguna vez a los trabajadores sobre el tema hacker?		
08	¿Está satisfecho con la seguridad de la información actual que cuenta la empresa?		
09	¿Usted teme por la seguridad de la información de la empresa que sea jaqueada?		
10	¿Usted alguna vez ha visto la instalación de un hacking ético?		

Segunda Dimensión: Necesidad de la Implementación hacking ético			
	Pregunta	SI	NO
01	¿Cree usted que el hacking ético solucionará la vulnerabilidad de la red?		
02	¿Cree Usted que las demás empresas cuentan con un hacking ético?		
03	¿Usted cree que hacking ético permitirá ahorrar tiempo y dinero en la empresa?		
04	¿Usted está de acuerdo con la implementación de hacking ético en la empresa?		
05	¿Usted considera factible el manejo de hacking ético?		
06	¿De acuerdo a su opinión, los clientes serán beneficiados con la implementación del hacking ético?		
07	¿Estaría de acuerdo que hacking ético tenga presentación activa y fascinante?		
08	¿Considera usted que todos los trabajadores estarán de acuerdo con la implementación de hacking ético?		
09	¿Recomendaría a otras empresas utilizar hacking ético para la seguridad?		
10	¿Cree usted que la propuesta presentará gratos beneficios a la empresa?		

ANEXO Nº4: VALIDACIÓN DEL INSTRUMENTO

Ficha de validación del instrumento (Experto 1)

UNIVERSIDAD CATOLICA LOS ANGELES DE CHIMBOTE
ESCUELA DE POSGRADO

FICHA DE EVALUACIÓN DEL INSTRUMENTO

1.1 Nombres y apellidos del validador: Mg. Victor del Castillo Holguin
1.2 Cargo e Institución donde labora: Ministerio Público - Tumbes
1.3 Nombre del Instrumento evaluado: Circunstancias Actuales y Implementación de Hacking Etico
1.4 Autor del Instrumento: Bach. Jean Carlos Bermeo Oyola

II ASPECTOS DE LA EVALUACIÓN

Revisar cada uno de los items del instrumento y marcar con un aspa dentro del recuadro (x), según la calificación que asigne a cada uno de los indicadores
1.-Deficiente (Si menos del 30% de los items cumplen con el indicador)
2.-Regular (Si entre el 31% y 70% de los items cumplen con el indicador)
3.-Buena (Si más del 70% de los items cumple con el indicador)

Aspectos de validación del instrumento		1	2	3	Observaciones Sugerencias
Criterios	Indicadores	D	R	B	
PERTINENCIA	Los items miden lo previsto en los objetivos de investigación	☐	☐	☒	
COHERENCIA	Los items responde a lo que se debe medir en la variable y sus dimensiones.	☐	☐	☒	
Congruencia	Los items son congruentes entre si y con el concepto que mide.	☐	☒	☐	
Suficiencia	Los items son suficientes en cantidad para medir la variable	☐	☒	☐	
Objetividad	Los items se expresan en comportamientos y acciones observables.	☐	☒	☐	
Consistencia	Los items se han formulado en concordancia a los fundamentos teóricos de la variable.	☐	☒	☐	
Organización	Los items están secuenciados y distribuidos de acuerdo a dimensiones e indicadores	☐	☐	☒	
Claridad	Los items están redactados en un lenguaje entendible para los sujetos a evaluar.	☐	☐	☒	
Formato	Los items están escritos respetando aspectos técnicos (tamaño de letra, espaciado, interlineado, nitidez).	☐	☒	☐	
Estructura	El instrumento cuenta con instrucciones, consignas opciones de respuesta bien definidas.	☐	☒	☐	
	CONTEO TOTAL (Realizar el conteo de acuerdo a puntuaciones asignada a cada indicador.)	C	12 B	12 A	24 Total

Ceficiente de validez: $\frac{A+B+C}{30}$ = 0.80

Intervalos	Resultado
0.00 - 0.49	Validez nula
0.50 - 0.59	Validez muy baja
0.60 - 0.69	Validez baja
0.70 - 0.79	Validez aceptable
0.80 - 0.89	Validez buena
0.90 - 1.00	Validez muy buena

III. CALIFICACION GLOBAL

Ubicar el coeficiente de validez obtenido en el intervalo respectivo y escriba sobre el espacio el resultado.

Validez Buena

Piura, Diciembre 2018

Ing. Mg. Victor de Castillo Holguin

Ficha de validación del instrumento (Experto 2)

UNIVERSIDAD CATOLICA LOS ANGELES DE CHIMBOTE
ESCUELA DE POSGRADO

FICHA DE EVALUACIÓN DEL INSTRUMENTO

1.1 Nombres y apellidos del validador: Mg. Victor del Castillo Holguin
1.2 Cargo e Institución donde labora: Ministerio Público - Tumbes
1.3 Nombre del Instrumento evaluado: Circunstancias Actuales y Implementación de Hacking Etico
1.4 Autor del Instrumento: Bach. Jean Carlos Bermeo Oyola

II ASPECTOS DE LA EVALUACIÓN

Revisar cada uno de los ítems del instrumento y marcar con un aspa dentro del recuadro (x), según la calificación que asigne a cada uno de los indicadores

1.-Deficiente (Si menos del 30% de los ítems cumplen con el indicador)
2.-Regular (Si entre el 31% y 70% de los ítems cumplen con el indicador)
3.-Buena (Si más del 70% de los ítems cumple con el indicador)

Aspectos de validación del instrumento		1	2	3	Observaciones Sugerencias
Criterios	Indicadores	D	R	B	
PERTINENCIA	Los ítems miden lo previsto en los objetivos de investigación	☐	☐	☒	
COHERENCIA	Los ítems responde a lo que se debe medir en la variable y sus dimensiones.	☐	☐	☒	
Congruencia	Los ítems son congruentes entre sí y con el concepto que mide.	☐	☒	☐	
Suficiencia	Los ítems son suficientes en cantidad para medir la variable	☐	☒	☐	
Objetividad	Los ítems se expresan en comportamientos y acciones observables.	☐	☒	☐	
Consistencia	Los ítems se han formulado en concordancia a los fundamentos teóricos de la variable.	☐	☒	☐	
Organización	Los ítems están secuenciados y distribuidos de acuerdo a dimensiones e indicadores	☐	☐	☒	
Claridad	Los ítems están redactados en un lenguaje entendible para los sujetos a evaluar.	☐	☐	☒	
Formato	Los ítems están escritos respetando aspectos técnicos (tamaño de letra, espaciado, interlineado, nitidez).	☐	☒	☐	
Estructura	El instrumento cuenta con instrucciones, consignas opciones de respuesta bien definidas.	☐	☒	☐	
	CONTEO TOTAL (Realizar el conteo de acuerdo a puntuaciones asignada a cada indicador.)	C	12 B	12 A	24 Total

Ceficiente de validez: $\frac{A+B+C}{30}$ = 0.80

Intervalos	Resultado
0.00 - 0.49	Validez nula
0.50 - 0.59	Validez muy baja
0.60 - 0.69	Validez baja
0.70 - 0.79	Validez aceptable
0.80 - 0.89	Validez buena
0.90 - 1.00	Validez muy buena

III. CALIFICACION GLOBAL

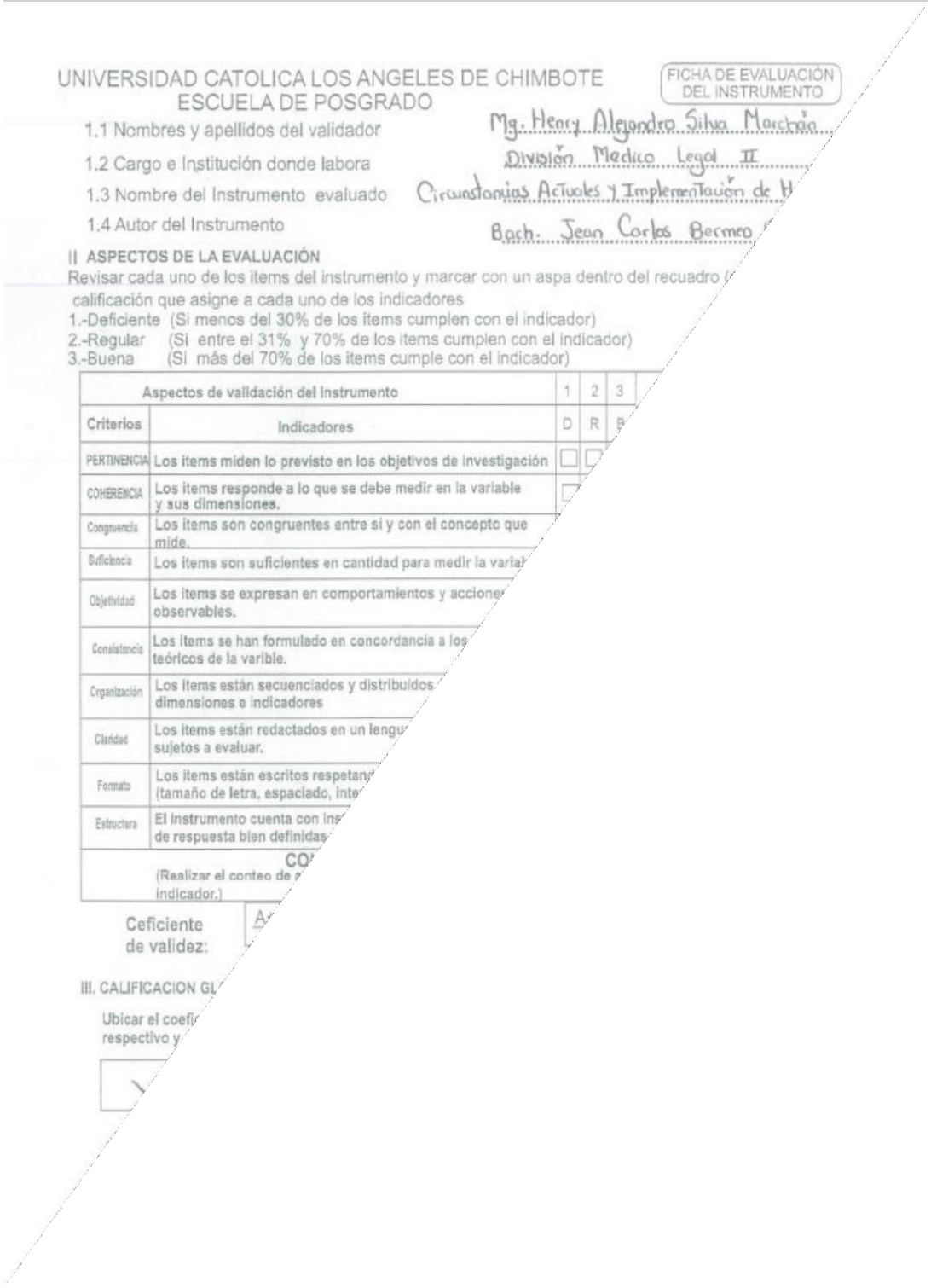
Ubicar el coeficiente de validez obtenido en el intervalo respectivo y escriba sobre el espacio el resultado.

Validez Buena

Piura, Diciembre 2018

Ing. Mg. Victor de Castillo Holguin

Ficha de validación del instrumento (Experto 3)



UNIVERSIDAD CATOLICA LOS ANGELES DE CHIMBOTE
ESCUELA DE POSGRADO

FICHA DE EVALUACIÓN DEL INSTRUMENTO

1.1 Nombres y apellidos del validador: Mg. Henry Alejandro Silva Marchán
1.2 Cargo e Institución donde labora: División Medico Legal II
1.3 Nombre del Instrumento evaluado: Circunstancias Actuales y Implementación de H
1.4 Autor del Instrumento: Bach. Jean Carlos Bermeo

II ASPECTOS DE LA EVALUACIÓN

Revisar cada uno de los ítems del instrumento y marcar con un aspa dentro del recuadro (
calificación que asigne a cada uno de los indicadores

1.-Deficiente (Si menos del 30% de los ítems cumplen con el indicador)
2.-Regular (Si entre el 31% y 70% de los ítems cumplen con el indicador)
3.-Buena (Si más del 70% de los ítems cumple con el indicador)

Aspectos de validación del instrumento		1	2	3
Criterios	Indicadores	D	R	B
PERTINENCIA	Los ítems miden lo previsto en los objetivos de investigación	☐	☐	
COHERENCIA	Los ítems responde a lo que se debe medir en la variable y sus dimensiones.	☐		
Congruencia	Los ítems son congruentes entre sí y con el concepto que mide.			
Suficiencia	Los ítems son suficientes en cantidad para medir la varia			
Objetividad	Los ítems se expresan en comportamientos y acciones observables.			
Consistencia	Los ítems se han formulado en concordancia a los teóricos de la varible.			
Organización	Los ítems están secuenciados y distribuidos dimensiones o indicadores			
Claridad	Los ítems están redactados en un lengu sujetos a evaluar.			
Formato	Los ítems están escritos respetan (tamaño de letra, espaciado, inte			
Estructura	El instrumento cuenta con ins de respuesta bien definidas			
	CO (Realizar el conteo de indicador.)			

Ceficiente de validez: A

III. CALIFICACION GL

Ubicar el coefi respectivo y