ANÁLISIS DE VULNERABILIDAD DE SISTEMAS INFORMÁTICOS EN LA UNIVERSIDAD DEL SINÚ SEDE PLAZA COLÓN

ALEXANDER FONSECA ALVAREZ
SAMUEL ALBERTO HENRIQUEZ AVILA

UNIVERSIDAD DEL SINU ELIAS BECHARA ZAINUM
SECCIONAL CARTAGENA
FACULTAD DE INGENIERIAS Y CIENCIAS EXACTAS
ESCUELA DE INGENIERIA DE SISTEMAS
CARTAGENA
MAYO DE 2018

ANÁLISIS DE VULNERABILIDAD DE SISTEMAS INFORMÁTICOS EN LA UNIVERSIDAD DEL SINÚ SEDE PLAZA COLÓN

ALEXANDER FONSECA ALVAREZ
SAMUEL ALBERTO HENRIQUEZ AVILA

PROYECTO DE GRADO

ASESOR DISCIPLINAR
RAFAEL E. MONTERROZA BARRIOS

ASESOR METODOLÓGICO
EUGENIA ARRIETA RODRIGUEZ

UNIVERSIDAD DEL SINU ELIAS BECHARA ZAINUM
SECCIONAL CARTAGENA
FACULTAD DE INGENIERIAS Y CIENCIAS EXACTAS
ESCUELA DE INGENIERIA DE SISTEMAS
CARTAGENA
MAYO DE 2018

UNIVERSIDAD DEL SINÚ
Elías Bechara Zainúm
Seccional Cartagena

AGRADECIMIENTO

Agradezco, principalmente, a Dios por darme la sabiduría y la ciencia para poder desarrollar completamente mi carrera y este proyecto. De igual manera, agradezco a mi familia por apoyarme, día tras día, para que mi meta se pudiese cumplir a cabalidad.

A mi novia por su incondicional apoyo durante muchos años compartidos y por su comprensión en cada etapa de nuestras vidas.

A la Universidad del Sinú por haberme brindado todos los conocimientos y las herramientas para formarme como profesional.

A los ingenieros Eugenia Arrieta Rodríguez y Rafael Monterroza por sus colaboraciones en el desarrollo de este proyecto.

Alexander Fonseca Álvarez

UNIVERSIDAD DEL SINÚ
Elías Bechara Zainúm
Seccional Cartagena

Acta de Calificación y aprobación

Notas de aceptación

_____

_____

_____

_____

Director de Escuela

_____

Director de Investigaciones

_____

Firma del jurado

_____

Firma del jurado

Cartagena de indias, 2018

UNIVERSIDAD DEL SINÚ
Elías Bechara Zainúm
Seccional Cartagena

EL DIRECTOR DE INVESTIGACIONES DE LA UNIVERSIDAD DEL SINU "ELIAS BECHARA ZAINUM" SECCIONAL CARTAGENA

HACE CONSTAR QUE:

En Cartagena, a los 23 días del mes de mayo del 2018, en la Oficina de la Dirección de Investigaciones de la Universidad, se aprobó por el jurado y se realizó la sustentación del Trabajo de Grado titulado "Análisis de vulnerabilidad de Sistemas Informáticos en la Universidad del Sinú sede Plaza Colón" que se desarrolló bajo la dirección de los Ingenieros Eugenia Arrieta Rodríguez y Rafael Monterroza Barrios y presentado por los estudiantes Alexander Fonseca Álvarez y Samuel Alberto Henríquez Ávila.

Los jurados designados fueron los ingenieros Alberto Jiménez Ortiz y German Herrera Vidal.

Teniendo en cuenta la aprobación emitida por el jurado, se encuentra que los estudiantes han cumplido con los requisitos de presentación y sustentación del trabajo de investigación, exigidos por el programa de INGENIERÍA DE SISTEMAS, Resolución 0178 de 15 de marzo de 2010.

Se expide esta constancia a los 23 días del mes de mayo de 2018

DIRECCIÓN DE INVESTIGACIONES
Universidad del Sinú

COORDINADOR DE INVESTIGACIONES
Escuela de Ingeniería de Sistemas

INTRODUCCIÓN

Actualmente, la gran mayoría de los equipos de cómputo de las empresas se encuentran conectados, ya sea a una intranet o a internet directamente, lo que les expone a ataques cibernéticos por personas mal intencionadas, las cuales buscan obtener el bien más preciado de esta era, la información. Muchos hackers buscan obtener algún beneficio económico al secuestrar la información de las empresas, aunque estas tomen medidas de seguridad, no son 100% confiables, debido a que muchas de las vulnerabilidades que se llegan a presentar en estos sistemas de seguridad son originados por el personal interno de la empresa.

Con el avance tecnológico se ha desarrollado hardware y software capaces de analizar y detectar vulnerabilidades dentro de los sistemas de cómputo, estas herramientas ayudan en gran medida, pero aun así debe existir un monitoreo a estas herramientas para un óptimo desempeño. Ahora, cuando los sistemas de seguridad son muy robustos, no dejando a la vista vulnerabilidad alguna, los ataques se realizan a través a otros medios, como lo es la ingeniería social, con el cual pueden burlar las barreras de seguridad aprovechándose de la confianza e ingenuidad del personal que interactúa con el sistema de cómputo.

Es posible disminuir el nivel de riesgo de forma significativa y con ello el éxito de las amenazas y la reducción del impacto sin necesidad de realizar inversiones grandes ni contar con mucho personal. Para ello se hace necesario conocer y gestionar de manera ordenada los riesgos a los que está sometido el sistema informático, considerar procedimientos adecuados y planificar e implantar los controles de seguridad que correspondan.

RESUMEN

Se realizaron distintas pruebas, ataques y mediciones de parámetros de la red inalámbrica de la Universidad del Sinú en las sedes Plaza Colón, usando diversas herramientas y aplicaciones primordialmente integradas en Bettercarp, al igual que otras aplicaciones ejecutadas en Linux; todo esto con el fin de determinar el nivel de desempeño y de seguridad que mantiene la red de la sede Plaza Colón.

La factibilidad para la recolección de la información fue óptima, logramos el propósito demostrar que la información manejada por el personal administrativo y la comunidad estudiantil se pudo ver comprometida gracias a una serie de herramientas informáticas que realizan la técnica ARP SPOOFING. El éxito que nos permitió alcanzar el objetivo fue mediante conexión directa a los Router provenientes de la misma Universidad del Sinú en la sede Plaza Colón, con lo cual pudimos capturar el tráfico porque mediante conexión a los Access Point de la universidad no era posible la captura de la información, ya que el sistema estaba con un nivel de seguridad alto.

TABLAS DE CONTENIDO DINÁMICAS

LISTA DE TABLAS DINÁMICAS

LISTA DE FIGURAS

1. DISEÑO METODOLÓGICO

1.1. PLANTEAMIENTO DEL PROBLEMA

DESCRIPCION DEL PROBLEMA

La vulnerabilidad en los sistemas de cómputo es un factor crítico para la pérdida de información confidencial e importante. Teniendo en cuenta esto, se ha observado que mucho del personal que interactúa con los sistemas de cómputo poseen bajas competencias en buenas prácticas para la prevención de ataques y protección de la información. Dentro de las malas prácticas de los usuarios se han detectado que las contraseñas de usuario de sesiones de plataforma, equipos y correos institucionales son conocidas por personas diferentes del propietario, se han detectado correos institucionales con sesión abierta en equipos de uso público en la institución. Estas se convierten fácilmente en fugas o alteración de información, o plagio de identidad.

Sabemos que hoy en día todas las organizaciones y personas utilizan computadores, redes inalámbricas, dispositivos inteligentes, etc. Y están expuestas a diferentes amenazas cibernéticas derivadas de la utilización de páginas web, aplicaciones, documentos, correos electrónicos, servicios de mensajería electrónica como los chats, redes sociales, etc.

La mayoría de estas amenazas están siendo creadas para tener acceso a información personal o corporativa y con éstos realizar ataques dañinos que vulneran la capacidad de tener acceso a documentos, a sistemas internos, para realizar transacciones, etc.

Mientras que hoy tenemos, por un lado, a la disposición cientos de servicios de interconexión entre personas y organizaciones, por el otro estamos teniendo mucha mayor exposición de nuestra información personal y corporativa hacia personas no autorizadas que utilizan diferentes métodos para atacar y estos están siendo cada vez más complejos, más difíciles de prevenir y sobre todo más

dañinos. Esto ha conllevado a que las organizaciones hagan mucho más énfasis en la ciberseguridad y los aspectos preventivos y correctivos ante un ataque.

Como una medida para minimizar estos incidentes se plantea el diseño de un plan de acción basado en un plan de seguridad orientado a reducir las vulnerabilidades de las páginas web dentro de un marco jurídico tecnológico.

FORMULACIÓN DEL PROBLEMA

¿Cómo mejorar las medidas de seguridad informática para evitar el robo de información del personal administrativo y estudiantil de la Universidad del Sinú sede Plaza Colón para el presente año?

OBJETIVOS

OBJETIVO GENERAL

Evaluar las vulnerabilidades de los sistemas de cómputo de la universidad del Sinú sede Plaza Colón, durante el primer cuatrimestre del 2018.

OBJETIVOS ESPECÍFICOS

- Seleccionar la técnica de ataque informático que permita detectar las vulnerabilidades de los sistemas de información de la Universidad del Sinú.
- Determinar el área con mayor grado de vulnerabilidad en las dependencias de la Universidad del Sinú en la sede Plaza Colón, aplicando técnicas de Ingeniería Social.
- Aplicar el ataque informático al área designada para confirmar el grado de vulnerabilidad.
- Determinar la calidad de la seguridad de la información en la universidad del Sinú sede Plaza Colón.

1.2. ESTADO DEL ARTE

En la universidad del Sinú se encontró un proyecto de análisis de infraestructura, realizada en el año 2015 por los estudiantes Julio García Ricardo y su compañero Roiman Romanos Ramírez. En este proyecto se realizó, de manera general, un estudio de la calidad de la infraestructura de red y los equipos con los que cuenta la institución para prestar los servicios de Internet por Wifi y, además, desarrolla un poco la temática de la ingeniería social.

En el año 2011, estudiantes de la facultad de Ingeniería de Sistemas de la Universidad de Cartagena diseñaron una metodología para la detección de vulnerabilidades de redes de datos, en el cual desarrollaron diferentes facetas.

1.3. MARCOS DE REFERENCIA

MARCO TEÓRICO

Ingeniería Social

La Ingeniería social es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Es una técnica que pueden usar ciertas personas, tales como investigadores privados, criminales, o delincuentes informáticos, para obtener información, acceso o privilegios en sistemas de información que les permitan realizar algún acto que perjudique o exponga la persona u organismo comprometido a riesgo o abusos [1].

Seguridad Informática

La seguridad informática, también conocida como ciberseguridad o seguridad de tecnologías de la información, es el área relacionada con la informática y la telemática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida en una computadora o circulante a través de las redes de computadoras. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La ciberseguridad comprende software (bases de datos, metadatos, archivos), hardware, redes de computadoras y todo lo que la organización valore y signifique un riesgo si esta información confidencial llega a manos de otras personas, convirtiéndose, por ejemplo, en información privilegiada [2].

Phishing

Phishing o suplantación de identidad es un término informático que denomina un modelo de abuso informático y que se comete mediante el uso de un tipo de ingeniería social, caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña, información detallada sobre tarjetas de crédito u otra información bancaria). El cibercriminal, conocido como

phisher, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantánea o incluso utilizando también llamadas telefónicas [3].

Vishing

El vishing consiste en realizar llamadas telefónicas encubiertas bajo encuestas con las que también se podría sacar información personal de forma que la víctima no sospeche. Por este motivo debemos tener cuidado y no proporcionar información personal, aunque se trate de nuestra compañía de móvil, electricidad o agua (entre otras), ya que podría ser un hacker que haya elegido casualmente la nuestra [1].

Baiting

En este caso se utiliza un dispositivo de almacenamiento extraíble (CD, DVD, USB) infectado con un software malicioso, dejándolo en un lugar en el cual sea fácil de encontrar (por ejemplo, baños públicos, ascensores, aceras, etc.). Cuando la víctima encuentre dicho dispositivo y lo introduzca en su ordenador, el software se instalará y permitirá que el hacker obtenga todos los datos personales del usuario [1].

TCP

Protocolo de control de trasmisiones (TCP), este el protocolo es una de las herramientas que permiten la comunicación de todos los sistemas electrónicos conectados a internet o red de computadora. Este es usado por la totalidad de empresas en el mundo y hogares, es una gran herramienta que ha permitido comunicar múltiples distancias entre las personas, el uso de este depende completamente de la finalidad de que tengas las empresas o personas [4].

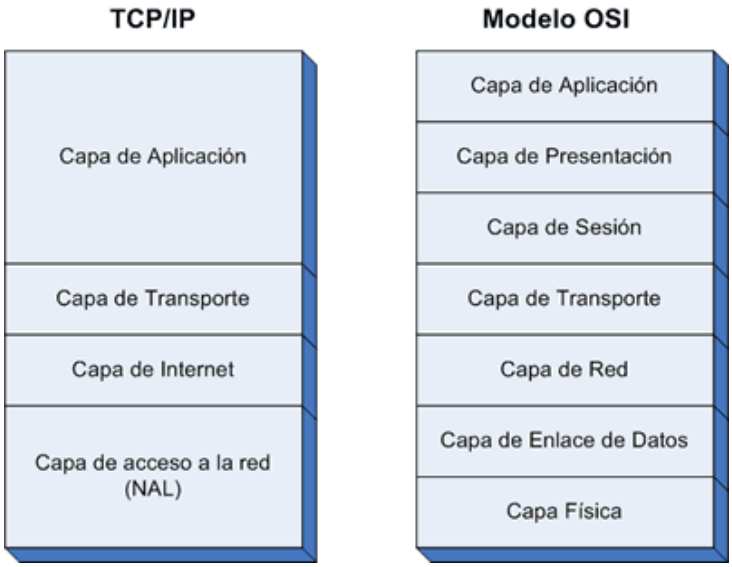


Figura 1 TCP/IP vs Modelo OSI

Fuente: https://www.textoscientificos.com/redes/tcp-ip/comparacion-modelo-osi

UDP

Protocolo de datagramas de usuario, permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera. Tampoco tiene confirmación ni control de flujo, por lo que los paquetes pueden adelantarse unos a otros; y tampoco se sabe si ha llegado correctamente, ya que no hay confirmación de entrega o recepción [5].

El protocolo UDP al no incluir información de control, reduce la cantidad de información extra en los paquetes por lo que es un protocolo más rápido que TCP y adecuado para transmisión de paquetes de información en tiempo real como lo es la voz [6].

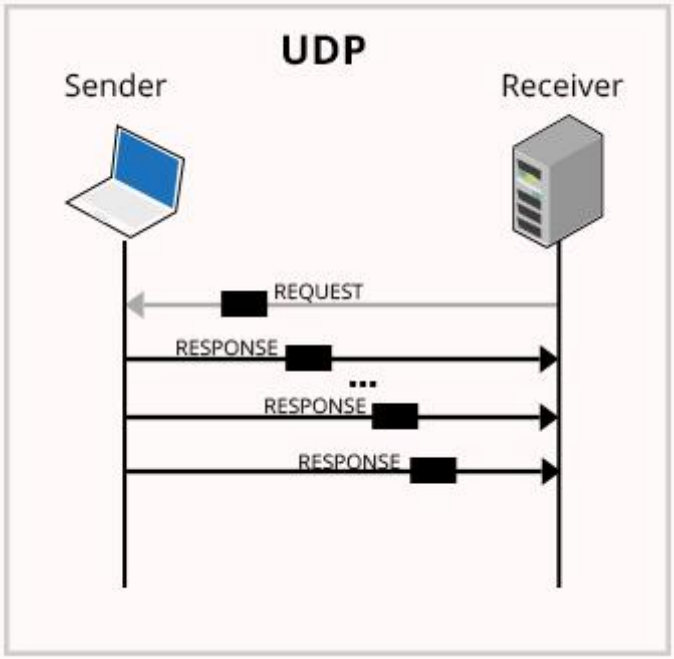


Figura 2 UDP.

Fuente: www.oodlestechnologies.com/blogs/Why-UDP-is-preferred-for-Live-Streaming.

HTTP

Hyper Text Transfer Protocol (Protocolo de transferencia de hipertexto), es el método más común de intercambio de información en la world wide web, el método mediante el cual se transfieren las páginas web a un computador. El protocolo de transferencia es el sistema mediante el cual se transfiere información entre los servidores y los clientes (por ejemplo, los navegadores) [7].

Este sería uno de los protocolos que día a día utilizamos al navegar por las diferentes páginas web en Internet

MITM (Man in the Middle)

Esta técnica permite al usuario interponerse entre 2 equipos de cómputo y recibir cada una de la información que se envían entre sí, de esta forma se puede obtener acceso a cualquier tipo de información.

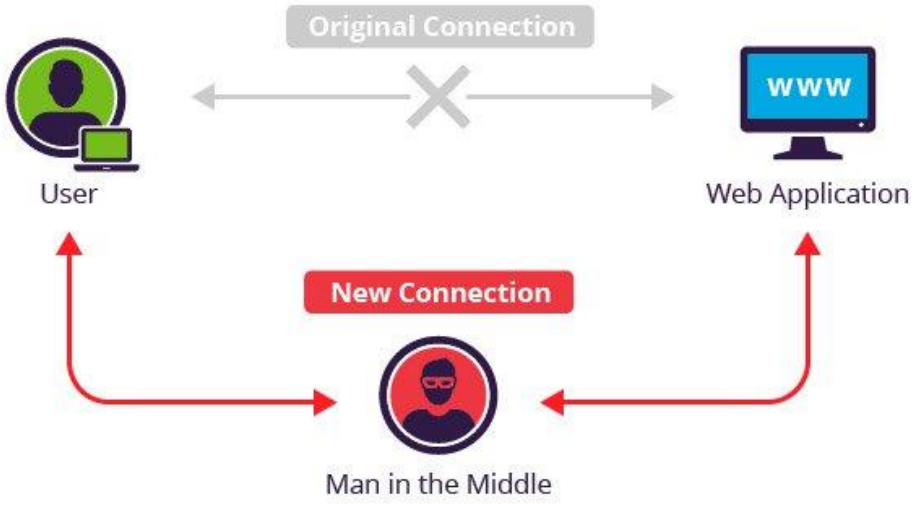


Figura 3 Man in the Middle.

Fuente: /tecnonucleous.com/2018/02/09/punto-de-acceso-inalambrico-man-in-the-middle-dentro-de-un-contenedor-de-docker/

Este tipo de técnicas son usadas en lugares de acceso público a internet, donde toda la información en esa área puede estar constantemente vigilada.

Wireshark

Esta es una herramienta que permite dar apoyo a la seguridad y mantenimiento a las redes de computo de alguna organización, pero su uso también depende a la orientación, ya que la funcionalidad de esta herramienta permite la captura de tráfico total de una red que incluya todos los protocolos de red existentes, se podría obtener acceso a cualquier tipo de información que solo es accesible a personal cualificado y con un gran conocimiento del funcionamiento total de los protocolos.

Ettercap

Ettercap en una suite completa para realizar ataques de hombre en el medio. Permite interceptar conexiones en vivo, filtrar contenido al vuelo y varios otros trucos interesantes. Soporta disección activa y pasiva de varios protocolos e incluye diversas características para el análisis de red y host. Ettercap generará un ataque “ARP Spoofing” la cual es una técnica donde un atacante envía mensajes ARP (Address Resolution Protocol) “Spoofed” o falsos en una Red Local Interna. Generalmente, la intención es asociar la dirección MAC del atacante con la dirección IP de otro host (como el gateway o pasarela por defecto), causando que cualquier tráfico destinado para esta dirección IP sea en su lugar enviada hacia el atacante [8].

Esta herramienta informática permite el uso de múltiples técnicas para el aprovechamiento de vulnerabilidades, su alcance permite obtener información de páginas web con protocolo HTTPS.

Figura 4 Ettercap.

Fuente: https://thehacktoday.com/how-to-setup-ettercap-on-kali-linux/

Bettercap

Bettercap es un conjunto de herramientas basada en la original (Ettercap), que permite analizar el tráfico de nuestra red, controlarlo y poder auditar la seguridad de una red y de los datos que viajan por ella. Existen muchas herramientas desarrolladas con fines similares, pero Bettercap es una de las herramientas más completas para esta función [9].

Las características más importantes de Bettercap son las siguientes:

- Es mucho más estable en redes de gran tamaño, pudiéndose escalar sin problemas.
- Permite ver sólo la información relevante, siendo mucho más precisa, rápida y sencilla de usar.

Figura 5 Bettercap.

Fuente: http://www.elladodelmal.com/2016/06/bettercap-una-katana-para-realizar.html

MARCO CONCEPTUAL

Archivos:

Es un conjunto de bits almacenado en un dispositivo. Un archivo es identificado por un nombre y la descripción de la carpeta o directorio que lo contiene. Los archivos informáticos se llaman así porque son los equivalentes digitales de los archivos en tarjetas, papel o microfichas del entorno de oficina tradicional. Los archivos informáticos facilitan una manera de organizar los recursos usados para almacenar permanentemente datos en un sistema informático [10].

Ataque informático:

Es un método en el que una persona intenta tener el control y desestabilizar un sistema informático a partir de otro sistema informático con el fin de obtener información confidencial [11].

Cibernético:

Es la ciencia que estudia interdisciplinariamente la estructura de los sistemas reguladores. Hoy en día, o cibernético se caracteriza por ser todo lo que se relaciona con la tecnología computacional, especialmente con Internet [12].

Correo electrónico:

Es un servicio de red que permite a los usuarios enviar, recibir mensajes y archivos rápidamente (también denominados mensajes electrónicos o cartas electrónicas) mediante sistemas de comunicación electrónicos. Normalmente utilizamos este nombre para definir al sistema que provee este servicio en Internet, mediante el protocolo SMTP [13].

Denegación de servicio:

Los ataques de denegación de servicio causan que el servicio o programa deje de funcionar o impide que otros hagan uso de ese servicio o programa. Estos

ataques pueden ser realizados al nivel de red enviando datagramas cuidadosamente preparados y malintencionados de tal forma que puedan causar que las conexiones de red fallen. También pueden realizarse a nivel de aplicación, donde órdenes cuidadosamente construidas se envían contra un programa para tratar que se vuelva muy ocupado o que pare su funcionamiento. Impedir que el tráfico de red sospechoso alcance sus máquinas y que lleguen órdenes y peticiones de programa sospechosos son las mejores formas de minimizar el riesgo de un ataque de denegación de servicio. Resulta muy útil conocer los detalles del método de ataque, por lo que debería aprender usted mismo todo lo posible de cada tipo nuevo de ataque que se haga público [14].

Fraude:

Es una acción que resulta contraria a la verdad y a la rectitud. El fraude se comete en perjuicio contra otra persona o contra una organización (como el Estado o una empresa) [15].

Hacker:

El Hacker es una persona o individuo que tiene un amplio conocimiento en informática y en redes de datos para utilizarlos con un objetivo. Dicho objetivos puede ser con buenos o malos fines. Además, podemos referirnos a la acción de utilizar estos conocimientos como *Hacking*.

Incidentes:

Se define como cualquier evento que atente contra la Confidencialidad, Integridad y Disponibilidad de la información y los recursos tecnológicos [16].

IP:

Es una etiqueta numérica que identifica, de manera lógica y jerárquica, a una interfaz (elemento de comunicación/conexión) de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (Internet Protocol), dicho número no se ha de confundir con la dirección MAC que es un

identificador de 48 bits para identificar de forma única a la tarjeta de red y no depende del protocolo de conexión utilizado ni de la red. La dirección IP puede cambiar muy a menudo por cambios en la red o porque el dispositivo encargado dentro de la red de asignar las direcciones IP, decida asignar otra IP, a esta forma de asignación de dirección IP se denomina dirección IP dinámica [17].

Malware:

Es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora sin el consentimiento de su propietario. El término malware es muy utilizado por profesionales de la informática para referirse a una variedad de software hostil, intrusivo o molesto [18].

Protocolo:

Es un conjunto de reglas usadas por computadores para comunicarse unas con otras a través de una red por medio de intercambio de mensajes. Éste es una regla o estándar que controla o permite la comunicación en su forma más simple, puede ser definido como las reglas que dominan la sintaxis, semántica y sincronización de la comunicación. Los protocolos pueden ser implementados por hardware, software, o una combinación de ambos. A su más bajo nivel, éste define el comportamiento de una conexión de hardware [19].

Red:

Es un conjunto de equipos informáticos y software conectados entre sí por medio de dispositivos físicos o inalámbricos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios [20].

Seguridad:

Es usado en el sentido de minimizar los riesgos a que están sometidos los bienes informáticos hasta llevarlos a niveles adecuados.

Servidor:

Es un software en ejecución capaz de realizar o atender las peticiones de uno o varios clientes con el fin de responder con algún resultado.

Sistema informático:

Es el conjunto de bienes informáticos de que dispone una entidad para su correcto funcionamiento y la consecución de los objetivos.

Spam:

También conocido como correo basura, este no es más que aquellos mensajes, con remitente desconocido, que no son solicitados ni deseados por el usuario y que, además, por norma general, son enviados en grandes cantidades. Por consiguiente, el spam se caracteriza por ser anónimo, masivo y no demandado [21].

Spoofing:

También conocido como suplantación de Identidad, hace referencia al uso de técnicas a través de las cuales un atacante, generalmente con usos maliciosos o de investigación, se hace pasar por una entidad distinta a través de la falsificación de los datos en una comunicación.

Los ataques de spoofing se pueden clasificar en: la suplantación de IP, suplantación de ARP, suplantación de DNS, suplantación web o suplantación de correo electrónico [22].

Vulnerabilidad:

En un sistema informático es un punto o aspecto susceptible de ser atacado o de dañar su seguridad; representan las debilidades o aspectos falibles o atacables en el sistema informático y califican el nivel de riesgo del mismo.

MARCO LEGAL

MARCO LEGAL	
Derechos de autor	Decisión 351 de la C.A.N. Ley 23 de 1982 Decreto 1360 de 1989 Ley 44 de 1993 Decreto 460 de 1995 Decreto 162 de 1996 Ley 545 de 1999 Ley 565 de 2000 Ley 603 de 2000 Ley 719 de 2001
Propiedad Industrial	Decisión 486 de la C.A.N. Decreto 2591 de 2000 Ley 463 de 1998 Ley 170 de 1994 Ley 178 de 1994
Propiedad Intelectual	Decisión 345 de la C.A.N. Decisión 391 de la C.A.N. Decisión 523 de la C.A.N.
Comercio Electrónico y Firmas Digitales	Ley 527 de 1999 Decreto 1747 de 2000 Resolución 26930 de 2000

Tabla 1 Marco Legal. Fuente: Autor propio.

El 5 de enero de 2009 se decretó la Ley 1273 de 2009, la cual añade dos nuevos capítulos al Código Penal Colombiano:

Capitulo Primero: De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos

Capitulo Segundo: De los atentados informáticos y otras infracciones.

ACTUALIZACIÓN AGOSTO 2013

LEY 603 DE 2000

Esta ley se refiere a la protección de los derechos de autor en Colombia. Recuerde: el software es un activo, además está protegido por el Derecho de Autor y la Ley 603 de 2000 obliga a las empresas a declarar si los problemas de software son o no legales.

LEY ESTATUTARIA 1266 DEL 31 DE DICIEMBRE DE 2008

Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

LEY 1273 DEL 5 DE ENERO DE 2009

Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

LEY 1341 DEL 30 DE JULIO DE 2009

Por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.

LEY ESTATUTARIA 1581 DE 2012

Entró en vigor la Ley 1581 del 17 de octubre 2012 de PROTECCIÓN DE DATOS PERSONALES, sancionada siguiendo los lineamientos establecidos por el Congreso de la República y la Sentencia C-748 de 2011 de la Corte Constitucional.

Como resultado de la sanción de la anunciada ley toda entidad pública o privada, cuenta con un plazo de seis meses para crear sus propias políticas internas de manejo de datos personales, establecer procedimientos adecuados para la atención de peticiones, quejas y reclamos, así como ajustar todos los procesos, contratos y autorizaciones a las disposiciones de la nueva norma.

Aspectos claves de la normatividad:

- Cualquier ciudadano tendrá la posibilidad de acceder a su información personal y solicitar la supresión o corrección de la misma frente a toda base de datos en que se encuentre registrado.

- Establece los principios que deben ser obligatoriamente observados por quienes hagan uso, de alguna manera realicen el tratamiento o mantengan una base de datos con información personal, cualquiera que sea su finalidad.

- Aclara la diferencia entre clases de datos personales construyendo las bases para la instauración de los diversos grados de protección que deben presentar si son públicos o privados, así como las finalidades permitidas para su utilización.

- Crea una especial protección a los datos de menores de edad.

- Establece los lineamientos para la cesión de datos entre entidades y los procesos de importación y exportación de información personal que se realicen en adelante.

- Define las obligaciones y responsabilidades que empresas de servicios tercerizados tales como Call y Contact Center, entidades de cobranza y, en general, todos aquellos que manejen datos personales por cuenta de un tercero, deben cumplir en adelante.

- Asigna la vigilancia y control de las bases de datos personales a la ya creada Superintendencia Delegada para la Protección de Datos Personales, de la Superintendencia de Industria y Comercio.

- Crea el Registro Nacional de Bases de Datos.

- Establece una serie de sanciones de carácter personal e institucional dirigidas a entidades y funcionarios responsables del cumplimiento de sus lineamientos.

DECRETO 1377 DE 2013

Protección de Datos, decreto por el cual se reglamenta parcialmente la Ley 1581 de 2012.

1.4. DISEÑO METODOLÓGICO

LÍNEA DE INVESTIGACIÓN

Redes

Este proyecto está enfocado directamente con la Escuela de Ingeniería de Sistemas en su semillero de DeArtica en la línea de Redes de Computadores para el fortalecimiento de ésta en la rama de Seguridad Informática, en el cual utilizamos técnicas de ataque en la red de la Universidad para tratar de conseguir información relevante, y así, determinar la calidad de la seguridad en la Institución.

TIPO DE INVESTIGACIÓN

Investigación Exploratoria

Nuestra investigación es exploratoria porque se realizarán investigaciones en diferentes dependencias de la Universidad del Sinú en la sede Plaza Colón, permitiendo comprobar si han sido víctimas de delitos informáticos e identificar las vulnerabilidades que presente.

DEFINICIÓN DE LA METODOLOGÍA

La metodología que utilizaremos va encaminada a la Obtención de Información mediante la técnica de ingeniería social directa e indirectamente de funcionarios de la universidad del Sinú y la comunidad estudiantil, además, utilizaremos la técnica de ARP Spoofing, con la que haremos envíos de correos solicitando información personal para verificar si estos funcionarios recurren a contestar con sus datos personales [23].

Para cumplir con el primer objetivo del proyecto que es determinar la técnica más apropiada de ataques informáticos para los sistemas de información de la Universidad del Sinú se deberá llevar acabo las siguientes actividades:

- Se realiza una revisión bibliográfica sobre los diferentes ataques informáticos más usados.
- Se realiza un laboratorio simulado con los diferentes ataques informáticos principales, lo cual nos ayudará a determinar la mejor técnica a emplear.
- Se debe realizar una comparación de efectividad para seleccionar la técnica que se ajusta al estudio.

Con el primer objetivo cumplido, pasaremos al segundo en el cual se detectará, en las dependencias de la universidad, las posibles vulnerabilidades utilizando la técnica seleccionada anteriormente. Se procede a realizar lo siguiente:

- Estudio de las posibles vulnerabilidades encontradas.
- Determinar el área de ataque según la efectividad y haciendo comparación entre las vulnerabilidades.
- Seleccionar el área con mayor factor de vulnerabilidad.

Para la continuación, ya establecido el método y el lugar del ataque, se procederá con acercamientos directos y pasivos a desarrollar el tercer punto:

- Determinar el nivel de acceso logrado.
- Establecer el nivel de información obtenida y privilegios.
- Detallar actividad de respuesta para solución del problema.

PRESUPUESTO

UNIVERSIDAD DEL SINÚ Elías Bechara Zainúm Seccional Cartagena	**PROCESO: INVESTIGACIÓN, CIENCIA E INNOVACIÓN** **TITULO: PRESUPUESTO PROYECTO DE INVESTIGACIÓN** **CODIGO: R-INVE-030** **VERSIÓN: 002**
Titulo del proyecto:	
Análisis de vulnerabilidades de los sistemas de información de la Universidad del Sinú sede Plaza Colón	
Nombre del grupo:	

Rubro	Recursos Unisinu Cartagena		Recursos Externos		Total
	Especie	Frescos	Especie	Frescos	
Personal	$ -	$ -	$ -	$ 1.130.000,00	$ 1.130.000,00
Servicios técnicos	$ -	$ -	$ -	$ -	$ -
Equipos de uso propio	$ -		$ 2.116.000,00		$ 2.116.000,00
Compra de equipos	$ -	$ -	$ -	$ -	$ -
Materiales / insumos / reactivos	$ -	$ -	$ -	$ 70.000,00	$ 70.000,00
Salidas de campo	$ -	$ -	$ -	$ -	$ -
Software	$ -	$ -	$ -	$ -	$ -
Viajes	$ -	$ -	$ -	$ -	$ -
Gastos de publicación	$ -	$ -	$ -	$ -	$ -
Gastos de patentes	$ -	$ -	$ -	$ -	$ -
Total	$ -	$ -	$ 2.116.000,00	$ 1.200.000,00	
TOTAL					$ 3.316.000,00

	Entidades	Total	Especie	Frescos
Caracterización de la inversión	Inversión unisinu	0 %	0 %	0 %
	Inversión externa	100 %	64 %	36 %

Para ver en detalle el presupuesto del proyecto puede ver el siguiente archivo:

Ver anexo 5

2. ANÁLISIS DEL PROBLEMA

Para determinar las actividades a desarrollar, se realizó una reunión con el Coordinador Disciplinar y el jefe de Sistemas de la universidad del Sinú seccional Cartagena, donde se evaluó y determinó la sede y las áreas donde la información fuera relevante para el caso de estudio, pero por restricciones a la información que se iba a tratar de obtener, por lo que se designó los funcionarios y estudiantes de la sede plaza colon de la información básica de tal manera que la información obtenida no fuera tan comprometedora.

Diagramas Phishing

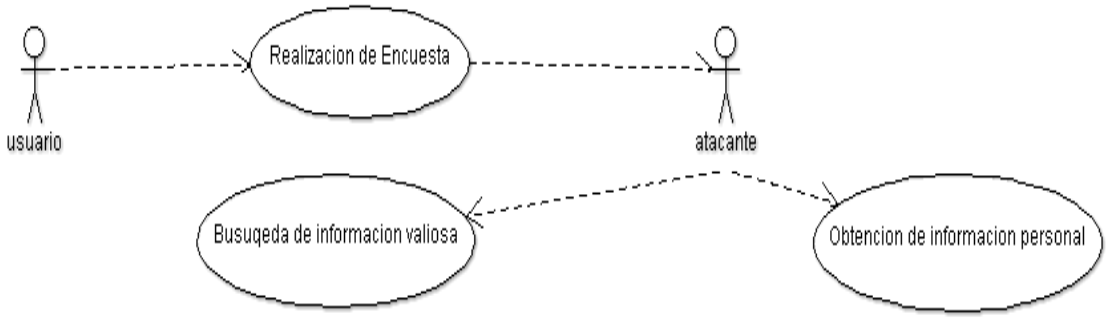


Figura 6 Diagrama del Phishing. Fuente: Autor propio.

Man in the Middle

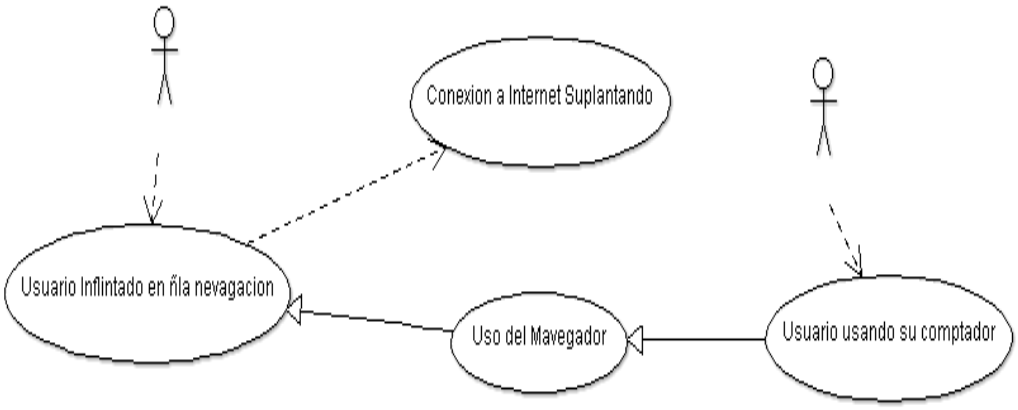


Figura 7 Diagrama Man in the Middle. Fuente: Autor propio.

Email Spoofing

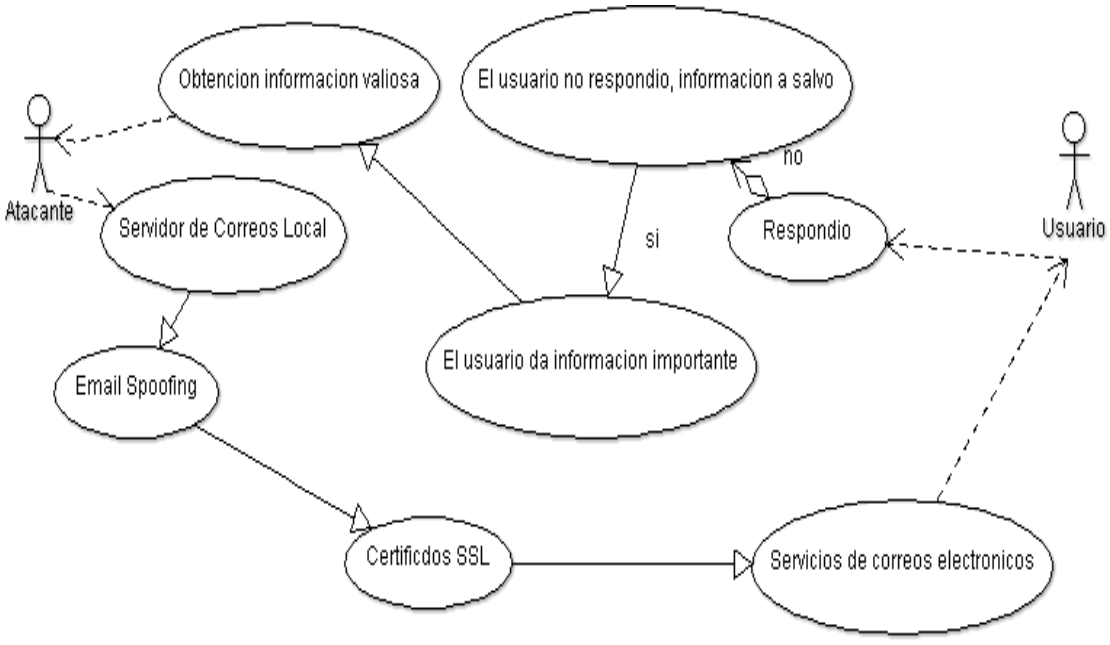


Figura 8 Diagrama de Email Spoofing. Fuente: Autor propio.

Diseño lógico de red

En la Figura 9, presentamos el diseño de red que pertenece a la Universidad del Sinú seccional Cartagena Sede Plaza Colón, donde se muestra la organización interna de dicha sede. La infraestructura de red tiene el Router que proporciona el Proveedor, dicho router está conectado, a su vez, a un Switch Cisco Catalyst 2960 de 24 puertos LAN. A este Switch hay conectados un Datacenter (Principal), donde está configurado el DNS primario y el DNS secundario, una Controladora Inalambrica Cisco 2504 y otro Datacenter Secundario que tiene conectado los 17 Access Point repartidos por toda la sede. La red, por seguridad, tiene configurada dos Vlan, una llamada **Estudiantes** que tiene un direccionamiento IP por DHCP 192.168.8.0 /21 y otra llamada **Administrativos** que tiene también direccionamiento IP por DHCP 192.168.16.0 /21.

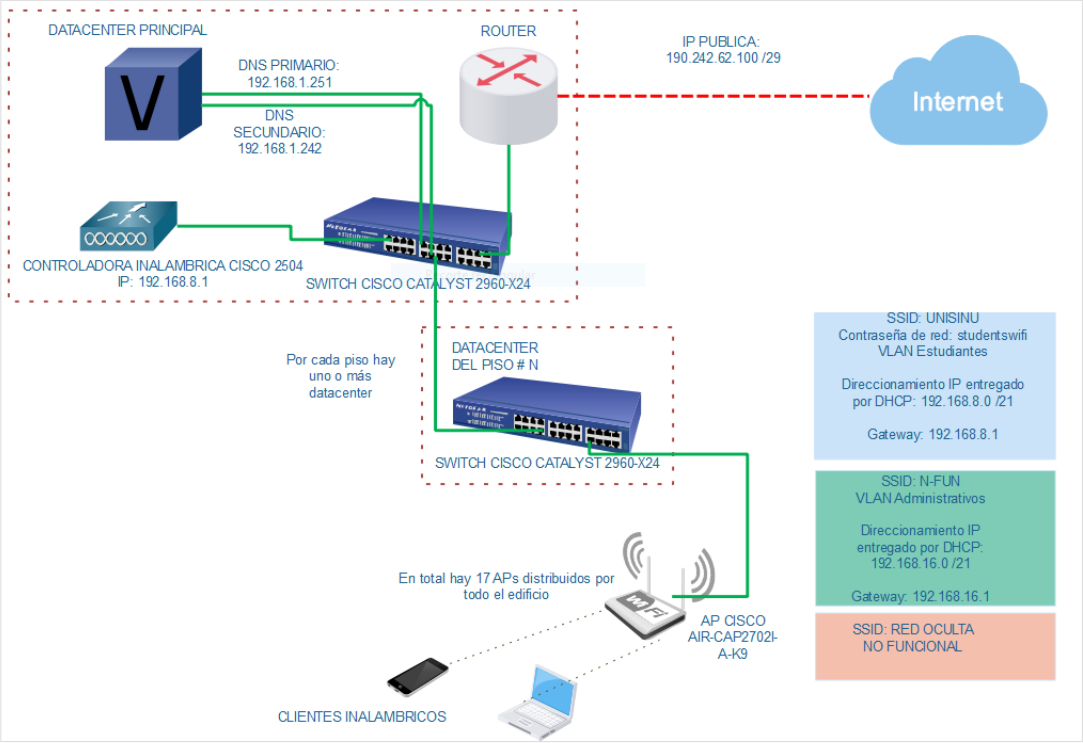


Figura 9 Diseño Lógico de Red - Sede Plaza Colón. Fuente: Autor propio.

3. DISEÑO DE LA SOLUCIÓN

Con el fin de obtener resultados usaremos las herramientas de recolección de información tales como:

- **La Encuesta**

  Se realizará encuestas a la comunidad estudiantil y el personal administrativo de ciertas áreas de la Universidad del Sinú sede Plaza Colón, con el fin de obtener datos personales o información institucional.

  Encuesta comunidad estudiantil: Ver anexo 2
  Encuesta personal Administrativo: Ver anexo 3

- **La Entrevista**

  Está dirigida al Jefe de Sistemas de la Universidad del Sinú para determinar la sede donde se desarrollaría el Análisis de vulnerabilidades en los sistemas informáticos de la Universidad del Sinú.

  Entrevista: Ver anexo 4

- **La Observación**

  Este método nos permite observar los diferentes casos que han ocurrido sobre delitos informáticos, y determinar que falencias los han causado.

4. DESARROLLO

Selección de la técnica

Para el desarrollo del proyecto se decidió utilizar la técnica de Ingeniería Social como el Phishing, gracias a su gran porcentaje de efectividad en vulnerabilidades y, además, la técnica de ARP Spoofing para la captura del tráfico en la red de la Universidad.

Para la realización del proyecto de grado de análisis de vulnerabilidades, se estipulan las siguientes actividades que se realizaron en la sede Plaza Colón con el único fin de estudiar la información obtenida de acuerdo con los lineamientos y autorizaciones que nos dió la Universidad a través del Ing. Alberto Jiménez, jefe de Tics. Las actividades desarrolladas fueron:

1. Se realizó un seguimiento a los estudiantes y funcionarios con ingeniería social usando la técnica de PHISHING como la mejor técnica de captura de información [24].
2. Se realizó el análisis de la información obtenida para determinar si algún dato es relevante para el estudio.
3. Se llevó a cabo una captura de tráfico de datos y metadatos bajo la supervisión del ingeniero responsable de la universidad, para el control de información [25].
    a. Opcional: Realización de un ataque MiTM o JANUS: suplantación digital de equipos para la obtención de información [26].
4. Envío de encuesta de información a estudiantes de diferentes áreas haciendo suplantación digital de miembros de personal de la universidad (siempre supervisado por personal del área de TI de la Universidad)
5. Entrega de información recopilada, junto con su análisis, al jefe de TI para determinar el uso que se le puede dar y que se puede divulgar de los resultados obtenidos para el desarrollo del trabajo de grado.

4.1. Aplicando el método de Denegación de Servicio.

Denegación de servicios de red de la universidad del Sinú.

Fecha: 10/04/18 6:10p.m.

Se realizó un ataque DOS que no permitió a estudiantes y funcionarios utilizar los servicios de Internet durante este tiempo.

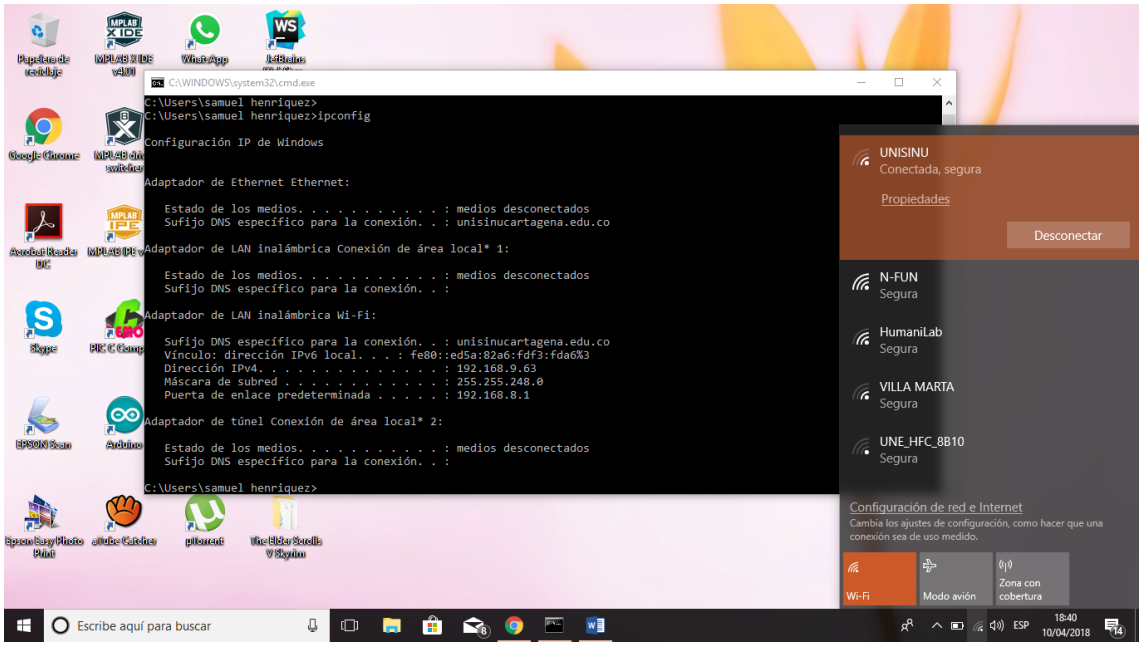


Figura 10 Servicio de Internet disponible en la Universidad. Fuente: Autor propio.

En la Figura 10, podemos notar que el equipo está conectado a la red Wifi de la Universidad del Sinú de SSID UNISINU con una dirección IP asignada dinámicamente 192.168.9.63, y tiene disponible el servicio de internet para navegar sin ningún tipo de Inconveniente.

Ahora bien, se procede a realizar un ataque de denegación de servicio con el fin de que todos los equipos conectados en la red pierdan la conexión a la navegación a Internet.

Las siguientes actividades se realizan para ataque de denegación de servicios:

1. Se utiliza un Smartphone con sistema operativo Android previamente rooteado para realización de la denegación.
2. Instalar Wifikill.apk para Android que no se encuentra en la tienda virtual Play Store de Google, pero si se puede descargar en una fuente externa.
3. Se inicia la aplicación donde procedemos a hacer:
    a. Detectar las conexiones de red SSID UNISINU.
    b. Se hace un escaneado para consumir las direcciones.
    c. Comienza a utilizar todas las direcciones disponibles.
4. Al utilizar todas las direcciones el Access Point es saturado, y no permite la navegación a Internet.

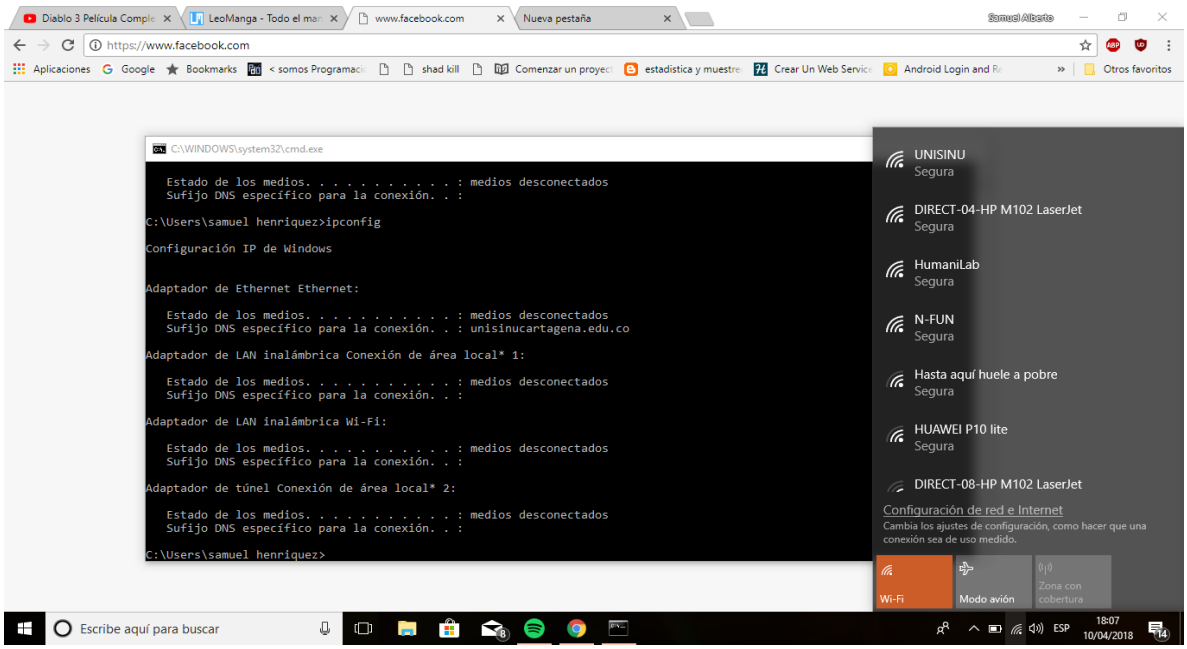


Figura 11 Denegación de servicio de Internet. Fuente: Autor propio.

4.2. Aplicando captura de tráfico con la herramienta Wireshark

La prueba de Wireshark se realizó, pero se necesita un conocimiento muy amplio en redes para el análisis de la información obtenida, ya que la cantidad de la información es sobreabundante, por lo que al realizar captura de todo el tráfico se detalla mucha información y la calidad de dicha información puede disminuir mucho.

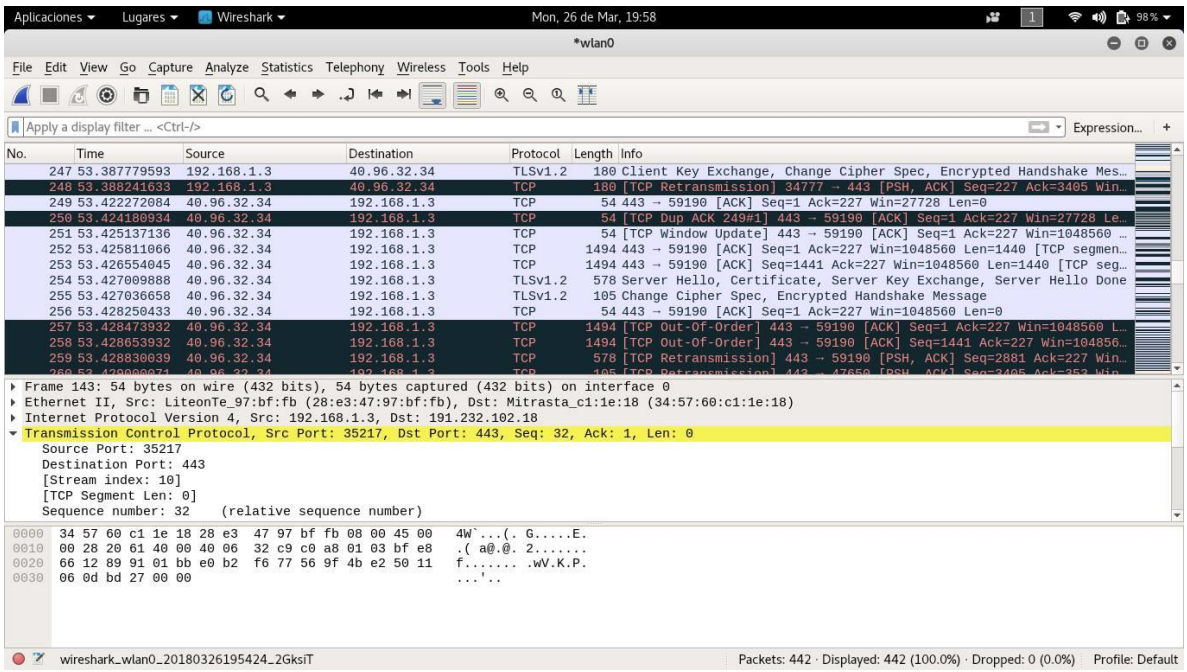


Figura 12 Captura de tráfico doméstico. Fuente: Autor propio.

La prueba realizada con la herramienta Wireshark se realizó en una red doméstica bastante pequeña para demostrar que es muy útil pero refleja demasiada información que resulta muy complejo de resolver. Ahora bien, si es muy grande la información en una red pequeña, como la de prueba, debemos imaginarnos cuán grande debe ser la información que revelará esta herramienta en una red tan grande como la de la Universidad del Sinú.

4.3. Aplicando captura de tráfico con Bettercap

En el desarrollo de las actividades se instala la herramienta bettercap, la cual es una herramienta que se especializa en hacer MIDLE THE MIDLE para hacer la captura de las actividades utilizando los navegadores web.

Instalación

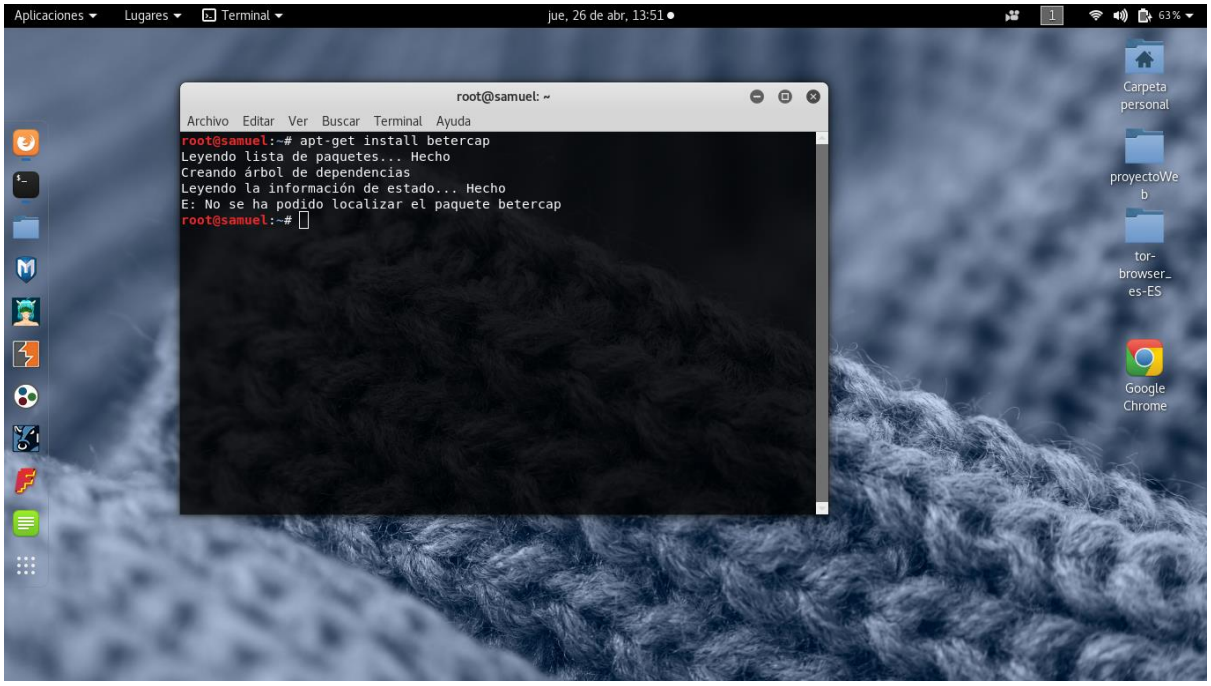


Figura 13 Instalación de Bettercap. Fuente: Autor propio.

Al estar instalado el Bettercap, se hace uso de la técnica de ARP SPOFFING que consiste en interceptar el tráfico que hay entre el router y el equipo, y con esto, capturar toda la actividad que este haga.

En esta actividad se usarán, para la captura del tráfico, los protocolos HTTP y HTTPS. El tráfico es obtenido exitosamente gracias a que esta herramienta utiliza certificados SSL para obtener los datos de las páginas web, no todo el tráfico puede ser capturado con solo el uso de estas herramientas para realizar en plenitud la captura de datos de páginas como Facebook, Twitter, etc. se

requiere, además, utilizar dispositivos especializados para la duplicación de certificados de estas páginas o de empresas.

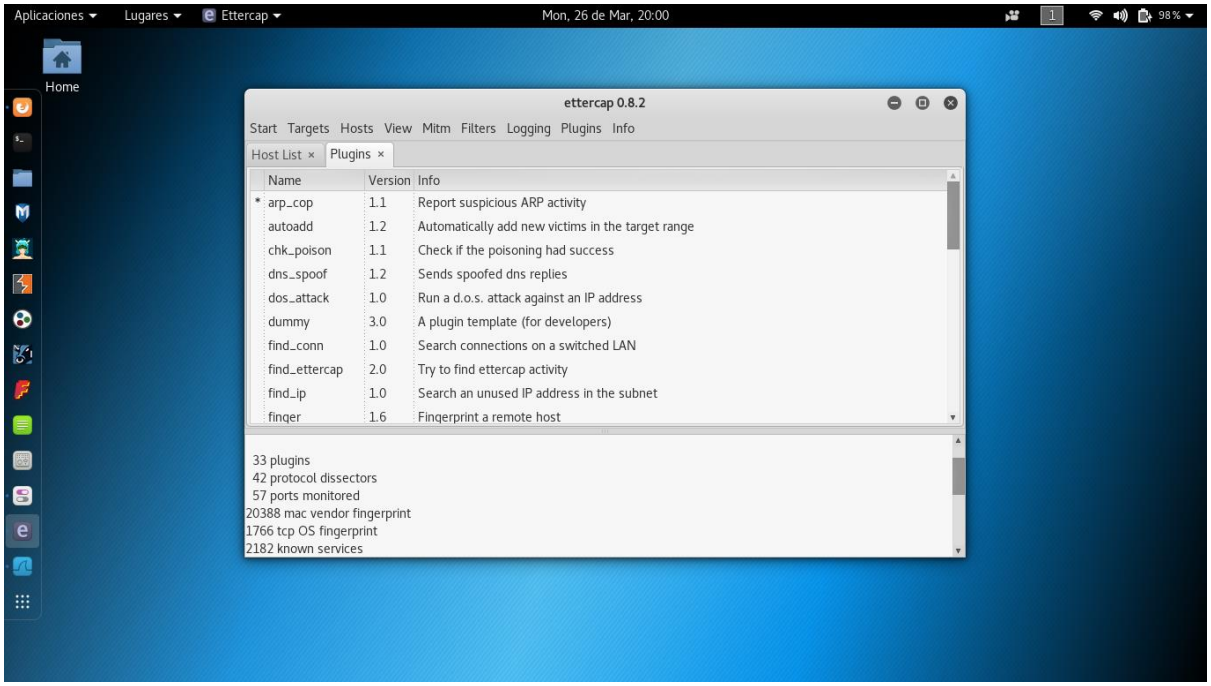


Figura 14 Programa Ettercap. Fuente: Autor propio.

Comienzo Captura de Datos

Se inicializa la terminal de comandos y se escribe el siguiente comando para la captura de tráfico HTTP:

- Bettercap -T xxx.xxx.xxx.xxx -- proxy -P -POST

Este comando sencillamente lo que hace es realizar una captura de los elementos enviados y recibidos por las páginas web y el navegador del usuario intervenido.

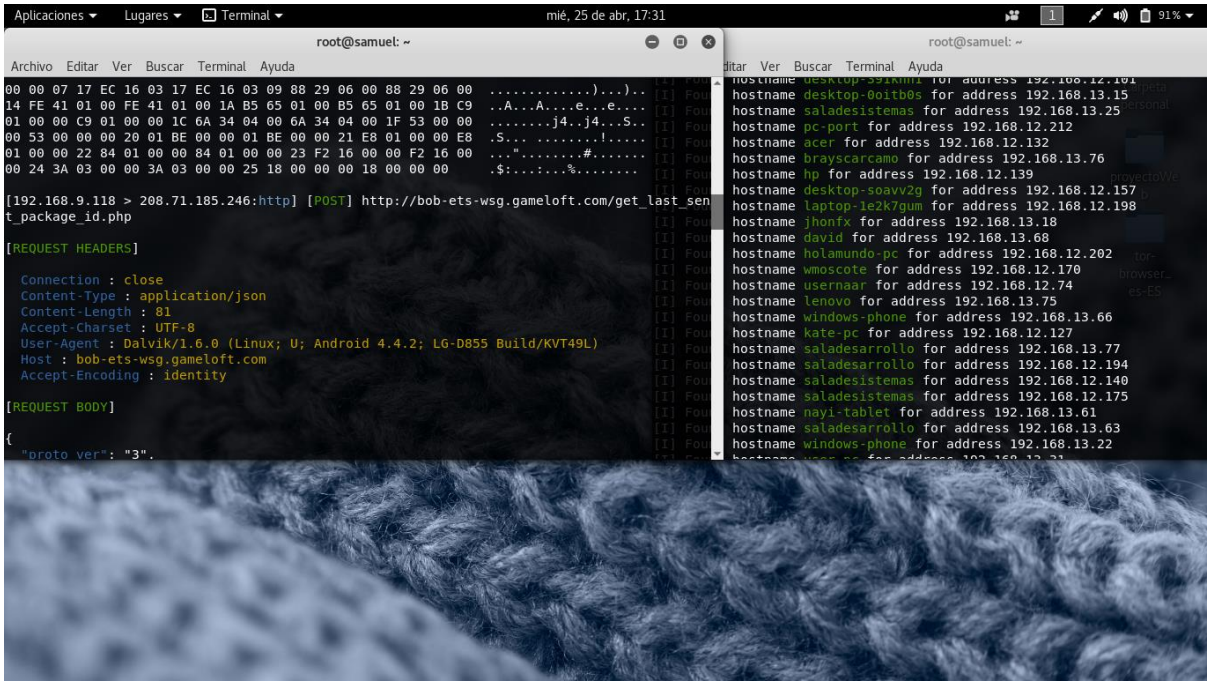


Figura 15 Captura del tráfico. Fuente: Autor propio.

Como se puede observar, en la ilustración anterior se muestran 2 terminales, en la terminal derecha se muestra la información de los equipos que se encuentran actualmente conectados en la red de la Universidad del Sinú seccional Cartagena - sede plaza colón, y en la terminal izquierda se muestra la captura de tráfico de algunos equipos con actividad en la red.

Nota: Esta captura de información se logró por el hecho de estar conectado a la red LAN de la Universidad, por el contrario, el uso de esta herramienta conectado a una red Wifi no es válido, ya que no puede conectarse al Access Point que se encuentra distribuyendo la red.

A continuación, se puede visualizar algunas imágenes obtenidas en el transcurso de la semana del tráfico en la red.

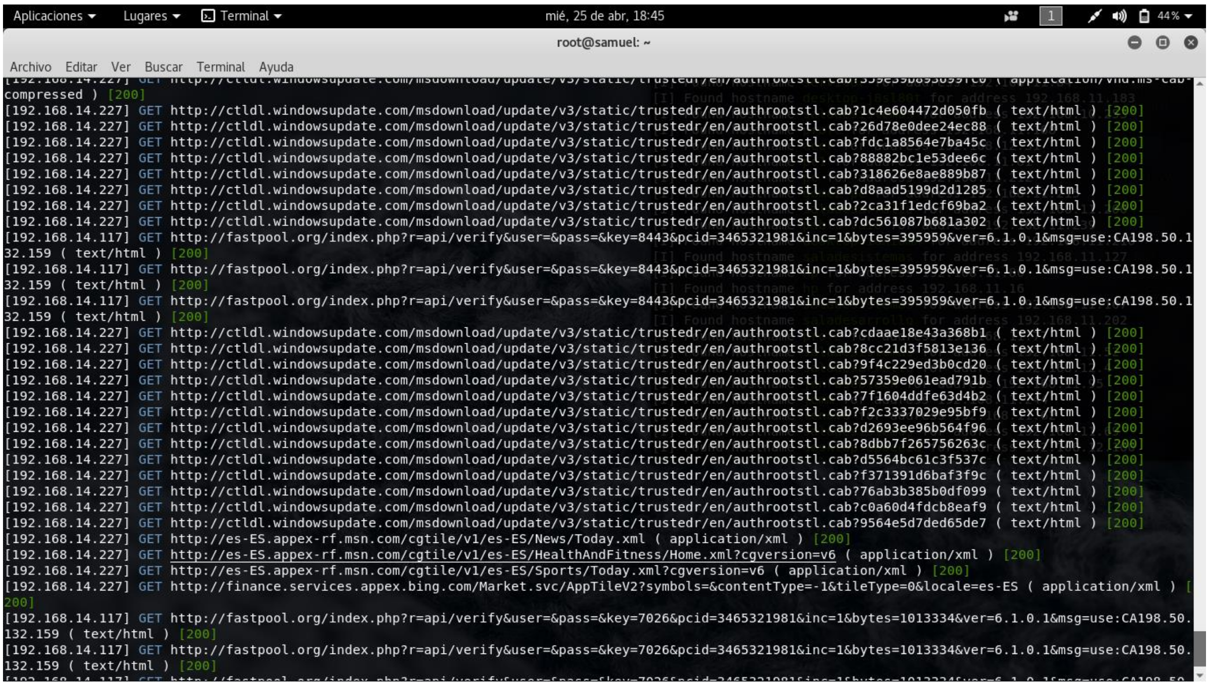


Figura 16 Captura de tráfico de un usuario aleatorio. Fuente: Autor propio.

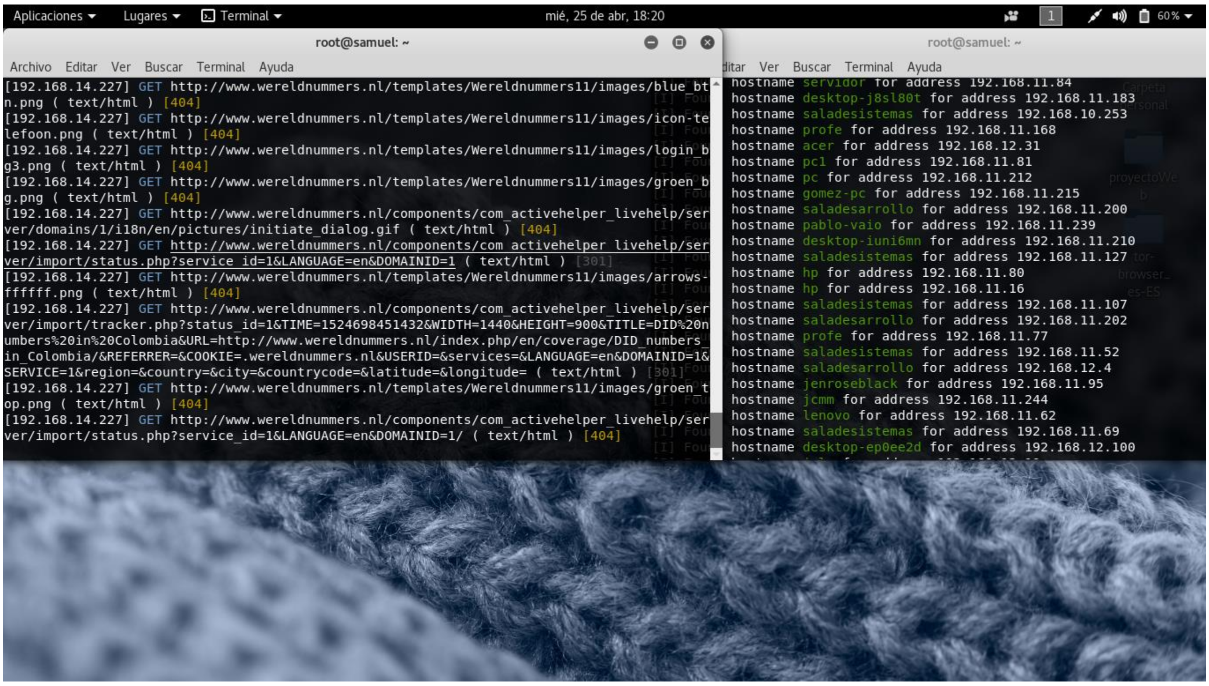


Figura 17 Alerta de código 404 en la web wereldnurners.nl. Fuente: Autor propio.

En la Figura 17 se puede evidenciar, con el código 404, cuando un usuario no obtuvo exitosamente el acceso a una página web, esto se debe a que

el equipo ha sido capaz de comunicarse con el servidor, pero no existe el recurso que ha sido pedido.

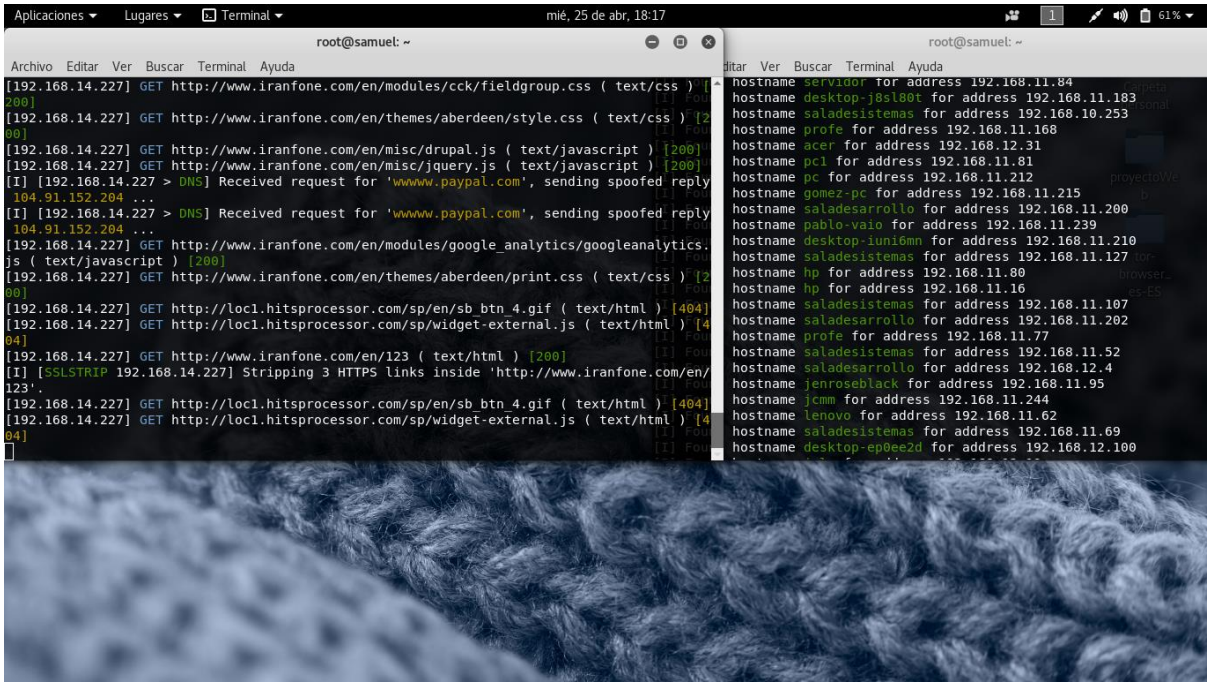


Figura 18 Alerta de código 404 en la web loc1.hitsprocessor.com. Fuente: Autor propio.

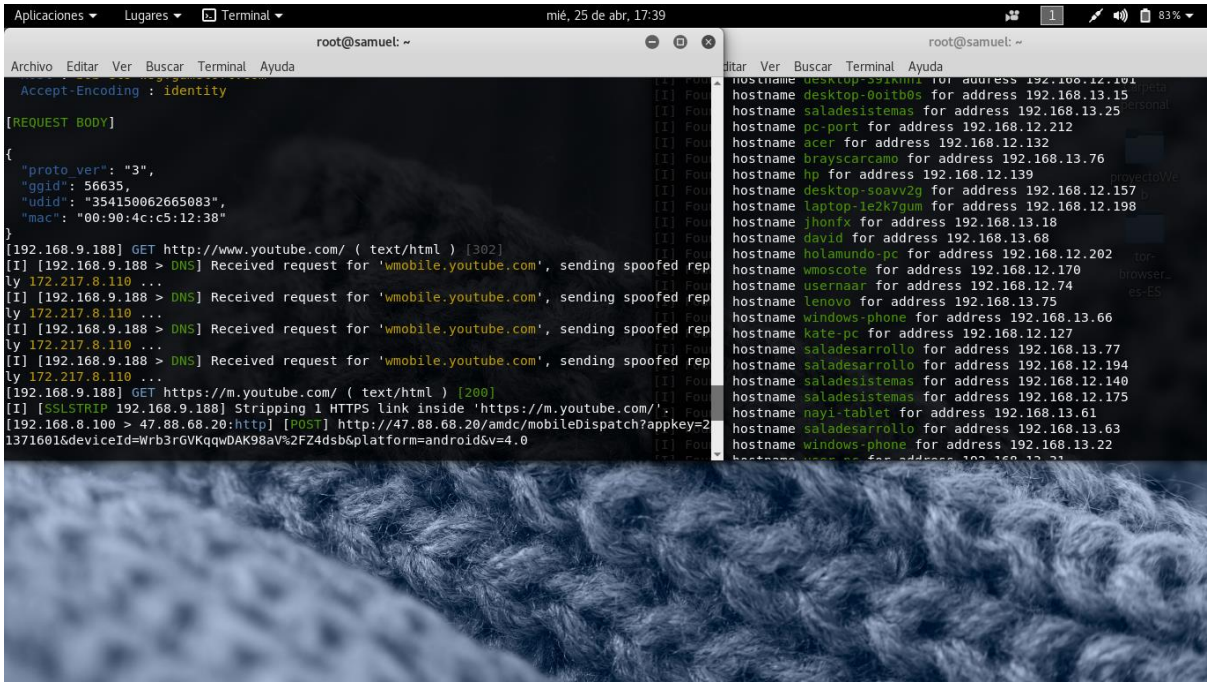


Figura 19 Smartphone consultando la web youtube.com. Fuente: Autor propio.

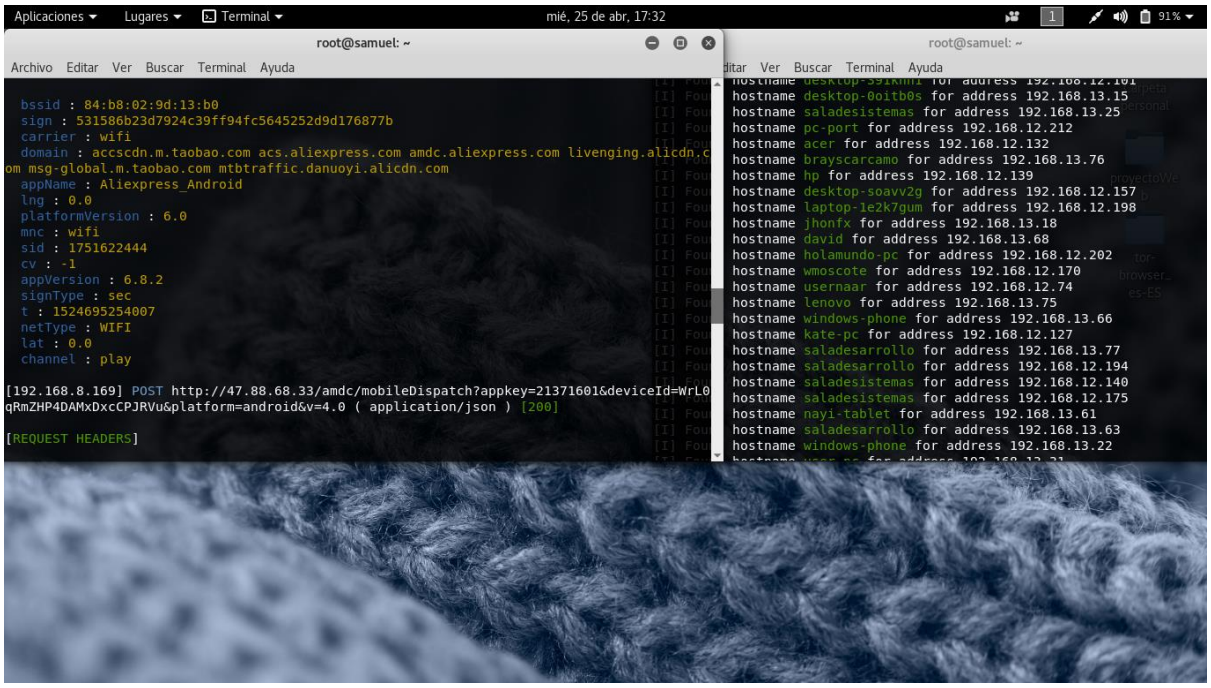


Figura 20 Smartphone utilizando la app Aliexpress. Fuente: Autor propio.

En las Figuras 19 y 20, se puede observar que se está utilizando un dispositivo móvil y, además, se puede diferenciar si el usuario está utilizando una aplicación o un navegador. En la Figura 19, el usuario está utilizando un navegador y consultando la web de youtube.com; por el contrario, en la Figura 20, el usuario está utilizando una aplicación actualmente muy reconocida como Aliexpress.

4.4. Email Spoofing

Se utilizará un servidor de correos con la herramienta POSTFIX para realizar una suplantación electrónica por medio de los correos electrónicos. Instalación del servidor y herramienta para su uso:

- apt-get install postfix
- apt-get install mailutils
- opcional: descargar el repositorio sees para la agilización de esta actividad.

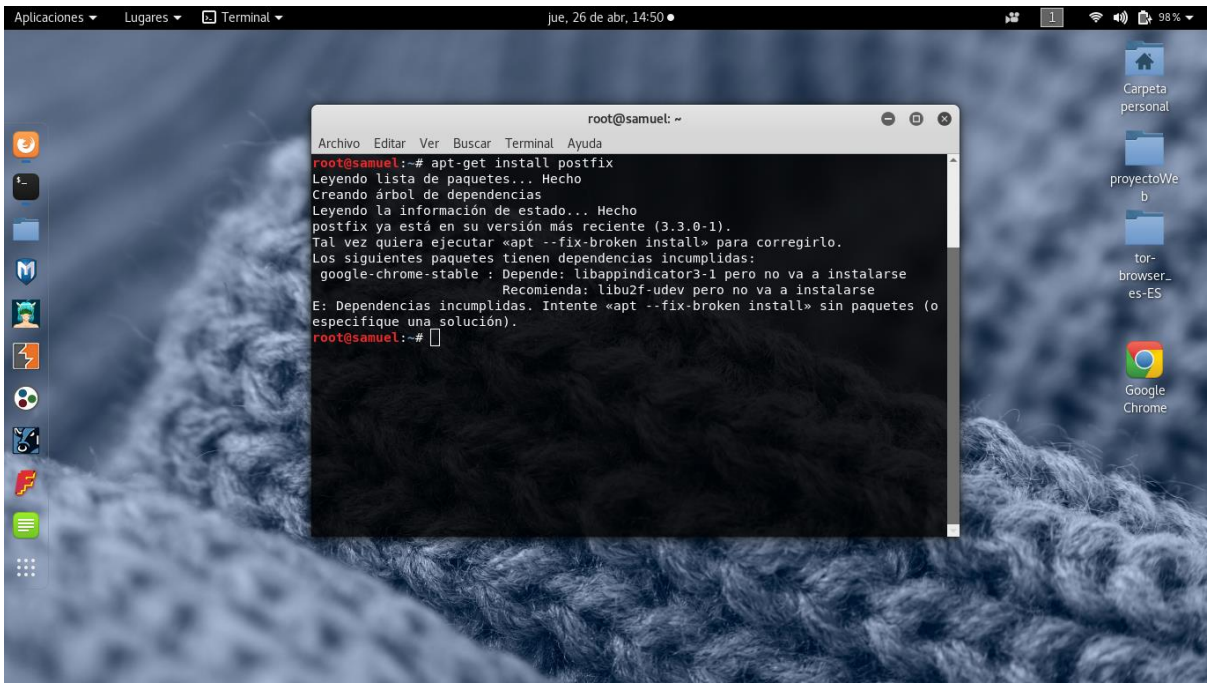


Figura 21 instalación en equipo Kali Linux del servidor de correos. Fuente: Autor Propio.

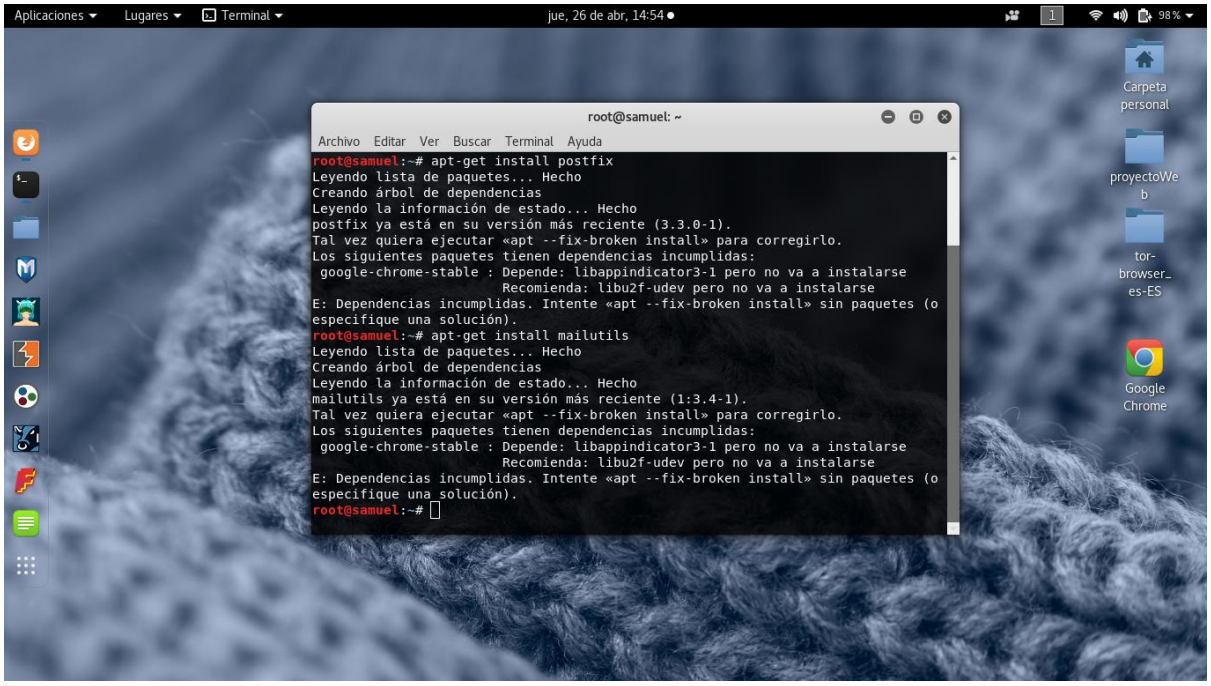


Figura 22 Uso de comandos para instalar herramientas adicionales. Fuente: Autor propio.

Se utiliza el comando sendemail para realizar el envío masivo de correos a los usuarios.

En el desarrollo del Email Spoofing, este no fue exitoso por diversos sucesos, tal como la seguridad en el logue con el protocolo Gmail.smtp-in.l.Google.com que no permitió su utilización al no presentar credenciales de logueo y certificados SSL actualizados, dificultad en el uso de herramientas de terceros como SEES, problemas de configuración en el equipo.

La captura de tráfico en la red de la Universidad del Sinú sede Plaza Colón, nos permitió analizar y deducir que se puede obtener información de las actividades que realiza un usuario en la red.

4.5. Aplicando escáner de vulnerabilidades en servidor(es) de alojamiento web de la Universidad del Sinú sede Plaza Colón, con la herramienta GoLismero 2.0

GoLismero, es una herramienta orientada a realizar auditorías de páginas web para buscar posibles agujeros de seguridad existentes en estas, aunque también podría ser utilizado para buscar fallos en cualquier otro tipo de servicios, tales como: redes, servidores, etc. Esta herramienta de seguridad viene integrada, por lo general, en la instalación del sistema operativo Kali Linux, es muy fácil de usar y completa para realizar un exhaustivo análisis de una página web.

Comando para ejecutar el escáner en busca de vulnerabilidades

root@samuel:~# golismero scan http://www.unisinucartagena.edu.co

```
root@samuel:~# golismero scan http://www.unisinucartagena.edu.co

/-------------------------------------------\
| GoLismero 2.0.0b6, The Web Knife          |
| Copyright (C) 2011-2014 GoLismero Project |
|                                           |
| Contact: contact@golismero-project.com    |
\-------------------------------------------/

GoLismero started at 2018-05-05 19:20:14.051957 UTC
[*] GoLismero: Audit name: golismero-TVpj0kyD
[!] Shodan: Plugin disabled, reason: Missing API key! Get one at: http://www.shodanhq.com/api_doc
[!] SpiderFoot: Plugin disabled, reason: SpiderFoot plugin not configured! Please specify the URL to connect to the SpiderFoot
[!] OpenVAS: Plugin disabled, reason: Missing hostname
[*] GoLismero: Added 4 new targets to the database.
[*] GoLismero: Launching tests...
[*] GoLismero: Current stage: Reconaissance
[*] theHarvester: Searching keyword 'unisinucartagena.edu.co' in google
[*] Web Spider: Spidering URL: http://www.unisinucartagena.edu.co/
[*] DNS Resolver: 11.11% percent done...
[*] DNS Resolver: 22.22% percent done...
[*] DNS Resolver: 33.33% percent done...
[*] DNS Resolver: 44.44% percent done...
[*] DNS Resolver: 55.55% percent done...
[*] DNS Resolver: 66.66% percent done...
[*] DNS Resolver: 77.77% percent done...
[*] DNS Resolver: 88.88% percent done...
[*] DNS Resolver: 100.00% percent done...
[!] PunkSPIDER: Query to PunkSPIDER failed, reason: [SSL: CERTIFICATE_VERIFY_FAILED] certificate verify failed (_ssl.c:726)
[*] PunkSPIDER: No results found for host: unisinucartagena.edu.co
[*] theHarvester (2): Searching keyword 'www.unisinucartagena.edu.co' in google
[*] theHarvester: Found 8 emails and 5 hostnames on google for domain unisinucartagena.edu.co
[*] theHarvester: Searching keyword 'unisinucartagena.edu.co' in bing
[*] theHarvester: 20.00% percent done...
[!] theHarvester: Invalid header name 'Cookie: SRCHHPGUSR=ADLT=DEMOTE&NRSLT=50'
[*] theHarvester: Searching keyword 'unisinucartagena.edu.co' in linkedin
[*] theHarvester: 40.00% percent done...
[!] PunkSPIDER: Query to PunkSPIDER failed, reason: [SSL: CERTIFICATE_VERIFY_FAILED] certificate verify failed (_ssl.c:726)
[*] PunkSPIDER: No results found for host: www.unisinucartagena.edu.co
```

Figura 23 Comienzo escáner de la red de la Universidad del Sinú sede Plaza Colón con GoLismero. Fuente: Autor propio.

En la Figura 23, logramos ver el inicio de la ejecución del escáner con la herramienta GoLismero en busca de vulnerabilidades. Además, podemos apreciar que la validación del certificado SSL para la web www.unisinucartagena.edu.co falló, debido a que probablemente este certificado ha caducado.

```
[*] GoLismero: Current stage: Scanning (non-intrusive)
[*] Bruteforce predictables discovery: Loaded 147 URLs to test.
[*] Bruteforce predictables discovery: 0.68% percent done...
[*] Plecost: No WordPress instalation found in 'http://www.unisi
[*] Bruteforce predictables discovery: 1.36% percent done...
[*] Bruteforce predictables discovery: 2.04% percent done...
[*] Bruteforce predictables discovery: 2.72% percent done...
[*] Bruteforce predictables discovery: 3.40% percent done...
[*] Bruteforce predictables discovery: 4.08% percent done...
[*] Bruteforce predictables discovery: 4.76% percent done...
[*] Bruteforce predictables discovery: 5.44% percent done...
[*] Bruteforce predictables discovery: 6.12% percent done...
[*] Bruteforce predictables discovery: 6.80% percent done...
[*] Bruteforce predictables discovery: 7.48% percent done...
[*] Bruteforce predictables discovery: 8.16% percent done...
[*] Bruteforce predictables discovery: 8.84% percent done...
[*] Bruteforce predictables discovery: 9.52% percent done...
[*] Bruteforce predictables discovery (2): Loaded 147 URLs to te
[*] Bruteforce predictables discovery: 10.20% percent done...
[*] Bruteforce predictables discovery: 10.88% percent done...
[*] Nikto: Launching Nikto against: old.unisinucartagena.edu.co
[*] Bruteforce predictables discovery: 11.56% percent done...
[*] Bruteforce predictables discovery: 12.24% percent done...
[*] Bruteforce predictables discovery: 12.92% percent done...
[*] Bruteforce predictables discovery: 13.60% percent done...
[*] Bruteforce predictables discovery: 14.28% percent done...
[*] Bruteforce predictables discovery: 14.96% percent done...
[*] Bruteforce predictables discovery: 15.64% percent done...
```

Figura 24 GoLismero intentando encontrar agujeros de seguridad. Fuente: Autor propio.

En la Figura 24, vemos una captura de GoLismero en ejecución, intentando encontrar algún directorio en el que se pueda realizar algún ataque de fuerza bruta.

```
[*] Bruteforce predictables discovery (2): 99.31% percent done...
[*] Nikto: Launching Nikto against: www.unisinucartagena.edu.co
[*] Nikto: - Nikto v2.1.5
[*] Nikto: ---------------------------------------------------------------------------
[*] Nikto: + Target IP:          192.168.1.114
[*] Nikto: + Target Hostname:    www.unisinucartagena.edu.co
[*] Nikto: + Target Port:        80
[*] Nikto: + Start Time:         2018-05-05 14:38:20 (GMT-5)
[*] Nikto: ---------------------------------------------------------------------------
[*] Nikto: + Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.4.16
[*] Nikto: + 6493 items checked: 0 error(s) and 0 item(s) reported on remote host
[*] Nikto: + End Time:           2018-05-05 14:38:30 (GMT-5) (10 seconds)
[*] Nikto: ---------------------------------------------------------------------------
[*] Nikto: + 1 host(s) tested
[*] Nikto: Nikto found 0 vulnerabilities for host: www.unisinucartagena.edu.co
```

Figura 25 Información del servidor de alojamiento y su IP. Fuente: Autor propio.

En la Figura 25, destacamos la información del servidor donde se aloja la página web de la Universidad del Sinú (www.unisinucartagena.edu.co). La dirección IP del servidor de alojamiento es la 192.168.1.114. Además, podemos ver en la última línea de la imagen que hace referencia a que no se ha encontrado vulnerabilidades en dicho servidor.

```
[*] Nmap: Initiating Parallel DNS resolution of 1 host. at 14:33
[*] Nmap: Completed Parallel DNS resolution of 1 host. at 14:33, 0.01s elapsed
[*] Nmap: Initiating SYN Stealth Scan at 14:33
[*] Bruteforce predictables discovery (2): 17.68% percent done...
[*] Nmap: Scanning www.unisinucartagena.edu.co (192.168.1.114) [1000 ports]
[*] Nmap: Discovered open port 80/tcp on 192.168.1.114
[*] Nmap: Discovered open port 22/tcp on 192.168.1.114
[*] Nmap: Discovered open port 443/tcp on 192.168.1.114
[*] Nmap: Discovered open port 3306/tcp on 192.168.1.114
[*] Nmap: Discovered open port 111/tcp on 192.168.1.114
[*] Nmap: Discovered open port 21/tcp on 192.168.1.114
[*] Bruteforce predictables discovery (3): 47.61% percent done...
[*] Bruteforce predictables discovery (2): 18.36% percent done...
[*] Bruteforce predictables discovery (3): 48.29% percent done...
[*] Nmap: Discovered open port 5060/tcp on 192.168.1.114
[*] Nmap: Discovered open port 2000/tcp on 192.168.1.114
[*] Bruteforce predictables discovery (2): 19.04% percent done...
[*] Nmap: Completed SYN Stealth Scan at 14:33, 1.62s elapsed (1000 total ports)
```

Figura 26 Descubrimiento de puertos abiertos en el servidor. Fuente: Autor propio.

En la Figura 26, se puede evidenciar los puertos que están abiertos en el servidor donde se aloja la página web de la Universidad del Sinú, tales como: 80, 22, 443, 3306, 111, 21, 5060 y el 2000.

```
*] Nmap: |_-----END CERTIFICATE-----
*] Nmap: |_ssl-date: TLS randomness does not represent time
*] Nmap: 2000/tcp open  tcpwrapped syn-ack ttl 62
*] Nmap: 3306/tcp open  mysql      syn-ack ttl 61 MySQL 5.5.56-MariaDB
*] Nmap: | mysql-info:
*] Nmap: |   Protocol: 10
*] Nmap: |   Version: 5.5.56-MariaDB
*] Nmap: |   Thread ID: 23684
*] Nmap: |   Capabilities flags: 63487
*] Nmap: |   Some Capabilities: LongColumnFlag, IgnoreSpaceBeforeParenthesis, Support
*] Nmap: |   Status: Autocommit
*] Nmap: |   Salt: MR4L`|sK]rD=D{c](O6]
*] Nmap: |_  Auth Plugin Name: 87
*] Nmap: 5060/tcp open  tcpwrapped syn-ack ttl 62
*] Nmap: Device type: general purpose
*] Nmap: Running: Linux 4.X
*] Nmap: OS CPE: cpe:/o:linux:linux_kernel:4.4
*] Nmap: OS details: Linux 4.4
```

Figura 27 Información de la Base de datos y el OS del Servidor. Fuente: Autor propio.

En la Figura 27, encontramos información relevante del motor de base de datos y el sistema operativo utilizado, del servidor de alojamiento. El servidor cuenta con un motor de base de datos MySQL versión 5.5.56-MariaDB y un Sistema Operativo Linux 4.4.

```
[*] Nikto: + Target IP:          192.168.1.242
[*] Nikto: + Target Hostname:    old.unisinucartagena.edu.co
[*] Nikto: + Target Port:        80
[*] Nikto: + Start Time:         2018-05-05 14:21:04 (GMT-5)
[*] Nikto: ---------------------------------------------------------
[*] Nikto: + Server: Apache/2.2.3 (CentOS)
[*] Bruteforce predictables discovery: 54.42% percent done
```

Figura 28 Información del servidor de alojamiento de subdominio 'old'. Fuente: Autor propio.

En la Figura 28, destacamos la información del servidor donde se aloja la página web antigua de la Universidad del Sinú (old.unisinucartagena.edu.co). La dirección IP del servidor de alojamiento es la 192.168.1.242.

```
[*] Nikto: + 6493 items checked: 0 error(s) and 0 item(s) reported on remote host
[*] Nikto: + End Time:           2018-05-05 14:21:16 (GMT-5) (12 seconds)
[*] Nikto: ---------------------------------------------------------------------------
[*] Nikto: + 1 host(s) tested
[*] Nikto: Nikto found 0 vulnerabilities for host: old.unisinucartagena.edu.co
```

Figura 29 Vulnerabilidad en el subdominio 'old'. Fuente: Autor propio.

En la Figura 29, podemos ver en la última línea de la imagen que hace referencia a que no se ha encontrado vulnerabilidades en dicho servidor.

```
[*] Nikto: Launching Nikto against: tic.unisinucartagena.edu.co
[*] Bruteforce predictables discovery (3): 47.61% percent done...
[*] SSLScan: Version: 1.11.11-static
[*] SSLScan: OpenSSL 1.0.2-chacha (1.0.2g-dev)
[*] SSLScan:
[*] SSLScan: Connected to 192.168.1.3
[*] SSLScan:
[*] SSLScan: Testing SSL server tic.unisinucartagena.edu.co on port 443 using SNI name tic.unisinucartagena.edu.co
[*] SSLScan:
[*] SSLScan:   TLS Fallback SCSV:
[*] SSLScan: Server supports TLS Fallback SCSV
[*] SSLScan:
[*] SSLScan:   TLS renegotiation:
[*] SSLScan: Secure session renegotiation supported
[*] SSLScan:
[*] SSLScan:   TLS Compression:
[*] SSLScan: Compression disabled
[*] SSLScan:
[*] SSLScan:   Heartbleed:
[*] SSLScan: TLS 1.2 not vulnerable to heartbleed
[*] SSLScan: TLS 1.1 not vulnerable to heartbleed
[*] SSLScan: TLS 1.0 not vulnerable to heartbleed
[*] SSLScan:
[*] SSLScan:   Supported Server Cipher(s):
[*] SSLScan: Preferred TLSv1.2  256 bits  ECDHE-RSA-AES256-GCM-SHA384    Curve P-256 DHE 256
```

Figura 30 Testeando el certificado SSL del subdominio 'tic'. Fuente: Autor propio.

En la Figura 30, vemos que se realiza una prueba para validar la información del servidor de certificado SSL, en el puerto 443 utilizando el subdominio tic.unisinucartagena.edu.co.

```
[*] SSLScan: Accepted  TLSv1.1  112 bits  EDH-RSA-DES-CBC3-SHA          DHE 1024 bits
[*] Nikto: - Nikto v2.1.5
[*] Nikto: ---------------------------------------------------------------------------
[*] Bruteforce predictables discovery (3): 48.29% percent done...
[*] Bruteforce predictables discovery (3): 48.97% percent done...
[*] Nikto: + Target IP:          192.168.1.3
[*] Nikto: + Target Hostname:    tic.unisinucartagena.edu.co
[*] Nikto: + Target Port:        80
[*] Nikto: + Start Time:         2018-05-05 14:24:40 (GMT-5)
[*] Nikto: ---------------------------------------------------------------------------
[*] Nikto: + Server: Apache/2.4.17 (Win32) OpenSSL/1.0.2d PHP/5.6.23
```

Figura 31 Información del servidor de alojamiento del subdominio 'tic'. Fuente: Autor propio.

En la Figura 31, destacamos la información del servidor donde se aloja el subdominio tic.unisinucartagena.edu.co. La dirección IP del servidor de alojamiento es la 192.168.1.3.

```
[*] SSLScan: Accepted  TLSv1.0  128 bits  IDEA-CBC-SHA
[*] SSLScan:
[*] SSLScan:   SSL Certificate:
[*] SSLScan: Signature Algorithm: sha1WithRSAEncryption
[*] SSLScan: RSA Key Strength:    1024
[*] SSLScan:
[*] SSLScan: Subject:  localhost
[*] SSLScan: Issuer:   localhost
[*] SSLScan:
[*] SSLScan: Not valid before: Nov 10 23:48:47 2009 GMT
[*] SSLScan: Not valid after:  Nov  8 23:48:47 2019 GMT
[*] SSLScan: SSLScan scan finished in 13.4505770206 seconds for target: tic.unisinucartagena.edu.co
[!] SSLScan: 'NoneType' object has no attribute 'group'
[*] SSLScan: Found 1 SSL vulnerabilities.
[*] Bruteforce predictables discovery (3): 49.65% percent done...
```

Figura 32 Vulnerabilidad del Servidor SSL. Fuente: Autor propio.

En la Figura 32, se evidencia en la penúltima línea que se ha encontrado una vulnerabilidad SSL.

```
[*] Bruteforce predictables discovery (3): 78.23% percent done...
[*] Nikto: Launching Nikto against: bibliotecavirtual.unisinucartagena.edu.co
[*] Nikto: - Nikto v2.1.5
[*] Nikto: ---------------------------------------------------------------------------
[*] Bruteforce predictables discovery (3): 78.91% percent done...
[*] Nikto: + Target IP:          192.168.1.250
[*] Nikto: + Target Hostname:    bibliotecavirtual.unisinucartagena.edu.co
[*] Nikto: + Target Port:        80
[*] Nikto: + Start Time:         2018-05-05 14:37:04 (GMT-5)
[*] Nikto: ---------------------------------------------------------------------------
[*] Nikto: + Server: EZproxy
[*] Nikto: + Root page / redirects to: http://bibliotecavirtual.unisinucartagena.edu.co/login
[*] Bruteforce predictables discovery (3): 79.59% percent done...
[*] Bruteforce predictables discovery (3): 80.27% percent done...
[*] Bruteforce predictables discovery (3): 80.95% percent done...
[*] Bruteforce predictables discovery (3): 81.63% percent done...
[*] Bruteforce predictables discovery (3): 82.31% percent done...
[*] Bruteforce predictables discovery (3): 82.99% percent done...
[*] Bruteforce predictables discovery (3): 83.67% percent done...
[*] Bruteforce predictables discovery (3): 84.35% percent done...
[*] Bruteforce predictables discovery (3): 85.03% percent done...
[*] Bruteforce predictables discovery (3): 85.71% percent done...
[*] Bruteforce predictables discovery (3): 86.39% percent done...
[*] Bruteforce predictables discovery (3): 87.07% percent done...
[*] Nikto: + 6493 items checked: 0 error(s) and 0 item(s) reported on remote host
[*] Nikto: + End Time:           2018-05-05 14:37:18 (GMT-5) (14 seconds)
[*] Nikto: ---------------------------------------------------------------------------
[*] Nikto: + 1 host(s) tested
[*] Nikto: Nikto found 0 vulnerabilities for host: bibliotecavirtual.unisinucartagena.edu.co
```

Figura 33 Información del Servidor de alojamiento del subdominio 'bibliotecavirtual'.

Fuente: Autor propio.

En la Figura 33, destacamos la información del servidor donde se aloja el subdominio bibliotecavirtual.unisinucartagena.edu.co. La dirección IP del servidor de alojamiento es la 192.168.1.250. Además, podemos ver en la última

línea de la imagen que hace referencia a que no se ha encontrado vulnerabilidades en dicho servidor.

```
[*] Bruteforce predictables discovery: 99.31% percent done...
[*] Nikto: Launching Nikto against: helpdesk.unisinucartagena.edu.co
[*] Nikto: - Nikto v2.1.5
[*] Nikto: ---------------------------------------------------------------------------
[*] Nikto: + Target IP:          192.168.1.76
[*] Nikto: + Target Hostname:    helpdesk.unisinucartagena.edu.co
[*] Nikto: + Target Port:        80
[*] Nikto: + Start Time:         2018-05-05 14:45:04 (GMT-5)
[*] Nikto: ---------------------------------------------------------------------------
[*] Nikto: + Server: Apache/2.2.15 (CentOS)
[*] Nikto: + 6493 items checked: 0 error(s) and 0 item(s) reported on remote host
[*] Nikto: + End Time:           2018-05-05 14:45:19 (GMT-5) (15 seconds)
[*] Nikto: ---------------------------------------------------------------------------
[*] Nikto: + 1 host(s) tested
[*] Nikto: Nikto found 0 vulnerabilities for host: helpdesk.unisinucartagena.edu.co
```

Figura 34 Información del Servidor de alojamiento del subdominio 'helpdesk'.

Fuente: Autor propio.

En la Figura 34, destacamos la información del servidor donde se aloja el subdominio helpdesk.unisinucartagena.edu.co. La dirección IP del servidor de alojamiento es la 192.168.1.76. Además, podemos ver en la última línea de la imagen que hace referencia a que no se ha encontrado vulnerabilidades en dicho servidor.

```
[*] Nikto: Launching Nikto against: calidad.unisinucartagena.edu.co
[*] Nikto: - Nikto v2.1.5
[*] Nikto: ---------------------------------------------------------------------------
[*] Nikto: + Target IP:          192.168.1.102
[*] Nikto: + Target Hostname:    calidad.unisinucartagena.edu.co
[*] Nikto: + Target Port:        8010
[*] Nikto: + Start Time:         2018-05-05 15:00:02 (GMT-5)
[*] Nikto: ---------------------------------------------------------------------------
[*] Nikto: + Server: Apache-Coyote/1.1
[*] Nikto: + 6493 items checked: 0 error(s) and 0 item(s) reported on remote host
[*] Nikto: + End Time:           2018-05-05 15:00:16 (GMT-5) (14 seconds)
[*] Nikto: ---------------------------------------------------------------------------
[*] Nikto: + 1 host(s) tested
[*] Nikto: Nikto found 0 vulnerabilities for host: calidad.unisinucartagena.edu.co
```

Figura 35 Información del Servidor de alojamiento del subdominio 'calidad'.

Fuente: Autor propio.

En la Figura 35, destacamos la información del servidor donde se aloja el subdominio calidad.unisinucartagena.edu.co. La dirección IP del servidor de alojamiento es la 192.168.1.102. Además, podemos ver en la última línea de la imagen que hace referencia a que no se ha encontrado vulnerabilidades en dicho servidor.

Mediante la ejecución de la utilidad GoLismero se logró encontrar lo siguiente:

1. El nombre de dominio utilizado por la Universidad del Sinú en internet.
2. El servidor de alojamiento de la Universidad y su dirección IP.
3. Dominios de nivel superior asociados con la Universidad.
4. Cinco subdominios de la forma X.unisinucartagena.edu.co.
5. Los puertos que se encuentran abiertos en los servidores.

Con toda la información recolectada, podemos deducir que la calidad de la seguridad de la información de la Universidad del Sinú sede Plaza colón, actualmente, es muy buena. Según los detalles arrojados por GoLismeros, los servidores no tienen vulnerabilidades, excepto el servidor SSL.

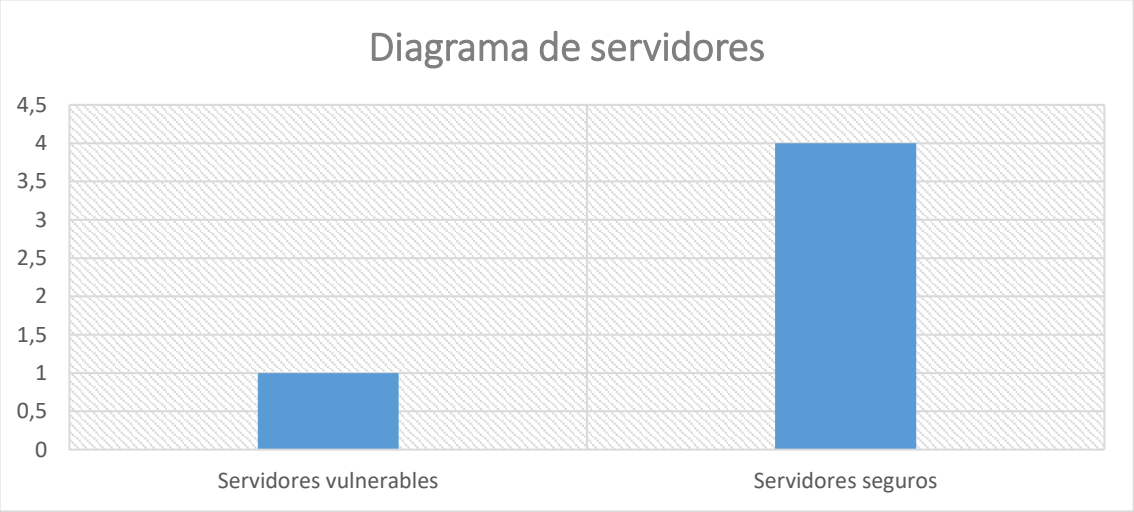


Figura 36 Diagrama de Servidores. Fuente: Autor propio.

En la Figura 36, se muestra la información obtenida, con respecto a la vulnerabilidad, de los servidores de la universidad encontrados por la herramienta GoLismero. Se logra apreciar que hay se encontraron 5 servidores en total de los cuales 4 no tienen vulnerabilidades y 1 presenta vulnerabilidades.

Cabe resaltar que todas las pruebas que se desarrollaron del proyecto, se realizaron con un equipo portátil con unas características básicas, pero resultó muy útil, aunque a veces, este se bloqueaba debido al procesador que tiene, que está por debajo de los 2.0 GHz recomendados para que tener un mejor desarrollo en los procesos. Ver anexo 1

4.6. Análisis Estadístico

En la Universidad del Sinú sede Plaza Colón, se desarrollaron encuestas que permitió evidenciar el grado de información, que tanto la comunidad estudiantil como el personal Administrativo respondieron satisfactoriamente, incluso sin antes haber sido notificados formalmente por algún directivo de dicha Universidad de la realización de la misma.

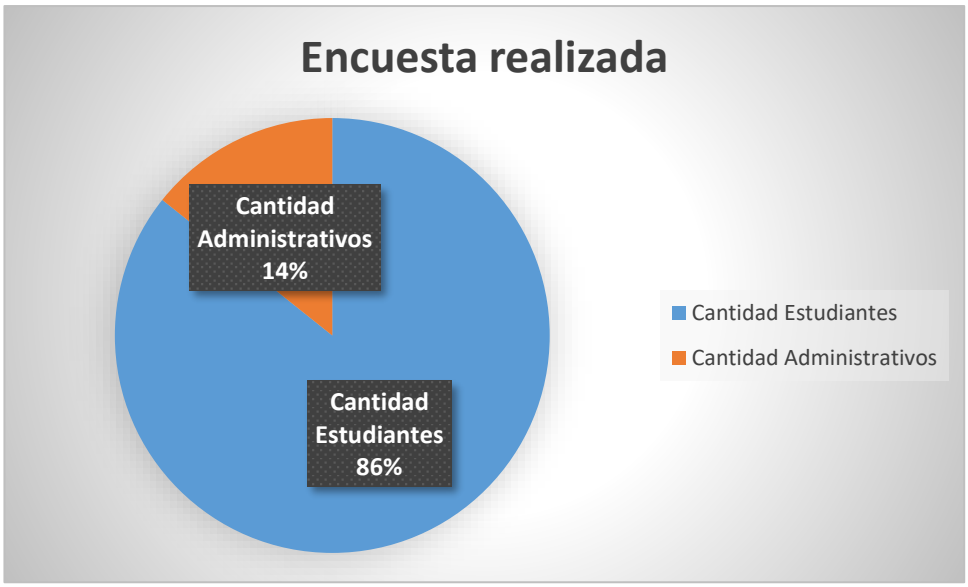


Figura 37 Diagrama de encuesta realizada. Fuente: Autor propio.

En la Figura 37, se logra evidenciar que la mayor parte de la comunidad estudiantil respondieron a la encuesta, con un porcentaje de 86%. Por el contrario, quienes menos respondieron la encuesta fue el personal administrativo con un porcentaje de 14%.

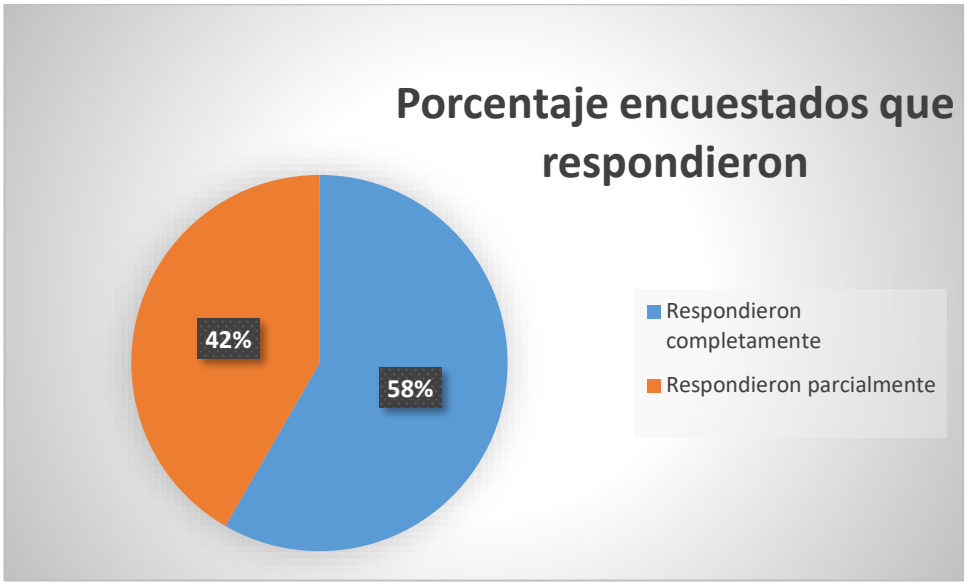


Figura 38 Diagrama de encuestados que respondieron. Fuente: Autor propio.

En la Figura 38, se puede evidenciar el porcentaje de encuestados que respondieron la encuesta con sus datos personales, ya sea total o parcialmente, omitiendo solo 2 preguntas de la encuesta en total.

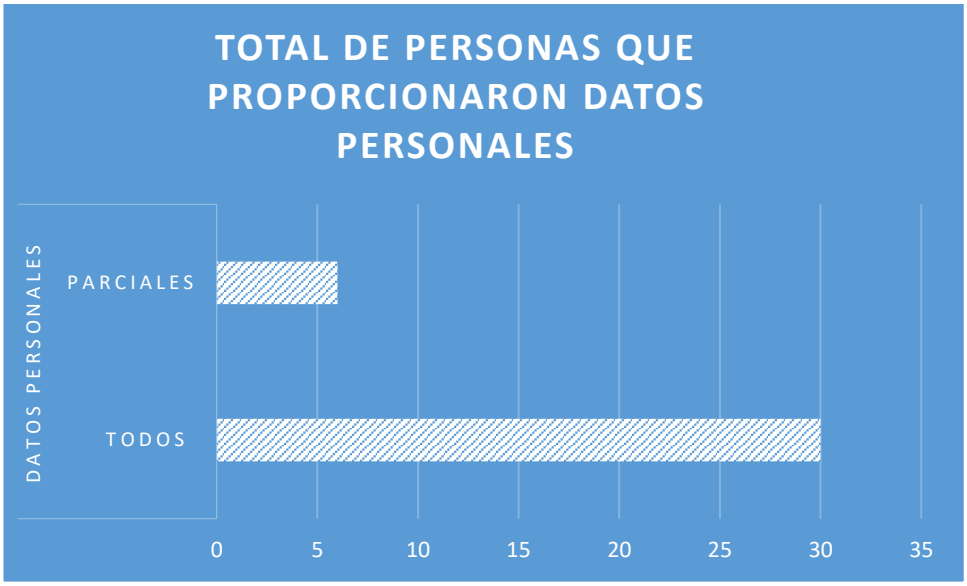


Figura 39 Diagrama de personas que proporcionaron datos personales. Fuente: Autor propio.

En la Figura 39, se logra evidenciar la cantidad de personas que respondieron a la encuesta sin ningún tipo de problema al realizarla, la totalidad de los encuestados dieron sus datos, totales o parciales, en la actividad de PHISING.

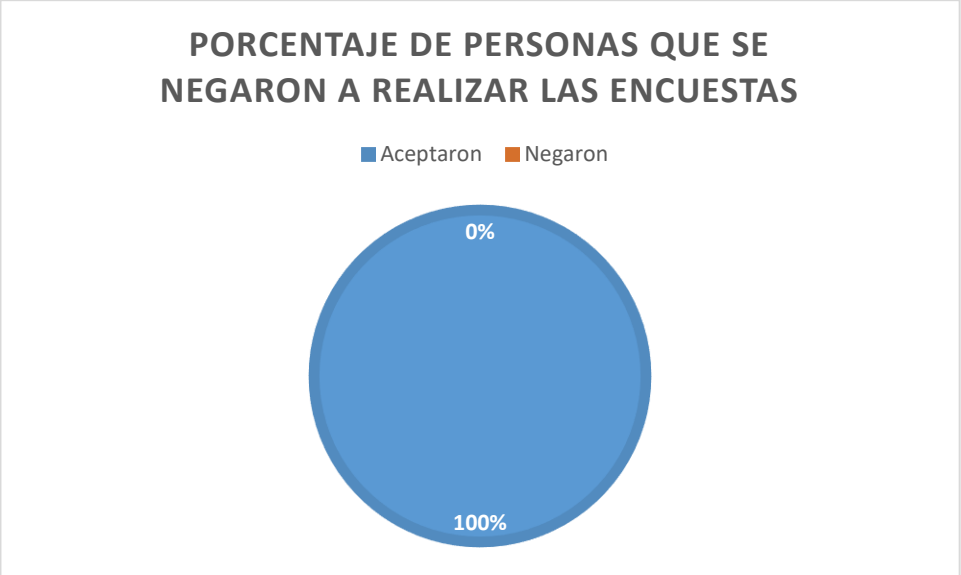


Figura 40 Diagrama de personas que se negaron a realizar la encuesta. Fuente: Autor propio.

En la Figura 40, se logra evidenciar el porcentaje de personas que aceptaron o negaron realizar la actividad de la encuesta. Notablemente, podemos deducir que todas las personas que se encuestaron decidieron realizar la encuesta, algunos de los ellos cuestionaron un poco la realización de dicha encuesta, pero de igual manera, decidieron realizarla al persuadirlos.

La muestra de prueba para la encuesta fue un total de 42 personas, se tomó una muestra pequeña para seguridad de la información obtenida y, no se presente divulgación de ésta bajo las directrices de la universidad y supervisión de esta.

El éxito de la encuesta se logró gracias al poco conocimiento sobre ingeniería social con que cuentan los estudiantes y funcionarios de la Universidad, dando una gran ventaja para obtener su información.

5. CONCLUSIONES

Con respecto al desarrollo del proyecto, se pueden destacar los logros que se alcanzaron de los objetivos propuestos como el de conseguir información personal tanto de los estudiantes como de los administrativos, con el uso de la Ingeniería Social enfocada, principalmente, en el Phishing. Dicha información recopilada sólo fue información personal, tal como: nombre, código, dirección de correo electrónico, semestre, facultad, etc. pero tanto los estudiantes como el personal administrativo no optaron por dar información, como la clave de acceso a su correo institucional o a la plataforma de la Universidad, lo cual indica que el personal administrativo y la comunidad estudiantil es muy consciente de que esa información es muy valiosa y no debe darla a otras personas. Podemos decir, que la calidad de la seguridad de la información en la Universidad del Sinú es muy buena en base a lo planteado anteriormente.

La comunidad estudiantil y el personal administrativo está propenso a recibir ataques informáticos, como el Phishing. Al realizar el ataque de Ingeniería Social con Phishing en la sede Plaza Colón, nos resultó muy fácil conseguir los datos personales de las personas anteriormente mencionadas, debido a que aceptaron, a primera vista, realizar o contestar las preguntas que estaban consignadas en las encuestas. Notamos que algunas personas no pusieron ni un grado de suspicacia ante tal evento y otras nos hicieron preguntas que, realmente, eran muy razonables, por ejemplo: ¿Y esta encuesta por qué no la notificó la persona responsable, en la Universidad, de manera anticipada? Sin embargo, esas personas accedieron a realizar las encuestas, pero no dieron información que comprometa altamente los sistemas informáticos de la Universidad del Sinú.

Por otro lado, las técnicas que se aplicaron durante el desarrollo del proyecto, tal como la denegación de servicios donde se logran saturar los equipos

objetivos y se altera el normal funcionamiento de la prestación de servicios, afecta de forma considerable la reputación de la Universidad del Sinú, la recomendación para mantenerse protegido contra este tipo técnicas, es tener parchados los sistemas operativos ya que así ayudan a mitigar el riesgo en gran medida.

6. RECOMENDACIONES

Para evitar que personas malintencionadas logren obtener resultados exitosos desarrollando este tipo de técnicas de ataques, dentro de la Universidad del Sinú sede Plaza Colón, los consejos de seguridad más recomendables son:

1. Dictar charlas tanto a la comunidad estudiantil como al personal administrativo para evitar, al máximo, este tipo de situaciones.

2. Constante monitoreo de la red con una herramienta que permita detectar actividades sospechosas, como Wireshark o implementando la tecnología de redes definidas por software (SDN).

3. Estipular una directriz para el personal administrativo, donde se establezca la importancia de no dar información personal o institucional en eventos como encuestas físicas, encuestas vía web o cualquier o medio, antes de recibir algún tipo de notificación que acredite su validez.

4. En un futuro, se puede validar nuevamente la vulnerabilidad con el servidor SSL y de persistir el problema se deben tomar cartas en el asunto realizando un estudio avanzado de la vulnerabilidad, con el fin de disiparla.

BIBLIOGRAFÍA

[1] "Ingeniería Social," Ingeniería social (seguridad informática), 28-Sep-2016. [Online].
Available: http://aprendeenlinea.udea.edu.co/lms/extension/mod/page/view.php?id=28962&lang=en.

[2] Wikipedia, "Seguridad Informática," Seguridad Informática, 11-May-2015. [Online]. Available: https://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica.

[3] Wikipedia, "Phishing," Phishing, 05-Mar-2018. [Online].
Available: https://es.wikipedia.org/wiki/Phishing.

[4] textoscientificos.com, "TCP/IP Y EL MODELO OSI," 10-Feb-2006. [Online].
Available: https://www.textoscientificos.com/redes/tcp-ip/comparacion-modelo-osi.

[5] Wikipedia, "Protocolo de datagramas de usuario," Wikipedia, 26-Mar-2018. [Online].
Available: https://es.wikipedia.org/wiki/Protocolo_de_datagramas_de_usuario.

[6] Franklin Matango, "Protocolos de transporte," Protocolo UDP | VoIP, 18-Aug-2016. [Online]. Available: http://www.servervoip.com/blog/tag/protocolo-udp/.

[7] Masadelante.com, "¿Qué significa http? - Definición de http," *masadelante.com*. [Online].
Available: http://www.masadelante.com/faqs/que-significa-http

[8] Alonso Eduardo Caballero Quezada, "Ataque De Envenenamiento ARP Utilizando Ettercap," ReYDeS's blog, 19-Jun-2014. [Online].
Available: http://www.reydes.com/d/?q=Ataque_de_Envenenamiento_ARP_utilizando_Ettercap.

[9] Rubén Velasco, "Bettercap," Analiza todo el tráfico de red con Bettercap, 08-Aug-2015. [Online]. Available: https://www.redeszone.net/2015/08/08/analiza-todo-el-trafico-de-red-con-bettercap/.

[10] Wikipedia, "Archivo," Wikipedia, 05-Jan-2018. [Online].
Available: https://es.wikipedia.org/wiki/Archivo_(inform%C3%A1tica).

[11] Wikipedia, "Ataque informático," Wikipedia, 18-Oct-2015. [Online].
Available: https://es.wikipedia.org/wiki/Ataque_inform%C3%A1tico.

[12] Wikipedia, "Cibernética," Wikipedia, 26-Apr-2018. [Online]. Available: https://es.wikipedia.org/wiki/Cibern%C3%A9tica.
[13] Wikipedia, "Correo electrónico," Wikipedia, 22-Oct-2012. [Online]. Available: https://es.wikipedia.org/wiki/Correo_electr%C3%B3nico.

[14] "Denegación de Servicios," Métodos de ataque. [Online]. Available: http://es.tldp.org/Manuales-LuCAS/GARL2/garl2/x-082-2-firewall.attacks.html.

[15] M. M. Julián Pérez Porto, "DEFINICIÓN DE FRAUDE," Definicion.de, 2013. [Online]. Available: https://definicion.de/fraude/.

[16] Miguel Ángel Núñez Martín, "Incidentes de seguridad informatica," SliderPlayer, 2017. [Online]. Available: http://slideplayer.es/slide/10286090/.

[17] EcuRed, "Dirección IP." [Online]. Available: https://www.ecured.cu/Direcci%C3%B3n_IP.

[18] Wikipedia, "Malware," Wikipedia, 23-Aug-2017. [Online]. Available: https://es.wikipedia.org/wiki/Malware.

[19] Francisco Hernández, "Protocolos," Dispositivos De Comunicación, 23-May-2015. [Online]. Available: http://telecomunicaciones5am.blogspot.com.co/2015/05/un-protocolo-es-un-conjunto-de-reglas.html.

[20] Wikipedia, "Red," Red de computadoras, 05-Aug-2018. [Online]. Available: https://es.wikipedia.org/wiki/Red_de_computadoras.

[21] "Spam," ValorTop, 11-May-2017. [Online]. Available: http://www.valortop.com/blog/que-significa-spam.

[22] Wikipedia, "Spoofing," Suplantación, 05-Apr-2018. [Online]. Available: https://es.wikipedia.org/wiki/Suplantaci%C3%B3n.

[23] enter.co, "INGENIERÍA SOCIAL," LA INGENIERÍA SOCIAL: EL ATAQUE INFORMÁTICO MÁS PELIGROSO, 25-Jul-2016. [Online]. Available: http://www.enter.co/guias/lleva-tu-negocio-a-internet/ingenieria-social/.

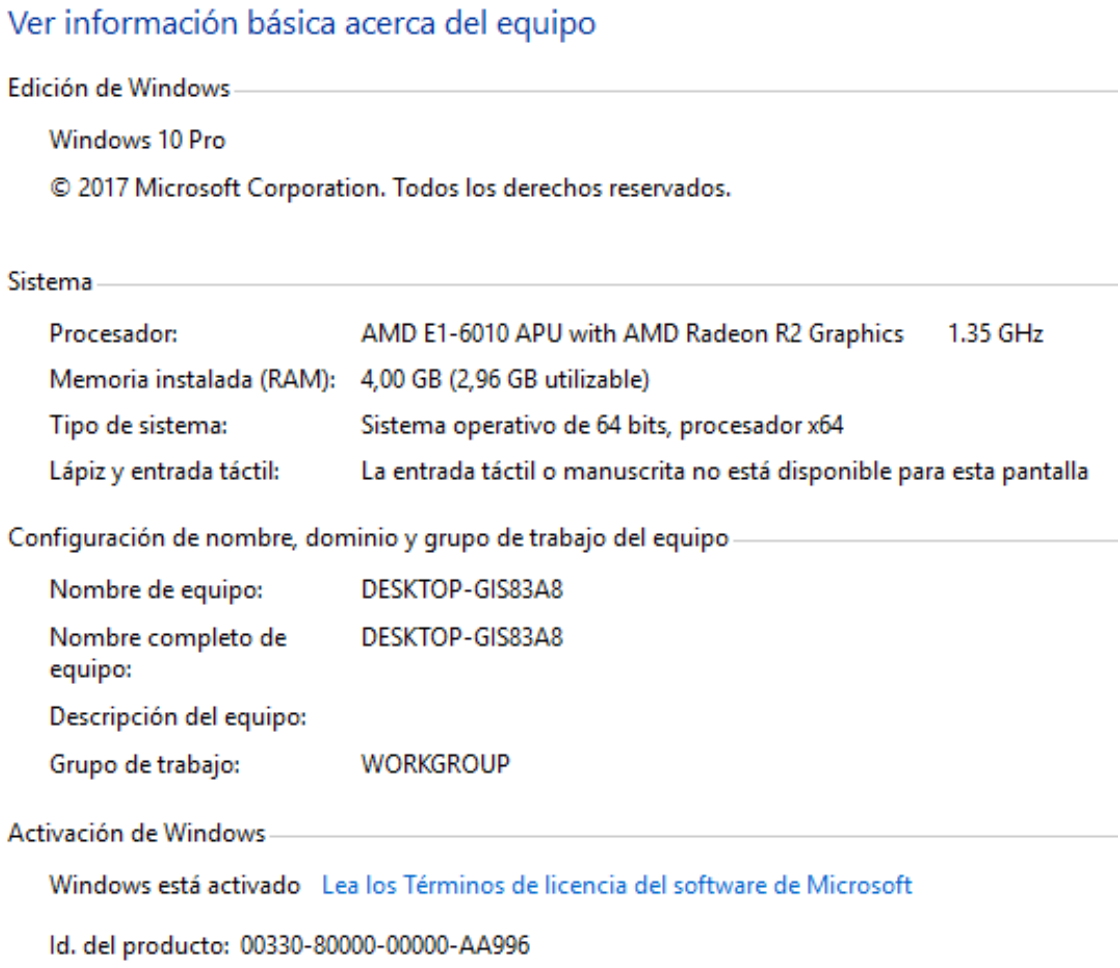
[24] Barry, Peter Crowley, Patrick. (2012). Modern Embedded Computing - Designing Connected, Pervasive, Media-Rich Systems - 14.2.7 Firewalls. Elsevier. Online version available at: https://app.knovel.com/hotlink/pdf/id:kt00BPZJZ3/modern-embedded-computing/firewalls

[25] Johns, Aaron. (2015). Mastering Wireless Penetration Testing for Highly Secured Environments - Scan, Exploit, and Crack Wireless Networks by Using the Most Advanced Techniques from Security Professionals - 8.5 Summary. Packt Publishing. Online version available at: https://app.knovel.com/hotlink/pdf/id:kt0113OFE6/mastering-wireless-penetration/data-captu-summary

[26] Ramachandran, Vivek. (2011). BackTrack 5 Wireless Penetration Testing - Beginner's Guide - 7.5 Session Hijacking over Wireless. Packt Publishing. Online version available at: https://app.knovel.com/hotlink/pdf/id:kt00BEF32A/backtrack-5-wireless/session-hijacking-over

ANEXOS

Anexo 1



Ver información básica acerca del equipo

Edición de Windows

Windows 10 Pro

© 2017 Microsoft Corporation. Todos los derechos reservados.

Sistema

Procesador:	AMD E1-6010 APU with AMD Radeon R2 Graphics	1.35 GHz
Memoria instalada (RAM):	4,00 GB (2,96 GB utilizable)	
Tipo de sistema:	Sistema operativo de 64 bits, procesador x64	
Lápiz y entrada táctil:	La entrada táctil o manuscrita no está disponible para esta pantalla	

Configuración de nombre, dominio y grupo de trabajo del equipo

Nombre de equipo:	DESKTOP-GIS83A8
Nombre completo de equipo:	DESKTOP-GIS83A8
Descripción del equipo:	
Grupo de trabajo:	WORKGROUP

Activación de Windows

Windows está activado Lea los Términos de licencia del software de Microsoft

Id. del producto: 00330-80000-00000-AA996

Anexo 2

UNIVERSIDAD DEL SINÚ
Elías Bechara Zainúm
Seccional Cartagena

ENCUESTA DE CALIDAD DE LOS EQUIPOS DE COMPUTO DE LA UNIVERSIDAD DEL SINÚ SEDE PLAZA COLÓN – COMUNIDAD ESTUDIANTIL

Fecha: ___ / ___ / ___

1. Nombre completo:
   _____
2. Documento de Identidad:
   _____
3. Código Estudiantil:
   _____
4. Correo Institucional:
   _____
5. Dirección residencial:
   _____
6. Número telefónico:
   _____
7. Semestre:
   _____
8. Facultad:
   _____
9. ¿Considera usted que la Universidad del Sinú cuenta con suficientes equipos en las salas de sistemas? Si, no y ¿Por qué?
   _____
   _____
   _____
10. Describa brevemente las mejoras que considera se deben realizar en la universidad con respecto a los equipos o a las salas de sistema.
    _____
    _____
    _____

Anexo 3

UNIVERSIDAD DEL SINÚ
Elías Bechara Zainúm
Seccional Cartagena

ENCUESTA DE CALIDAD DE EQUIPOS DE LA UNIVERSIDAD DEL SINÚ SEDE PLAZA COLÓN – ADMINISTRATIVOS

Fecha: ___ / ___ / ___

1. Nombre completo:
   _____
2. Documento de Identidad:
   _____
3. Código:
   _____
4. Correo Institucional:
   _____
5. Dirección residencial:
   _____
6. Número telefónico:
   _____
7. Cargo:
   _____
8. Departamento/oficina:
   _____
9. ¿Considera usted que la Universidad del Sinú cuenta con equipos de cómputos adecuado para el personal administrativo? Si, no y ¿Por qué?
   _____
   _____
   _____
10. Describa brevemente las mejoras que considera se deben realizar en la Universidad con respecto a los equipos tecnológicos de oficina.
    _____
    _____
    _____

Anexo 4

Título: Entrevista a personal del departamento de Sistemas

Descripción: Entrevista a Alberto Jiménez, Jefe de Sistemas de la Universidad del Sinú, seccional Cartagena, con el fin de obtener información precisa y detallada de la red de la sede Plaza Colon de la Universidad.

Preguntas:

1. **¿En qué sede se realizará las pruebas de las técnicas de ataque?**
   Respuesta del Jefe de Sistema:
   Por conveniencia se escogió la sede Plaza Colón como lugar de realización de pruebas.

2. **¿Cuáles son las áreas con mayor impacto, en información delicada?**
   Respuesta del Coordinador disciplinar:
   Las áreas con mayor impacto en la sede sería admisiones, jurídica, tesorería, crédito y cartera, mercadeo y las escuelas de Ingeniería, psicología y derecho.

3. **¿Cuál sería el área con el que estudiaremos la vulnerabilidad?**
   Respuesta del Jefe de Sistema:
   Por organización del proyecto se decide que se debe estudiar el área, en general, por el tiempo y el método de Ataque como lo es el Phishing, por lo que no se define un área específica.

4. **¿Limitantes que nos exige el departamento de sistemas para llevar a cabo el desarrollo del proyecto, sin inconvenientes?**
   Respuesta del Jefe de Sistema:
   Autorizo la realización del proyecto de análisis de vulnerabilidades bajo las directrices de no acceder al contenido estrictamente privado del personal de la universidad.

Anexo 5

Hacer doble clic a la siguiente imagen para abrir el documento donde encontrará la información completa y detallada del presupuesto estimado para el desarrollo del proyecto.

R-INVE-030
PRESUPUESTO PROY