UTMACH

UNIDAD ACADÉMICA DE INGENIERÍA CIVIL

CARRERA DE INGENIERÍA DE SISTEMAS

IMPLEMENTACIÓN DE MEDIDAS DE SEGURIDAD EN UN SERVIDOR DE CORREOS QUE MINIMICEN EL IMPACTO DE VULNERABILIDADES BASADAS EN EMAIL.

AGUIRRE VERA BRYAN VINICIO
INGENIERO DE SISTEMAS

MACHALA
2019

UTMACH

UNIDAD ACADÉMICA DE INGENIERÍA CIVIL

CARRERA DE INGENIERÍA DE SISTEMAS

IMPLEMENTACIÓN DE MEDIDAS DE SEGURIDAD EN UN SERVIDOR DE CORREOS QUE MINIMICEN EL IMPACTO DE VULNERABILIDADES BASADAS EN EMAIL.

AGUIRRE VERA BRYAN VINICIO
INGENIERO DE SISTEMAS

MACHALA
2019

UTMACH

UNIDAD ACADÉMICA DE INGENIERÍA CIVIL

CARRERA DE INGENIERÍA DE SISTEMAS

EXAMEN COMPLEXIVO

IMPLEMENTACIÓN DE MEDIDAS DE SEGURIDAD EN UN SERVIDOR DE CORREOS QUE MINIMICEN EL IMPACTO DE VULNERABILIDADES BASADAS EN EMAIL.

AGUIRRE VERA BRYAN VINICIO
INGENIERO DE SISTEMAS

MOROCHO ROMAN RODRIGO FERNANDO

MACHALA, 31 DE ENERO DE 2019

MACHALA
31 de enero de 2019

Nota de aceptación:

Quienes suscriben, en nuestra condición de evaluadores del trabajo de titulación denominado Implementación de medidas de seguridad en un servidor de correos que minimicen el impacto de vulnerabilidades basadas en email., hacemos constar que luego de haber revisado el manuscrito del precitado trabajo, consideramos que reúne las condiciones académicas para continuar con la fase de evaluación correspondiente.

MOROCHO ROMAN RODRIGO FERNANDO
0703820464
TUTOR - ESPECIALISTA 1

REDROVAN CASTILLO FAUSTO FABIAN
0702739228
ESPECIALISTA 2

RIVAS ASANZA WILMER BRAULIO
0702580192
ESPECIALISTA 3

Fecha de impresión: martes 29 de enero de 2019 - 18:26

URKUND

Urkund Analysis Result

Analysed Document:	CASO PRACTICO AGUIRRE VERA BRYAN VINICIO.docx (D47093624)
Submitted:	1/21/2019 11:57:00 PM
Submitted By:	bvaguirre_est@utmachala.edu.ec
Significance:	0 %

Sources included in the report:

Instances where selected sources appear:

0

CLÁUSULA DE CESIÓN DE DERECHO DE PUBLICACIÓN EN EL REPOSITORIO DIGITAL INSTITUCIONAL

El que suscribe, AGUIRRE VERA BRYAN VINICIO, en calidad de autor del siguiente trabajo escrito titulado Implementación de medidas de seguridad en un servidor de correos que minimicen el impacto de vulnerabilidades basadas en email., otorga a la Universidad Técnica de Machala, de forma gratuita y no exclusiva, los derechos de reproducción, distribución y comunicación pública de la obra, que constituye un trabajo de autoría propia, sobre la cual tiene potestad para otorgar los derechos contenidos en esta licencia.

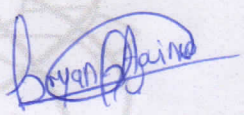
El autor declara que el contenido que se publicará es de carácter académico y se enmarca en las dispociones definidas por la Universidad Técnica de Machala.

Se autoriza a transformar la obra, únicamente cuando sea necesario, y a realizar las adaptaciones pertinentes para permitir su preservación, distribución y publicación en el Repositorio Digital Institucional de la Universidad Técnica de Machala.

El autor como garante de la autoría de la obra y en relación a la misma, declara que la universidad se encuentra libre de todo tipo de responsabilidad sobre el contenido de la obra y que asume la responsabilidad frente a cualquier reclamo o demanda por parte de terceros de manera exclusiva.

Aceptando esta licencia, se cede a la Universidad Técnica de Machala el derecho exclusivo de archivar, reproducir, convertir, comunicar y/o distribuir la obra mundialmente en formato electrónico y digital a través de su Repositorio Digital Institucional, siempre y cuando no se lo haga para obtener beneficio económico.

Machala, 31 de enero de 2019



AGUIRRE VERA BRYAN VINICIO
0704471671

DEDICATORIA

A Dios, a mis padres por ser parte fundamental para culminar mis metas y terminar con éxito mis estudios universitarios.

Sr. Bryan Vinicio Aguirre Vera.

AGRADECIMIENTO

En primer lugar, agradezco a Dios por ser mi fortaleza para cumplir con mis objetivos propuestos, por acompañarme en todo momento y brindarme sabiduría para tomar decisiones correctas. En segundo lugar, a mi familia por ser mi apoyo incondicional para seguir adelante con mis estudios. A mis docentes por brindarme el conocimiento primordial.

RESUMEN

La comunicación por email hoy en día es algo normal e importante en las empresas y hogares permitiendo al usuario el envío y recepción de información valiosa, debido a esto habrá personas mal intencionadas que se dediquen a hallar vulnerabilidades en los servidores de correo ocasionando fallas y perdidas, estos ataques basados en correos en la actualidad son diversos, en el presente documento se hablará de 4 tipos que son archivos adjuntos maliciosos (Attachment-based), suplantación de correos (email spoofing), la retransmisión de email (Open relay) y los homoglyphs. Estos ataques se originan por la falta de seguridad en el envío de emails y una mala configuración del servidor de correo. Con la ayuda de herramientas como telnet y emkei.cz se logró simular los ataques en el servidor alojado en Digital Ocean con su dominio pruebabryan.com para posteriormente aplicar los controles. La solución se basa en implementar políticas en la parte del cliente para evitar ataques por medio de virus, en la parte del servidor se configuro algunas herramientas como son SPF (Sender politicy framwork) convenio de remitentes y en la configuración de los archivos main y master de postfix aplicando parámetros TLS para evitar la retransmisión de correo.

Palabras claves: Email spoofing, Open relay, homoglyphs, SMTP, IMAP/POP.

ABSTRACT

The communication by email today is something normal and important in companies and homes allowing the user to send and receive valuable information, due to this there will be malicious people who are dedicated to finding vulnerabilities in the mail servers causing failures and losses , these attacks based on emails are currently diverse, in this document we will talk about 4 types that are attachment-based, email spoofing, open relay and homoglyphs. These attacks originate from the lack of security in the sending of emails and a bad configuration of the mail server. With the help of tools such as telnet and emkei.cz it was possible to simulate the attacks on the server hosted in Digital Ocean with its domain pruebabryan.com to subsequently apply the controls. The solution is based on implementing policies on the part of the client to avoid attacks by means of viruses, in the part of the server some tools are configured such as SPF (Sender politicy framwork) and in the configuration of main and master files of postfix applying TLS parameters to prevent mail relaying.

Key words: Email spoofing, Open relay, homoglyphs, SMTP, IMAP/POP.

CONTENIDO

INDICE DE ILUSTRACIONES

1. INTRODUCCIÓN

Con el crecimiento de las telecomunicaciones el email se ha convertido en un medio importante de comunicación en la sociedad, negocios y en la educación, permitiendo estar siempre en contacto y compartiendo información; así mismo al estar siempre en línea los peligros aumentan debido a la gran cantidad de datos que se manejan. [1]

En el presente informe, se detallará 4 ataques basados en correo electrónico como son:

- attachment-based (archivos adjuntos)
- email spoofing (suplantación de correos)
- an open relay (retransmisión de correo abierto)
- homoglyphs (caracteres de texto que tiene similitudes).

El attachment-based hace referencia a archivos adjuntos maliciosos que suelen ser documentos u hojas de cálculos, al hacer clic el malware infecta a nuestro ordenador y posteriormente propagarse por nuestra red.

Email spoofing es cuando una persona envía un correo donde el remitente es falso, de tal manera podría decirse que el correo lo ha enviado algún conocido o cualquier empresa [2].

La retransmisión de correo a veces llamado relay inseguro es cuando un servidor de correo SMTP permite la retransmisión de correos de terceros, permitiendo enrutar grandes volúmenes de correo no deseado. En cuanto a los homoglyphs es un carácter de texto con formas similares entre sí, permitiendo la realización de ataques como el phishing.

Capítulo 1: En este capítulo se detalla la introducción, su marco contextual en donde se indica y justifica el problema, además de los objetivos que se desean lograr con el documento.

Capítulo 2: En esta parte del capítulo se especifica el marco teórico donde existe toda la fundamentación teórica para lograr la solución del problema y así mismo, se detalla los resultados obtenidos.

Capítulo 3: Por último, en esta parte de documento se redactan las conclusiones que es una muestra del cumplimiento de los objetivos del documento.

1.1. Marco contextual

Mantener una infraestructura requiere implementar controles que apoyen con la seguridad para enviar información. SMTP es el protocolo para la transferencia simple de correo permitiendo el envío de email en internet, este se asocia junto con otros como el pop3 o el imap. Estos protocolos no garantizan que los datos sean entregados a su destino, debido a que pueden ser vulnerables a ataques.

Entre los ataques que puede sufrir un servidor de correos tenemos, la incrustación de archivos maliciosos, suplantación de email, retransmisión de correos y los caracteres de texto similares entre sí.

1.2. Problema

¿Examinar los ataques basados en correo permitirá tomar mejores decisiones en la implementación de un servidor de correos con un menor impacto, cuando estos ataques se realicen?

1.3. Objetivo general

Implementar medidas de seguridad en un servidor de correos mediante la aplicación de controles para minimizar el impacto de vulnerabilidades basadas en email.

2. DESARROLLO

2.1. Marco teórico

2.1.1. SMTP

SMTP es un protocolo de transferencia de correo electrónico utilizado para retransmitir mensajes electrónicos entre servidores. Es una tecnología que permite utilizar mecanismos para el almacenamiento y reenvió de email. Una gran cantidad de agentes de transferencia de correo implementan SMTP. [3] [4]

2.1.2. IMAP

El protocolo imap (internet message Access protocol) hace referencia a la posibilidad de administrar los correos directamente desde el servidor, es decir los emails que recibas no se descargarán en tu dispositivo final, sino que recibes una lista de tus mensajes y sus correspondientes asuntos, además de crear tu carpeta en el servidor y organizar tus mensajes allí. [5]

2.1.3. Attachment-based

Los archivos adjuntos maliciosos consisten en la propagación de virus por medio de un ejecutable o documento, permitiendo al atacante realizar diversos tipos de ataques como el phishing, implantación de ransomware, etc. [6]

2.1.4. Email spoofing

Email spoofing es una técnica que permite falsificar la fuente de correo electrónico de tal manera que parezca el correo haber venido de otra fuente, normalmente es usado para ataques de phishing con el fin de ganarse la confianza de que proviene de un servidor legítimo y hacer que abra el documento malicioso. [7] [8]

2.1.5. Open Relay

Esta técnica conocida como retransmisión de correo o insegura, hace referencia al servidor de correo electrónico SMTP que retransmite los emails de terceros, se usaban para mejorar la transferencia entre sistemas de correos electrónicos cerrados, pero esto los atacantes están explotando para enviar spam y hacer phishing sin ser notados. [9]

2.1.6. Homoglyphs

Es un carácter que tiene una apariencia similar al original, permitiendo realizar ataques como phishing engañando a los usuarios. Esta técnica crea nombre de dominios que son visualmente similares a los legítimos o reconocidos. [10] [11]

2.1.7. Thunderbird

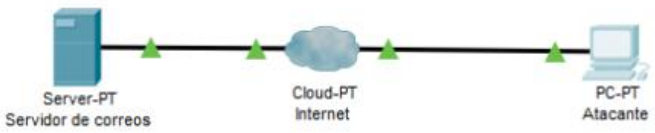
Es una aplicación de código abierto para el manejo de correos electrónico, donde se manejan filtros de correos, además soporta protocolos imap/pop, correo html, noticias, rss. [12]

2.2. Solución del problema

2.2.1. Diseño e implementación del escenario.

Para el desarrollo del esquema en donde se realizarán los ataques se implementó un entorno en un VPS (Servidores privados virtuales) para alojar un servidor con su respectiva interfaz, así mismo para las pruebas se virtualizo una maquina en virtualbox como muestra la ilustración 1.

Ilustración 1 Servidor de correo



***Fuente**: Elaboración propia*

El servidor de correo tiene una interfaz WAN (IP pública) que brinda el VPS de DigitalOcean donde se aloja un servidor de correo con ip 68.183.167.162 que apunta a un servidor de nombre de dominios en este caso pruebabryan.com. En la maquina víctima se instalará Windows 7 como sistema operativo.

2.2.2. Exploración de las vulnerabilidades basadas en email.

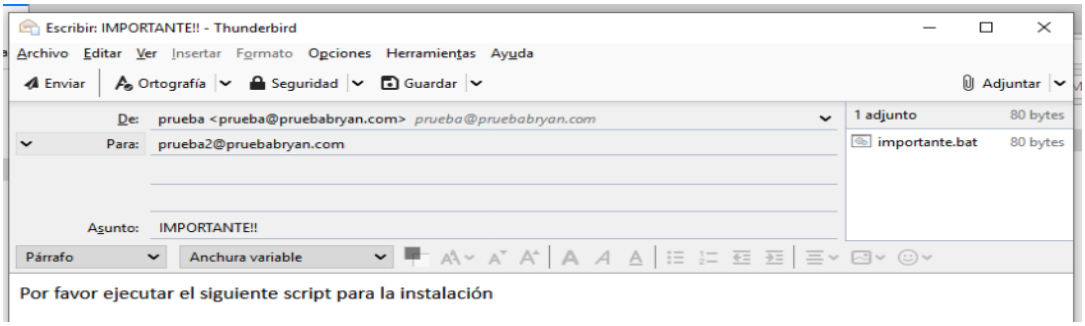
Para la realización de los ataques se necesitó de diversas herramientas como son un archivo .dat para la creación de un virus para el ataque de contenido malicioso en archivos comerciales, la siguiente página https://emkei.cz/*Kk* para la suplantación de correo malicioso, la herramienta telnet, para verificar si un servidor de correo es open relay; por último se creara un página web con url ww2.pruebabryan.com, donde se reemplazara con www.pruebabryan.com caracterizando los homoglyphs.

Los ataques se efectuarán de la siguiente forma:

2.2.2.1. Attachment-based.

Para realizar este tipo de ataque se necesita un archivo infectado en este caso se crea uno que le muestre un mensaje y posterior a eso se apagó la computadora (Ver Anexo A).

Ilustración 2 attachment-based



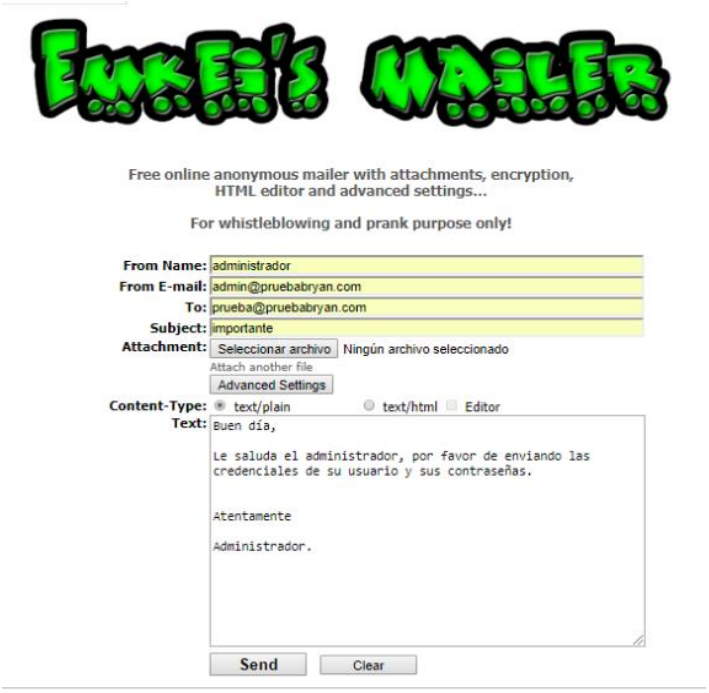
Fuente: Elaboración propia

Como se puede observar en la ilustración 2 se envía un archivo adjunto que le mostrará el siguiente mensaje al usuario “Su equipo se apagará en 1 minuto” y posteriormente se apagará su computadora.

2.2.2.2. Email Spoofing.

Para la realización de este ataque (Ver anexo B) se necesitó de una página llamada emkei.cz que permite realizar suplantación de email.

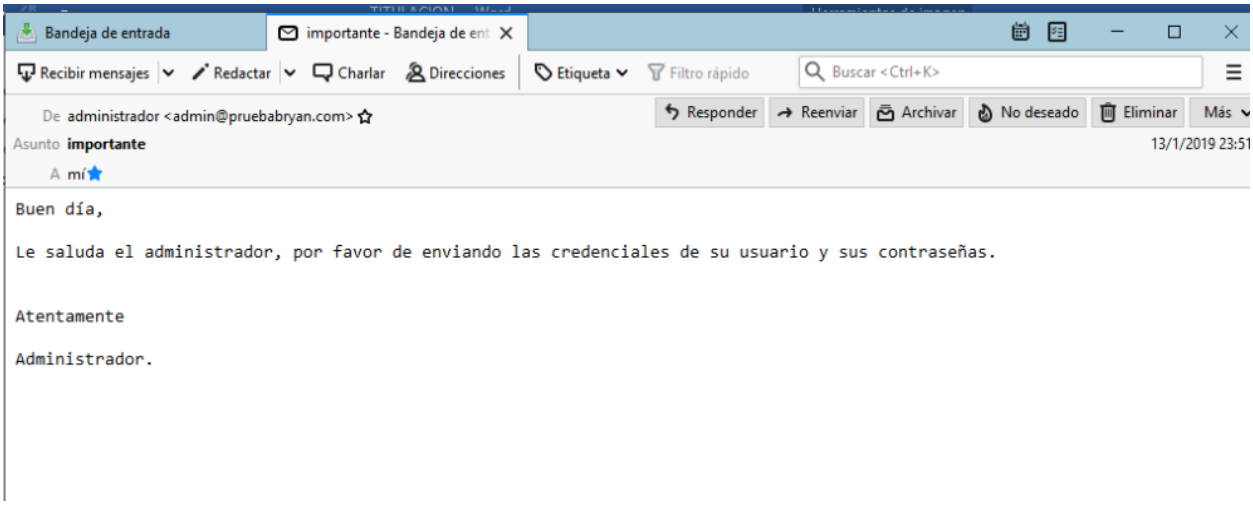
Ilustración 3 Email Spoofing



Fuente: emkei.cz

En la ilustración 2 se puede observar como se va a realizar el ataque, donde from name es la persona a quien se va a suplantar, from email es el email falso, to es el destinatario, por último, el subject y lo que se va a enviar de texto.

Ilustración 4 ataque email spoofing



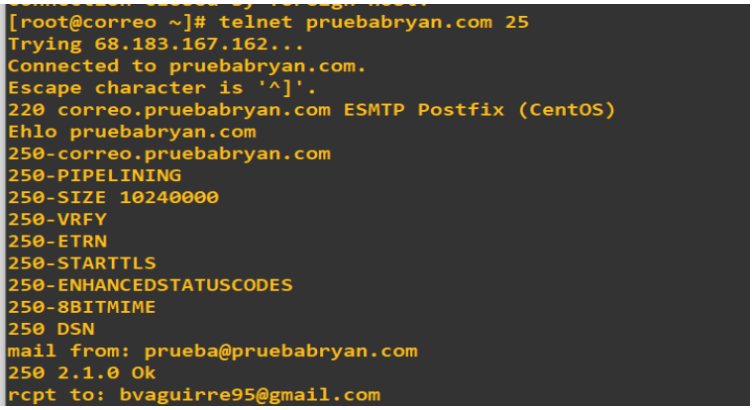
Fuente: Elaboración propia

La ilustración 3 se puede observar que ha llegado el correo a mi buzón de entrada, verificando que el ataque basado en spoofing se ha logrado.

2.2.2.3. Open Relay

Para la realización de este ataque se necesitó la ayuda de la herramienta telnet donde se ejecutará el siguiente comando: telnet pruebabryan.com 25.

Ilustración 5 ataque open relay



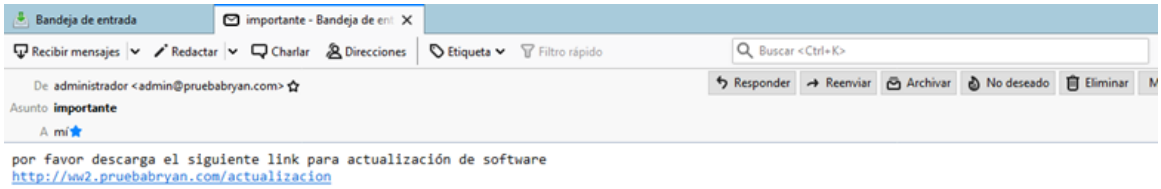
Fuente: Elaboración propia

Como se muestra en la figura 5 se puede ingresar al servidor mediante telnet en donde se ejecutarán los comandos necesarios para el envió de un email.

2.2.2.4. Homoglyphs

Homoglyphs hace referencia al cambio de caracteres que sean similares a su original, en la actualidad existen diversas herramientas para generar caracteres similares. En este caso usaremos la siguiente dirección ww2.pruebabryan.com/actualizacion en vez de la original www.pruebabryan.com.

Ilustración 6 homoglyphs



Fuente: Elaboración propia

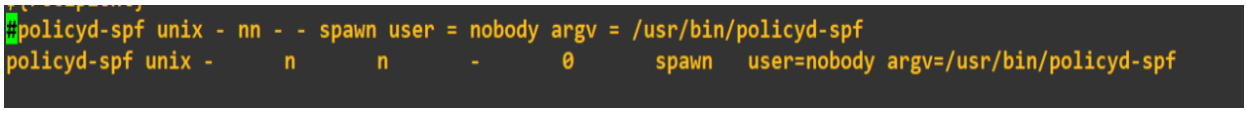
2.2.3. Implementación de controles.

Para evitar el attachment-based y homoglyphs, se deben establecer políticas de seguridad, como:

- La implementación de antivirus
- Capacitar a los usuarios sobre los diferentes tipos de amenazas que se presentan al ejecutar un archivo desconocido.
- Revisar las extensiones de los archivos.
- Validar si la página es legítima
- Validar que la conexión de esa página sea segura.

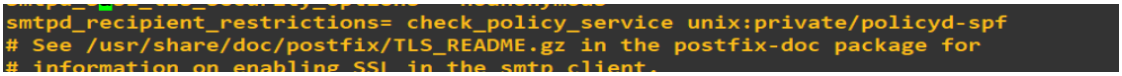
Para el caso de email spoofing se implementó SPF en la configuración del servidor de correos electrónicos (Ver Anexo C), evitando la suplantación de email.

Ilustración 7 Configuración archivo master.cf



Fuente: Elaboración propia

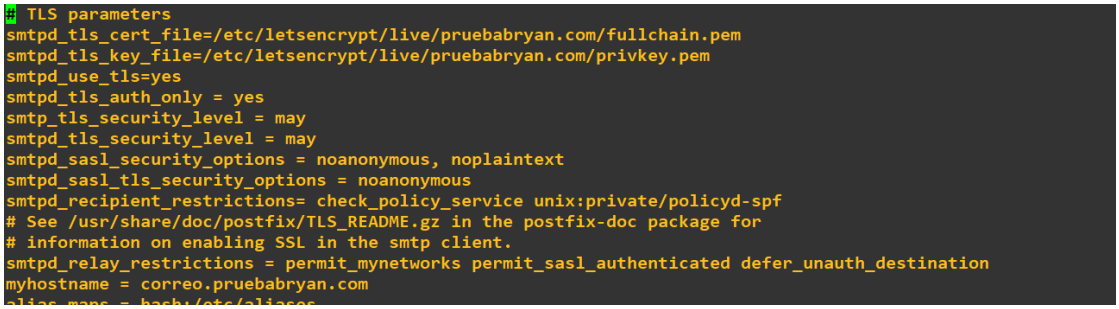
Ilustración 8 Configuración en el archivo main.cf



Fuente: Elaboración propia

Por último, para evitar el open relay se debe configurar el archivo main.cf para denegar el acceso a usuarios que quieran enviar correos desde nuestro servidor.

Ilustración 9 control de open relay



Fuente: Elaboración propia

En la ilustración 9 se muestra la configuración del archivo main.cf de postfix, en donde se configura los parámetros TLS y smtpd_relay_restrictions para que solo envié correos mediante un usuario local y con autentificación.

2.3. Resultados

Mediante la investigación de las vulnerabilidades basadas en email, se pudo comprobar los errores que se comenten al implementar un servidor de correos por medio de

ataques de suplantación de emails, enviando archivos maliciosos, la retransmisión de correos y los homoglyphs, permitiendo efectuar controles a nivel cliente con la capacitación de los usuarios, ejecución de antivirus, asegurarse de usar paginas seguras; en cuanto al servidor configurando SPF (Sender policy framework) convenio de remitentes, evitando la falsificación de direcciones en el envío de correos electrónicos y configurando reglas para evitar el open relay.

3. CONCLUSIONES

- Se implementó un sistema de validación de correo (SPF) en un servidor de correos, para de esta manera evitar que los spammers envíen correos electrónicos no autorizados desde un determinado dominio.
- Se logró impedir el aprovechamiento de vulnerabilidades basadas en email, mediante la aplicación de controles y con ello combatir a la suplantación de correos electrónicos.
- La configuración de un servidor SMTP posibilita que desde Internet cualquier usuario lo utilice para enviar correos electrónicos a través de él.
- Es de vital importancia tomar precauciones en los correos electrónicos, ya que con frecuencia utilizan un mensaje de email para enviar archivos con contenido malicioso.

BIBLIOGRAFÍA

[1] P. Rajendran, M. Janaki, S. M. Hemalatha y B. Durkananthini, «Adaptive privacy policy prediction for email spam filtering,» de *2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave)*, Coimbatore, India, 2016.

[2] T. Fowdur y L. Veerasoo, «An email application with active spoof monitoring and control,» de *2016 International Conference on Computer Communication and Informatics (ICCCI)*, Coimbatore, India, 2016.

[3] K. Okokpujie, E. Noma-Osaghae, S. John y R. Oputa, «Development of a facial recognition system with email identification message relay mechanism,» de *2017 International Conference on Computing Networking and Informatics (ICCNI)*, Lagos, 2017.

[4] S. Bal y S. K. Deb, «Shared parameters with symmetric key in E-MAIL security,» de *2015 International Conference and Workshop on Computing and Communication (IEMCON)*, Vancouver, BC, Canada, 2015.

[5] W. Z. Khan, M. K. Khan, F. T. B. Muhaya, M. Y. Aalsalem y H.-C. Chao, «A Comprehensive Study of Email Spam Botnet Detection,» *IEEE Communications Surveys & Tutorials,* vol. 17, nº 4, pp. 2271-2295, 2015.

[6] P. S. Rompas y R. S. Perdana, «Securing Confidential Documents in Local Network Using an Email Filtering Technique,» de *2018 International Workshop on Big Data and Information Security (IWBIS)*, Jakarta, 2018.

[7] R. P. Iyer, P. K. Atrey, G. Varshney y M. Misra, «Email spoofing detection using volatile memory forensics,» de *2017 IEEE Conference on Communications and Network Security (CNS)*, Las Vegas, NV, USA, 2017.

[8] A. Jayan y S. Dija, «Detection of spoofed mails,» de *2015 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)*, Madurai, India, 2015.

[9] D. L. Msongaleli y K. Kucuk, «Electronic mail forensic algorithm for crime investigation and dispute settlement,» de *2018 6th International Symposium on Digital Forensic and Security (ISDFS)*, Antalya, Turkey, 2018.

[10] A. Ginsberg y C. Yu, «Rapid Homoglyph Prediction and Detection,» de *2018 1st International Conference on Data Intelligence and Security (ICDIS)*, South Padre Island, TX, USA, 2018.

[11] J. Woodbridge, H. S. Anderson, A. Ahuja y D. Grant, «Detecting Homoglyph Attacks with a Siamese Neural Network,» de *2018 IEEE Security and Privacy Workshops (SPW)*, San Francisco, CA, USA, 2018.

[12] J. C. S. Santos, A. Peruma, M. Mirakhorli, M. Galstery, J. V. Vidal y A. Sejfia, «Understanding Software Vulnerabilities Related to Architectural Security Tactics: An Empirical Investigation of Chromium, PHP and Thunderbird,» de *2017 IEEE International Conference on Software Architecture (ICSA)*, Gothenburg, Sweden, 2017.

ANEXOS

En el anexo A se puede observar el código que se empleará para la creación del virus.

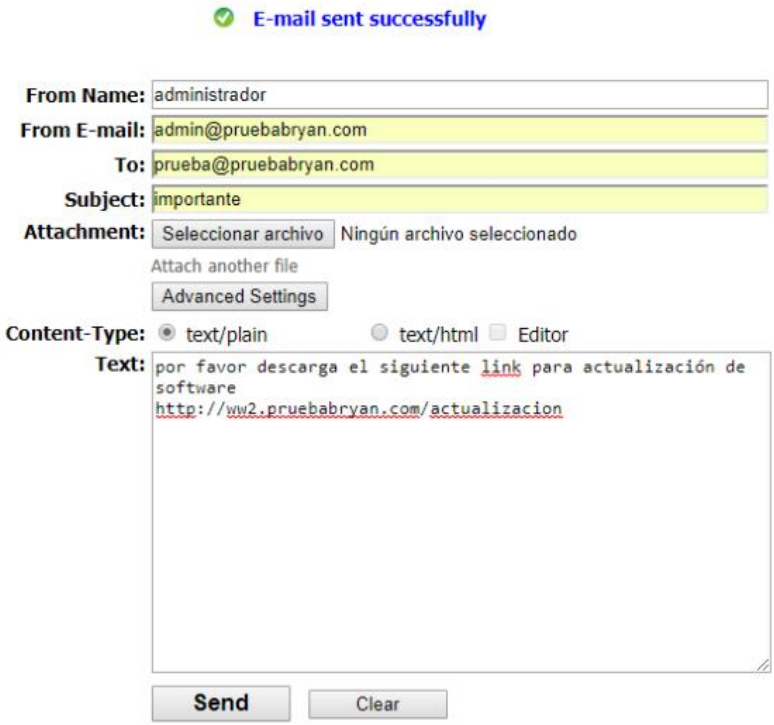
Ilustración 10 Código del virus (Anexo A)

Fuente: *Elaboración propia*

En el anexo B se muestra la ejecución de ataque de suplantación de correo. Que consta de los siguientes campos:

- From Name: Es el nombre de quien envía el mensaje en este caso administrador.
- From email: Es la persona que envía el mensaje, es decir el correo que se va a suplantar.
- To: Persona que va dirigida el mensaje
- Text: Es el cuerpo del mensaje

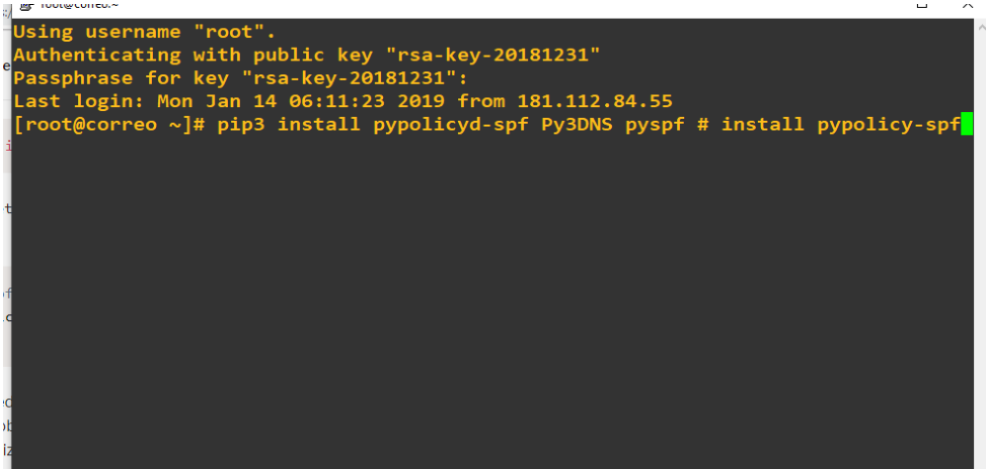
Ilustración 11 Anexo B. Configuración para email spoofing



Fuente: Elaboración propia

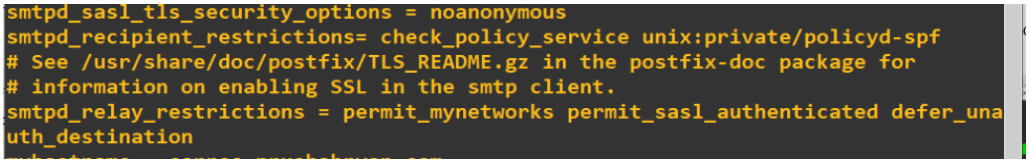
Para el anexo C para evitar el email spoofing se implementó SPF, a continuación, se muestra la instalación y configuración de este control.

Ilustración 12 Anexo C instalación de spf



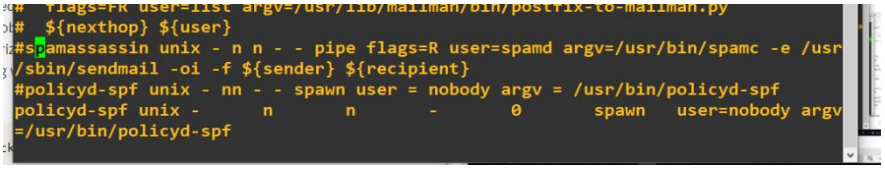
Fuente: Elaboración propia

Ilustración 13 Configuración de main.cf



Fuente: Elaboración propia

Ilustración 14 Configuración de master.cf



Fuente: Elaboración propia