UNIVERSIDAD NACIONAL DE CHIMBORAZO

FACULTAD DE INGENIERÍA

CARRERA DE SISTEMAS Y COMPUTACIÓN

Proyecto de Investigación previo a la obtención del título de Ingeniería en Sistemas y Computación

TRABAJO DE TITULACIÓN

"ANÁLISIS DE LOS MECANISMOS DE DEFENSA CONTRA EL CIBERATAQUE SMTP SPOOFING EN LA INFRAESTRUCTURA DE RED IPV4 DE LA UNIVERSIDAD NACIONAL DE CHIMBORAZO"

Autores:

Alex Gabriel Auquilla Guamantaqui

Henry Daniel Espin Robles

Tutor:

Ing. Lorena Molina., Ph.D.

Riobamba – Ecuador

Año

2019

Los miembros del Tribunal de Graduación del proyecto de investigación titulado "**Análisis de los mecanismos de defensa contra el ciberataque SMTP Spoofing en la infraestructura de red ipv4 de la Universidad Nacional de Chimborazo**".

Presentado por: Alex Gabriel Auquilla Guamantaqui, Henry Daniel Espin Robles y dirigido por: Ing. Lorena Paulina Molina Valdiviezo. PhD.

Una vez escuchada la defensa oral y revisado el informe final del proyecto de investigación con fines de graduación escrito en la cual se ha constatado el cumplimento de las observaciones realizadas, remite la presente para uso y custodia en la biblioteca de la Facultad de Ingeniería de la UNACH.

Para constancia de lo expuesto firman:

Ing. Lorena Molina
Tutora del Proyecto

Firma

Ing. Gonzalo Allauca
Miembro del Tribunal

Firma

Ing. Danny Velasco
Miembro del Tribunal

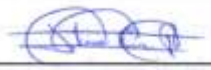
Firma

AUTORÍA DE LA INVESTIGACIÓN

"El contenido de este proyecto de titulación está bajo las ideas, experimentación, y resultados que corresponden exclusivamente a: Alex Gabriel Auquilla Guamantaqui y Henry Daniel Espin Robles con la tutoría de la Ing. Lorena Paulina Molina Valdiviezo y el patrimonio intelectual de la Universidad Nacional de Chimborazo"

Alex Gabriel Auquilla Guamantaqui

060484237-7



Henry Daniel Espin Robles

060412995-7

Página de dedicatoria

Dedico este trabajo a Dios, por darme la oportunidad de vivir y por estar conmigo en cada paso que doy, por haber puesto en mi camino a aquellas personas que han sido mi soporte y compañía durante todo el periodo de estudio. A mi madre Irma, por darme la vida, quererme mucho, creer en mí y porque siempre me apoyaste. También a mi abuelita Bertha y mis tíos Leonardo, Cristian y Fernando, por quererme y apoyarme siempre, esto también se lo debo a ustedes

A mis amigos Brayan y Henry porque fueron más que amigos durante toda la vida universitaria y además compartimos mucho más que un aula. También una mención a un amigo en especial Paul Vinueza con el cual llevamos una larga amistad desde el colegio, porque sin importar los caminos diferentes que elegimos seguimos siendo amigos y hermanos.

Todos aquellos familiares y amigos que no recordé al momento de escribir esto. Ustedes saben quiénes son.

Alex Gabriel Auquilla Guamantaqui

Dedico este trabajo a Dios por darme la salud y la oportunidad de formarme como profesional y aquellas personas que a lo largo de la vida me han acompañado en cada paso que he dado ya que sin ellos no sería la persona que soy ahora. A mi madre Hidirma por darme la vida y por ser mi guía en mi vida. A mi padre Luis † que desde los cielos me ha de brindar su bendición y a mi hermano por ser mi mayor inspiración.

Henry Daniel Espin Robles

Agradecimiento

Agradezco por la culminación del trabajo de investigación a Dios por todas sus bendiciones, a mi madre y mi abuelita, por ser el pilar más importante y por demostrarme siempre su cariño y apoyo incondicional sin importar nuestras diferencias de opiniones, a nuestros docentes de la Escuela de Sistemas y Computación de la Universidad Nacional de Chimborazo, por haber compartido sus conocimientos a lo largo de la preparación de nuestra profesión, de manera especial, a la Ing. Lorena Molina Valdiviezo tutora de nuestro proyecto de investigación quien ha guiado con su paciencia, y su rectitud como docente.

Alex Gabriel Auquilla Guamantaqui

Agradezco el apoyo brindado de todas aquellas personas que en su momento me han brindado sin dudarlo. A mis padres y mi hermano por ser un apoyo inmenso. A mis amigos Cristian, Fabricio, Alex, Dany, Kevin, Francisco por compartir momentos inolvidables a lo largo de toda mi vida estudiantil y a mi enamorada Tatiana por apoyarme en momentos emocionalmente difíciles, a nuestros docentes de la Escuela de Sistemas y Computación de la Universidad Nacional de Chimborazo, por haber compartido sus conocimientos a lo largo de la preparación de nuestra profesión, de manera especial, a la Ing. Lorena Molina Valdiviezo tutora de nuestro proyecto de investigación quien ha guiado con su paciencia, y su rectitud como docente.

Henry Daniel Espin Robles

Índice general

Lista de cuadros

Lista de figuras

Resumen

En la actualidad las organizaciones se han vuelto dependientes de la tecnología, al suceder esto, los ciberdelincuentes buscan la manera de vulnerar la información mediante ataques. Con lo mencionado, la presente investigación permite realizar implementaciones de mecanismos de defensa contra ataques SMTP spoofing a una red simulada de la Universidad Nacional de Chimborazo al aplicar DKIM, SPF, DMARC para mitigar las vulnerabilidades y con ello se desarrolló un manual de prevención.

La metodología que se utilizó en la investigación es inferencial por el análisis pre y post acerca de las vulnerabilidades y riesgos, además se muestra el análisis de 2 escenarios, el primero mientras el ataque esté activo sin ningún mecanismo de defensa y el segundo donde se implementan los mecanismos de defensa, reduciéndose así la cantidad de ataques en el escenario simulado.

Se utilizó Wilcoxon para la comprobación de la hipótesis en el que se obtuvo los siguientes resultados: en la red simulada se presentó un 45.42% de ataques de SMTP spoofing sin implementar los mecanismos de defensa en el servidor de correos y a diferencia que al implementar los mecanismos de defensa se redujo a un 5% el ataque de SMTP spoofing. Con estos valores se llega a la conclusión de que se reduce en un 40,42% los ataques, reduciéndose a un porcentaje muy aceptable, por lo que se recomienda implementar los mecanismos de defensa estudiados en la presente investigación.

Palabras claves: Ciberseguridad, Email Spoofing, SPF, DKIM, DMARC.

Abstract

Abstract

Nowadays, organizations have become dependent on technology, as this happens, cybercriminals look for different ways to violate the information through attacks.

With the above, the present research allows the implementation of defense mechanisms against SMTP spoofing attacks in a simulated network of the Universidad Nacional de Chimborazo applying DKIM, SPF, DMARC to mitigate the vulnerabilities and a manual of prevention was developed.

The methodology used in the research was inferential by the pre and post analysis about the vulnerabilities and risks, also it shows the analysis of 2 scenarios, the first, while the attack is active without any defense mechanism and the second where the defense mechanisms have been implemented, thus reducing the number of attacks in the simulated scenario.

Wilcoxon was used to verify the hypothesis in which the following results were obtained: in the simulated network, 45.42% of SMTP spoofing attacks were presented without implementing the defense mechanisms in the mail server and, unlike, implementing the mechanisms of defense it reduced to 5% the attack of SMTP spoofing. These values leads us to the conclusion the attacks reduced at 40.42%, and this percentage reduction is very acceptable, so it is recommended to implement this defense mechanisms developed in the present research.

Keywords: Cybersecurity, Email Spoofing, SPF, DKIM, DMARC.

Translation reviewed by:

Msc. Elizabeth Diaz

CAPÍTULO I

3.1 Introducción

En los últimos años con el aumento de los servicios en línea, se ha incrementado exponencialmente el nivel de los riesgos y ataques en la implementación de nuevas tecnologías, para el intercambio comercial de información. Paralelamente, al desarrollo tecnológico, los instrumentos de los ciberdelincuentes han evolucionado facilitando así su forma de adquirir información vital ilegalmente de las entidades públicas y privadas mediante diferentes tipos de ataques informáticos (Ojeda-Pérez, 2010).

Las organizaciones de diferente índole han sido víctimas de centenares de ciberataques efectuados por ciberdelincuentes. Se puede definir a un ciberataque como una secuencia de operaciones que ponen en riesgo la seguridad de un sistema (Acens, 2017), y un ciberdelincuente es la persona que mediante el empleo de un ordenador y las redes de comunicación llevan a cabo delitos.

Entre los posibles ciberataques están los Address Spoofing los mismos que roban la identidad a nivel de equipamiento, también están los de Session Hijacking que roban la identidad a nivel de usuario, además Manipulación de paquetes/protocolos los mismos que cambian de paquetes de comunicación entre equipos, también existe el denominado Modificación de datos de registro (logs) el mismo que altera el registro de eventos con el objeto de ocultar actividades no autorizadas o maliciosas.

Dando paso así al delito informático o ciberdelincuencia, y esta es toda aquella acción ilegal que se da por vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet. Muchos de estos delitos, al no estar tipificados en la ley, se definen como abusos informáticos. La criminalidad informática o cibercrimen tiene un alcance mayor, donde se incluyen delitos como el fraude, el robo, el chantaje, la falsificación y la malversación de caudales públicos al utilizar ordenadores y redes como medio para realizarlos (Urueña Centeno, 2015).

Los delitos informáticos o ciberdelitos en el Ecuador es toda una actividad ilícita que van desde el fraude hasta el espionaje, los mismos que son denunciados en la fiscalía; desde la aparición del internet se dieron nuevas formas de delincuencia que ponen en riesgo la

información de organizaciones tanto públicas como privadas y la seguridad en la navegación de los usuarios (Fiscalía General del Estado, 2015). Desde que entró en vigencia el Código Orgánico Integral Penal (COIP), el 10 de agosto de 2014, contempla y sanciona los delitos informáticos como por ejemplo: la revelación ilegal de base de datos, la interceptación ilegal de datos, la transferencia electrónica de dinero obtenido de forma ilegal, el ataque a la integridad de sistemas informáticos y los accesos no consentidos a un sistema telemático o de telecomunicaciones, la pornografía infantil, el acoso sexual (Policía Nacional del Ecuador, 2015).

La Universidad Nacional de Chimborazo no es invulnerable a este tipo de ataques, debido a este motivo se deberá analizar y prevenir las amenazas en la seguridad de la red, por ende, el presente trabajo de investigación se centrará en los ataques SMTP Spoofing para ello es necesario conocer cómo trabajan los ataques SMTP Spoofing. Por lo cual, para manejar este tipo de situaciones se propone crear un ambiente de red simulado con sus componentes necesarios para así de esta manera identificar, analizar, detectar, contrarrestar los ataques mencionados con anterioridad.

Al utilizar un ambiente simulado permitirá reducir los costos de implementación de hardware, costos de mantenimiento, el tiempo invertido en la experimentación y principalmente no provocar un colapso en la red de funcionamiento.

Este documento obedece a la siguiente estructura: En el capítulo I, se aborda el planteamiento del problema, además de la justificación y los objetivos de la investigación.

En el capítulo II, conlleva lo que es marco teórico relacionado a la temática; la metodología es abordada en el capítulo III en la cual se crea el diseño de la topología de la red, la realización de ataque y la aplicación de los mecanismos de defensa, en el capítulo IV se visualiza los resultados obtenidos durante la aplicación de los mecanismos de defensa que se aplicaron a la red simulada de la Universidad Nacional de Chimborazo.

Las conclusiones y recomendaciones finalizan este documento conjuntamente con la propuesta la cual es el plan de acción que se deberá seguir para cumplir con los objetivos y de esta manera desarrollar el manual de seguridad para la red de la Universidad Nacional de Chimborazo.

3.2 Planteamiento del problema

Según estudios realizados por expertos en seguridad informática las redes a nivel mundial ya sean públicas o privadas son susceptibles a ataques maliciosos por lo que la red de la Universidad Nacional de Chimborazo no es la excepción, ésta ha sufrido diversos ataques informáticos situando en riesgo los servicios que esta ofrece a estudiantes, docentes y personal administrativo.

Con los resultados del proyecto de investigación:" MEJORAS EN LA SEGURIDAD DE LA RED INALÁMBRICA DE LA UNIVERSIDAD NACIONAL DE CHIMBORAZO APLICANDO HACKING ÉTICO", (Martínez & Oñate, MEJORAS EN LA SEGURIDAD DE LA RED INALÁMBRICA DE LA UNIVERSIDAD NACIONAL DE CHIMBORAZO APLICANDO HACKING ÉTICO, 2017) los autores determinaron con su estudio que una de las principales vulnerabilidades que tiene la red son los ataques spoofing razón por la cual este proyecto de investigación pretende analizar los mecanismos de defensa SPF y DKIM para proteger a la red en el presunto ataque SMTP Spoofing, el mismo que se llevará a efecto con entornos de simulación para lograr una mayor seguridad en la red de la Universidad Nacional de Chimborazo frente a este tipo de ataque, esto dará lugar a mantener la integridad en la información institucional.

3.3 Objetivos

1.3.1 Objetivo General

- Analizar los mecanismos de defensa contra los ataques SMTP spoofing en la infraestructura de red ipv4 de la Universidad Nacional de Chimborazo.

1.3.2 Objetivos Específicos

- Analizar las casusas y efectos del ataque SMTP spoofing a la red de la Universidad Nacional de Chimborazo y sus mecanismos de defensa.
- Diseñar, implementar y simular diversos escenarios de ataques SMTP spoofing y sus mecanismos de defensa en la red virtual.
- Analizar los resultados de los mecanismos de defensa frente al ataque SMTP spoofing a través de simulaciones.
- Elaborar un manual de prevención para garantizar la seguridad de la red ipv4 de la Universidad Nacional de Chimborazo ante ataques SMTP spoofing.

CAPÍTULO II

En la actualidad con el progreso que tiene la tecnología en una institución los ataques van de la mano con su desarrollo, por este motivo, las entidades son vulnerables a robos de información mediante un ataque cibernético.

El spoofing es una técnica utilizada por atacantes con intenciones maquiavélicas, que en una red de tecnología usurpan la identidad y se hace pasar por un ente distinto a través de falsificación de datos, esto se conoce comúnmente como "hacerse pasar por otro". Existen distintos tipos de spoofing entre ellos están: el IP spoofing en el que suplanta una IP distinta a la nuestra, el ARP spoofing asocia la dirección MAC del atacante con la dirección IP de otro nodo, como por ejemplo la puerta de enlace predeterminada, el DNS spoofing modifica la biblioteca DNS para redirigir a la víctima a páginas presumiblemente maliciosas cuando intenta entrar en páginas legítimas, y el Web spoofing o el e-mail (smtp) spoofing que es el conjunto de técnicas utilizadas para hacerse pasar por otro emisor en un correo electrónico (Muñoz de Frutos, 2016).

2.1. Seguridad Informática

Es un conjunto de medidas de prevención, detección y corrección, orientadas a proteger la confidencialidad, la integridad y la disponibilidad de los recursos informáticos. Se destaca la elegancia de la definición, dada la gran cantidad de conceptos que incluye y la amplitud del espectro de conocimientos que pretende abarcar (Benchimol, Buenos Aires).

2.2. Seguridad de la Información

La seguridad de la información no solo contempla los procesos por equipos informáticos y sistemas, también abarca algún escrito confidencial como por ejemplo: procesos de contingencia y continuidad del negocio, leyes, normas, procedimientos y políticas internas propias de cada empresa (Benchimol, Buenos Aires).

Es decir, la seguridad de la información de una organización es netamente responsabilidad de los administradores de la red, para así garantizar la seguridad, confidencialidad e integridad de la información.

2.3. Amenazas Informáticas

Las organizaciones deben contar con la suficiente experiencia para identificar los diferentes tipos de riesgos tecnológicos por los cuales se puede vulnerar su continuidad en

el negocio, estos tipos de riesgos pueden ser clasificados como amenazas internas y externas a la empresa (Flórez R., Arboleda S., & Cadavid A., Enero-Junio 2012).

Las amenazas según el tipo de alteración o daño que puedan causar se clasifican en:

- De interrupción
- De intercepción
- De modificación
- De fabricación

Los ataques informáticos son realizados por personas expertas a quien se les denomina atacantes informáticos o ciberdelincuentes. En las siguientes subsecciones, se describe brevemente a los tipos de atacantes.

2.3.1. Hacker

La palabra hacker es un neologismo, que en informática se utiliza para referirse a un gran experto en algún área de dominio. Si bien se lo relaciona más con los conocimientos técnicos e informáticos, es posible extender el concepto hacia otras disciplinas (Benchimol, Buenos Aires).

Se podrá decir que hacker puede ser cualquier persona que con su pasión al conocimiento se abre campo en el descubrimiento, el aprendizaje y el funcionamiento de las cosas ya sea en diversas ramas informáticas tales como programación, networking, entre otras.

2.3.2. Cracker

El término cracker proviene del vocablo inglés crack (romper). Aplicado a la informática, se puede decir que es alguien que viola la seguridad de un sistema de forma similar a un hacker, solo que ilegalmente y con diferentes fines (Benchimol, Buenos Aires).

Un cracker es aquella persona que, con su conocimiento puede acceder a la red y romper la seguridad informática, trabaja a beneficio propio o para hacer daño a un objetivo.

2.3.3. Otros Personajes

Entre los protagonistas de esta película, además de los ya vistos hackers y crackers, también se encuentran otros actores, cuyos nombres se leen de entre las páginas del

ciberespacio. Se pueden encontrar algunos términos como: newbie, que significa principiante; lammer, persona que presume tener conocimientos que realmente no posee; phreaker, hacker orientado a los sistemas telefónicos; y script kiddie, quien utiliza programas creados por terceros sin conocer su funcionamiento (Benchimol, Buenos Aires).

2.4.Tipos de Ataques en la red

Un ataque es cualquier cosa que pueda alterar la operación, funcionalidad, disponibilidad o integridad de una red o sistema (Alulema Chiluiza, 2008).

Existen varios tipos de ataques con diferentes técnicas cada vez más avanzadas y automatizadas, que pueden ser dirigidas al sistema operativo, a las aplicaciones, errores en configuraciones o errores en protocolos (Benchimol, Buenos Aires). Existen decenas de ataques, pero se dividen en dos grandes grupos, como son los siguientes:

2.4.1. Ataques Pasivos

Estos ataques son muy difíciles de detectar ya que el atacante no modifica ni altera en ningún momento la información que escucha, monitorea u observa mientras dicha información está siendo transmitida. Para evitar estos ataques se puede recurrir al cifrado de la información (Izaskun, Fernando, & Amaia, 2006).

2.4.2. Ataques Activos

Estos ataques realizan algún tipo de modificación del flujo de datos transmitido ya sea al modificar la corriente de datos o la creación de un falso flujo de datos (Izaskun, Fernando, & Amaia, 2006). Existen numerosos ataques activos a una red los que se mencionaran a continuación:

2.4.2.1. Spoofing

Ataque que consiste en emplear un terminal cliente al que se han asociado validadores estáticos (por ejemplo, la dirección IP) de una red WLAN para suplantar la identidad de algún miembro de la comunicación. Ataques derivados de él son los ataques de secuestro de sesiones y Man in the Middle (Izaskun, Fernando, & Amaia, 2006).

2.4.2.2. Hombre en el medio (Man in the Middle)

El ataque de Hombre en el Medio, también conocido como Man in the Middle, se sirve del spoofing para interceptar y selectivamente modificar los datos de la comunicación para suplantar la identidad de una de las entidades implicadas en la comunicación (Izaskun, Fernando, & Amaia, 2006).

2.4.2.3. El secuestro de sesiones (Hijacking)

El secuestro de sesiones o hijacking es una amenaza de seguridad que se vale del spoofing, pero ésta consiste en tomar una conexión existente entre dos computadores. Tras monitorizar la red el atacante puede generar tráfico que parezca venir de una de las partes envueltas en la comunicación, al robar la sesión de los individuos envueltos (Izaskun, Fernando, & Amaia, 2006).

2.5. Vulnerabilidad en la red

Las vulnerabilidades de un sistema son una puerta abierta para posibles ataques, de ahí que sea tan importante tenerlas en cuenta; que en cualquier momento podrían ser aprovechadas (INFOSEGUR, 2013).

2.6. Tipo de Ataque: SMTP (E-mail) Spoofing

E-mail spoofing es un término que describe la actividad de correo electrónico fraudulenta en la cual la dirección de remitente y otras partes de la cabecera del correo son cambiadas para aparecer como si el e-mail proviene de una fuente diferente. E-mail spoofing es una técnica comúnmente usada para el spam y phishing. Cambiando ciertas propiedades del e-mail, como los campos from, return-path and reply-to (que se encuentran en la cabecera del mensaje), un usuario mal intencionado puede hacer que el e-mail parezca ser de remitido por alguien que en realidad no es (Garcia Ciyi, 2010).

El e-mail spoofing es posible porque el protocolo simple mail transfer (SMTP), el principal protocolo utilizado para el envío de correo electrónico no incluye un mecanismo de autenticación. Este permite a un cliente SMTP negociar un nivel de seguridad con un servidor de correo, si bien esta precaución no siempre se toma. Si no se toman las precauciones adecuadas cualquiera que tenga los conocimientos necesarios puede conectarse al servidor y utilizarlo para enviar mensajes. Para enviar un correo electrónico falsificado, los remitentes introducen comandos en las cabeceras que alteran la información del mensaje (spoffing) (Méndez, 2014).

2.6.1. La suplantación de identidad

La suplantación de identidad va desde extorsiones, pasando por fraudes, hackeos de la más diversa índole, hasta la pérdida de trabajo y amistades. Para las organizaciones de diferente índole y muchos profesionales, el correo electrónico es una pieza fundamental ya que con ella se pueden comunicar con clientes, amigos y hasta con algunos familiares.

2.6.2. Ingeniería social y el impacto del SMTP Spoofing

Las diferentes técnicas de ataques como puede ser la ya clásica de utilizar subdominios usar un correo haciéndose pasar por @google.com enviado desde un @google.payment52.com, el uso de correos homográficamente parecidos, es decir, en vez de @google.com, utilizar @google.com, que aunque parezcan iguales en el segundo caso utiliza un código Unicode no recogido en nuestro abecedario, pero sí disponible en Internet o con errores de typosquatting que pasan desapercibidos por ejemplo un correo @google.com lanzado desde otro correo @googel.com, en el que se produce un gran problema ya que la sociedad ni siquiera se suele fijar en esto, y claramente, son mucho más sencillos de ejecutar (Iglesias, 2018).

Actualmente, es posible *que el servicio de email que la mayoría de los usuarios utiliza hubiera marcado como potencialmente peligroso los tres ejemplos anteriormente dichos, y enviándolos directamente a la carpeta de Spam y así poder minimizar el riesgo*. Por otra parte, cualquiera con un poco de conocimientos en programación, puede crearse una herramienta para enviar masivamente correo desde la dirección que desee el obstáculo es que la mayoría de los nombres de dominios "importantes" han sido definidos a nivel de configuración de servidor de manera que no certifican que un correo enviado desde fuera es, en verdad, un correo legítimo y como cada vez más herramientas de lectura de correo tienen en cuenta este tipo de situaciones *el correo llega a la carpeta Spam de la víctima, o marcado como potencialmente peligroso* (Iglesias, 2018).

2.6.3. ¿Cómo funciona?

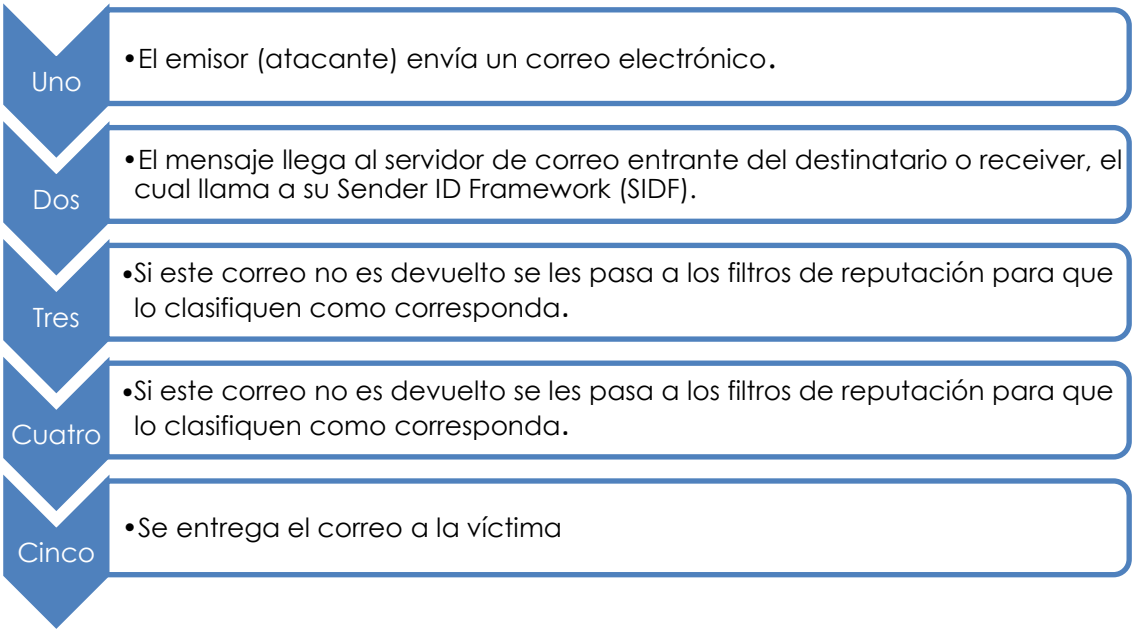


Figura 1.Como funciona SMTP spoofing

(Méndez, 2014)

En la Fig.2 se puede observar como el correo es enviado desde su emisor pasando así por los servidores hasta llegar a su destino.

Figura 2. Ataque a un Servidor SMTP

(Méndez, 2014)

2.6.4. Protocolos de defensa anti-SMTP Spoofing: SPF, DKIM y DMARC

2.6.5. SPF (Sender Policy Framework o Convenio de remitentes)

Es un protocolo de seguridad que se encarga de identificar la identidad del correo remitente a través de la IP desde dónde se envía y por medio de los registros del DNS, que deben

coincidir con los servidores de correo SMTP autorizados a realizar ese envío (Iglesias, 2018).

2.6.5.1. Funcionamiento SPF

Para entender el funcionamiento de SPF se debe conocer que cada mensaje de correo electrónico contiene dos encabezados, el primero que es visible y todo usuario lo puede observar encontrándose en la parte superior del mensaje de correo electrónico, y el segundo que es oculto a nivel técnico, no obstante, se puede observar este encabezado, pero varía según el proveedor de correos (Guntrip, 2016).


Mensaje original

ID de mensaje	<CAHLU+H4hrU8KOT6PvZO8Xt8p5AcUCZM-V1=rRP5jPvy1A85kRg@mail.gmail.com>
Creado a las:	14 de enero de 2019, 0:14 (entregado en 0 segundos)
De:	@gmail.com>
Para:	Genesis Rojasxoxo <genesisrojasxoxo@gmail.com>
Asunto:	Re:

Figura 3. Primer encabezado visible.


Detalles de mensaje

Received: from CY4PR2201MB1736.namprd22.prod.outlook.com (2603:10b6:104:5::31) by MWHPR22MB0638.namprd22.prod.outlook.com with HTTPS via CO2PR04CA0201.NAMPRD04.PROD.OUTLOOK.COM; Wed, 6 Feb 2019 17:46:48 +0000
Authentication-Results: unach.edu.ec; dkim=none (message not signed) header.d=none;unach.edu.ec; dmarc=none action=none header.from=unach.edu.ec;
Received: from CY4PR2201MB1495.namprd22.prod.outlook.com (10.171.241.15) by CY4PR2201MB1736.namprd22.prod.outlook.com (10.165.90.39) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.1601.17; Wed, 6 Feb 2019 17:46:44 +0000
Received: from CY4PR2201MB1495.namprd22.prod.outlook.com ([fe80::39c0:e760:55a9:e66b]) by CY4PR2201MB1495.namprd22.prod.outlook.com ([fe80::39c0:e760:55a9:e66b%4]) with mapi id 15.20.1601.016; Wed, 6 Feb 2019 17:46:44 +0000
Content-Type: application/ms-tnef; name="winmail.dat"
Content-Transfer-Encoding: binary
From:
To:
Subject: RV: [Ticket#2019020604000336] [CSIRT Cedia] Reporte de Alerta/s de Seguridad
Thread-Topic: [Ticket#2019020604000336] [CSIRT Cedia] Reporte de Alerta/s de Seguridad

Figura 4. Segundo encabezado oculto.

Antes de hacer llegar el mensaje a su destinatario, los proveedores de correo electrónico verifican el registro SPF para lo cual buscan el dominio que se incluye en la dirección de "remitente de sobre" (que también se conoce como ruta de devolución o "mfrom") en el

encabezado técnico oculto del mensaje. Si la dirección IP que envía el mensaje en nombre de este dominio no está en la lista de dominios del registro SPF, el mensaje no pasa la autenticación SPF (Guntrip, 2016).

2.6.5.2. Importancia de SPF

Tomando en cuenta que es poco probable que los filtros de spam agreguen a la lista negra a dichos correos suplantados. Este protocolo de verificación optimiza en su servidor de correos aumentado la probabilidad de entrega del correo legítimo y así, poder disuadir a los ciberdelincuentes que intenten suplantar en el dominio de su entidad o empresa (Guntrip, 2016).

Además, SPF por sí solo no es suficiente para bloquear los mensajes de suplantación de identidad que se dirijan a su dominio, tienes sus puntos débiles los cuáles se lista a continuación:

- **Exactitud:** los proveedores verificados que envían mensajes de correo electrónico a menudo cambian y se diversifican. Si no cuenta con visibilidad en esos cambios en tiempo real, los registros SPF se tornarán obsoletos.
- **Tolerancia:** Si el correo electrónico no pasa la autenticación SPF no garantiza que el mensaje se vaya a bloquear.
- **Inmunidad**: Si se reenvía un mensaje, el registro SPF se rompe.
- **Protección:** SPF no protege la dirección de "remitente de encabezado", la cual ve el usuario en los clientes de correo electrónico, a fin de que no se suplante. Los ciberdelincuentes pueden pasar la autenticación de SPF mediante la inclusión de un dominio de su propiedad en la dirección de "remitente de sobre" y todavía suplantar el dominio legítimo de la marca en la dirección de remitente visible.

Favorablemente, otro protocolo de autenticación de correo electrónico puede tapar esos agujeros de correo llamado DKIM.

2.6.6. DKIM (DomainKeys Identified Mail)

Se encarga de asociar un nombre de dominio a un mensaje de tal forma que los proveedores de buzones pueden verificarlo, lo que nos permite responsabilizar el envío a una persona u organización (Iglesias, 2018).

2.6.6.1. Funcionamiento de DKIM

Según (Guntrip, 2016) los pasos para el proceso de firma DKIM son:

1. El emisor identifica los campos que desea incluir en su firma DKIM, dichos campos incluyen la dirección "desde", el cuerpo y el sujeto, así como muchos otros. Estos campos deben permanecer sin cambios en el tránsito caso contrario la autenticación DKIM fallará.
2. La plataforma de correo electrónico del emisor creará un hash de los campos de texto incluidos en la firma DKIM. Por ejemplo:

   De: Emisor <emisor@ejemplo.com>
   Asunto: Prueba

   se asigna la cadena de hash:

   3303baf8986f910720abcfa607d81f53

3. Una vez que se genera el hashstring, se cifra con una clave privada, a la que solo tiene acceso el remitente.
4. Enviado el correo electrónico, depende del proveedor de correo electrónico para validar la firma DKIM. Para hacerlo, necesita encontrar la clave pública que coincidirá perfectamente con la clave privada, descifrando así la firma DKIM de nuevo a su cadena de hash original.
5. El receptor genera su propio hash de los campos incluidos en la firma DKIM y lo compara con la cadena de hash que acaba de descifrar. Si coinciden, los campos en la firma DKIM no se cambiaron en tránsito y que el firmante (receptor verificado) es el verdadero dueño del correo electrónico.

2.6.6.2. Importancia DKIM

DKIM ayuda a informar a los receptores de correo electrónico que puede contener contenido malicioso o spam, también valida que los datos incluidos en la firma DKIM no se modificaron en tránsito. Pero debido a que DKIM es más difícil de implementar, menos remitentes lo han adoptado. Además, DKIM no hace nada para evitar que los ciberdelincuentes falsifiquen las partes visibles de un campo de correo electrónico, incluida la dirección de correo electrónico, el nombre para mostrar y el dominio (Guntrip, 2016).

2.6.7. DMARC (Mensaje basado en el dominio de autenticación, generación de informes y de conformidad*)*

Más que un protocolo es una política indicando que los correos electrónicos enviados desde ese dominio están protegidos por SPF y/o DKIM, dando a las herramientas de correo una serie de instrucciones en caso de que alguno de ellos no sea validado se marque como Spam (Iglesias, 2018).

2.6.7.1. Funcionamiento DMARC

Un correo electrónico pasa la alineación de SPF cuando el dominio de dirección "visible" coincide con el dominio de dirección de correo "oculto" (también conocido como: desde o mfrom) dentro del encabezado del correo electrónico (Guntrip, 2016).

Si un mensaje falla la autenticación DMARC los remitentes pueden:

- Supervisar todos los mensajes fallidos para comprender su autenticación.
- Poner en cuarentena los mensajes que fallan en DMARC (pasar a la carpeta de correo no deseado).
- Rechazar los mensajes que fallan en DMARC (marcar como potencialmente peligroso).

Luego, los receptores envían informes DMARC a los remitentes, dándoles visibilidad sobre qué mensajes se autentican, qué mensajes no y por qué.

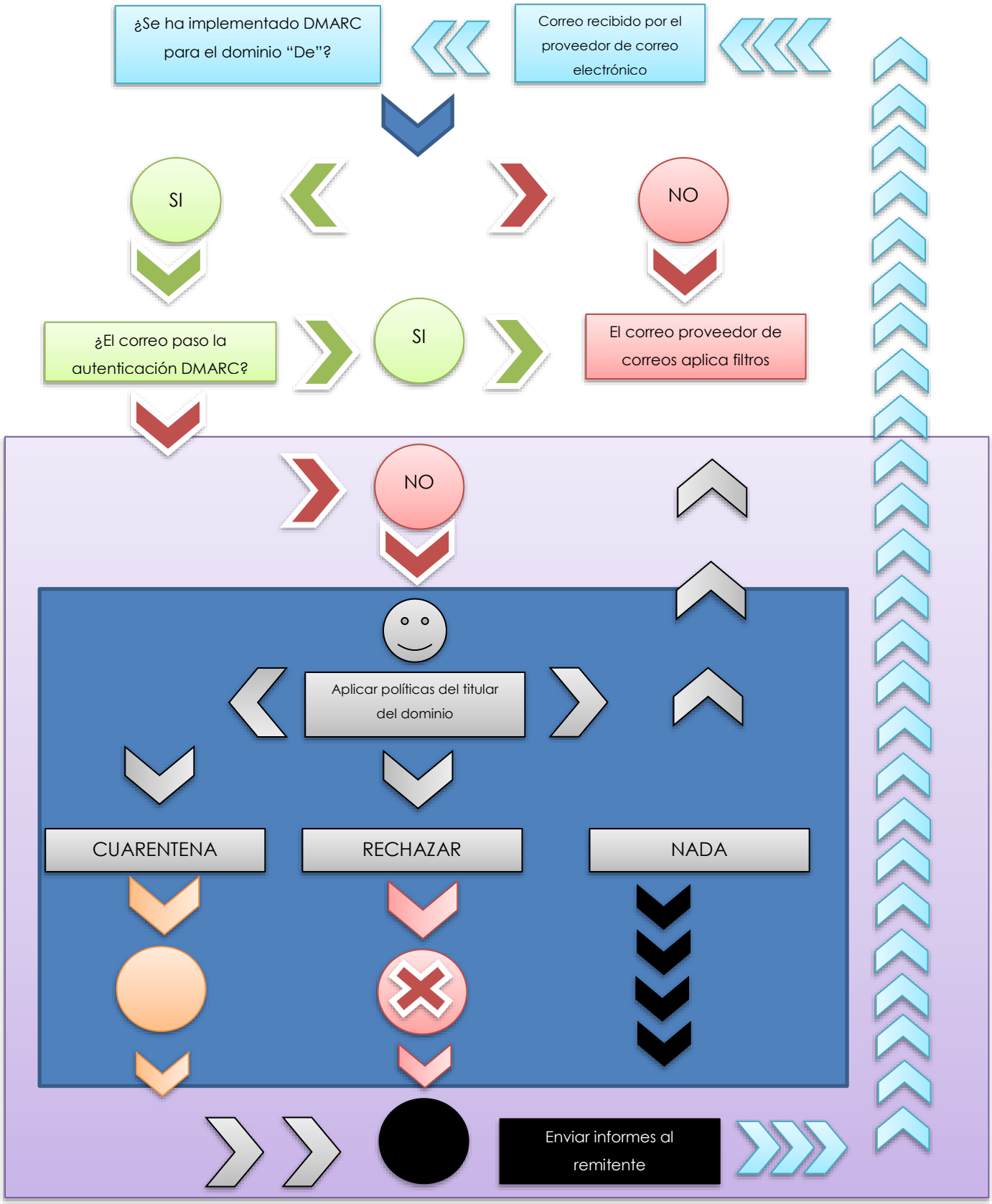


Figura 5. Algoritmo DMARC

2.6.7.2. Importancia DMARC

> Si bien educar a los usuarios finales sobre la defensa contra el fraude por correo electrónico es fundamental, no puede ser la primera línea de defensa de su organización. DMARC elimina las conjeturas para empleados y clientes, anulando una clase completa de mensajes de phishing (Guntrip, 2016).

Ya con estos tres elementos bien configurados se ofrece al receptor la capacidad de discernir si en efecto un correo que le llega a la bandeja de entrada es o no legítimo. Son parches que hemos tenido que ir aplicando encima del protocolo SMTP ya que como ocurriera con el HTTP, en su creación inicial no se tuvo en cuenta los posibles usos malintencionados de la actualidad (todos los que utilizaban al principio SMTP eran usuarios académicos). Hay que tomar en cuenta que así configuremos SPF, DKIM y la política DMARC de nuestro correo correctamente, todavía depende de un cuarto elemento que es ajeno al control: la herramienta de correo utilizada por el receptor (Iglesias, 2018).

2.7.Herramientas para la simulación

2.7.1. VMware

VMware es un sistema de virtualización que simula un sistema físico (un computador, un hardware) con unas características de hardware determinadas. Cuando se ejecuta el programa (simulador), proporciona un ambiente de ejecución similar a todos los efectos a un computador físico (excepto en el puro acceso físico al hardware simulado), con CPU (puede ser más de una), BIOS, tarjeta gráfica, memoria RAM, tarjeta de red, sistema de sonido, conexión USB, disco duro (pueden ser más de uno), entre otros (nubedigital.co).

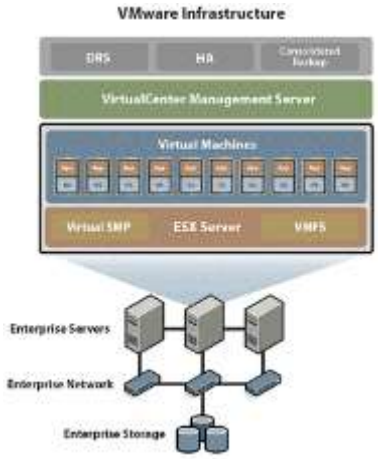


Figura 6. Infraestructura del VMware

(nubedigital.co)

2.7.2. VirtualBox

Es un software de virtualización creado originalmente por la empresa alemana innotek GmbH. Es desarrollado actualmente por la compañía Oracle como parte de su familia de productos para la virtualización. Este software permite instalar sistemas operativos adicionales, conocidos como sistemas invitados, dentro de otro sistema operativo anfitrión, cada uno con su entorno independiente (ecured, s.f.).

2.7.3. GNS3

GNS3 es un software de código abierto para emular, configurar, probar y solucionar problemas de redes virtuales y reales. GNS3 le permite ejecutar una pequeña topología que consta de solo unos pocos dispositivos en su computadora portátil, a aquellos que tienen muchos dispositivos alojados en múltiples servidores o incluso alojados en la nube (Telectrónika, 2018).

2.7.4. Kali Linux

Kali es una distribución de Linux basada en Debian. Su objetivo es simple; incluya tantas herramientas de penetración y auditoría de seguridad como sea posible en un paquete conveniente. Kali entrega también muchas de las mejores herramientas de código abierto para realizar pruebas de seguridad que se recopilan y están listas para usar (maslinux, 2018).

Kali es desarrollado y mantenido por Offensive Security. Son una presencia conocida y confiable en el mundo de la seguridad, e incluso certifican a los profesionales de la seguridad con algunas de las certificaciones más respetadas disponibles (maslinux, 2018).

Es una solución conveniente, también. Kali no requiere que mantengas una instalación de Linux ni recopile su propio software y dependencias. Es llave en mano. Todo el trabajo está fuera del camino, por lo que puedes concentrarte en el trabajo real de auditar el sistema que hayas establecido para probar (maslinux, 2018)**.**

CAPÍTULO III

3. Metodología

El diseño de la investigación utilizó un tipo de estudio bibliográfico ya que con dicho estudio se garantizó adquisición de conocimiento y calidad en fundamentos teóricos y prácticos de toda la investigación.

Según el nivel de medición y análisis de la información fue una investigación descriptiva e inferencial ya que se realizó un análisis previo y post acerca de las vulnerabilidades y riesgos en la red ante ataques tipo SMTP Spoofing mediante la utilización de herramientas de simulación y mecanismos de defensa.

Según las variables fue experimental ya que como investigadores se experimentó y se probó en varios escenarios de simulación diferentes mecanismos de defensa anti-SMTP spoofing para proteger la red de la Universidad Nacional de Chimborazo, además de la manipulación de las variables para poder comprobar la hipótesis de la investigación.

3.1. Hipótesis

3.1.1. Comprobación de la Hipótesis

La comprobación de la hipótesis estadística es una regla que basada en una hipótesis nula H_0 ayuda a decidir si ésta se acepta o no. Para la justificación de la hipótesis se utilizó la distribución de Wilcoxon en dos muestras relacionadas, y debido a que los datos no se distribuyen normalmente se realiza la comprobación mediante su rango medio.

3.1.2. Planteamiento de la Hipótesis

Hi= La implementación de mecanismos de defensa en un ambiente simulado permite proyectar la disminución de ataques SMTP spoofing en la infraestructura de red ipv4 de la Universidad Nacional de Chimborazo.

Ho= La implementación de un mecanismo de defensa en un ambiente simulado no permite minimizar los ataques SMTP spoofing en la infraestructura de red ipv4 de la Universidad Nacional de Chimborazo.

3.1.3. Nivel de Significancia

El valor del nivel de significancia es de α=0.05 = 5%

3.2. Identificación de variables

Variable Independiente

Ataque SMTP spoofing en el ambiente simulado de la red ipv4 de la Universidad Nacional de Chimborazo.

Variable Dependiente

Mecanismos de defensa contra el ataque SMTP Spoofing

3.3. Operacionalización de las variables

Tabla 1. Operacionalización de variables.

VARIABLE	TIPO	DEFINICIÓN CONCEPTUAL	DIMENSIÓN	INDICADORES
Ataque SMTP spoofing en el ambiente simulado de la red ipv4 de la Universidad Nacional de Chimborazo.	Independiente	La suplantación de identidad en e-mails ocurre en el campo FROM (remitente) cuando este es falso, de forma que se muestra el correo recibido de cualquier entidad o empresa que el atacante quiera suplantar.	e-mails Hijacking	- Porcentaje de usuarios afectados con correo suplantado. - Porcentaje de credenciales obtenidas.
Mecanismos de defensa contra los ataques smtp spoofing.	Dependiente	Son estrategias psicológicas inconscientes puestas en juego por diversas entidades para hacer frente a la realidad y mantener la autoimagen.	Ataque activo tipo SMTP-Spoofing Mitigar ataques SMTP spoofing Consumo de recursos en Servidor de Correos	- Porcentaje de ataques detectados. - Porcentaje de dispositivos afectados - Porcentaje de ataques controlados aplicando los mecanismos de defensa anti-smtp spoofing. - Uso de memoria - Uso de CPU

3.4. Tipo y Diseño de Investigación

Se utilizo la técnica de simulación que se base en realizar simulaciones de escenarios reales, ya que la investigación se basó en observar el comportamiento de las simulaciones de la red IPv4 de la Universidad Nacional de Chimborazo frente a un ataque SMTP spoofing, además de su comportamiento al utilizar los mecanismos de defensa.

3.5. Unidad de análisis

La simulación se llevó a efecto durante 4 días, y cada día durante 3 periodos en la mañana, tarde y noche. Los datos obtenidos en ese periodo fueron registrados y analizados en el software estadístico R.

3.6. Población de estudio

Serán todos los usuarios vigentes conectados en la red simulada de la Universidad Nacional de Chimborazo.

3.7. Tamaño de muestra

Al ser una población infinita la muestra será la cantidad de usuarios conectados a la red en la Facultad de Ingeniería afectados por ataque SMTP spoofing en la red de la Universidad Nacional de Chimborazo para obtener datos en el que los investigadores determinarán el tiempo en que la muestra será tomada, en este caso la muestra es no aleatoria de una población infinita.

3.8. Técnicas de recolección de Datos

En base a la técnica de investigación seleccionada, el instrumento de recolección de datos es en una escala de valoración.

3.9. Técnicas de Análisis e interpretación de la información

- Realización del estudio previo del tipo de ataque SMTP spoofing a la red.
- Análisis de funcionamiento del ataque y como contrarrestarlo con los mecanismos de defensa.
- Instalación de las herramientas de simulación.

- Diseño de la topología de la red de la Universidad Nacional de Chimborazo utilizando herramientas de simulación.
- Simulación del ataque SMTP spoofing y sus mecanismos de defensa.
- Procesamiento de los datos en el software estadístico R.
- Análisis de los resultados.
- Elaboración del manual de prevención.

Una vez obtenida la información se procedió a ingresar los datos en un software estadístico informático llamado “R”, para verificar la hipótesis planteada emitiendo conclusiones y recomendaciones en base al estudio realizado.

CAPÍTULO IV

4. Resultados y Discusión.

4.1. Topología antes del ataque.

A continuación, se presenta el escenario simulado con el cual se experimentó cumpliendo los indicadores propuestos en la hipótesis planteada.

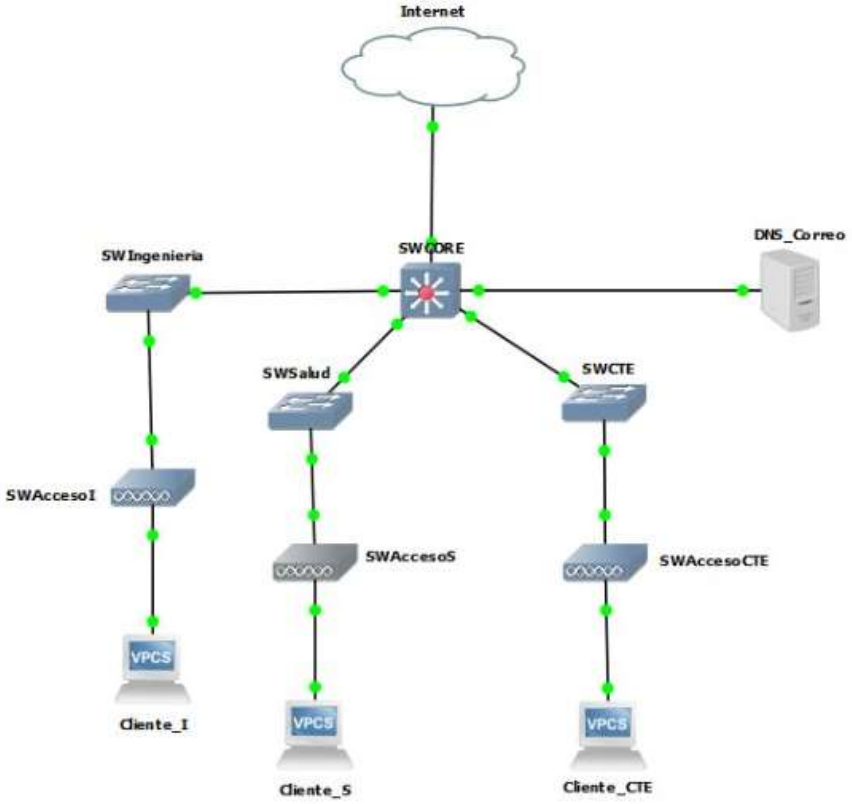


Figura 7. Topología de la red de la Universidad Nacional de Chimborazo

Como se visualiza en la Fig. 7, la topología no cuenta con el firewall porque este dispositivo no posee alguna configuración para evitar los ataques smtp spoofing, por esta razón se omitió en el escenario de simulación. Además, el firewall controla el puerto SMTP el cual evita sólo el envío masivo de correos ya que los protocolos de seguridad se configuran directamente en el servidor de correos.

4.2. Topología durante el ataque.

Continuando con la simulación, se presenta el escenario en el cual se implementa el ataque. Este ataque de smtp spoofing se lo realiza de manera externa, el que se basa en un total de 60 correos, entre ellos: correos de usuarios legítimos y usuarios suplantados, analizados

diariamente por 4 días, adicionalmente por el mismo periodo de días se recolectó datos del consumo de recursos (memoria y CPU) del servidor de correos.

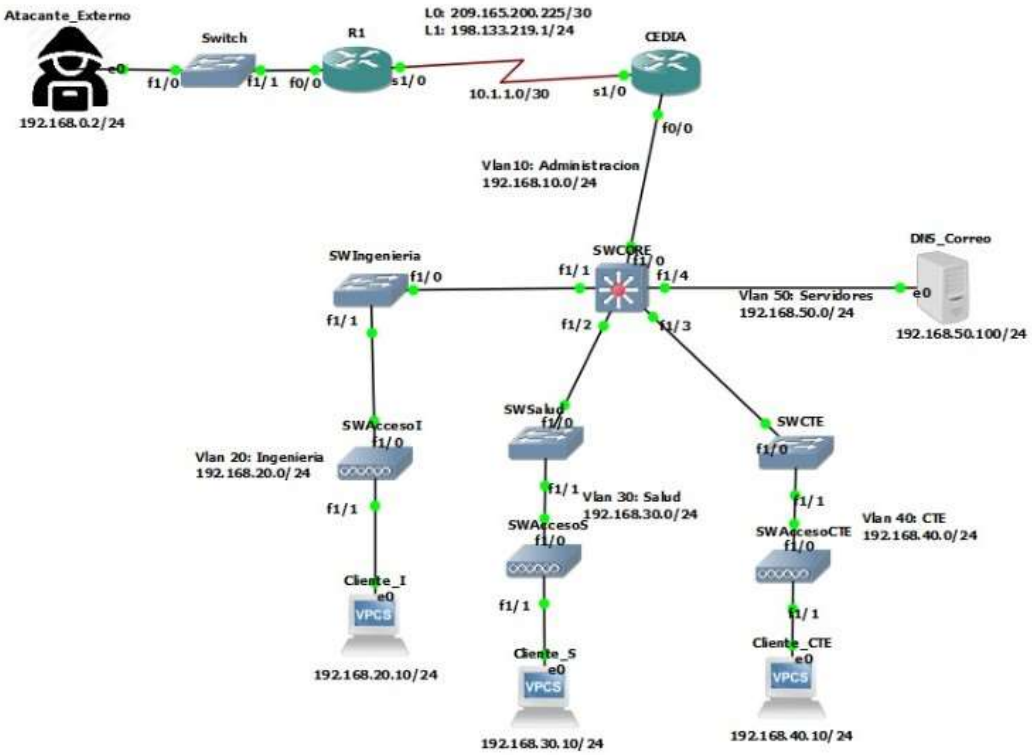


Figura 8. Topología con el ataque

Los resultados de la simulación realizado durante el período de 4 días se pueden visualizar en la fig. 9. En dicha figura se muestra que todos los días la red estuvo bajo ataque de SMTP spoofing, en el que se obtuvo como resultado un 45.42% de correos de usuarios suplantados.

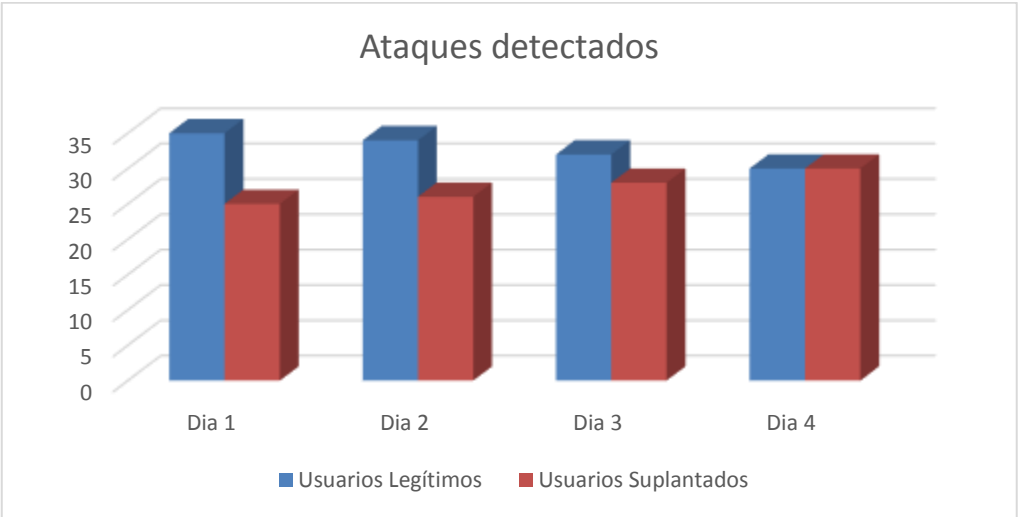


Figura 9. Ataques detectados

El ambiente simulado (Fig.8) cuenta con 3 clientes conectados a la red y consumiendo el servicio SMTP del servidor de correos, con los cuáles se experimentó desde un atacante externo conectado a la internet y se procedió a enviar el ataque smtp spoofing en el que se puede observar que sin la implementación de protocolos de defensa no existe resistencia alguna, dando lugar a que el correo suplantado llegue a cada uno de los clientes.

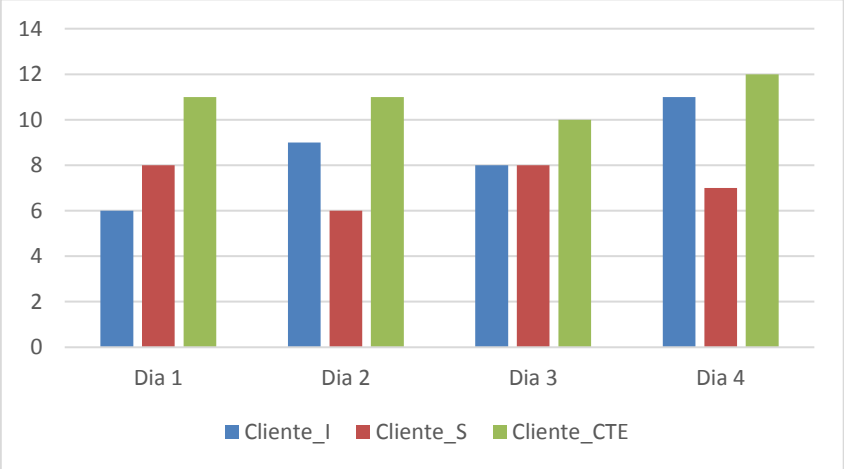


Figura 10. Dispositivos atacados

En la fig. 10, existe la cantidad de 100% de usuarios afectados con el ataque smtp spoofing. Estando expuestos hacia los peligros maquiavélicos que el correo puede contener, estos pueden ser de diferente índole dependiendo de la habilidad del atacante.

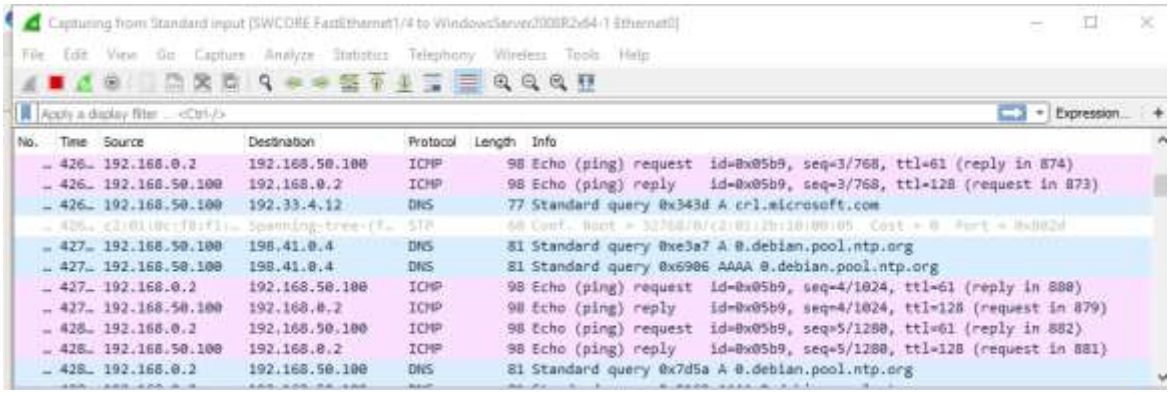


Figura 11. Envío de correo Atacante-Servidor

Adicionalmente, se puede apreciar en la fig. 11 los resultados arrojados mediante la herramienta Wireshark, en el que se observó que el atacante externo realiza una petición de

envío y el receptor en este caso el servidor de correos le da una respuesta de servidor DNS, dando paso absoluto a los correos suplantados.

Finalmente, los resultados de la simulación referente a los recursos que consume el servidor de correos durante 4 días se obtiene un promedio de 4.08% (Fig.12) en uso del CPU mientras tanto en uso de memoria llego 75.88% (Fig. 11).

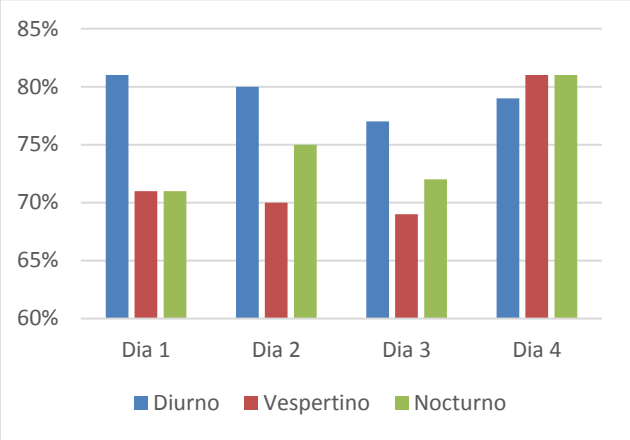


Figura 12. Uso de memoria sin protocolos

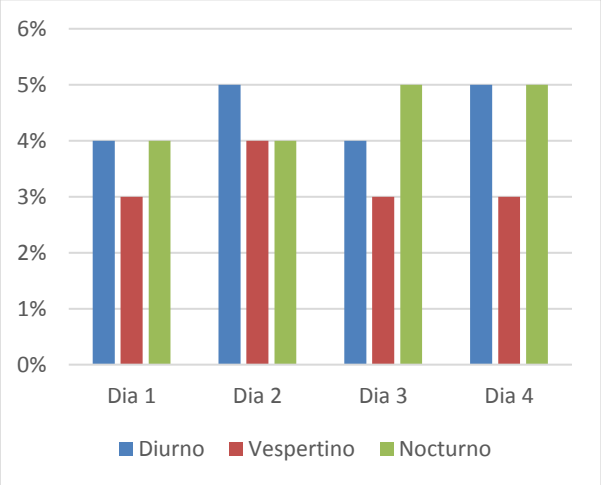


Figura 13. Uso del CPU sin protocolos

4.3. Topología durante el ataque y aplicación de los mecanismos de defensa.

En esta etapa de la simulación, se presenta el escenario en el cual se implementa los mecanismos de defensa. Estos mecanismos son implementados en el servidor de correos los cuales ayudan a reducir el ataque de smtp spoofing que se realiza de manera externa.

Los datos recolectados se basan en 60 correos analizados diariamente por 4 días, también por el mismo periodo de días se analiza el consumo de recursos (memoria RAM y CPU) del servidor de correos.

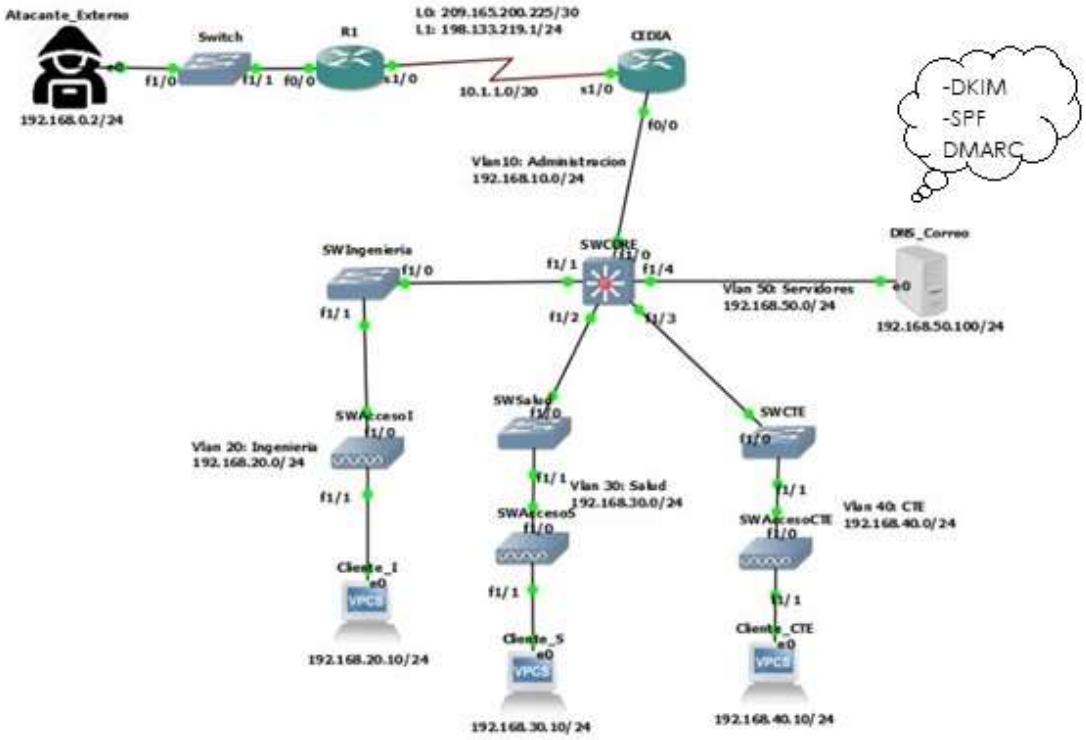


Figura 14. Topología con los mecanismos de defensa

Los resultados de la simulación realizado durante el período de 4 días se pueden visualizar en la fig. 15. Durante todos los días los mecanismos de defensa redujeron el porcentaje de correos de usuarios suplantados a un 5% de un total de 45.42%. Se puede observar que los mecanismos de defensa lograron reducir en un 40.42% los ataques.

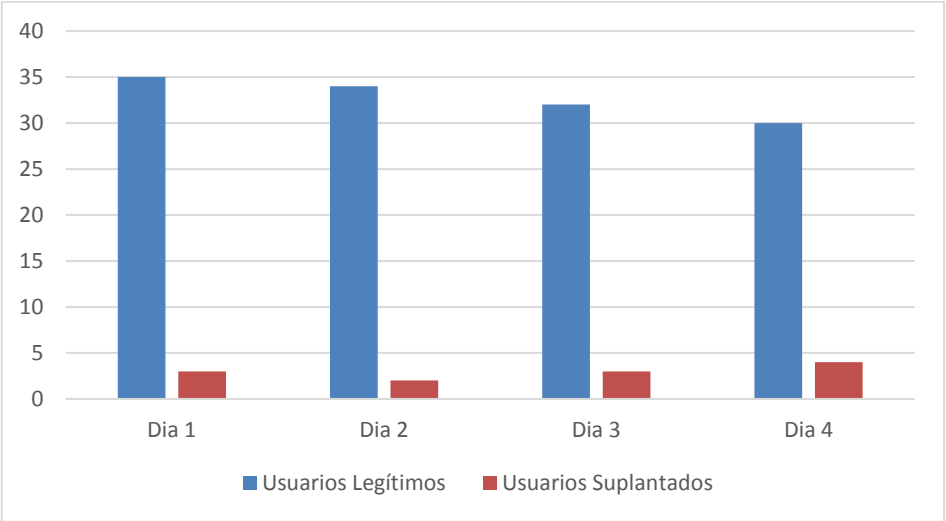


Figura 15. Ataques controlados

Se puede comprobar en la fig. 16 que mediante la herramienta Wireshark arroja un resultado de problema de conexión entre el atacante externo hacia el servidor de correos.

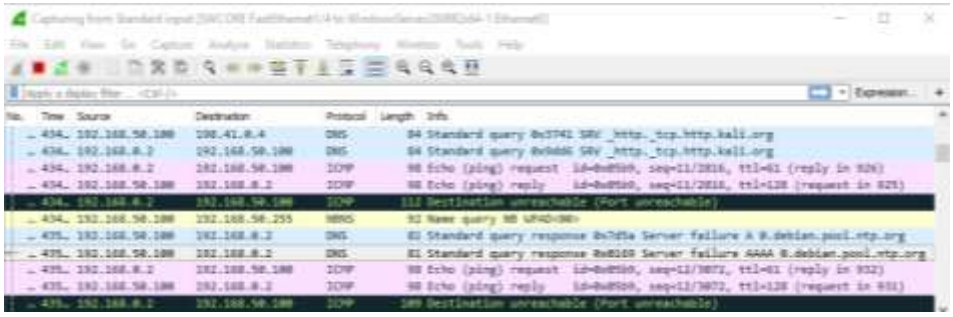


Figura 16. Problema de conexión entre atacante externo-servidor de correos

Con lo cual se procedió a verificar en la fig. 17 el origen del problema, wireshark resalta con amarillo el motivo por el cual el servidor rechaza la petición de envío de correo.

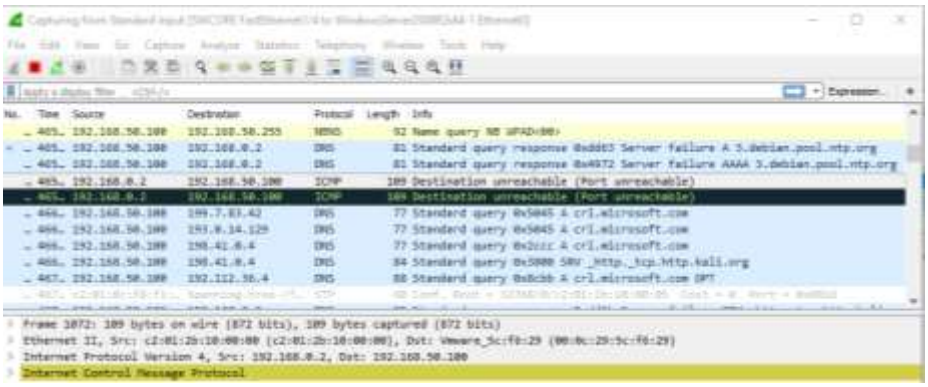


Figura 17. Motivo del rechazo de envio de correo

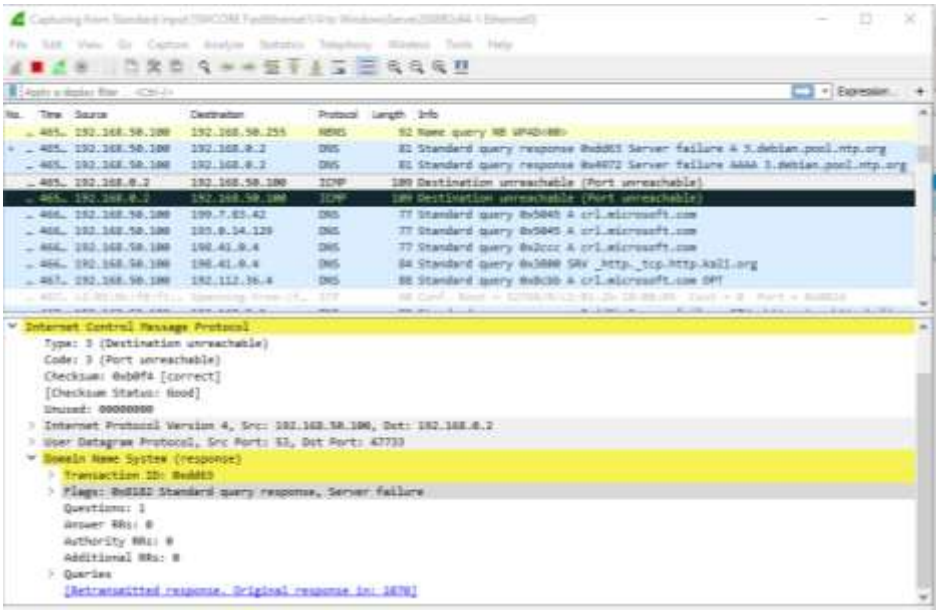


Figura 18. DNS rechaza la petición del atacante

En la fig.18 se observa que el servidor DNS rechaza la petición del atacante bloqueando la comunicación y así evitando que el correo suplantado llegue con éxito a la víctima.

4.3. Test de Normalidad y pruebas de Wilcoxon

Con la elaboración del test de normalidad para los datos del ataque sin mecanismos de defensa tiene un p-valor = 0.346, con este resultado se deduce que estos datos se distribuyen normalmente, pues tiene más de 0.05 de p-valor, como se muestra en las siguientes figuras 19 y 20.

```
> # Prueba 1
> prueba=read.table("Spoofing.txt",header=T)
> prueba
   Ataque Mitigacion
1      10          1
2       3          0
3      12          2
4      13          1
5       5          0
6       8          1
7      14          2
8       3          0
9      11          1
10      7          1
11     14          2
12      9          1
>
> shapiro.test(prueba$Ataque)

        Shapiro-Wilk normality test

data:  prueba$Ataque
W = 0.92666, p-value = 0.346
```

Figura 19. Test de normalidad - datos del ataque sin mecanismos de defensa

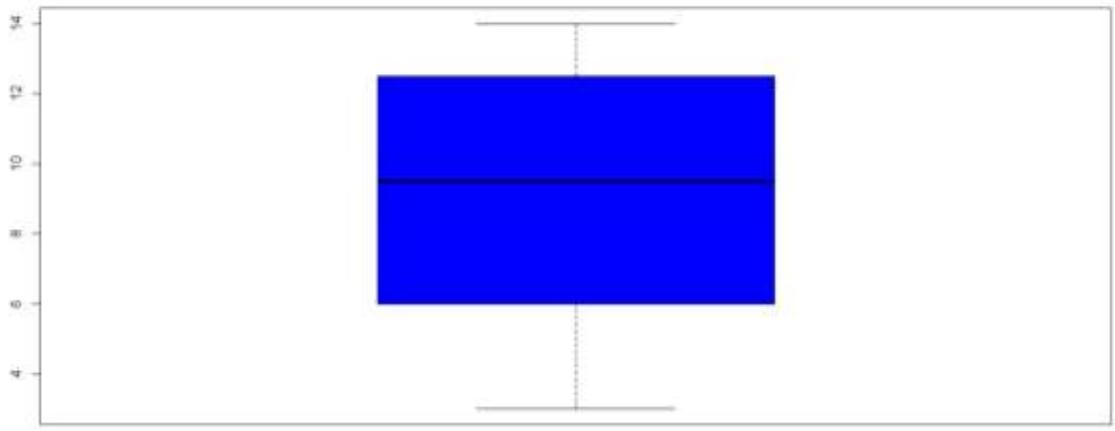


Figura 20.Representacion de los datos normales sin mecanismos de defensa

Al elaborar el test de normalidad para los datos del ataque con los mecanismos de defensa tiene un p-valor = 0.01994, con este resultado se deduce que estos no se distribuyen normalmente, pues tiene menos de 0.05 de p-valor esto se muestra en las siguientes figuras 21 y 22.

```
> # Prueba 1
> prueba=read.table("Spoofing.txt",header=T)
> prueba
   Ataque Mitigacion
1      10          1
2       3          0
3      12          2
4      13          1
5       5          0
6       8          1
7      14          2
8       3          0
9      11          1
10      7          1
11     14          2
12      9          1
> shapiro.test(prueba$Mitigacion)

        Shapiro-Wilk normality test

data:  prueba$Mitigacion
W = 0.82816, p-value = 0.01994
```

Figura 21.Test de normalidad - datos del ataque con los mecanismos de defensa

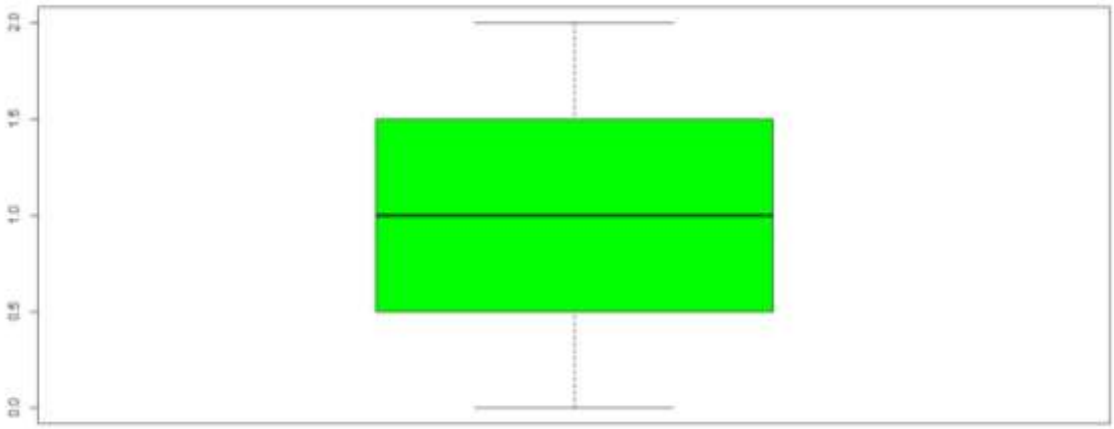


Figura 22. Representación de los datos normales con los mecanismos de defensa

Como se muestra en la fig.15 los ataques de SMTP spoofing se mitigan en una cantidad considerable. Mediante el test de Wilcoxon que permite comparar 2 muestras relacionadas pero que no se distribuye normalmente, se obtiene un p_valor = 3.059e-05 aceptando la hipótesis alternativa la cual es: “La implementación de mecanismos de defensa en un ambiente simulado permite proyectar la disminución de ataques SMTP spoofing en la

infraestructura de red ipv4 de la Universidad Nacional de Chimborazo", dado que el valor mencionado tiende a cero. (fig. 23 y fig. 24)

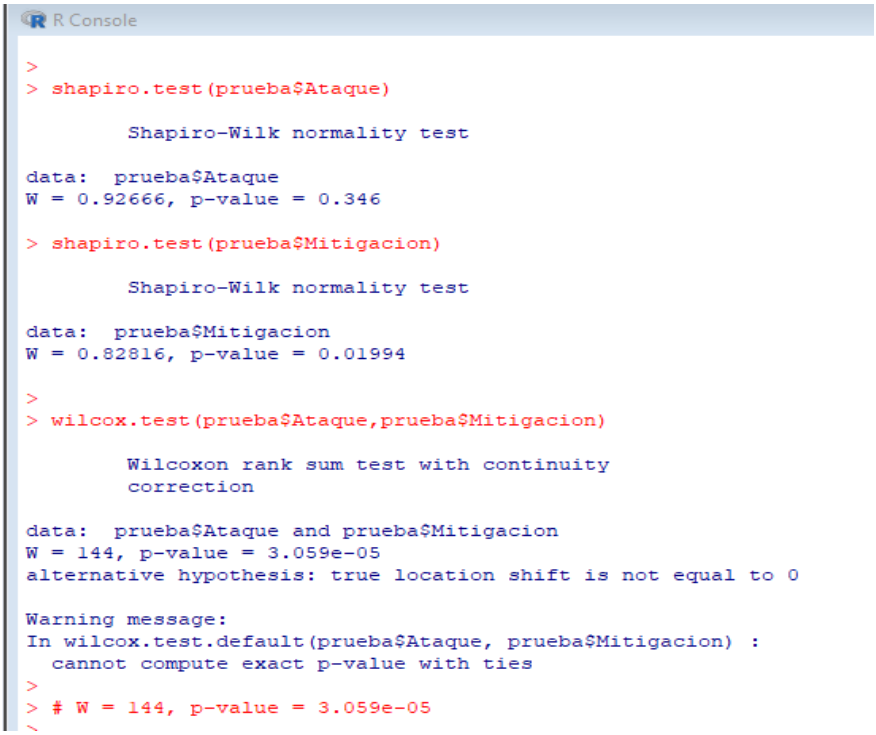


Figura 23. Test Wilcoxon – datos para la comprobación de la hipotesis

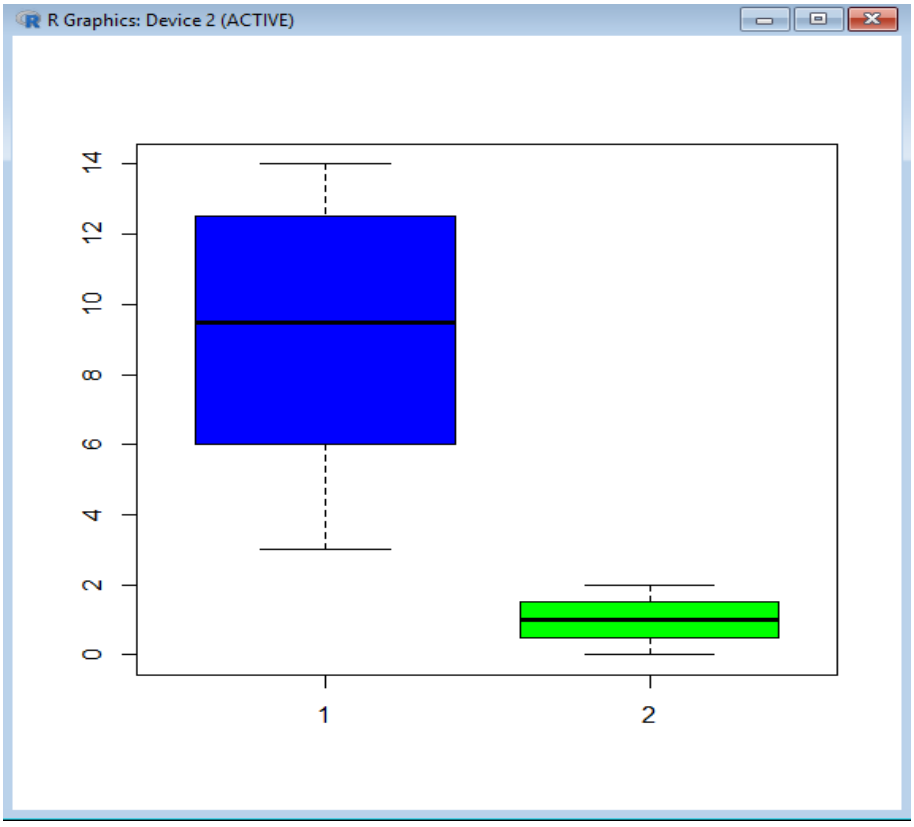


Figura 24. Test Wilcoxon – Representación de los datos obtenidos en los 2 escenarios

Además, los resultados de la simulación referente a los recursos que consume el servidor de correos durante 4 días se obtiene un promedio de 23.25% (fig. 26) en uso del CPU mientras tanto en uso de memoria RAM llegó 82.34% (fig.25).

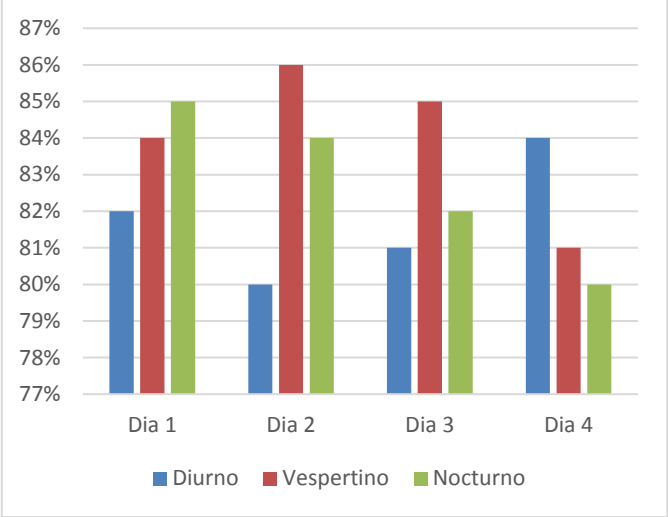


Figura 25. Uso de memoria RAM con protocolos

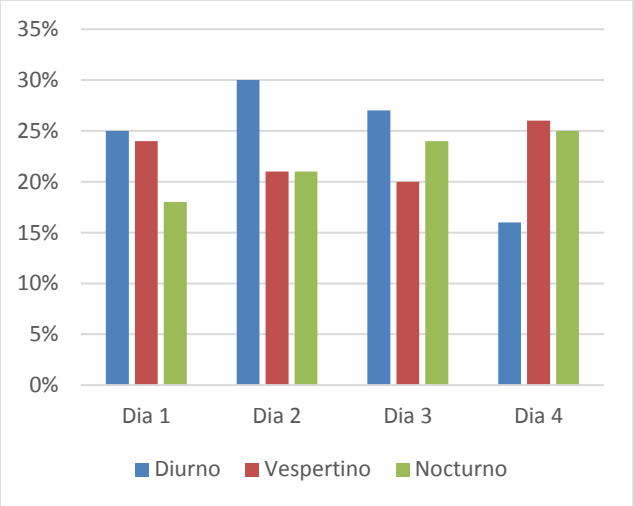


Figura 26. Uso del CPU con protocolos

5. CONCLUSIONES

Las diversas amenazas relacionadas con los ataques de suplantación de identidad pueden contener desde hijacking hasta phishing, varían según la habilidad del atacante. Por ello con la implementación de SPF se comprueba que el correo entrante es de un dominio o host autorizado, sin embargo pueden existir remitentes autorizados en los que SPF no puede estar configurado, es allí donde DKIM verifica que es un dominio correcto ya que con la implementación de una criptografía de clave pública puede determinar de manera creíble que el correo es enviado por un dominio autorizado, adicionalmente; DMARC coordina los resultados de los dos mecanismos ya existentes en alineación del dominio con el campo de encabezado "De: usuario remitente; Para: usuario final", finalizando el proceso en el que evita el abuso excesivo de suplantación de identidad.

Según la investigación y las pruebas realizadas al escenario de simulación se determinó que cada mecanismo no puede implementarse sólo, sino que; estos mecanismos deben complementarse, asegurándose con este proceso de verificación que en el servidor DNS lleguen los correos desde un dominio verificado.

Se observó en la fig. 12 y 13 que el uso de memoria RAM y CPU respectivamente, antes de implementar los mecanismos de defensa anti SMTP spoofing se obtuvo un promedio de consumo del 4.08% en el CPU y en memoria RAM llegó al 75.88%, mientras que con la implementación de los mecanismos de defensa se obtuvo un promedio del 23.25% en uso del CPU (fig. 26) y en memoria RAM llegó al 82.34% (fig. 25). Al comparar el consumo de recursos pre y post, se deduce que en el servidor de correos la memoria RAM tiene un aumento elevado, mientras que el uso de CPU no varía considerablemente.

El ambiente simulado de la red ipv4 de la Universidad Nacional de Chimborazo en la cual se realizó el ataque de SMTP spoofing se obtuvo en un principio el 45.42% de correos de usuarios suplantados del total de 60 correos enviados diariamente en un periodo de 4 días, posteriormente al configurar e implementar los mecanismos de defensa DKIM, SPF y DMARC el porcentaje se redujo a un 5%, logrando reducir el ataque en un 40.42%.

El manual de usuario tiene la finalidad de guiar en la correcta configuración e implementación de protocolos de defensa SPF, DKIM y DMARC; concluyéndose por lo tanto que el establecimiento de parámetros de configuración puede variar de acuerdo a las infraestructuras donde se desee aplicar dicho manual.

6. RECOMENDACIONES

Revisar a detalle las diversas configuraciones que tiene cada mecanismo de defensa y tomar esta investigación como guía para las entidades que poseen un servidor de correo propio, pues este documento presenta las configuraciones recomendables de SPF, DKIM y DMARC para controlar considerablemente los ataques de smtp spoofing.

Implementar un servidor de correos propio en lugar de un servidor compartido en la nube, por razones fundamentalmente de privacidad y control de funcionalidad, sin restricciones a las configuraciones y políticas de uso. Por ende, se asegura que la configuración de seguridad se adecue a las necesidades y funciones requeridas por cada entidad.

Investigar actualizaciones de los diferentes mecanismos de defensa para que la integridad de la información de correo permanezca segura, puesto que los mecanismos de defensa reducen el ataque de smtp spoofing más no lo eliminan por completo, no obstante; con el pasar del tiempo la ciberdelincuencia está a la orden del día y pueden mejorar sus técnicas a la par que la ciberseguridad avanza.

Capacitar a los usuarios finales propietarios de las cuentas de correo, en el uso y acciones correctas para detectar ataques de Spoofing y desecharlos.

7. REFERENCIAS BIBLIOGRÁFICAS

Academy, C. N. (10 de Junio de 2017). *NetAcad.* Obtenido de NetAcad: https://www.netacad.com/

Acens. (Diciembre de 2017). *acensTechnologies.* Obtenido de acensTechnologies: https://www.acens.com/wp-content/images/2017/12/spoofing-wp-acens.pdf

Alulema Chiluiza, D. V. (2008). *ESTUDIO Y DISEÑO DE UN SISTEMA DE SEGURIDAD PERIMETRAL PARA LA RED QUITO MOTORS, UTILIZANDO TECNOLOGÍA UTM.* Quito: Tesis.

Benchimol, D. (Buenos Aires). *Hacking desde cero.* 2011: Fox Andina.

ecured. (s.f.). *ecured*. Obtenido de ecured: https://www.ecured.cu/VirtualBox

Fiscalía General del Estado, E. (Junio de 2015). *FGE*. Obtenido de FGE: https://www.fiscalia.gob.ec/los-delitos-informaticos-van-desde-el-fraude-hasta-el-espionaje/

Flórez R., W., Arboleda S., C. A., & Cadavid A., J. F. (Enero-Junio 2012). SOLUCIÓN INTEGRAL DE SEGURIDAD PARA LAS PYMES MEDIANTE UN UTM. *Ing. USBMed, Vol 3*, 35-42.

FORTINET. (2018). *Fortinet*. Obtenido de Fortinet: https://www.fortinet.com/solutions/small-business/connected-utm.html

Fraile, A. R. (Febrero de 2011). *intypedia*. Obtenido de intypedia: http://www.criptored.upm.es/intypedia/docs/es/video5/DiapositivasIntypedia005.pdf

Garcia Ciyi, C. (26 de Agosto de 2010). *Hacking Ético*. Obtenido de Hacking Ético: https://hacking-etico.com/2010/08/26/hablemos-de-spoofing/

Guntrip, M. (07 de Diciembre de 2016). *proofpoint*. Obtenido de proofpoint: https://www.proofpoint.com/es/corporate-blog/post/what-is-sender-policy-framework-spf

Iglesias, P. F. (17 de Enero de 2018). *Mundo Hacker*. Obtenido de Mundo Hacker: https://www.pabloyglesias.com/email-spoofing/

INFOSEGUR. (2012 de Noviembre de 2013). *INFOSEGUR*. Obtenido de INFOSEGUR: https://infosegur.wordpress.com/tag/vulnerabilidades/

Izaskun, P., Fernando, A., & Amaia, L. (23 de Junio de 2006). *Enpresa Digitala.* Obtenido de Enpresa Digitala: www.enpresadigitala.net

Martínez, C., & Oñate, O. (2017). *MEJORAS EN LA SEGURIDAD DE LA RED INALÁMBRICA DE LA UNIVERSIDAD NACIONAL DE CHIMBORAZO APLICANDO HACKING ÉTICO.* Riobamba: Universidad Nacional de Chimborazo.

maslinux. (2018). *maslinux.es*. Obtenido de maslinux.es: https://maslinux.es/que-es-kali-gnu-linux/

Méndez, A. L. (25 de Agosto de 2014). *Webempresa*. Obtenido de Webempresa: https://www.webempresa.com/blog/que-es-el-mail-spoofing-y-como-evitarlo-usando-spf.html

Muñoz de Frutos, A. (19 de Septiembre de 2016). *Computer Hoy*. Obtenido de Computer Hoy: https://computerhoy.com/noticias/software/que-es-spoofing-51236

nubedigital.co. (s.f.). VMWARE. *Nube Digital*.

Ojeda-Pérez, J. E. (2010). Delitos Informáticos y entorno jurídico vigente en Colombia. *Cuadernos de Contabilidad*, 41-66.

Policía Nacional del Ecuador. (02 de Septiembre de 2015). *Policía Nacional del Ecuador*. Obtenido de Policía Nacional del Ecuador: http://www.policiaecuador.gob.ec/delitos-informaticos-o-ciberdelitos/

Rivero, M. (2014-2018). *Info Spyware*. Obtenido de Info Spyware: https://www.infospyware.com/articulos/que-son-los-malwares/

Telectrónika. (29 de Abril de 2018). *telectronika.com*. Obtenido de telectronika.com: https://telectronika.com/articulos/que-es-gns3/

Urueña Centeno, F. J. (16 de Enero de 2015). *IEEE*. Obtenido de IEEE: www.ieee.es

ANEXOS

Anexo A: Escenarios de la Investigación.

1.1. Escenario de la UNACH con su topología.

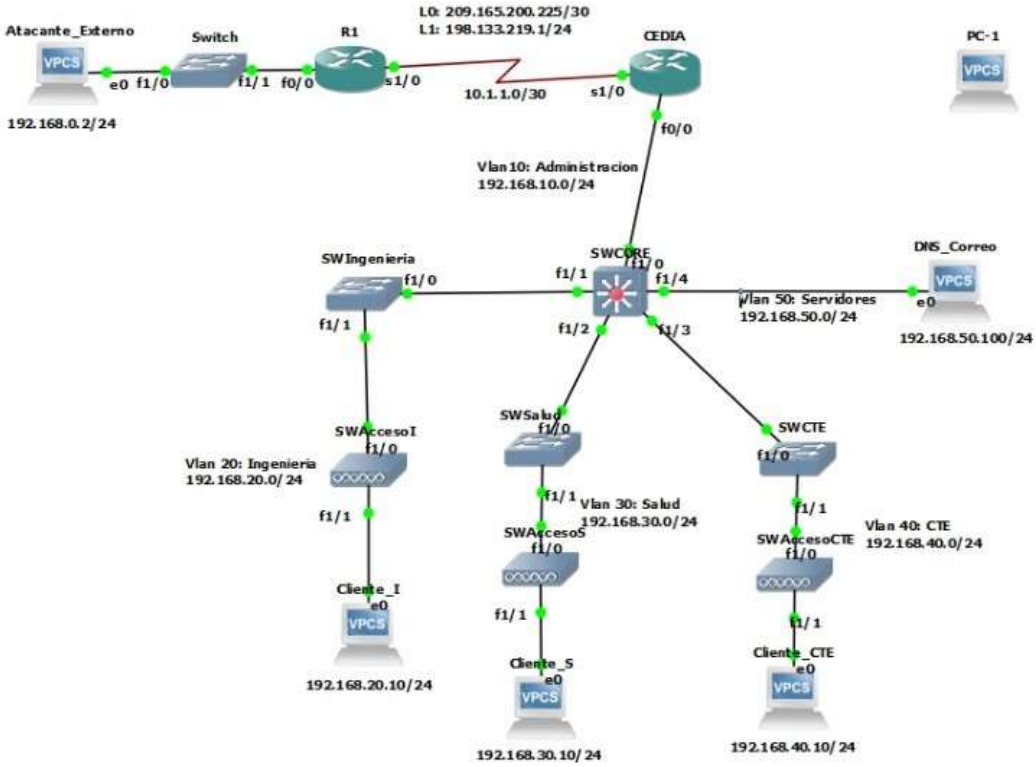


Figura 27. Topología de la red de UNACH sin ataque

Fuente: Autores

En la fig. 27, se muestra la topología en la cual se trabajó con el ataque y el mecanismo de defensa; el ataque se lo realizo mediante el sistema operativo Kali Linux, al enviar el ataque exteriormente, a parte también se realizó en la misma topología la configuración e instalación de los mecanismos de defensa.

1.2. Escenario de la UNACH con su topología y ataque externo a la red.

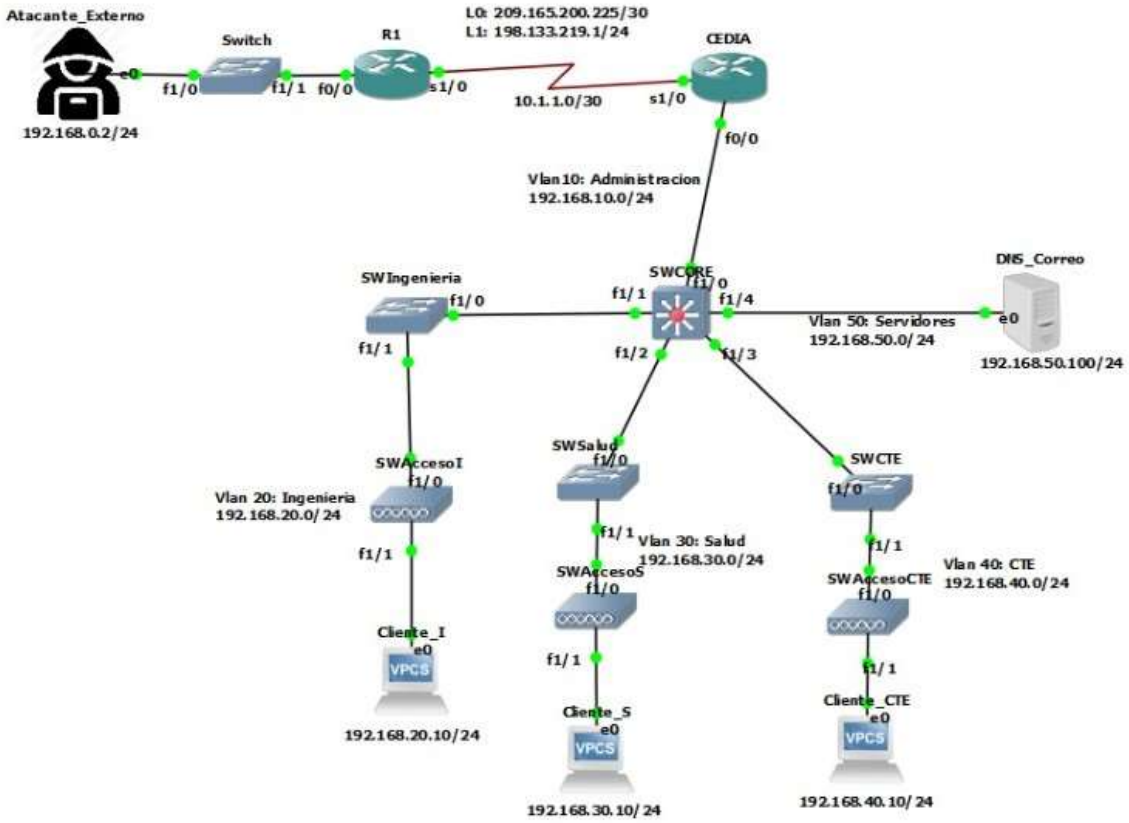


Figura 28. Topología de la red de la UNACH bajo ataque

En la fig. 28, se muestra a la red de la UNACH bajo un ataque externo (usando una máquina virtual Kali Linux) conectado a la internet realizando el ataque al servidor de correos.

1.3. Máquina virtual kali-linux

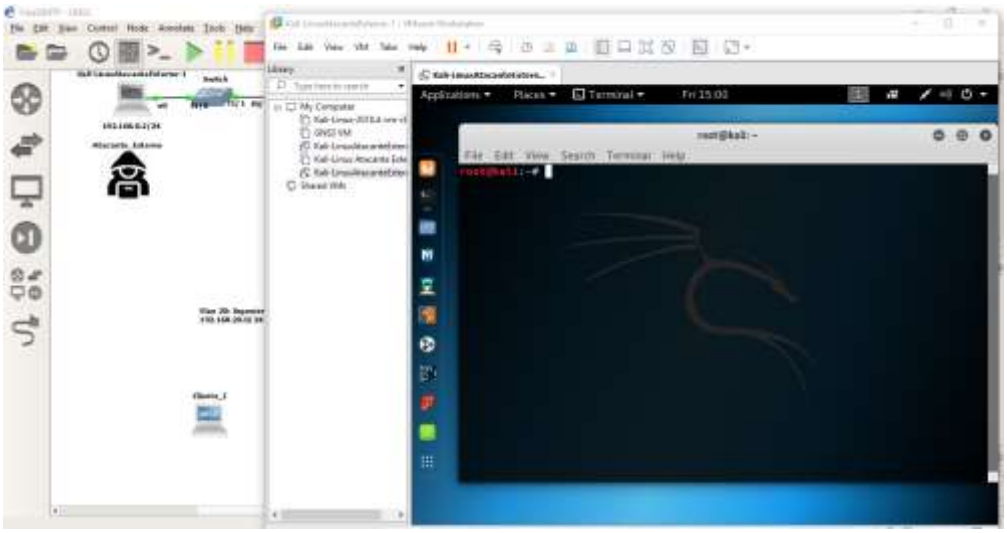


Figura 29. Máquina virtual kal-linux

En la Fig. 29, se muestra la máquina de Kali linux en la cual está configurado el ataque de smtp spoofing, esta máquina se encuentra de manera independiente a la red simulada de la Universidad Nacional de Chimborazo, pues un ataque es más común que se lo realice de manera externa y en el caso de ser smtp spoofing es el caso.

1.4. Máquina virtual Windows server 2008.

Figura 30. Windows Server 2008

En la fig. 30, se muestra la máquina virtual de Windows server 2008 la misma que posee la configuración del servidor de correos y el servidor DNS, las cuales van a ser vulneradas por el smtp spoofing a través de la máquina virtual de Kali linux.

1.5. Máquina virtual Windows XP.

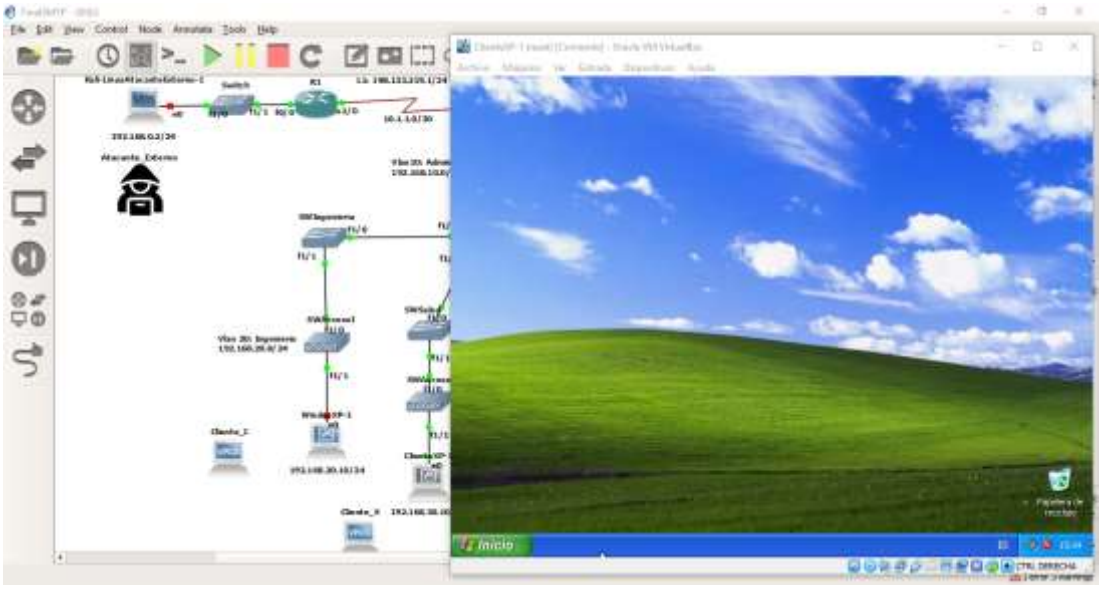


Figura 31. Máquina virtual cliente Windows XP.

En la Fig.31, se muestra la máquina virtual de Windows XP en la cual se configuró el cliente conectado al servidor de correos, pues es aquel que consume los servicios del servidor de correos.

Anexo B: Tablas de tabulación de datos

2.1 Dispositivos afectados en el ambiente simulado.

Se realizó el análisis de los ciberataques SMTP Spoofing durante la mañana, tarde y noche en los cuales, se procedió a capturar los ataques registrados en cada usuario individualmente. Esto se realizó durante el periodo de 4 días elegidos aleatoriamente. En la tabla 2 se encuentra la información tabulada en el primer día del ataque a los usuarios de un total de 60 correos, en donde el 41.67% son usuarios suplantados.

Tabla 2. Dispositivos afectados Dia 1

Usuarios	**Dia 1**		
	Diurno	**Vespertino**	**Nocturno**
Cliente_I	3	0	3
Cliente_S	2	1	5
Cliente_CTE	5	2	4
Total	10	3	12

En la tabla 3, se encuentra la información tabulada del primer día del ataque a los 3 usuarios de un total de 60 correos, en donde el 43.33% son usuarios suplantados.

Tabla 3. Dispositivos afectados Dia 2

Usuarios	**Dia 2**		
	Diurno	**Vespertino**	**Nocturno**
Cliente_I	5	2	2
Cliente_S	3	0	3
Cliente_CTE	5	3	3
Total	13	5	2

En la tabla 4, se encuentra la información tabulada del primer día del ataque a los 3 usuarios de un total de 60 correos, en donde el 46.66% son usuarios suplantados.

Tabla 4. Dispositivos afectados Dia 3

Usuarios	Dia 3		
	Diurno	Vespertino	Nocturno
Cliente_I	4	0	4
Cliente_S	4	0	4
Cliente_CTE	4	3	3
Total	14	3	11

En la tabla 5, se encuentra la información tabulada del primer día del ataque a los 3 usuarios de un total de 60 corres, en donde el 50% son usuarios suplantados.

Tabla 5. Dispositivos afectados Dia 4

Usuarios	Dia 4		
	Diurno	Vespertino	Nocturno
Cliente_I	3	5	3
Cliente_S	2	2	3
Cliente_CTE	2	7	3
Total	7	14	9

2.2. Ataques detectados sin protocolos de defensa en el ambiente simulado.

En la tabla 6, se trabajó con un total de 240 correos durante los 4 días, además cada uno de los días se trabajó con 20 correos durante las 3 jornadas dando un total de 60 correos por día. Cada día se envió 60 correos en los cuales el 54.58% son correos de usuarios auténticos y el 45.42% son usuario son correos suplantados.

Tabla 6. Ataques detectados sin protocolos

Jornada	Días							
	1		2		3		4	
	Usuarios Legítimos	Usuarios Suplantados	Usuarios Legítimos	Usuarios Suplantados	Usuarios Legítimos	Usuarios Suplantados	Usuarios Legítimos	Usuarios Suplantados
Diurno	10	10	7	13	6	14	13	7
Vespertino	17	3	15	5	17	3	6	14
Nocturno	8	12	12	8	9	11	11	9
TOTAL	35	25	34	26	32	28	30	30

2.3. Uso de memoria y CPU sin protocolos de defensa en el ambiente simulado.

En la tabla 7, se puede obcecar el consumo de recursos de memoria durante todo el periodo del ataque, pero en este caso omitiendo la implementación de los mecanismos de defensa.

Tabla 7. Uso de memoria RAM sin protocolos

Jornada	Sin protocolos			
	Memoria			
	Dia 1	Dia 2	Dia 3	Dia 4
Diurno	81%	80%	77%	79%
Vespertino	71%	70%	69%	81%
Nocturno	71%	75%	72%	81%
Porcentaje	74.33%	75%	72.67%	80.33%

En la tabla 8, se da a conocer el consumo de recursos del CPU durante todo el periodo del ataque, pero en este caso omitiendo la implementación de los mecanismos de defensa.

Tabla 8. Uso de CPU sin protocolos

Jornada	Sin protocolos			
	CPU			
	Dia 1	Dia 2	Dia 3	Dia 4
Diurno	4%	5%	4%	5%
Vespertino	3%	4%	3%	3%
Nocturno	4%	4%	5%	5%
Promedio	3.66%	4.33%	4%	4.33%

2.4. Ataques controlados con protocolo de defensa SPF, DKIM y políticas DMARC en el ambiente simulado.

En la tabla 10, se da a conocer el consumo de recursos de memoria durante todo el periodo del ataque, pero en este caso con la implementación de los mecanismos de defensa.

Tabla 9. Uso de memoria RAM con protocolos

Jornada	Protocolos SPF, DKM y DMARC			
	Memoria			
	Dia 1	Dia 2	Dia 3	Dia 4
Diurno	82%	80%	81%	84%
Vespertino	84%	86%	85%	81%
Nocturno	85%	84%	82%	80%
Promedio	83.67%	83.33%	82.67%	81.67%

En la tabla 11, se muestra el consumo de recursos del CPU durante todo el periodo del ataque, pero en este caso con la implementación de los mecanismos de defensa.

Tabla 10. Uso de CPU con protocolos

Jornada	Protocolos SPF, DKM y DMARC			
	CPU			
	Dia 1	Dia 2	Dia 3	Dia 4
Diurno	25%	30%	27%	18%
Vespertino	24%	21%	20%	26%
Nocturno	18%	21%	24%	25%
Promedio	22.33%	24%	23.67%	23%

Anexo C: Cuadros de parámetros de SPF y DKIM

3.1. Parámetros del SPF.

Tabla 11. Parámetros del SPF

Mecanismo	Sintaxis	Definición	Ejemplo
all	**All**	Este mecanismo siempre coincide. Por lo general, va al final del registro SPF.	**"v=spf1 mx -all"** Permitir que los MXes del dominio envíen correo para el dominio, prohibir todos los demás. **"v=spf1 -all"** El dominio no envía ningún correo en absoluto. **"v=spf1 +all"** El propietario del dominio cree que SPF es inútil y / o no le importa.
ip4	**ip4: <ip4-address>** **ip4: <ip4-network> / <prefix-length>**	El argumento del " ip4:" mecanismo es un rango de red IPv4. Si no se proporciona una longitud de prefijo, se asume / 32 (seleccionando una dirección de host individual).	**"v=spf1 ip4:192.168.0.1/16 -all"** Permitir cualquier dirección IP entre 192.168.0.1 y 192.168.255.255.
ip6	**ip6: <ip6-address>** **ip6: <ip6-network> /**	El argumento del " ip6:" mecanismo es un rango de red IPv6. Si no se proporciona una	**"v=spf1 ip6:1080::8:800:200C:417A/96 -all"** Permita cualquier dirección IPv6 entre 1080 :: 8: 800: 0000: 0000 y

	<prefix-length>	longitud de prefijo, se asume / 128 (se señala una dirección de host individual).	1080 :: 8: 800: FFFF: FFFF. **"v=spf1 ip6:1080::8:800:68.0.3.1/96 -all"** Permita cualquier dirección IPv6 entre 1080 :: 8: 800: 0000: 0000 y 1080 :: 8: 800: FFFF: FFFF.
a	**a / <prefix-length>** **a: <dominio>** **a: <dominio> / <prefix-length>**	odos los registros A para dominio son probados. Si la IP del cliente se encuentra entre ellos, este mecanismo coincide. Si la conexión se realiza a través de IPv6, en su lugar se realiza una búsqueda de AAAA. Si el dominio no se especifica, la corriente de dominio se utiliza. Los registros A deben coincidir exactamente con la IP del cliente, a menos que se proporcione una	**"v=spf1 a -all"** Se utiliza el dominio actual . **"v=spf1 a:example.com -all"** Equivalente si el dominio actual es example.com. **"v=spf1 a:mailers.example.com -all"** Quizás example.com haya elegido enumerar explícitamente todos los correos salientes en un registro especial A en mailers.example.com. **"v=spf1 a/24 a:offsite.example.com/24 -all"** Si example.com se resuelve en 192.0.2.1, se buscará la IP del cliente en toda la clase C de 192.0.2.0/24. Del mismo modo para offsite.example.com. Si se devolviera más de un registro A, cada uno se expandiría a una subred CIDR.

		longitud de prefijo, en cuyo caso cada dirección IP devuelta por la búsqueda A se expandirá a su correspondiente prefijo CIDR, y se buscará la IP del cliente dentro de esa subred.	
mx	**mx / <prefix-length>** **mx: <dominio>** **mx: <domain> / <prefix-length>**	odos los registros A para todos los registros MX para dominio se prueban en orden de prioridad MX. Si la IP del cliente se encuentra entre ellos, este mecanismo coincide. Si el dominio no se especifica, la corriente de dominio se utiliza. Los registros A deben coincidir exactamente con la IP del cliente, a	"**v=spf1 mx mx:deferrals.domain.com -all"** Quizás un dominio envíe correo a través de sus servidores MX más otro conjunto de servidores cuyo trabajo es reintentar el correo para diferir los dominios. **"v=spf1 mx/24 mx:offsite.domain.com/24 -all"** Tal vez los servidores MX de un dominio reciben correo en una dirección IP, pero envían correo en una dirección IP diferente pero cercana.

		menos que se proporcione una longitud de prefijo, en cuyo caso cada dirección IP devuelta por la búsqueda A se expandirá a su correspondiente prefijo CIDR, y se buscará la IP del cliente dentro de esa subred.	
ptr	**ptr** **ptr: <dominio>**	El nombre de host o los nombres de host para la IP del cliente se buscan mediante consultas PTR. Luego se validan los nombres de host: al menos uno de los registros A para un nombre de host PTR debe coincidir con la IP del cliente original. Los nombres de host no válidos se descartan. Si un	**"v=spf1 ptr -all"** Un dominio que controla directamente todas sus máquinas (a diferencia de un ISP de acceso telefónico o de banda ancha) permite que todos sus servidores envíen correo. Por ejemplo, hotmail.com o paypal.com pueden hacer esto. **"v=spf1 ptr:otherdomain.com -all"** Se designa cualquier servidor cuyo nombre de host termine en otrodominio.com.

		nombre de host válido termina en el dominio, este mecanismo coincide. Si el dominio no se especifica, la corriente de dominio se utiliza. Si es posible, debe evitar usar este mecanismo en su registro SPF, ya que resultará en un número mayor de búsquedas de DNS costosas.	
exists	**existe: <dominio>**	Realice una consulta A en el dominio proporcionado. Si se encuentra un resultado, esto constituye una coincidencia. No importa cuál sea el resultado de la búsqueda, podría ser 127.0.0.2.	En el siguiente ejemplo, la IP del cliente es 1.2.3.4 y el dominio actual es example.com. **"v=spf1 exists:example.com -all"** Si example.com no se resuelve, el resultado es un error. Si se resuelve, este mecanismo resulta en una coincidencia.

		Cuando utiliza macros con este mecanismo, puede realizar búsquedas de IP invertida de estilo RBL o configurar excepciones por usuario.	
incluye	**include:<domain>**	El dominio especificado se busca una coincidencia. Si la búsqueda no devuelve una coincidencia o un error, el procesamiento continúa con la siguiente directiva. Advertencia: si el dominio no tiene un registro SPF válido, el resultado es un error permanente. Algunos receptores de correo rechazarán basándose en un PermError.	En el siguiente ejemplo, la IP del cliente es 1.2.3.4 y el dominio actual es example.com. **"v=spf1 include:example.com -all"** Si example.com no tiene un registro SPF, el resultado es PermError. Supongamos que el registro SPF de example.com fuera **"v = spf1 a -all".** Busque el registro A para example.com. Si coincide 1.2.3.4, devuelve el Pase. Si no hay ninguna coincidencia, que no sea la " -all" del dominio incluido, la inclusión como un todo no coincide; el resultado final sigue siendo Error de la directiva externa establecida en este ejemplo.

3.2. Parámetros del DKIM.

Tabla 12. Parámetros del DKIM

Parámetro	**Descripción**
Dominio remitente	La firma DKIM se basa en el dominio de la dirección de correo electrónico del remitente. No es nada acerca de su nombre de servidor. Por ejemplo, si desea firmar el correo electrónico de *@emailarchitect.net, ingrese emailarchitect.net a Sender Domain.
Selector	Para admitir varias claves públicas simultáneas por dominio de envío, el espacio de nombres DNS se subdivide con "selectores". Los selectores son nombres arbitrarios debajo de "_domainkey". espacio de nombres. Para obtener más información, consulte la sección Selector. Para un nuevo dominio, simplemente puede usar el valor predeterminado "s1024"
Activo	Si tiene esta opción desactivada, se deshabilitará DKIM para este dominio.
Firma	El valor predeterminado es: DKIM y DomainKeys. También puede elegir "Sólo DKIM" o "Sólo claves de dominio". Ya que "DomainKeys" está obsoleto ahora y "DKIM Only" tiene un mejor rendimiento, le recomendamos que seleccione "DKIM Only".
Algoritmo de canonización	Se recomienda nofws / relajado y tiene mejor compatibilidad.
Algoritmo de firma DKIM	En Windows 2000/2003 / XP, rsa-sha1 es la única opción. En Windows Vista /

	7/2008 o versión posterior, puedes elegir "rsa-sha1" o "rsa-sha256". "rsa-sha1" ofrece un mejor rendimiento mientras que "rsa-sha256" es más seguro. Se recomienda "rsa-sha1".
Nombre del archivo de certificado / Contraseña / Tipo	Si no tiene un certificado (par de clave pública / privada) para su dominio, el administrador DKIM creará un certificado para su dominio automáticamente (recomendado); Si tiene un certificado existente, impórtelo de su disco local e ingrese su contraseña de protección del certificado. Si elige "no tiene un certificado ...", el administrador de DKIM intentará crear un certificado desde su máquina local automáticamente. Si la operación falla, el administrador DKIM descargará un certificado de nuestro servidor de forma remota. Si tiene otro servidor que usa nuestro software DKIM para firmar el mismo dominio y usa el mismo selector, debe copiar el certificado de ese servidor y usar el mismo certificado. Consulte: Implementar DomainKeys / DKIM en múltiples servidores con el mismo dominio. Si tiene otro servidor que no utiliza nuestro software DKIM para firmar el mismo

	dominio, seleccione "No tengo un certificado ..." y use un selector diferente. Para obtener más información, consulte la sección Selector. Longitud de clave de certificado Se recomienda 1024 longitud de la llave. La clave pública 2048 es demasiado larga para un solo registro TXT en el servidor DNS, el desarrollo de la clave pública es más difícil.
Encabezados firmados	Especifique qué encabezados de mensaje deben firmarse. El encabezado "remitente" y el encabezado "desde" son DEBEN. Se recomienda utilizar la configuración predeterminada.
Firma una parte del mensaje	De forma predeterminada, DKIM firma todo el cuerpo del mensaje, sin embargo, puede especificar la longitud máxima del cuerpo del mensaje a firmar. Si su servidor transmite un mensaje a través de un MTA remoto, y este MTA agrega renuncia de responsabilidad o cambia el contenido del cuerpo del correo electrónico, le sugiero que use "firmar parte del mensaje" y establezca "Longitud máxima del cuerpo del mensaje para firmar" en cero.
Longitud máxima del cuerpo del mensaje a firmar	Si la longitud se establece en cero, solo se firmarán los encabezados de los mensajes.
Firmar mensaje del sistema	De forma predeterminada, el complemento DKIM no firma el mensaje del sistema (informe de no entrega), porque se supone

	que esos mensajes se transfieren internamente. Sin embargo, si el servidor envía un mensaje del sistema a Internet, debe habilitar esta opción.
Firmar mensaje interno de MAPI	De forma predeterminada, el complemento DKIM no firma el mensaje MAPI interno para aumentar el rendimiento, buf si necesita enviar un mensaje MAPI a Internet (este no es el comportamiento predeterminado del servidor Exchange), debe habilitar esta opción.
Corregir encabezados incorrectos en el mensaje incrustado	A veces, el servicio SMTP de Exchange envuelve los encabezados doblados de los mensajes incrustados nuevamente después de que se firma la firma DKIM. Este comportamiento puede corromper el hash del cuerpo del mensaje. Habilitar esta opción puede solucionar este problema.
Ajustar la dirección de correo electrónico con <> en el encabezado del correo electrónico automáticamente.	A veces, el encabezado original del correo electrónico no envuelve la dirección de correo electrónico con <>, sin embargo, después de que se firma DKIM, algunos MTA de retransmisión pueden ajustar la dirección de correo electrónico automáticamente, este comportamiento corrompe la firma DKIM. Esta opción puede evitar el problema. No tiene que marcar esta opción (problema de rendimiento) excepto que el MTA de retransmisión corrompió la firma.
Destinatarios discapacitados	Si los destinatarios del mensaje contienen la siguiente dirección de correo electrónico, desactive la firma DKIM. Por

	favor, separe las múltiples direcciones por salto de línea. Se admite comodín (* y?)
Instalar el certificado PFX actual en el almacén de la máquina.	Esta opción instalará el certificado actual en el almacén de la máquina para obtener un mejor rendimiento. Después de instalar el certificado, asegúrese de hacer clic en "Guardar" para actualizar el cambio.

Anexo D: Script para el test de la normal y wilcoxon.

4.1 Script para la verificación de la normalidad.

El siguiente script se lo utilizo para el test de normalidad a datos recolectados durante el ataque sin mecanismos de defensa y para los datos recolectados durante el ataque con los mecanismos de defensa,

“prueba=read.table("Spoofing.txt",header=T)
prueba
shapiro.test(prueba$Ataque)
shapiro.test(prueba$Mitigacion)
boxplot(prueba$Ataque,col=c("blue"))
boxplot(prueba$Mitigacion,col=c("green"))”

4.2 Script para el test de wilcoxon.

El siguiente script se lo utilizo para el test de wilconxon para los datos durante el ataque sin mecanismos de defensa y para los datos durante el ataque con los mecanismos de defensa para de esta manera poder comprobar la hipótesis.

“prueba=read.table("Spoofing.txt",header=T)
prueba
wilcox.test(prueba$Ataque,prueba$Mitigacion)
boxplot(prueba$Ataque,prueba$Mitigacion,col=c("blue","green"))”

Anexo E: Carta de Aceptación del Manual de Implementación protocolos de defensa anti smtp-spoofing.

DIRECCIÓN ACADÉMICA
VICERRECTORADO ACADÉMICO

SGC
SISTEMA DE GESTIÓN DE LA CALIDAD

UNACH-RGF-01-04-02.14

ACTA DE ENTREGA RECEPCIÓN

MANUAL DE INSTALACIÓN DE LOS MECANISOS DE DEFENSA

En la cuidad de Riobamba, a los 11 días del mes de marzo de 2019, los señores estudiantes Alex Gabriel Auquilla Guamantaqui y Henry Daniel Espin Robles realizaron la entrega del manual de instalación de los protocolos de defensa, después de realizar el proyecto de investigación titulado: "**ANÁLISIS DE LOS MECANISMOS DE DEFENSA CONTRA EL CIBERATAQUE SMTP SPOOFING EN LA INFRAESTRUCTURA DE RED IPV4 DE LA UNIVERSIDAD NACIONAL DE CHIMBORAZO**" al Ingeniero Daniel Haro, Administrador de la red de a Universidad Nacional de Chimborazo, con el objetivo de dar constancia en la Entrega Recepción de conformidad del trabajo realizado.

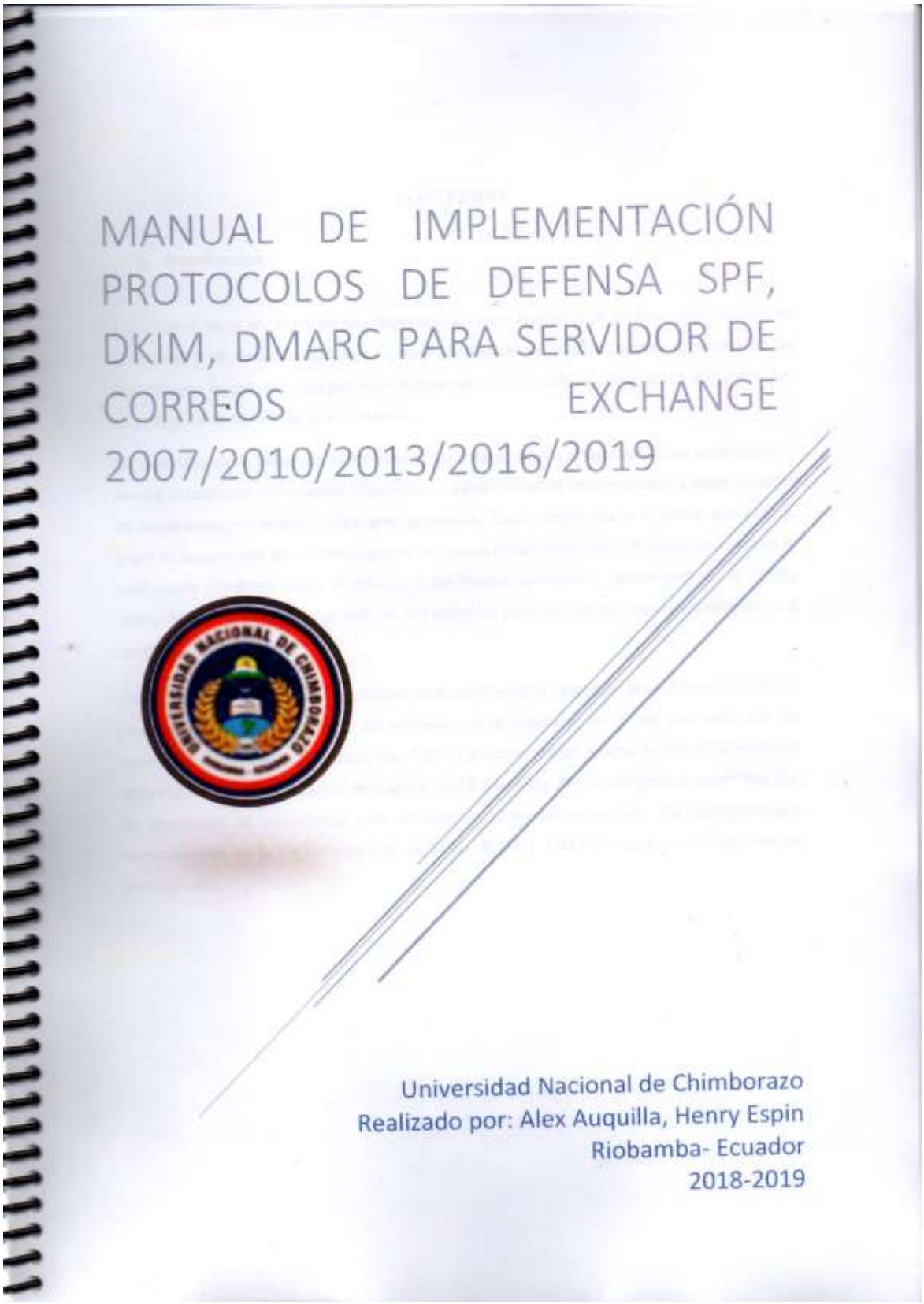
ENTREGUÉ CONFORME
Alex Auquilla

ENTREGUÉCONFORME
Henry Espin

RECIBÍ CONFRME
Ing. Daniel Haro

Anexo F: Manual

5.1. Manual de Implementación protocolos de defensa anti smtp-spoofing.



CONTENIDO

1. Introducción

La información es un activo de alta importancia en una entidad para su desarrollo continuo de la misión y el cumplimiento del objetivo de la misma, lo cual genera la necesidad de implementar mecanismos que permitan proteger la confidencialidad, integridad y disponibilidad en todo el ciclo de vida de la información.

La seguridad de la información ha tomado gran auge, debido a las cambiantes condiciones y nuevas plataformas tecnológicas disponibles. La posibilidad de interconectarse a través de redes ha traído consigo la aparición de nuevas amenazas. Estos riesgos que se enfrentan han llevado a que se implemente mecanismos que se orientan a evitar intrusiones de atacantes externos lo cual puede ocasionar serios problemas a los bienes, servicios y operaciones de la misma institución, los mecanismos de defensa son definidos partiendo de un ataque denominado smtp spoofing.

La Universidad Nacional de Chimborazo no es invulnerable a este tipo de ataques, debido a este motivo se analizó y se previno las amenazas en la seguridad de la red, por ende, con los resultados obtenidos en el ambiente simulado en donde se realizó pruebas se obtuvo un resultado muy aceptable en la mitigación de ataques SMTP Spoofing. Por lo cual, para manejar este tipo de situaciones se realizó esta guía de usuario en el que se muestra las configuraciones recomendadas en la implementación de SPF, DKIM y DMARC para mitigar los ataques mencionados.

2. Requisitos para la instalación de Exchange-Servidor de correos 2007/2010/2013/2016/2019

2.1. ¿Qué se necesita saber antes de la instalación?

- Comprobar que el servicio de Active Directory y sus complementos están correctamente instalados (Comprobar en el Administrador de Servidores).
- Compruebe que el equipo se haya asociado al dominio Active Directory interno.
- Comprobar si el sistema operativo está instalado las actualizaciones más recientes (comprobar en Windows Update).

2.2. Requisitos previos de software

- .NET Framework 4.7.2 o posterior (revizar en la página official de Microsoft)
- Instalar el paquete Redistributable de Visual C++ apra Visual Studio 2012
- Instalar el complemento Unified Communications Managed API 4.0.
- Tener instalado en el cliente Outlook 2007/2010/2013/2016/2019.

2.3. Requisitos previos de conocimientos en parámetros SPF

SPF (Sender Policy Framework) es un método usado para impedir la falsificación de la dirección de un remitente, es decir, el uso de direcciones falsas. Este permite al servidor de correo verificar que los correos procedentes de un dominio proceden de un host autorizado por el administrador de dicho dominio.

Activación o desactivación de SPF en el servidor

Cuando activa SPF para comprobar los correos entrantes, el servidor de correo efectúa una búsqueda DNS en el host del remitente para localizar algún registro DNS relacionado con SPF. Pueden definirse los siguientes grupos de reglas:

Reglas locales. - Reglas usadas por el filtro antispam antes de que el servidor de correo inicie la comprobación SPF.

Nota: estas reglas se concatenan con las reglas especificadas en el registro DNS relacionado con SPF o el remitente. Por ejemplo, si el remitente tiene la siguiente directiva SPF: **example.com. txt v=spf1 +a +mx –all** y la regla local es **a:ejemplo.com**, la directiva resultante será example.com. **txt v=spf1 +a +mx +a:ejemplo.com –all**.

Reglas de conjetura - Reglas aplicadas a los dominios que no publican registros SPF ejemplo.com. TXT v=spf1 +a +mx +a:ejemplo.com -all

Tabla 1. Parámetros SPF

Parte	Descripción
v=spf1	El dominio usa SPF de la versión 1.
+a	Todos los hosts de los registros "A" pueden enviar correos.
+mx	Todos los hosts de los registros "MX" pueden enviar correos.
+a:ejemplo.com	El dominio *ejemplo.com* puede enviar correos.
-all	Todos los demás dominios no pueden enviar correos.

2.4. Requisitos previos de conocimientos en parámetros DKIM

DKIM (DomainKeys Identified Mail) es un método usado para asociar la identidad de un nombre de dominio con un correo saliente. Asimismo, también sirve para validar la identidad de un nombre de dominio asociado con un correo entrante mediante autenticación criptográfica.

Activación o desactivación de DKIM en el servidor

Para activar la funcionalidad DKIM en su servidor, vaya a Herramientas y configuración -> Configuración del servidor de correo (en el grupo Correo) y desplácese a la sección Protección antispam DKIM. Las siguientes opciones le permiten gestionar DKIM en su servidor:

- **Permitir firmar correo saliente**. Esta opción permite a los clientes activar la firma con DKIM de los correos salientes por dominios. Tenga en cuenta que esta opción no activa la firma de todos los correos salientes de forma automática. Para poder usar DKIM, los usuarios deben activarlo para los dominios individuales.
- **Comprobar correo entrante**. Esta opción activa el análisis de todos los correos entrantes por parte de DKIM. Se analizan todos los correos y, de experimentarse algún error durante el análisis, los correos pertinentes se marcan con un encabezado especial.

Tenga en cuenta que cada una de estas opciones puede seleccionarse de forma independiente. Puede optar por habilitar la firma de correo saliente, comprobar el correo entrante o ambas.

Una vez activado DKIM para un dominio, añade los siguientes dos registros a la zona DNS del dominio:

- **default._domainkey.<ejemplo.com>** - contiene la parte pública de la clave generada.
- **_domainkey.<ejemplo.com>** - contiene la directiva DKIM.

2.5. Requisitos previos en conocimiento de las políticas DMARC

DMARC (Domain-based Message Authentication, Reporting and Conformance) es una tecnología que permite ampliar las capacidades de los métodos SPF y DKIM. La directiva DMARC define la forma en la que el receptor debería tratar los correos en función de los resultados de la comprobación DKIM y SPF.

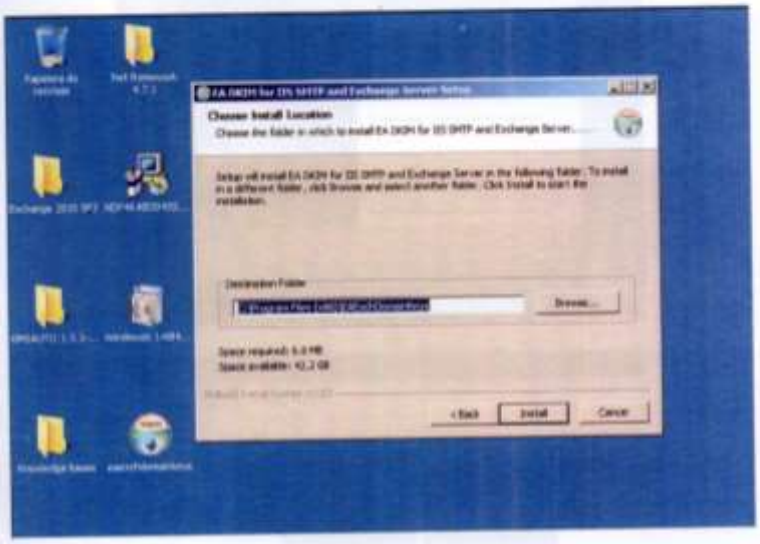
3. Implementación de mecanismos de defensa en servidor de correos Exchange.

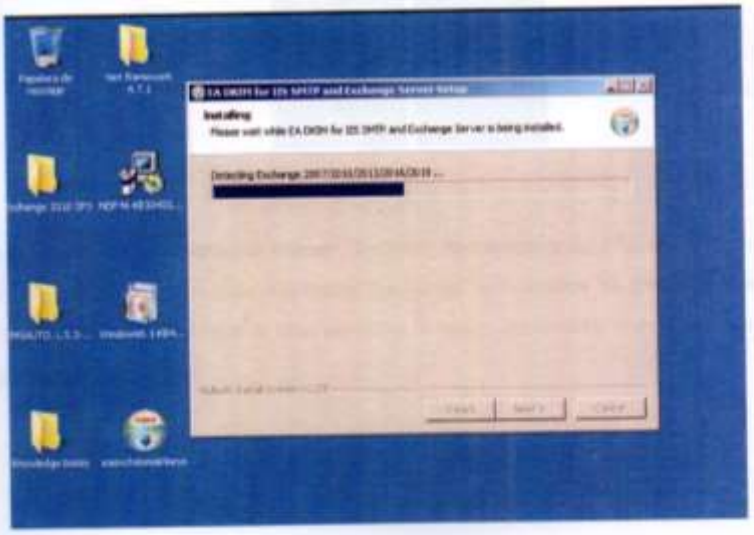
3.1. Implementación de DKIM en servidor Exchange

Para la instalación del dkim se procede a descargar el instalador desde el siguiente enlace: https://www.emailarchitect.net/webapp/download/eaexchdomainkeys.exe. Una vez descargado se procede a abrirlo. Después de ejecutarlo click en siguiente.

Se mostrará la siguiente pantalla en la cual se dará click en "*I agree*" para continuar con la instalación.

En la siguiente ventana, clic en "*Install*" sin modificar la ubicación de la instalación y esperamos que la instalación se cargue.

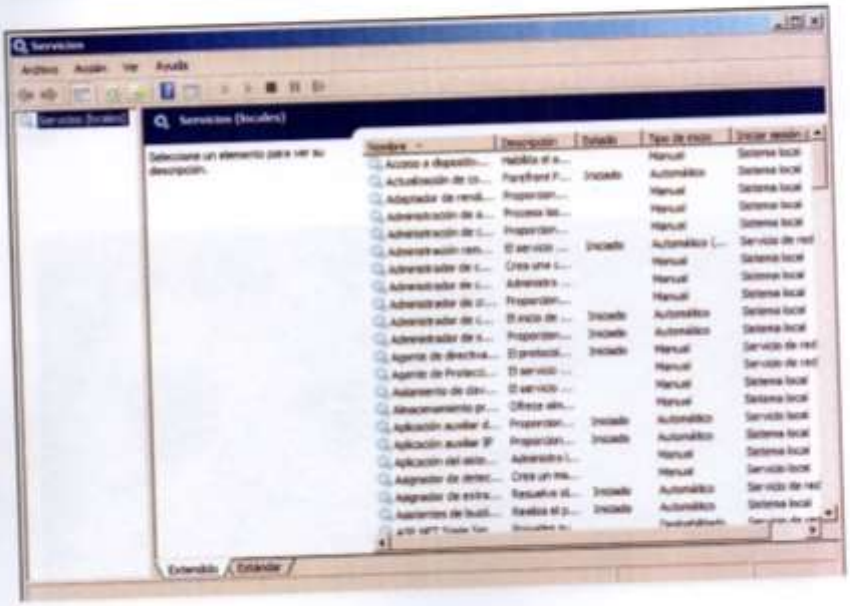




Para continuar dar clic en "Finish" para finalizar con la instalación de DKIM y se mostrará la siguiente ventana.

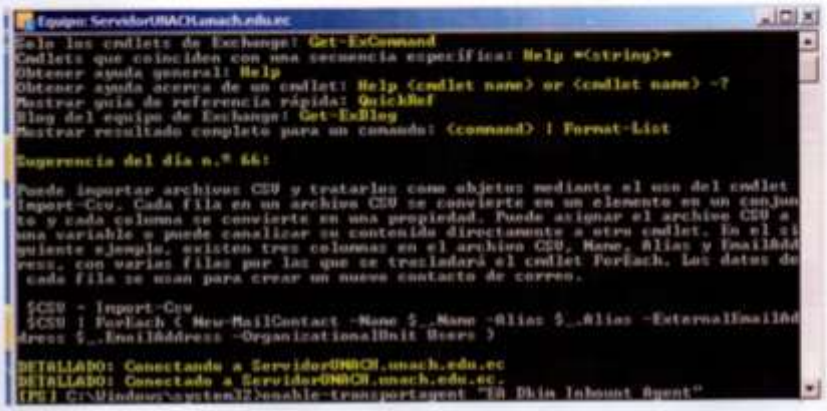
Una vez completada la instalación marcar "Servicio de transporte de Microsoft Exchange" y "Servicio de envío de correo de Microsoft Exchange" ubicándose en panel de control -> administrar servicios y verifique si esos servicios se están ejecutando, si esos servicios no se están ejecutando, inícielo.


Todos los elementos de Panel de control
Panel de control
Ajustar la configuración del equipo
Ver por:
Administración del color
Administrador de credenciales
Administrador de dispositivos
Barra de tareas y menú Inicio
Centro de accesibilidad
Centro de actividades
Centro de redes y recursos compartidos
Configuración regional y de idioma
Cuentas de usuario
Dispositivos e impresoras
Fecha y hora
Firewall de Windows
Fuentes
Herramientas administrativas
Iconos del área de notificación
Iniciador iSCSI
Mouse
Opciones de carpeta
Opciones de energía
Opciones de Internet
Pantalla
Programas predeterminados
Programas y características

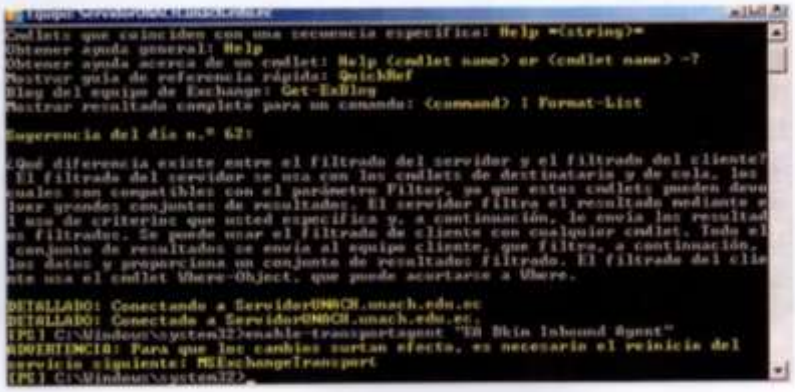

Servicios
Archivo
Acción
Ver
Ayuda
Servicios (locales)
Seleccione un elemento para ver su descripción.
Nombre
Descripción
Estado
Tipo de inicio
Iniciar sesión como
Extendido
Estándar

En la siguiente ventana se muetra como desde la Shell de Exchange se habilita el agente de transporte entrante DKIM pues, el complemento DKIM sólo habilita el agente saliente al finalizar la instalación, realizarlo manualmente.

Comando: enable-transportagent "EA Dkim Inbound Agent"



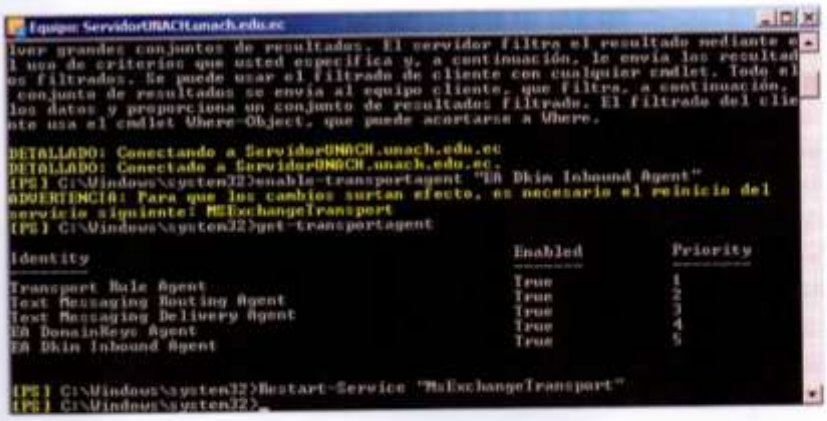
Como se muestra en la ventana siguiente notifica el sistema que es necesario reiniciar el servicio.



Verificar que el servicio se añadió y se procede a reiniciar con los comandos descritos a continuación:

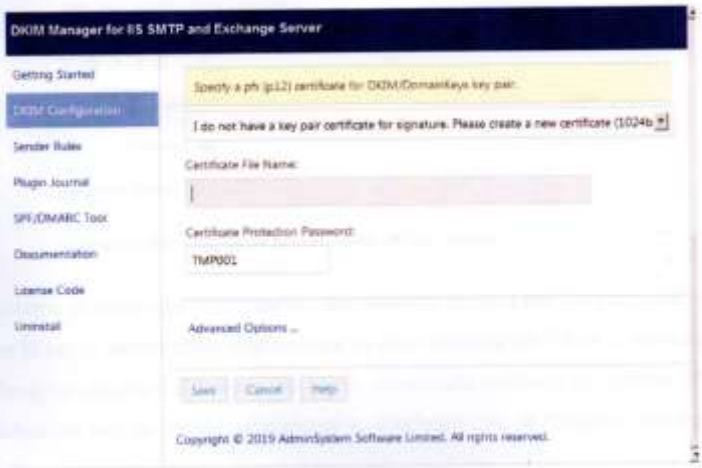
Comandos: get-transportagent

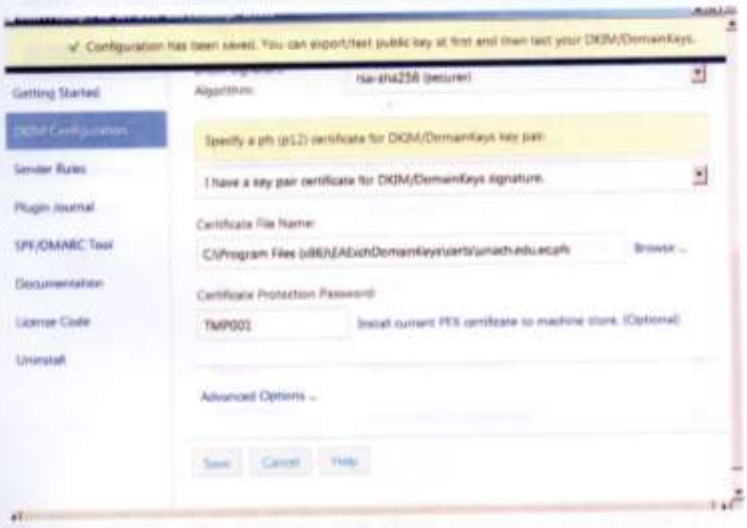
Restart-Service "MSExchangeTransport"



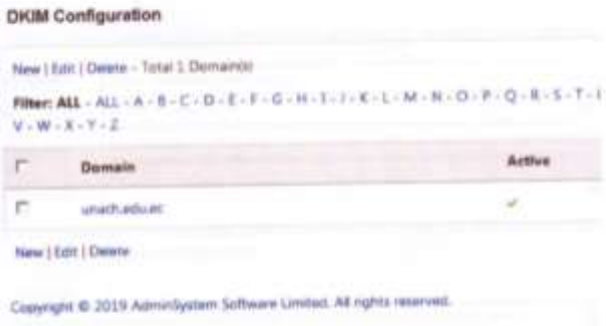
Ahora para configurar el DKIM haga clic en "DKIM Cofiguration" y crear una nueva firma DKIM de dominio. La firma DKIM se basa en el dominio de la dirección de correo electrónico del remitente. No es nada sobre el nombre del servidor.

Simplemente ingrese su dominio, use la configuración predeterminada para otros parámetros, finalmente haga clic en "Guardar" para crear su firma DKIM. En el caso que no tener debe usar el certificado emitido por autoridades de terceros, se recomienda utilizar el administrador DKIM para generar el certificado automáticamente.

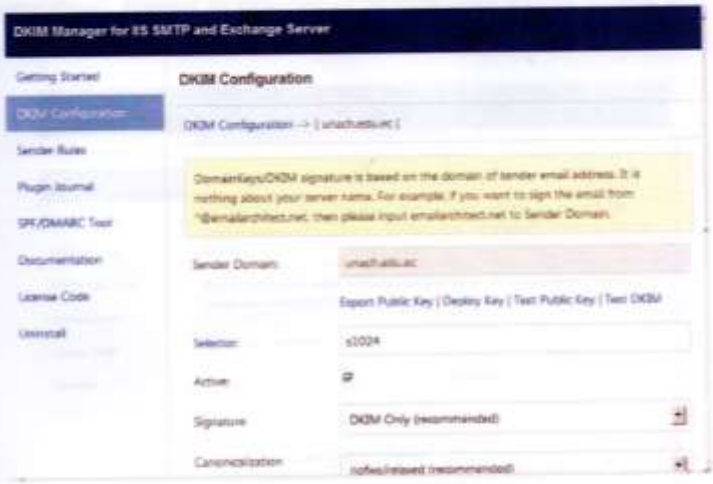




Como se muestra a continuación se ha creado la firma DKIM de dominio para el servidor. En este ejemplo el dominio es: unach.edu.ec



Ahora el sistema de correo del destinatario debe consultar la clave pública para verificar la firma DKIM. Por lo tanto, necesitamos implementar la clave pública DKIM en el servidor DNS del dominio, luego el sistema del destinatario puede consultarla mediante el servidor DNS. Ahora volver al administrador de DKIM, seleccionar su dominio y clic en "Exportar clave pública":



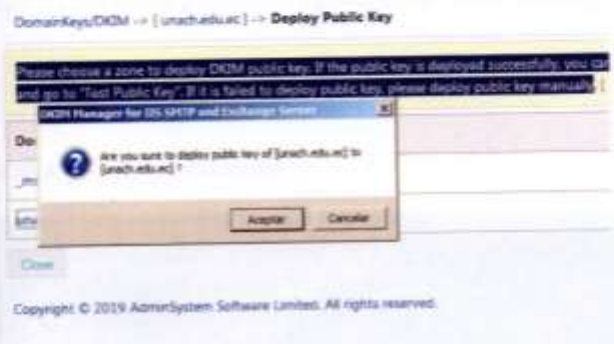
Aparecerá una ventana que mostrará una clave pública y un registro TXT para la implementación en su servidor DNS.

Si su dominio está alojado en el servidor DNS de Windows en la LAN local, después de agregar un dominio en DKIM Plugin Manager, puede seleccionar el dominio y hacer clic en

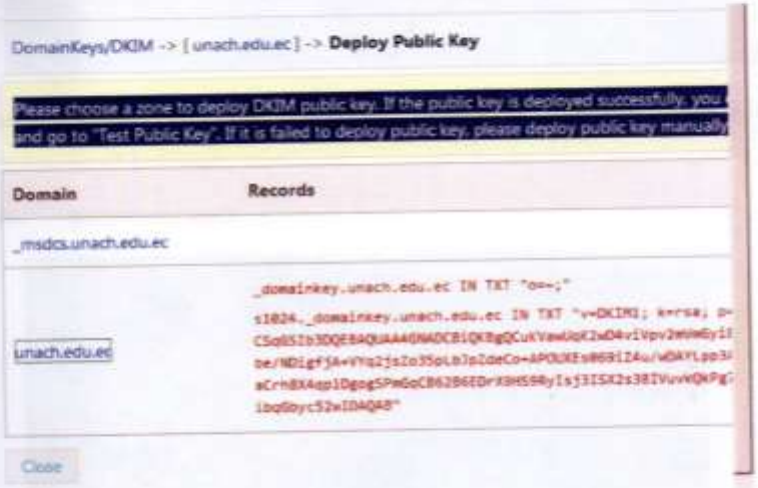
"Implementar clave", ingresar su dirección de servidor DNS y elegir la zona DNS, la clave pública se implementará en el servidor DNS automáticamente.

En la ventana siguiente se puede observar que se la clave púbica se ha añadió satisfactoriamente.

Abrir la clave publica y damos en aceptar en el cuadro de dialogo que aparecerá.



Después de realizada la implementación de la clave pública, verificarsi esta se añadió a nuestro dominio.



3.1. Comprobación de implementación DKIM

Después de añadir la clave púbica procedemos a probarla con a través del cmd.

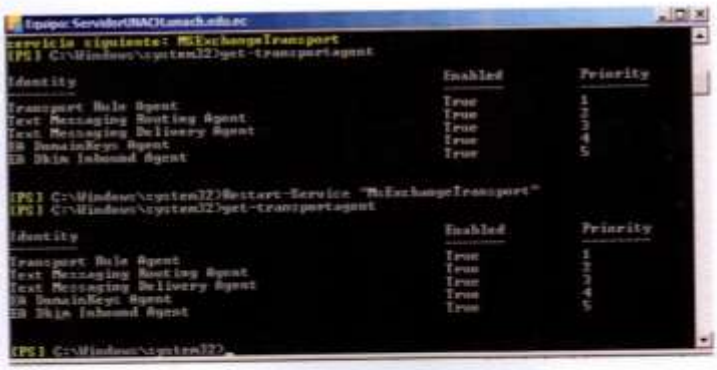
Comandos: nslookup

set type=txt

s1024._domainkey.sudominio

Verificar la instalación del agente de transporte de Exchange, esto lo haremos a través de la shell de administración de Exchange.

Comando: get-transportagent

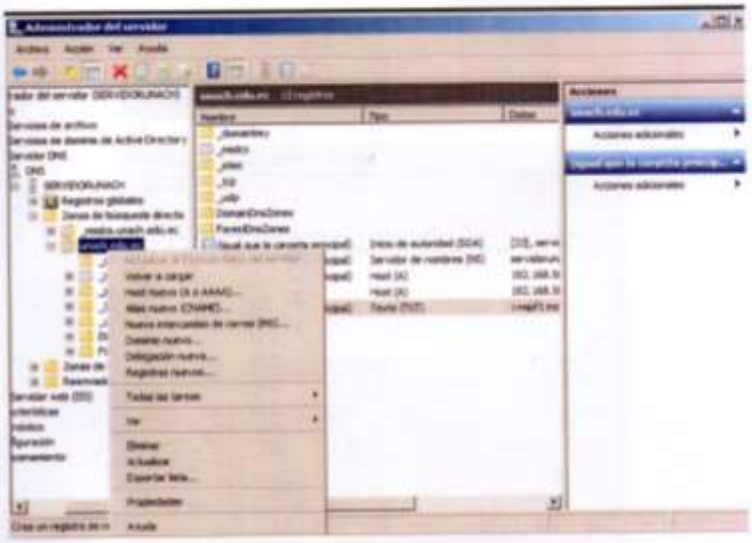


3.2. Implementación SPF

Para continuar con la configuración del SPF se deberá abrir DKIM Manager después se dirige a la opción SPF / DMARC Tool" continuando con "SPF" estado en esta opción se ingresa el dominio y hacer clic en "Inicio"

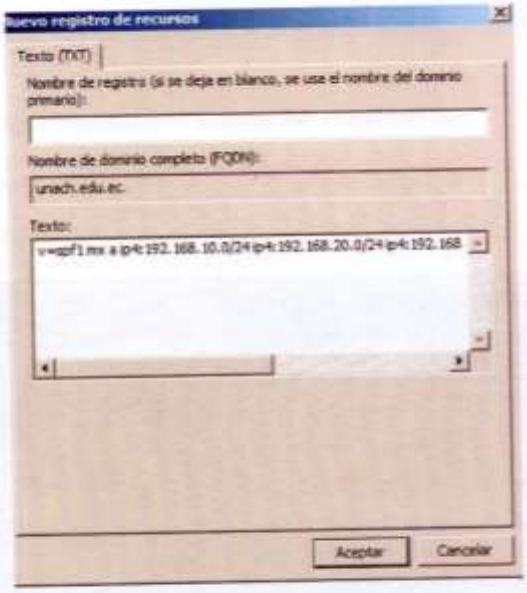
Nota: si nuestro servidor está conectado a Internet el sistema lo implementará automáticamente, caso contrario se lo debe realizar manualmente. Se recomienda implementar manualmente de acuerdo a las necesidades de cada administrador de servidor de correos.

Abrir el servidor DNS -> seleccionar el dominio al que desea agregar un registro SPF, dar clic con el botón derecho en la lista de registros y seleccione "registros nuevos" en el menú de opciones.



Seleccione el tipo de registro de texto (TXT) y elic en el botón "Crear registro".

Copie el valor (v = spf1) del valor de registro y péguelo en el cuadro de texto "texto" y no ingrese nada en "Nombre de registro". Clic en el botón Aceptar.



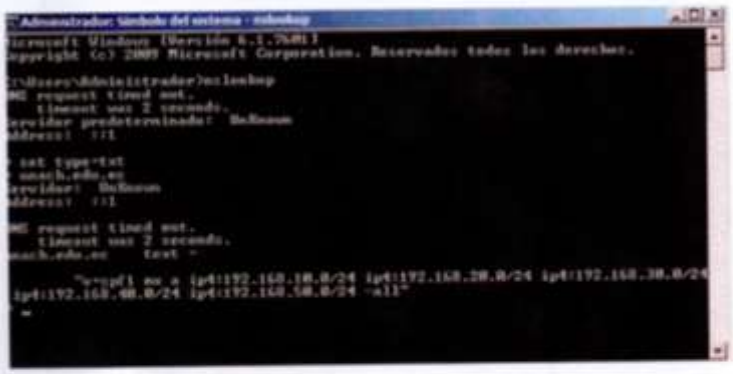
Como se puede observar el registro se ha creado satisfactoriamente.

3.2.1. Comprobación de implementación SPF

Después de añadir el registro procedemos a comprobar a través del cmd.

Comandos: nslookup

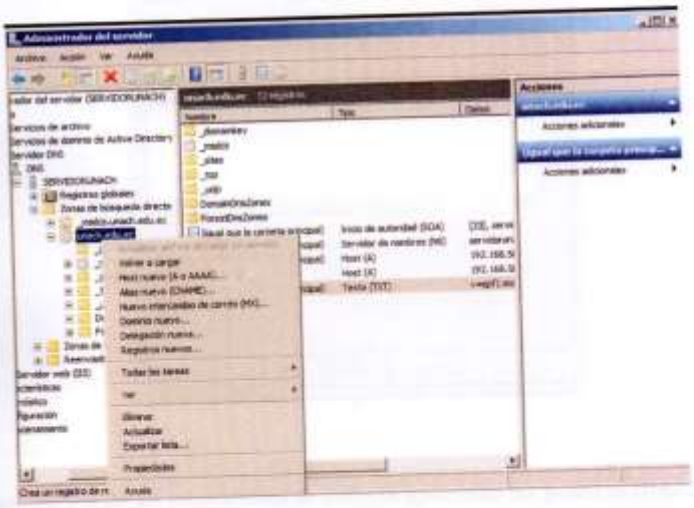
sudominio



Se observa en la imagen anterior que con satisfacción el registro SPF se ha implementado, ya que automáticamente lo reconoce.

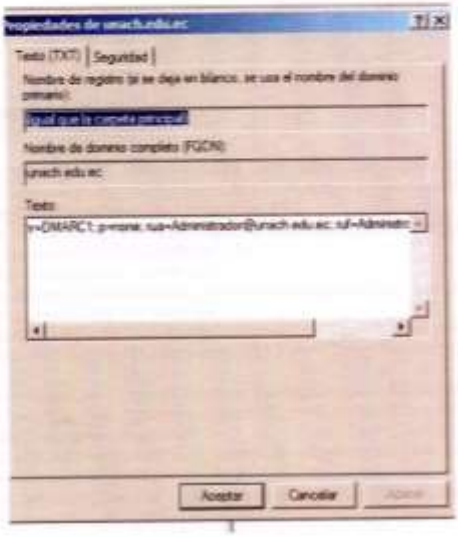
3.3. Implementación DMARC

Seleccionar y abrir en el servidor DNS y el dominio en el que se desea agregar un registro DMARC. Clic con el botón derecho en la lista de registros y seleccione "registros nuevos." en el menú de opciones.



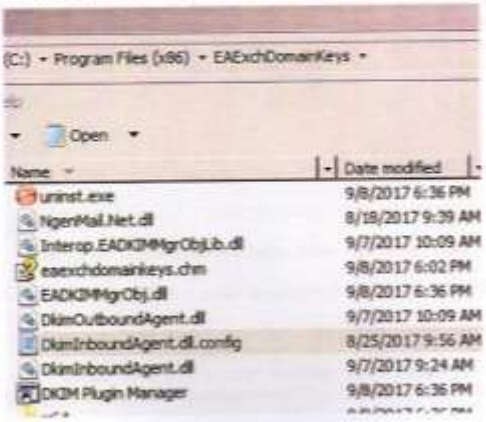
Seleccione el tipo de registro de texto (TXT) y haga clic en el botón "Crear registro".

Copie el valor (v = DMARC1) del Valor de registro y péguelo en el cuadro de texto "Texto" e ingrese "_dmarc" en Nombre de registro. Clic en el botón "Aceptar".



3.3.1. Comprobación de los mecanismos de defensa aplicando las políticas DMARC

Para la comprobación de la correcta implementación de las políticas DMARC, independientemente de cómo se haya implementado ya sea con la herramienta o manualmente. Se procede a ir al directorio raíz de instalación de EAExchDomainKeys por defecto está en:



C:\Archivos de Programa(x86)\EAExchDomainKeys.

Una vez en este directorio, abrir el archivo "*DkimInboundAgent.dll.config*" con un editor de texto. A continuación, se puede observar el contenido predeterminado del archivo de configuración:

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
<configSections>
    <section name="spfResultToReject"  type="System.Configuration.AppSettingsSection,
System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" />
    <section name="ignoredGatewayIPAddressesForSpfCheck"
type="System.Configuration.AppSettingsSection, System.Configuration, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" />
    <section name="ignoredGatewayNameForSpfCheck"
type="System.Configuration.AppSettingsSection, System.Configuration, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" />
    <section name="ignoreSpfResultDomains" type="System.Configuration.AppSettingsSection,
System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" />

    <section name="dkimResultToReject" type="System.Configuration.AppSettingsSection,
System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" />
    <section name="ignoreBodyHashErrorDomains"
type="System.Configuration.AppSettingsSection, System.Configuration, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" />
    <section name="ignoreDkimResultDomains" type="System.Configuration.AppSettingsSection,
System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" />

    <section name="dmarcResultToReject" type="System.Configuration.AppSettingsSection,
System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" />
    <section name="ignoreDmarcResultDomains" type="System.Configuration.AppSettingsSection,
System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" />

    <section name="blockedIPAddresses" type="System.Configuration.AppSettingsSection,
System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" />
    <section name="blockedSenderOrHeloDomain" type="System.Configuration.AppSettingsSection,
System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" />

    <section name="trustedIPAddresses" type="System.Configuration.AppSettingsSection,
System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" />
    <section name="trustedSenderOrDomain" type="System.Configuration.AppSettingsSection,
System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" />
</configSections>

<spfResultToReject>
    <!--
    <add key="fail" value="550 5.7.1 your message from [%source_ip%] is against our SPF
policy (fail)" />
    <add key="softfail" value="550 5.7.1 your message from [%source_ip%] is against our SPF
policy (softfail)" />
    <add key="none" value="550 5.7.1 your message from [%source_ip%] is against our SPF
policy (none)" />
    <add key="neutral" value="550 5.7.1 your message from [%source_ip%] is against our SPF
policy (neutral)" />
    <add key="temperror" value="451 4.4.3 your message from [%source_ip%] encountered a
temporal error with SPF verification (temperror)" />
    <add key="permerror" value="550 5.7.1 your message from [%source_ip%] encountered a
permanent error with SPF verification (permerror)" />
```

```
    -->
</spfResultToReject>

<!--
    ignoredGatewayIPAddressesForSpfCheck:

    If your Exchange server is behind of a gateway/MTA,
    the SPF check will be incorrect due to original IP address is hidden by gateway or MTA.

    You can add your gateway/MTA IP address to skip the gateway IP/domain to detect original
IP address/helo domain from message headers.

    CIDR syntax is supported in IP address.
    -->
<ignoredGatewayIPAddressesForSpfCheck>
    <!--
    <add key="192.168.0.8" value="ignore"/>
    -->
</ignoredGatewayIPAddressesForSpfCheck>


<!--
    ignoredGatewayNameForSpfCheck:

    If your Exchange server is behind of a gateway/MTA,
    the SPF check will be incorrect due to original IP address/helo domain is hidden by
gateway or MTA.

    You can add your gateway/MTA name to skip the gateway IP/domain to detect original IP
address/helo domain from message headers.

    You can use regular expression like this "/^emailarchitect\.(net|com)$/"

    "/^emailarchitect\.(net|com)$/" matches "emailarchitect.net" and "emailarchitect.com"

    "/.*emailarchitect\.net$/" matches "*.emailarchitect.net" and "emailarchitect.net"
    -->
<ignoredGatewayNameForSpfCheck>
    <!--
    <add key="dispatch.gateway.net" value="ignore"/>
    -->
</ignoredGatewayNameForSpfCheck>

<!--
    ignoreSpfResultDomains does not take effect to the following domains even the result
matches spfResultToReject

    You can use regular expression like this "/^emailarchitect\.(net|com)$/"

    "/^emailarchitect\.(net|com)$/" matches "emailarchitect.net" and "emailarchitect.com"

    "/.*emailarchitect\.net$/" matches "*.emailarchitect.net" and "emailarchitect.net"
    -->
<ignoreSpfResultDomains>
    <!--
    <add key="emailarchitect.net" value="ignore"/>
    -->
</ignoreSpfResultDomains>


<dkimResultToReject>
```

```
    <!--
    <add key="fail" value="550 5.7.1 your message from [%header_from%] is against our DKIM
policy (fail)" />
    <add key="none" value="550 5.7.1 your message from [%header_from%] is against our DKIM
policy (none)" />
    <add key="neutral" value="550 5.7.1 your message from [%header_from%] is against our
DKIM policy (neutral)" />
    <add key="temperror" value="451 4.4.3 your message from [%header_from%] encountered a
temporal error with DKIM verification (temperror)" />
    <add key="permerror" value="550 5.7.1 your message from [%header_from%] encountered a
permanent error with DKIM verification (permerror)" />
    -->
</dkimResultToReject>

<!--
    ignoreBodyHashErrorDomains:

    If the sender or signer domain is in the ignoreBodyHashErrorDomains list, body hash
error with DKIM verification is ignored, only the signature is verified.

    Office 365 default DKIM signature has a common body hash error problem, so you can add
/.?onmicrosoft.com$/ to bypass body hash check for office 365.

    you can use regular expression like this "/^emailarchitect\.(net|com)$/"

    "/^emailarchitect\.(net|com)$/" matches "emailarchitect.net" and "emailarchitect.com"

    "/.?emailarchitect\.net$/" matches "*.emailarchitect.net" and "emailarchitect.net"
    -->
<ignoreBodyHashErrorDomains>
    <!--
    <add key="/.?onmicrosoft.com$/" value="ignore"/>
    -->
</ignoreBodyHashErrorDomains>


<!--
    ignoreDkimResultDomains does not take effect to the following domains even the result
matches dkimResultToReject

    You can use regular expression like this "/^emailarchitect\.(net|com)$/"

    "/^emailarchitect\.(net|com)$/" matches "emailarchitect.net" and "emailarchitect.com"

    "/.?emailarchitect\.net$/" matches "*.emailarchitect.net" and "emailarchitect.net"
    -->
<ignoreDkimResultDomains>
    <!--
    <add key="emailarchitect.net" value="ignore"/>
    -->
</ignoreDkimResultDomains>


<dmarcResultToReject>
    <!--
    <add key="fail" value="550 5.7.1 your message from [%header_from%] is against our DMARC
policy (fail)" />
    <add key="none" value="550 5.7.1 your message from [%header_from%] is against our DMARC
policy (none)" />
    <add key="temperror" value="451 4.4.3 your message from [%header_from%] encountered a
temporal error with DMARC verification (temperror)" />
```

```
    <add key="permerror" value="550 5.7.1 your message from [%header_from%] encountered a
permanent error with DMARC verification (permerror)" />
    -->
</dmarcResultToReject>


<!--
    ignoreDmarcResultDomains does not take effect to the following domains even the result
matches dmarcResultToReject

    you can use regular expression like this "/^emailarchitect\.(net|com)$/"

    "/^emailarchitect\.(net|com)$/" matches "emailarchitect.net" and "emailarchitect.com"

    "/.*emailarchitect\.net$/" matches "*.emailarchitect.net" and "emailarchitect.net"
    -->
<ignoreDmarcResultDomains>
    <!--
    <add key="emailarchitect.net" value="ignore"/>
    -->
</ignoreDmarcResultDomains>


<!--
blockedIPAddresses:

The email from the following IP address(es) will be rejected directly regardless of SPF/DKIM
result.
CIDR syntax is supported in IP address.
    -->
<blockedIPAddresses>
    <!--
    <add key="127.0.0.2" value="550 5.7.1 your message from [%source_ip%] is in our black
list." />
    <add key="192.168.0.0/24" value="550 5.7.1 your message from [%source_ip%] is in our
black list." />
    -->
</blockedIPAddresses>

<!--
blockedSenderOrHeloDomain
The email from (SMTP MAIL FROM or HELO DOMAIN) the following address(es)/domain(s) will be
rejected directly regardless of SPF/DKIM result.
-->
<blockedSenderOrHeloDomain>
    <!--
        You can use regular expression like this: "/^(support|sales)@emailarchitect\.net$/"

        "/^(support|sales)@emailarchitect\.net$/" matches "support@emailarchitect.net" and
"sales@emailarchitect.net".

        "/^[^@]+@emailarchitect\.net$/" matches "*@emailarchitect.net"
    -->
    <!--
    <add key="faked-emailarchitect.net" value="550 5.7.1 your message from
[%blocked_domainOrAddress%] is in our black list." />
    <add key="spoof@faked-emailarchitect.net" value="550 5.7.1 your message from
[%blocked_domainOrAddress%] is in our black list." />
    -->
</blockedSenderOrHeloDomain>
```

```
<!--
trustedIPAddresses:

The email from the following IP address(es) will be accepted directly regardless of SPF/DKIM
result.
CIDR syntax is supported in IP address.
    -->
<trustedIPAddresses>
    <add key="127.0.0.1" value="pass"/>
    <add key="::1" value="pass"/>
    <!--
    <add key="192.168.0.0/24" value="pass"/>
    -->
</trustedIPAddresses>

<!--
trustedSenderOrDomain:

The email from (rfc822.header.from) the following address(es)/domain(s) will be accepted
directly regardless of SPF/DKIM result.
    -->
<trustedSenderOrDomain>
    <!--
        You can use regular expression like this: "/^(support|sales)@emailarchitect\.net$/"

        "/^(support|sales)@emailarchitect\.net$/" matches "support@emailarchitect.net" and
"sales@emailarchitect.net".

        "/^[^@]+@emailarchitect\.net$/" matches "*@emailarchitect.net"
    -->
    <!--
    <add key="support@emailarchitect.net" value="pass"/>
    <add key="emailarchitect.net" value="pass"/>
    -->
</trustedSenderOrDomain>

<appSettings>
    <add key ="logLevel" value="OnlyError"/>
    <!-- <add key ="logLevel" value="FullDebug"/> -->
    <add key ="trackingSender" value="*"/>
    <add key ="trackingSourceIP" value="*"/>
    <add key ="useLastExternalIPAddress" value="false"/>
    <!-- System default DNS server is used by default, you don't have to set this value
manually
    If you want to use specified DNS server address, you must input DNS server IP address.
    For example, you can use 8.8.8.8 (Google Public DNS Server) as the DNS server address.
-->
    <add key ="dnsServerAddress" value=""/>
</appSettings>
</configuration>
```

En el que se debe modificar el agente de transporte entrante, cambiar la siguiente línea:

```
<add key ="logLevel" value="OnlyError"/>
```

por:

```
<add key ="logLevel" value="FullDebug"/>
```

Rechazar correos electrónicos basado en DKIM / SPF / DMARC en el servicio SMTP

Aunque se puede usar los resultados de autenticación para filtrar el correo electrónico a la carpeta de correo no deseado, este consume recursos y almacenamiento del servidor. Por lo tanto, la mejor manera es rechazar el correo electrónico en el servicio SMTP directamente en función de los resultados de autenticación.

- Para rechazar el correo electrónico contra la política de SPF, puede cambiar la sección: spfResultToReject.
- Para rechazar el correo electrónico en contra de la política DKIM, puede cambiar la sección dkimResultToReject.
- Para rechazar el correo electrónico contra la política de DMARC, puede cambiar la sección: dmarcResultToReject.

A continuación, se observará la configuración predeterminada para rechazar correos en configuración de bajo nivel:

```
<spfResultToReject>
    <add key="fail" value="550 5.7.1 your message from [%source_ip%] is against our SPF
policy (fail)" />
    <add key="softfail" value="550 5.7.1 your message from [%source_ip%] is against our SPF
policy (softfail)" />
</spfResultToReject>

<dkimResultToReject>
    <add key="fail" value="550 5.7.1 your message from [%header_from%] is against our DKIM
policy (fail)" />
</dkimResultToReject>

<dmarcResultToReject>
  <add key="fail" value="550 5.7.1 your message from [%header_from%] is against our DMARC
policy (fail)" />
</dmarcResultToReject>
```

Configuración de nivel medio:

```
<spfResultToReject>
    <add key="fail" value="550 5.7.1 your message from [%source_ip%] is against our SPF
policy (fail)" />
    <add key="softfail" value="550 5.7.1 your message from [%source_ip%] is against our SPF
policy (softfail)" />
    <add key="none" value="550 5.7.1 your message from [%source_ip%] is against our SPF
policy (none)" />
    <add key="neutral" value="550 5.7.1 your message from [%source_ip%] is against our SPF
policy (neutral)" />
    <add key="temperror" value="451 4.4.3 your message from [%source_ip%] encountered a
temporal error with SPF verification (temperror)" />
    <add key="permerror" value="550 5.7.1 your message from [%source_ip%] encountered a
permanent error with SPF verification (permerror)" />
</spfResultToReject>

<dkimResultToReject>
    <add key="fail" value="550 5.7.1 your message from [%header_from%] is against our DKIM
policy (fail)" />
</dkimResultToReject>

<dmarcResultToReject>
  <add key="fail" value="550 5.7.1 your message from [%header_from%] is against our DMARC
policy (fail)" />
</dmarcResultToReject>
```

A continuación, se observa la configuración recomendada para el nivel más alto, ya que hay muchos servidores SMTP que no implementan la firma DKIM o el registro DMARC, esta configuración no se recomienda, ya que rechaza todos los correos electrónicos sin "spf = pass" y "dkim = pass" en el servicio SMTP.

```
<spfResultToReject>
    <add key="fail" value="550 5.7.1 your message from [%source_ip%] is against our SPF
policy (fail)" />
    <add key="softfail" value="550 5.7.1 your message from [%source_ip%] is against our SPF
policy (softfail)" />
    <add key="none" value="550 5.7.1 your message from [%source_ip%] is against our SPF
policy (none)" />
    <add key="neutral" value="550 5.7.1 your message from [%source_ip%] is against our SPF
policy (neutral)" />
    <add key="temperror" value="451 4.4.3 your message from [%source_ip%] encountered a
temporal error with SPF verification (temperror)" />
    <add key="permerror" value="550 5.7.1 your message from [%source_ip%] encountered a
permanent error with SPF verification (permerror)" />
</spfResultToReject>

<dkimResultToReject>
    <add key="fail" value="550 5.7.1 your message from [%header_from%] is against our DKIM
policy (fail)" />
    <add key="none" value="550 5.7.1 your message from [%header_from%] is against our DKIM
policy (none)" />
    <add key="neutral" value="550 5.7.1 your message from [%header_from%] is against our
DKIM policy (neutral)" />
    <add key="temperror" value="451 4.4.3 your message from [%header_from%] encountered a
temporal error with DKIM verification (temperror)" />
```

```
    <add key="permerror" value="550 5.7.1 your message from [%header_from%] encountered a
permanent error with SPF verification (permerror)" />
</dkimResultToReject>

<dmarcResultToReject>
    <add key="fail" value="550 5.7.1 your message from [%header_from%] is against our DMARC
policy (fail)" />
    <add key="none" value="550 5.7.1 your message from [%header_from%] is against our DMARC
policy (none)" />
    <add key="temperror" value="451 4.4.3 your message from [%header_from%] encountered a
temporal error with DMARC verification (temperror)" />
    <add key="permerror" value="550 5.7.1 your message from [%header_from%] encountered a
permanent error with DMARC verification (permerror)" />
</dmarcResultToReject>
```

También se puede configurar en manera de direcciones IP de confianza en el que se puede agregar direcciones IP a la sección: trustedIPAddresses, el agente de DKIM / SPF entrante no verificará el correo electrónico de esas direcciones IP. Es compatible con una sola dirección IP o sintaxis CIDR.

Por ejemplo:

```
<trustedIPAddresses>
    <add key="127.0.0.1" value="pass"/>
    <add key="192.168.0.0/24" value="pass"/>
</trustedIPAddresses>
```

Otra manera de configurar es mediante remitente o dominio de confianza en el que se puede agregar direcciones o dominios de remitentes a la sección trustedSenderOrDomain, el agente de DKIM / SPF entrante no revisará el correo electrónico de esos remitentes o dominios.

Por ejemplo:

```
<trustedSenderOrDomain>
  <!--
      You can use regular expression like this: "/^(support|sales)@emailarchitect\.net$/"

      "/^(support|sales)@emailarchitect\.net$/" matches "support@emailarchitect.net" and
"sales@emailarchitect.net".

      "/^[^@]+@emailarchitect\.net$/" matches "*@emailarchitect.net"
  -->
  <add key="support@emailarchitect.net" value="pass"/>
  <add key="emailarchitect.net" value="pass"/>
</trustedSenderOrDomain>
```

En la configuración el administrador de servidores puede bloquear direcciones mediante IP en el que puede agregar direcciones IP a la sección: blockedIPAddresses, el agente de DKIM / SPF entrante rechazará el correo electrónico de esas direcciones directamente, independientemente del resultado de SPF / DKIM. Es compatible con una sola dirección IP o sintaxis CIDR.

```
<blockedIPAddresses>
    <add key="127.0.0.2" value="550 5.7.1 your message from [%source_ip%] is in our black
list." />
</blockedIPAddresses>
```