ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

MODELO DE SEGURIDAD CONTRA ATAQUES DE DENEGACIÓN DE SERVICIO (Dos) DE TRÁFICO SIP EN SERVICIOS VOIP PARA REDES LAN CORPORATIVAS.

JUANA KARINA ARELLANO AUCANCELA

Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo, presentado ante el Instituto de Posgrado y Educación Continua de la ESPOCH, como requisito parcial para la obtención del grado de MAGÍSTER EN SEGURIDAD TELEMÁTICA.

RIOBAMBA - ECUADOR
Marzo - 2017

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

CERTIFICACIÓN:

El Tribunal del PROYECTO DE INVESTIGACIÓN CERTIFICA QUE:

El proyecto de investigación titulado "MODELO DE SEGURIDAD CONTRA ATAQUES DE DENEGACIÓN DE SERVICIO (Dos) DE TRÁFICO SIP EN SERVICIOS VOIP PARA REDES LAN CORPORATIVAS", de responsabilidad de la Ing. Juana Karina Arellano Aucancela, ha sido prolijamente revisado y se autoriza su presentación.

Tribunal:

Ing. Oswaldo Geovanny Martínez Guashima, M. Sc. **PRESIDENTE**	**FIRMA**
Ing. Diego Fernando Ávila Pesántez., M.Sc. **DIRECTOR**	**FIRMA**
Ing. Luis Marcelo Donoso Velasteguí., M. Sc. **MIEMBRO**	**FIRMA**
Ing. Edwin Fernando Mejía Peñafiel., M. Sc. **MIEMBRO**	**FIRMA**

Riobamba, 2017

DERECHOS INTELECTUALES

Yo, Juana Karina Arellano Aucancela, declaro que soy responsable de las ideas, doctrinas y resultados expuestos en el **Trabajo de Investigación modalidad Proyectos de Investigación y Desarrollo,** y que el patrimonio intelectual generado por la misma pertenece exclusivamente a la Escuela Superior Politécnica de Chimborazo.

_____
Juana Karina Arellano Aucancela
No. Cédula: 060426593-4

DECLARACIÓN DE AUTENTICIDAD

Yo, Juana Karina Arellano Aucancela, declaro que el presente **Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo**, es de mi autoría y que los resultados del mismo son auténticos y originales. Los textos constantes en el documento que provienen de otra fuente están debidamente citados y referenciados.

Como autora, asumo la responsabilidad legal y académica de los contenidos de este proyecto de investigación de maestría.

Riobamba, Marzo de 2017

_____

Juana Karina Arellano Aucancela
No. Cédula: 060426593-4

DEDICATORIA

A mi Señor, Jesús, quien me dio la fe, la fortaleza, la salud y la esperanza para culminar este trabajo. A mis padres, José Alberto y María Teresa quienes me enseñaron desde siempre a luchar para alcanzar mis metas y sobre todo por siempre, siempre creer en mí. A mis hermanos/as, quienes supieron brindarme su comprensión y cariño el cual me ha ayudado e impulsado a seguir adelante constantemente. Al ser que con su amor, comprensión, paciencia y apoyo estuvo presente en cada momento de esta etapa motivándome con cada palabra, el complemento de mi alegría, Paúl. A mi pequeño amor José Martín.

Juana Karina

AGRADECIMIENTO

Agradezco infinitamente a Dios por guiarme en el cumplimiento de mis metas y anhelos, sin su bendición esto no hubiera sido posible. Al Ingeniero Diego Ávila P. por su confianza, sus apreciados y relevantes aportes, críticas, y sugerencias y sobre todo por su gran apoyo en la ejecución de este trabajo. A los Miembros del Tribunal del Trabajo de Titulación por su tiempo, y acertada orientación en el desarrollo de este trabajo. Muchas Gracias.

A mi familia y amigos, por su apoyo en los momentos justos y sobre todo por vuestra compañía incondicional.

Juana Karina

CONTENIDO

INDICE DE TABLAS

INDICE DE FIGURAS

INDICE DE GRAFICOS

RESUMEN

En la presente investigación se implementó un Modelo de Seguridad contra ataques de denegación de servicio (DoS) para tráfico de protocolo de inicio de sesión (SIP) en redes de voz sobre IP (VoIP). Se analizaron las principales vulnerabilidades y amenazas encontradas comúnmente en ambientes VoIP. Para la construcción del Modelo planteado, se analizó la Metodología OSSTMM 2.1 y técnicas de recopilación del hacking, se consideró algunas recomendaciones de estándares y normas de seguridad en ambientes VoIP. El Modelo de Seguridad MS-DoS-SIP, está enfocado en ataques de DoS para tráfico SIP, se divide en cuatro etapas que son: a) Reconocer la red VoIP, b) Identificar Vulnerabilidades SIP y Valorar su Impacto en la Disponibilidad, c) Examinar la Seguridad de la Red VoIP y d) Aplicar las medidas de seguridad. Mediante la implementación del Modelo de Seguridad MS-DoS-SIP, en un ambiente de red VoIP simulado se logró minimizar en un 92% las vulnerabilidades en relación del mismo escenario sin mecanismos de seguridad implementados. Se concluyó que al reducir notablemente las vulnerabilidades se consiguió incrementar la disponibilidad del servicio. Es recomendable el uso de un sistema de correlación de eventos en las redes de VoIP y las futuras recomendaciones de seguridad en SIP.

PALABRAS CLAVE: <TECNOLOGÍA Y CIENCIAS DE LA INGENIERÍA>, <INFORMÁTICA>, <SEGURIDAD INFORMÁTICA>, <PROTOCOLO DE INICIO DE SESIÓN (SIP)>, <DENEGACIÓN DE SERVICIOS (DoS)>, <VULNERABILIDADES>, <MODELO DE SEGURIDAD>, <ATAQUES DE DENEGACIÓN DE SERVICIOS>.

ABSTRACT

In this investigation, a Security Model against Denial of Service attacks (DoS) for the Session Initiation Protocol (SIP) in voice network over IP (VoIP) was implemented. The main vulnerabilities and threats commonly found in VoIP environments were analyzed. For the construction of the proposed model, we analyze the Open Source Security Testing Methodology Manual (OSSTMM) 2.1 and hacking techniques. We consider some recommendations of safety standards and norms in VoIP environments. a) Recognize VoIP network, b) Identify SIP Vulnerabilities and assess their Impact on Availability, c) Examine VoIP Network Security, d) Implement security measures. Through the implementation of the MS-DoS-SIP Security Model, in a simulated VoIP network environment, it was possible ti minimize the vulnerabilities in the relation of the same scenario without security mechanisms implemented by 92%. It was recommended to use an event correlation system in VoIP networks and future SIP security recommendations.

KEYWORDS: <ENGINEERING TECHNOLOGY AND SCIENCES>, <COMPUTER SCIENCE>, <COMPUTER SECURITY>, <SESSION INITIATION PROTOCOL (SIP)>, <DENIAL OF SERVICES (DoS)>, <VULNERABILITIES>, <SECURITY MODEL>, <DENIAL OF SERVICES ATTACKS>.

CAPITULO I

1. MARCO REFERENCIAL

1. 1. Introducción

Las amenazas de seguridad en redes de Voz sobre IP (VoIP) actualmente son una preocupación importante y latente ya que cada día se desarrollan nuevos ataques que afectan directamente al protocolo SIP, puesto que es uno de protocolos dominantes de señalización en servicios de VoIP, sin embargo, presenta importantes vulnerabilidades como la inundación basada en el ataque de denegación de servicios, la misma que se ha identificado como la principal amenaza para el protocolo SIP. A pesar de que se han desarrollado investigaciones para asegurar el servicio de VoIP y mitigar ataques de denegación de servicio (Jouravlev, 2008), (Martin & Hung, 2005),(Shan & Jiang, 2009), sólo una pequeña proporción ha sido específica para el protocolo de señalización SIP (Rehman & Abbasi, 2014), (Rafique, Akbar, & Farooq, 2009), (Lee, Cho, Lee, & Kim, 2014).

Actualmente, es imprescindible que las redes corporativas VoIP cuenten con un modelo de seguridad que permitan proteger y salvaguardar la información, conservando la confidencialidad, disponibilidad e integridad del servicio de VoIP, partiendo de que un Modelo de Seguridad es un conjunto de medidas preventivas y correctivas. Algunos de los modelos estándar en la implementación de redes VoIP, son: ISO/IEC 27002, NIST, UIT-T Series X, entre otras que veremos más adelante.

El propósito fundamental de este proyecto de investigación busca determinar las medidas de protección que permitan contrarrestar las amenazas, vulnerabilidades y riesgos de los ataques de DoS en la tecnología de voz sobre IP (VoIP) basada en el protocolo de Inicio de Sesión (SIP), y posterior elaborar un modelo de seguridad en base a políticas, normas y procedimientos de seguridad, orientado a las organizaciones que utilizan una plataforma de telefonía IP basada SIP, con el propósito de concientizar a los administradores o encargados del área informática a

precautelar sus servicios de VoIP, para en lo posible mitigar este tipo de amenazas y sus efectos negativos que causan en los sistemas.

1. 2. Planteamiento del problema

1. 2. 1 *Situación problemática*

En la actualidad el tema de las comunicaciones se ha convertido en un medio necesario para el progreso de las organizaciones, tal es el caso de la voz sobre IP (VoIP), una tecnología que se hace cada vez más popular, ya que permite la integración de voz y datos por medio de la convergencia e interconexión de las redes clásicas de telecomunicaciones y las redes IP. Sin embargo a medida que crece su popularidad, también aumenta la posibilidad de que la tecnología VoIP sea más vulnerable respecto a la seguridad y la calidad de servicio.

Las organizaciones pueden ser vulnerables a diversos ataques, tales como: denegación del servicio, robo de información confidencial, usurpación de identidad, interceptación de conversaciones, redirección y secuestro de llamadas y en general a todas aquellas amenazas a las que sea susceptible la red de datos. Las amenazas siempre han existido, la diferencia es que ahora el atacante es más rápido, más difícil de detectar y mucho más audaz. Es por esto, que toda organización debe estar en alerta y saber implementar mecanismos de seguridad para evitar o minimizar las consecuencias no deseadas.

Es así que la seguridad informática se ha convertido ineludiblemente en una necesidad; ya que los atacantes informáticos buscan aprovecharse de la mínima o nula robustez de seguridad de las tecnologías IP; para de esta manera afectar negativamente a cualquier organización sin mucho esfuerzo o conocimiento técnico. Hoy en día los mecanismos de seguridad en redes VoIP no son considerados importantes, ya que se tiene la falsa concepción de que son gastos innecesarios y procesos complejos; y por consecuencia se implementan servidores de VoIP muy inseguros y vulnerables ante los ataques, provocando que las organizaciones experimenten pérdidas como resultado de los ataques a las redes de datos. Pueden ser atacados todos los elementos que integran la infraestructura de VoIP, como dispositivos de la red de datos, servidores, sistemas operativos y protocolos usados, etc.

Es por eso que los modelos de seguridad son de vital importancia ya que ayudan al administrador de la red a mantener la continuidad de los servicios, y es urgente que todas las organizaciones que hacen uso del servicio de VoIP cuenten con la ejecución de un modelo de seguridad.

1. 2. 2 *Formulación del problema*

¿El modelo de seguridad planteado permitirá reducir las vulnerabilidades en tráfico SIP ante ataques de DoS aumentando la disponibilidad del servicio de VoIP en redes LAN Corporativas?

1. 2. 3 *Preguntas directrices o específicas de la investigación*

- Cuáles son los ataques más comunes de Denegación de Servicio en Voz sobre IP basados en SIP?
- Cuáles son las consecuencias de un ataque de DoS al servicio de VoIP?
- Que impacto produce la disminución o perdida de disponibilidad de servicio de VoIP en una organización?
- Qué contramedidas se usan para mitigar los ataques de Denegación de Servicio en comunicaciones SIP?

1. 3. Justificación de la investigación

La voz sobre IP (VoIP) ofrece varias ventajas, pero también introduce amenazas de seguridad. Hoy en día el protocolo SIP es usado como un estándar de señalización para la tecnología VoIP. (Rehman & Abbasi, 2014) revela que la mayoría de los ataques a la arquitectura VoIP tienen éxito debido a la debilidad de SIP. Es así que los sistemas de VoIP basados en SIP son altamente vulnerables ante ataques de Denegación de Servicio (DoS), y es una de las amenazas más alarmantes. Un ataque DoS intenta hacer que un nodo de red no esté disponible, inundándolo de paquetes ilegítimos, usurpando su ancho de banda y/o sobrecargando sus recursos. Las amenazas de denegación de servicio son intentos maliciosos para degradar o inhabilitar el funcionamiento del sistema, afectando la ***disponibilidad*** del mismo.

Generalmente los ataques de DoS, se basan en inundaciones o Flooding mediante el envío masivo de mensajes legítimos, mensajes ilegítimos, mensajes con formato incorrecto o mensajes falsos, con el objetivo de consumir todos sus recursos o un protocolo específico con el fin de saturar las peticiones. Estos comúnmente atacan a la memoria, CPU y ancho de banda del servidor que contiene el servicio de VoIP. Los ataques de Dos basados en inundaciones son la mayor amenaza a la que se enfrenta un servicio de VoIP. (Deng, 2008)

Debido a que esta investigación se enfoca en ataques de Denegación de Servicio en sistemas de VoIP basado en SIP, serán objeto de estudio los ataques específicos de SIP, para ello se realizará un testeo de seguridad en sistemas VoIP frente a ataques basados en Flooding y Fuzzing, como: INVITE Flood to Proxy, INVITE Flood to Phones, Malformación en mensajes INVITE, Eliminación de Registro de Usuarios SIP, y sus contramedidas para mitigarlos. Debido a que SIP puede también hacer uso de TCP, se estudiará el ataque común en este protocolo, SYN flood.

Los ataques SIP Flooding se producen cuando los teléfonos IP generan peticiones o respuestas para enviar a un UA específico, llamado víctima. Como resultado, un solo UA está ocupado por la recepción de excesivos mensajes SIP dentro de un corto período de tiempo, por lo que la UA no puede proporcionar los servicios normales. Un taque INVITE Flood es uno de los ataques más típicos. El caso de INVITE Flood, podría ser el ataque más molesto para el usuario de VoIP ya que deberá atender muchas solicitudes de llamadas.

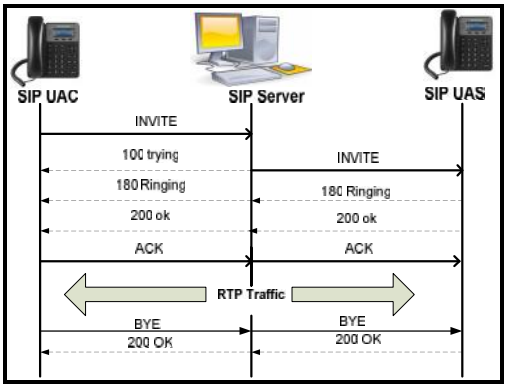


Figura 1-1: Modelo de llamada SIP
Fuente: (Rafique et al., 2009)

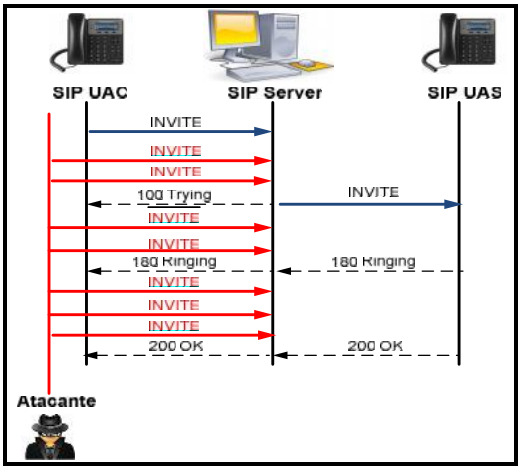


Figura 2-1: Ataque INVITE Flood
Fuente:(Rafique et al., 2009)

El objetivo de **InviteFlood**, es el de enviar masivamente peticiones INVITE a un servidor con el fin de colapsarlo. El servidor tratará de atender a todas las llamas generadas consumiendo una gran cantidad de recursos.

Hoy en día muchos de los administradores de redes, han dejado en segundo plano el tema de la seguridad, por eso se torna urgente e importante que toda organización cuente con un Modelo de Seguridad, es decir que cuenten con un conjunto de estándares, normas, políticas y procedimientos que permita resguardar los servicios frente a cualquier amenaza, falla y/o daño, con esta premisa el presente trabajo de investigación busca brindar una herramienta a los administradores mediante el desarrollo de un Modelo de Seguridad que integra las mejores prácticas y recomendaciones de seguridad en específicamente en redes VoIP en una sola guía a de fácil entendimiento para el personal relacionado con seguridad en redes IP; debido a que no se ha encontrado algún tipo de recurso que detalle un modelo genérico completo y mucho menos seguro que permita que un administrador pueda documentarse para el diseño, implementación, configuración, y puesta en marcha de una red segura de VoIP basado específicamente en el protocolo SIP.

El desarrollo de esta investigación, a más de contribuir con las líneas de investigación de la Escuela Superior Politécnica de Chimborazo, brinda la posibilidad de elaborar una propuesta que permita conocer diversas formas de hacer más segura la telefonía IP, ofreciéndole mayor confianza a las organizaciones que manejan esta tecnología, y una alternativa distinta de comunicación a las que aún no la poseen.

1. 4. Objetivo general de investigación

- Implementar un Modelo de Seguridad contra ataques de Denegación de Servicio de tráfico SIP en servicios VoIP, para redes LAN corporativas que permitan disminuir las vulnerabilidades e incrementar la disponibilidad del servicio de VoIP.

1. 5. Objetivos específicos de investigación

- Determinar los ataques de DoS en sistemas VoIP basados en SIP, de mayor impacto en la disponibilidad para establecer su patrón de comportamiento.
- Diseñar el Modelo de Seguridad que permita mitigar ataques de DoS basados en SIP, y resguardar la disponibilidad del servicio de VoIP.
- Establecer un escenario de pruebas para la puesta en marcha de los ataques de DoS identificados y seleccionados.
- Aplicar el Modelo de Seguridad que permita mitigar ataques de DoS en tráfico SIP, e incrementar el tiempo de la disponibilidad del servicio de VoIP en un ambiente organizacional.

1. 6. Planteamiento de la hipótesis

Con el Modelo de Seguridad para mitigar ataques de Denegación de Servicio en tráfico SIP en servicios VoIP, se conseguirá reducir la vulnerabilidad ante ataques de DoS incrementando la disponibilidad del servicio de VoIP en redes LAN Corporativas.

CAPITULO II

2. MARCO TEÓRICO

2.1. Antecedentes del problema

La Voz sobre Protocolo de Internet (VoIP), es un protocolo de la capa de aplicación que proporciona una alternativa barata frente a la red telefónica pública (PSTN). El término VoIP se utiliza para definir la telefonía por Internet que envía los datos de voz y multimedia. VoIP es popular debido a su flexibilidad, fiabilidad y de bajo coste. (Rehman & Abbasi, 2014). Las amenazas de seguridad son consideradas mínimas en las redes de conmutación de circuitos actuales. Montar un ataque a un servidor de telefonía es muy simple. Esto se debe a que los servicios de voz sobre IP (VoIP) se basan en estándares y tecnologías abiertas como SIP, H.323, entre otras. (Sisalem, Kuthan, Ehlert, & others, 2006)

(Ormazabal, Nagpal, Yardeni, & Schulzrinne, 2008) muestran diversas vulnerabilidades SIP que pueden dar lugar a ataques de denegación de servicio. En el trabajo de (Keromytis, 2010), se define que la principal causa de ataques a la tecnología VoIP, se debe a las vulnerabilidades del protocolo de señalización SIP. El Protocolo de Iniciación de Sesión (SIP) es un protocolo de capa de aplicación basada en TCP/IP diseñado para ser independiente de la capa de transporte, está diseñado para establecer o terminar una sesión entre dos usuarios. (Sun, Mkwawa, Jammeh, & Ifeachor, 2013). SIP está establecido como el estándar de facto para los servicios de VoIP y las redes de próxima generación. (Sisalem et al., 2006). SIP crea un gran número de oportunidades potenciales para los ataques de denegación de servicio ya que las entidades SIP se abren al Internet público con el fin de recibir solicitudes de hosts IP en todo el mundo. (Chen, 2006)

Los ataques de Denegación de Servicio (DoS) son intentos explícitos para deshabilitar un objetivo, evitando así a los usuarios legítimos hacer uso de sus servicios. Los ataques de denegación siguen siendo la principal amenaza que enfrentan los operadores de red.(Ormazabal, Nagpal, Yardeni, & Schulzrinne, 2008). (Keromytis, 2012), identifica dos áreas específicas: la denegación de servicio y el abuso de servicios, que han sido escasamente investigadas en

relación a su importancia en el estudio de las vulnerabilidades, por otra parte, identifica los errores de ejecución y errores de configuración como dos áreas problemáticas generales que merecen mucho más análisis, determinando así que los diversos tipos de ataques de ***denegación de servicio*** constituyen la mayor parte de las vulnerabilidades en servicios de VoIP, y determina que más del 90% de vulnerabilidades se deben a problemas de aplicación y el 7% a la mala configuración.

Para mitigar esta tendencia de malicia informática, se han realizado diferentes trabajos de investigación local denominados ***"Análisis de Vulnerabilidades en Protocolos utilizados en Centrales VoIP con Ipv6 utilizando troncales SIP"*** (Cáceres Guayanlema, 2014), y ***"Protección de tráfico SIP en redes de telefonía IP a través del Análisis de Técnicas de Seguridad en Redes Corporativas"*** (Chapalbay Santillán, 2012), estos trabajos han permitido inmiscuirse en el tema de seguridad en sistemas VoIP, sin embargo no se están enfocados en ataques de Denegación de Servicio y técnicas de mitigación.

Además, estudios como el artículo científico "***Secure SIP: A Scalable Prevention Mechanism for DoS Attacks on SIP Based VoIP Systems"*** (Ormazabal et al., 2008)**,** en donde los autores realizan un estudio de funcionalidad y rendimiento de los sistemas de prevención de DoS mediante una herramienta en el que se incluye los tipos de ataque basado en tráfico SIP falso, y presenta los resultados experimentales, esto lo hacen mediante la implementación de un servidor de Firewall con varias reglas basadas en SIP, capaz de detectar y mitigar los ataques de denegación de servicio (DoS) basados en SIP a nivel de señalización. El servidor Firewall filtra el tráfico SIP contra los ataques de spoofing; y request, response y floods.

Para complementar se cita el trabajo de investigación denominado "***Mitigating Denial-of-Service Attacks on VoIP Environment"***(Jouravlev, 2008)**,** en donde los autores analizan las principales amenazas de DoS en entorno de VoIP que las empresas pueden experimentar, así como las mejores contramedidas que se pueden utilizar para prevenir y hacer del entorno de VoIP más seguro. Finalmente, se analizó la investigación ***"A Comprehensive Survey of Voice over IP Security Research"*** (Keromytis, 2012), presenta un estudio exhaustivo de seguridad de Voz sobre IP, utilizando un conjunto de 245 publicaciones de investigación académica sobre el tema, los clasifica de acuerdo con una versión extendida de la Alianza de Seguridad de VoIP (VOIPSA) según la taxonomía de amenazas, con el objetivo es proporcionar una hoja de ruta para los investigadores que buscan entender las capacidades existentes y para identificar las deficiencias en el tratamiento de las numerosas amenazas y vulnerabilidades presente en los

sistemas de VoIP. Identifica dos áreas problemáticas específicas (denegación de servicio, y el abuso de servicio) que exige más atención por parte la comunidad de investigación.

Por lo expuesto anteriormente, es sumamente importante la presente investigación, puesto que al desarrollar un Modelo de Seguridad enfocado a los ataques de DoS más utilizados por usuarios mal intencionados, en comunicaciones VoIP basadas en SIP, se brindará una ayuda a los encargados de la seguridad en las empresas, ya que actualmente no se encuentran recursos donde se detalle un modelo genérico completo y mucho menos seguro donde un administrador pueda documentarse para la implementación, configuración , uso y puesta en marcha de una red segura de VoIP basado específicamente en el protocolo SIP.

2.2. Bases teóricas

2.3. Voz sobre IP (VOIP)

VoIP es la tecnología de voz sobre el protocolo IP, abarca metodologías, tecnologías, protocolos de comunicación y técnicas de transmisión utilizadas para el establecimiento de sesiones de video y de comunicaciones de voz mediante redes basadas en el protocolo de Internet (IP), es decir que se envía la señal de voz y/o video en forma digital en paquetes de datos.(Rico J, 2013) . Proporciona una gran cantidad de ventajas frente a la telefonía tradicional como servicios de costes bajos y flexibles a los usuarios, lo que hace que sea más popular que PSTN, sin embargo se debe considerar que está expuesta a diferentes amenazas, ataques y vulnerabilidades. (Rehman & Abbasi, 2014). Entre los componentes principales que forman parte de la infraestructura de VoIP se tienen los terminales (teléfonos o softphones), nodos de control, nodos de gateways y la red basada en IP. (Butcher, Li, & Guo, 2007)

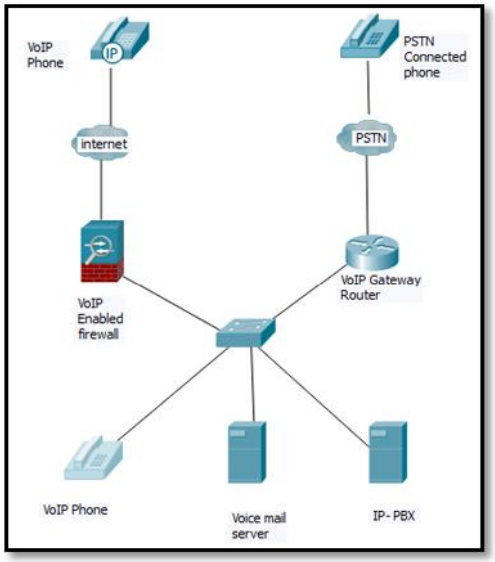


Figura 1-2: Estructura típica de Red de VoIP
Fuente: (Butcher et al., 2007)

En la Figura 2-2 se observan los protocolos fundamentales en una pila típica del protocolo de VoIP, estos se dividen en dos categorías que son: protocolos de señalización y protocolos de transmisión de voz. Los protocolos de señalización son los encargados de crear, gestionar, controlar y terminar una sesión. Los protocolos de transmisión de voz son responsables de la transmisión de los datos de voz reales a través de la red. Entre los principales protocolos de señalización VoIP están **H.323** y el **Protocolo de Iniciación de Sesión (SIP)**. (Deng, 2008)

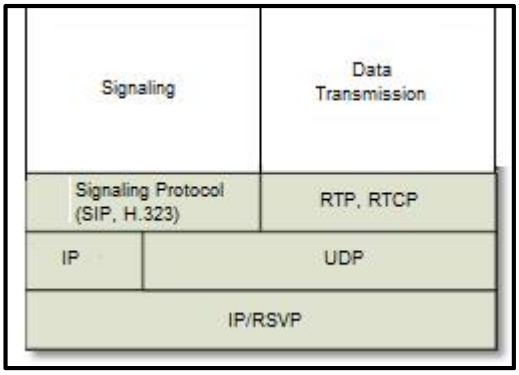


Figura 2-2: Protocolos de la pila de VoIP
Fuente: (Deng, 2008)

2.4. Protocolo de inicio de sesión (SIP)

Hennin Schulzrinne y Mark Handley diseñaron un protocolo de capa de aplicación llamado SIP en 1996; su propósito fue proporcionar un marco flexible y simplificado, lo que ayuda a crear,

modificar y finalizar la sesión de usuario. En 2000, el Proyecto Asociación de Tercera Generación (3GPP) aceptó utilizar SIP permanentemente como protocolo de señalización. En 2002, el IETF anuncia SIP en RFC- 3261. (Rehman & Abbasi, 2014). Es así que SIP es un protocolo de señalización que maneja el establecimiento, control y terminación de las sesiones de comunicación, se basa en una arquitectura cliente/servidor en la que el cliente inicia la llamada y el servidor responde. Los protocolos que interactúan en la comunicación con SIP, son:

- **RTP (Real-time Transport Protocol).-** generalmente una vez que SIP ha establecido la llamada se produce el intercambio de paquetes RTP, que son los encargados de transportar el contenido de la voz.
- **SDP (Session Description Protocol).-** los mensajes de este protocolo se transportan mediante el protocolo SIP y se utilizan negociar las capacidades de los participantes.

2.4.2. *Componentes SIP*

SIP es un protocolo basado en el modelo cliente-servidor. Los clientes SIP envían peticiones (*Requests Messages*) a un servidor, el cual una vez procesada contesta con una respuesta (*Response Messages)*. Los terminales SIP pueden generar tanto peticiones como respuestas al estar formados por el denominado cliente del agente de usuario (UAC) y servidor del agente de usuario (UAS).(Moreno, Soto, & Larrabeiti, 2001). Los componentes principales para una comunicación SIP, se detallan en la Tabla 1-2.

Tabla 1-2: Componentes de SIP

Componente	Descripción
Agente de Usuarios (UA)	Interactúa con el usuario final para completar una solicitud SIP. Puede actuar como cliente o servidor. El agente de usuario cliente (UAC) es responsable de iniciar peticiones como registro, invite, bye, o cancelar. El agente de usuario servidor (UAS) procesa la solicitud y responde en términos de provisional, el éxito, o redirigir, al cliente correspondiente.
Servidor Proxy SIP	Realiza las funciones intermediador entre el UAC y el UAS. Una vez que llega una petición de inicio de llamada de UAC decide a que servidor debería ser enviada y entonces retransmite la petición, que en algunos casos pude llegar a atravesar varios proxys SIP antes de llegar a su destino.
Servidor de Registro	Es un servidor que acepta peticiones de registro de los usuarios y guarda la información de estas peticiones para suministrar un servicio de localización y traducción de direcciones en el dominio que controla. Procesa mensajes REGISTER, y asignan los usuarios URI su localización actual. Por ejemplo, 2001@testbed.com puede ser asignada a 2001@192.168.2.4:5060, donde 192.168.2.4 es la dirección IP actual del cliente 2001 y 5060 es el puerto en el que el Agente de Usuario (UA) SIP está escuchando.

Servidor de Localización	Se utiliza para almacenar las localizaciones de los usuarios registrados. Es utilizado por un proxy para encontrar la posible localización de clientes destino. Esta función se realiza con mayor frecuencia por el servidor de registro.

Realizado por: Arellano Karina, 2016
Fuente: (Rehman & Abbasi, 2014)

2.4.3. *Mensajes SIP*

SIP utiliza mensajes de cabecera similares a HTTP para comunicarse. El cuerpo del mensaje se utiliza ya sea para describir requisitos de sesión o para encapsular varios tipos de señalización. Las direcciones SIP son como las direcciones de correo electrónico; un ejemplo de una dirección SIP es ***sip:2001@testbed.com***. Existen dos tipos de mensajes SIP: ***request***, y ***response*** a un mensaje de solicitud correspondiente. (Ver Tabla 2-2 y 3-2). Los mensajes de ***request*** son utilizados por UAC, y ***response*** por los UAS, cuando un usuario **A** requiere hacer una llamada telefónica al usuario **B**, el usuario **A UAC** generará un mensaje INVITE, y lo enviará al usuario **B UAS**, entonces, el usuario **B UAS** procesará esta solicitud y enviará las respuestas correspondientes.

Tabla 2-2: Mensajes comunes de SIP Request

Mensaje	Propósito
INVITE	Se usa para hacer nuevas llamadas y es enviado hacia la central telefónica.
BYE	Se usa para terminar una llamada de forma normal. Con él, se da término a una llamada establecida por medio del mensaje INVITE
OPTIONS	Es utilizado por un terminal para consultar a otro terminal o a una central telefónica sobre sus capacidades y descubrir los métodos soportados, tipos de contenido, extensiones y códec. Este mensaje se envía antes de establecer una llamada.
REGISTER	Con este mensaje, un cliente puede registrarse y des-registrarse desde un proxy o una central telefónica. Esto significa que se realiza un registro de los terminales, con parámetros (dirección IP, número telefónico e identificador de usuario) que lo identifican y que permiten la comunicación con el terminal.
ACK	Es utilizado para responder a un mensaje de estado de SIP, en el rango 200-699 en una llamada establecida.
CANCEL	Usando el mensaje CANCEL una conexión puede interrumpirse antes de establecer la llamada. También se usa en situaciones de error.
INFO	Son típicamente utilizados para intercambiar información entre los terminales, necesaria para aplicaciones que no tienen que ver necesariamente con la llamada en curso.

Realizado por: Arellano Karina, 2016
Fuente: (Sun, Mkwawa, Jammeh, & Ifeachor, 2013)

Los mensajes de ***SIP response*** son códigos de tres dígitos similar a HTTP (ejemplo: 404 no encontrado, y 200 OK). El primer dígito indica la categoría de las respuestas.

Tabla 3-2: Mensajes comunes de SIP Response

Mensaje	Propósito
1xx	Para indicar un estado temporal, como 100 TRYING (intentando) o 180 RINGING (teléfono sonando).
2xx	Respuestas de éxito. Por ejemplo 200 OK indica que una llamada se ha establecido exitosamente
3xx	Redirección de llamadas. Por ejemplo 301 MOVED PERMANENTLY indica que el terminal cambio de dirección IP y ya no se encuentra en esa dirección.
4xx	Fallo en la petición, error de terminal. Por ejemplo el mensaje 401 UNAUTHORIZED que indica un fallo de autenticación.
5xx	Fallo de servidor. Por ejemplo 500 INTERNAL ERROR comunica error interno del servidor.
6xx	Fallos globales del sistema. Por ejemplo 600 BUSY EVERYWHERE comunica que el sistema está completamente ocupado

Realizado por: Arellano Karina, 2016
Fuente: (Sun et al., 2013)

2.4.4. *Estructura SIP*

De acuerdo con RFC-3261, SIP se describe en una pila de capas. Cada capa se distancia de otra capa sobre la base de sus funcionalidades. En la Tabla 4-2 se observa el descripción de cada una de estas capas.

Tabla 4-2: Capas de la estructura de SIP

Capa	Descripción
Sintaxis y codificación	Es la capa más baja. Es un conjunto de reglas que define el formato y la estructura de un mensaje SIP. Esta capa es obligatorio para cada elemento de red SIP.
Transporte	Son los elementos de red SIP para enviar y recibir solicitudes SIP y las respuestas. Todos los elementos de la red SIP debe ser compatible con la capa de transporte
Transacción	Es la capa responsable de manejar todas las transacciones SIP. Las transacciones SIP se pueden definir como solicitudes SIP y las respuestas generadas por UAs. Maneja retransmisiones, tiempos de espera y la correlación entre las solicitudes SIP y las respuestas. Sólo está disponible en los UA y los proxies con estado.
Transacción de Usuario	Crea transacciones de los clientes, tales como un INVITE con la dirección IP de destino y número de puerto

Realizado por: Arellano Karina, 2016
Fuente: (Sun et al., 2013), (Rehman & Abbasi, 2014)

2.4.5. *Operación SIP*

Existen dos tipos de transacciones de mensajes SIP, es decir, solicitar (request) y responder (response). Para iniciar una llamada basada en SIP, el usuario que llama requiere primero registrarse con un servidor de VoIP apropiado. En la Figura 3-2, se observa el flujo del

escenario de establecimiento de llamada, en el que la operación que SIP realiza para establecer la comunicación se inicia cuando el usuario-A realiza una solicitud para establecer una sesión de VoIP con el usuario B. Inicialmente Usuario-A (el que llama) envía una invitación al usuario B a través de un servidor proxy. User-B recibió una invitación de servidor y las respuestas proxy, si User-B está dispuesto a hablar. Usuario-A (el que llama), recibió una respuesta del User-B (destinatario) y envia un ACK, lo que garantiza que el Usuario-A también está dispuesto a hablar. De este modo las llamadas VoIP se establecen entre ambas entidades. Para terminar la sesión, BYE es enviado por un usuario y la llamada será terminada después de recibir un OK.(Rehman & Abbasi, 2014)

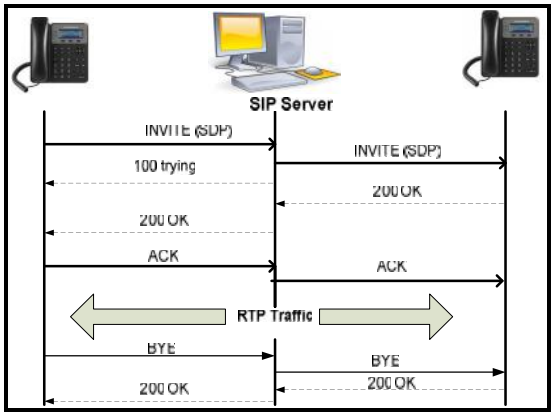


Figura 3-2: Establecimiento de llamada SIP
Fuente: (Rehman & Abbasi, 2014)

2.5. Vulnerabilidades de seguridad de un sistema VOIP

La gran parte de los problemas de seguridad en sistemas de VoIP son similares a los que se enfrentan las aplicaciones de Internet, puesto que los dispositivos de VoIP heredan muchas de las vulnerabilidades y fallas de seguridad de los servicios e infraestructuras a su alrededor. La Figura 4-2, muestra las vulnerabilidades encontradas comúnmente en los sistemas de telefonía IP en función de la pirámide de seguridad VoIP, propuesta por (Endler & Collier, 2007).

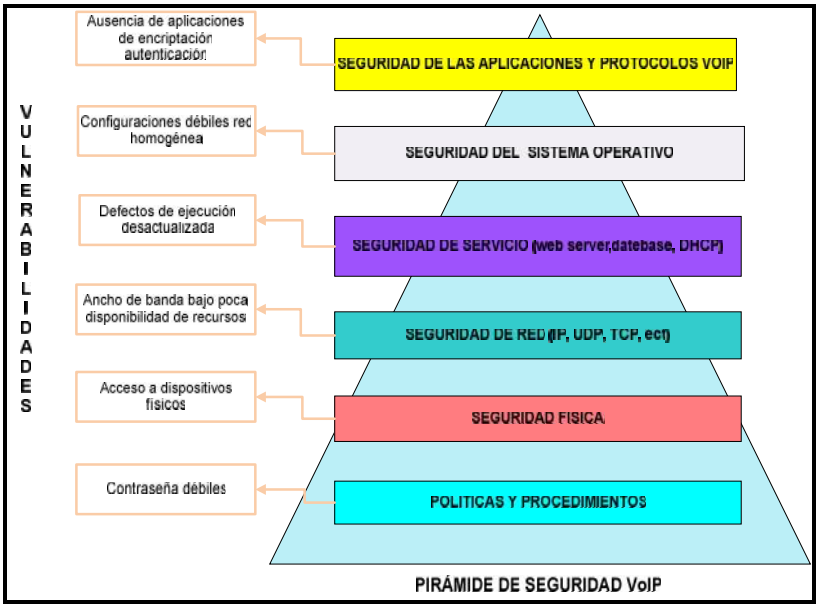


Figura 4-2: Vulnerabilidades de la Pirámide de Seguridad VoIP
Realizado por: Arellano Karina, 2016
Fuente: (Endler & Collier, 2007)

Todas las vulnerabilidades y fallas de seguridad pueden ser usadas para causar daños en la infraestructura VoIP. Para encontrarlas, los atacantes utilizan una serie de técnicas de reconocimiento convencional y no convencional. (Endler & Collier, 2007), identifican ciertas vulnerabilidades comúnmente encontradas en ambientes VoIP y se detallan en la Tabla 5-2, en la que se describe las causas que provocan estas vulnerabilidades y los efectos que producen en el servicio.

Tabla 5-2: Vulnerabilidades de la Pirámide de Seguridad VoIP

Vulnerabilidad	Causa	Efecto
Ausencia de aplicaciones de encriptación	Ocurre cuando no se cifran los mensajes enviados de un dispositivo de VoIP a otro, incluso si existen mecanismos de cifrado disponibles.	Permite que los datos confidenciales puedan ser objeto de ataques de espionaje.
Autenticación	Ocurre cuando una aplicación VoIP permite a un atacante el acceso a contenido privilegiado o funcionalidades si haberse autenticado.	Expone a los usuarios a ataques de secuestro de sesiones
Manejo de errores	En sistemas SIP, el control de errores de registro se maneja de forma insegura, ya que proporciona al usuario información que puede ser usada para atacar la red VoIP. Esto se presenta cuando un mensaje de registro con un número de teléfono no válido arroja un código de error 404: "No encontrado", mientras que un número de teléfono válido se traduce en un código de error 401: "No autorizado".	Permite al atacante conocer las cuentas válidas y realizar ataques de spam a través de telefonía de Internet (SPIT).
Configuraciones débiles	Se produce cuando se instalan de forma incorrecta las aplicaciones VoIP. Esto ocurre por varios factores como la negligencia o desconocimiento de algunos conceptos mínimos de seguridad por parte	Exponen los sistemas a diversos ataques, que van desde la ejecución de un código malicioso hasta la negación de servicio

	del usuario.	
Red homogénea	Se presenta cuando la infraestructura de la red VoIP depende de una determinada marca de teléfono, proxy o un firewall.	Un ataque automatizado, como un virus o un gusano, puede bloquear toda la red
Defectos de ejecución	Se presenta cuando la implementación no es minuciosa con el filtrado de contenidos activos, como las consultas SQL a partir de los datos proporcionados por el usuario: nombres de usuario, contraseñas y direcciones SIP.	Permite realizar ataques de inserción de secuencias SQL
Desactualización	Cuando no se adquieren las actualizaciones y parches que proporcione el fabricante de las aplicaciones VoIP.	Permite al atacante usar las vulnerabilidades publicadas de las versiones anteriores para causar daños en los sistemas de telefonía IP
Ancho de banda bajo	Se produce cuando el servicio de VoIP no es construido de forma que pueda manejar la carga de toda la red, es decir que cada persona perteneciente a la red pudiera hacer una llamada al mismo tiempo.	Cuando el número de abonados a un servicio de VoIP es bajo, esto no es un gran problema. Pero cuando un servicio es intencionalmente inundado con miles de clientes, o cuando hay un incidente que resulta en una carga enorme por los abonados, el resultado podría ser el bloqueo total del servicio
Poca disponibilidad de recursos	Se presenta especialmente en los dispositivos integrados, donde los recursos que las implementaciones de VoIP pueden utilizar, son escasos. Es decir, que posean poca memoria RAM o baja capacidad de procesamiento (CPU).	Esta vulnerabilidad podría hacer más fácil para un atacante bloquear los servicios de VoIP
Acceso a dispositivos físicos	Esto sucede cuando no se colocan las restricciones de identificación y control de acceso a las instalaciones, datacenters, servidores, medios y procesos de almacenamiento de la infraestructura de VoIP.	Permite al atacante desencadenar diversos ataques, que van desde la ejecución de un código malicioso hasta la negación de servicio
Contraseñas débiles	Ocurre cuando el identificador único de un cliente VoIP es el número de teléfono o dirección SIP y la contraseña.	El punto débil está en que las contraseñas se almacenan en un servidor de registro, de modo que si las mismas se encuentran en un formato fácil de descifrar, cualquier persona con acceso a ese servidor puede obtener el nombre de usuario y contraseña simultáneamente
Insuficiencia de sistemas de respaldo	Cuando un sistema esta caído, porque eventualmente puede llegar a suceder, debe existir un sistema de respaldo para que los usuarios puedan nuevamente conectarse.	La disponibilidad de los servicios en telefonía es crítica.

Realizado por: Arellano Karina, 2016
Fuente: (Endler & Collier, 2007)

2.6. Amenazas de seguridad en redes VOIP

La norma ISO 27001 define amenaza como *"una causa potencial de un incidente indeseado, que puede dar lugar a daños a un sistema o a una organización"*. VoIP es sustancialmente

vulnerable ante ataques de red, tales como ataques a usuarios con código malicioso (gusanos, virus, troyano), de Denegación de Servicio (DoS), accesos a servicios y acceso remoto. Estos ataques afectan al consumo de recursos de estos sistemas, provocando una congestión en la infraestructura de red haciendo que los usuarios legítimos comprometan la información confidencial, y los datos. (Martin & Hung, 2005). Cada amenaza de seguridad puede ser clasificada de acuerdo como afecte a los conceptos de seguridad como la: ***confidencialidad, integridad y disponibilidad*** en el sistema de VoIP. Es así como se puede elegir las contramedidas adecuadas.

Según (Endler & Collier, 2007), las amenazas frecuentemente utilizadas en la Seguridad de las Aplicaciones y Protocolos VoIP, se muestran en la Figura 5-2, y se describen en la Tabla 6-2.

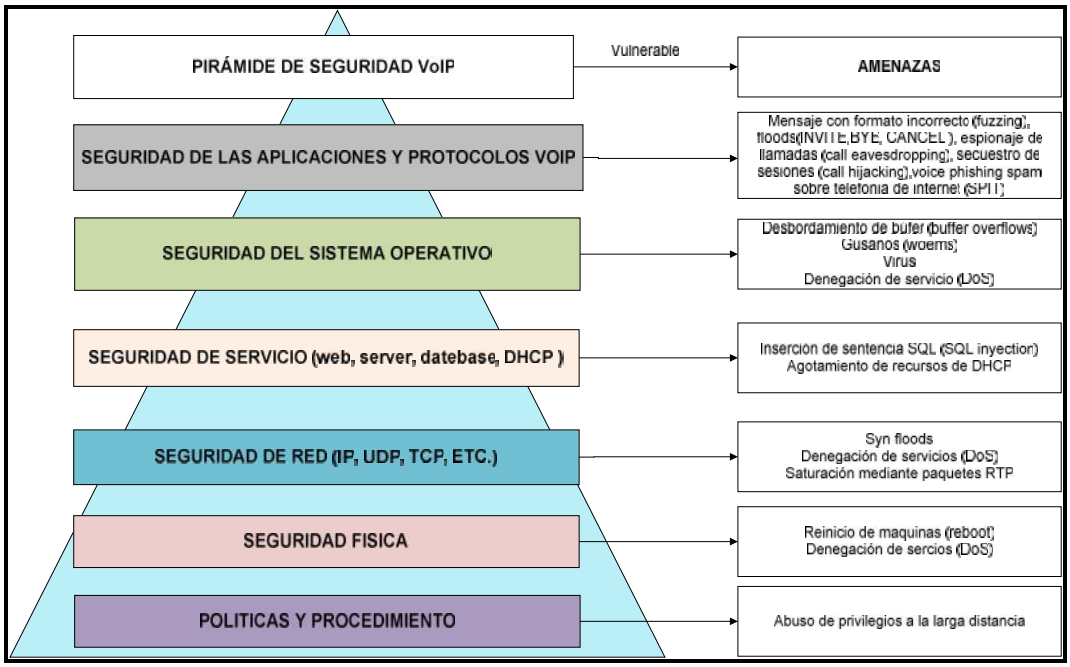


Figura 5-2: Amenazas de la Pirámide de Seguridad VoIP
Realizado por: Arellano Karina, 2016
Fuente: (Endler & Collier, 2007)

Tabla 6-2: Amenazas a SIP

Amenaza	Descripción
Denegación de Servicio (DoS)	Son intentos maliciosos para degradar o inhabilitar el funcionamiento del sistema, afectando la ***disponibilidad*** del mismo
Accesos NO autorizados	Se enfocan en los sistemas de control de llamadas, administración, facturación, y otras funciones de telefonía que requieren autentificación. Cada uno de estos sistemas puede contener datos que, si son comprometidos, pueden facilitar una estafa.
Fraude Telefónico (Toll fraud)	Es el intento por parte de un atacante para recibir dinero por tener un gran volumen de llamadas realizadas a un número de teléfono que tiene una gran tasa asociada a la conexión con ese número.

Redirección de Llamadas	Un atacante puede redirigir el número de teléfono de la víctima a un lugar de su elección, lo que así podría ser capaz de suplantar la identidad de la víctima por tener sus llamadas redirigidas al teléfono del atacante.
Espionaje (Eavesdropping)	El espionaje es cuando la conversación de la víctima se supervisa en secreto por el atacante. Normalmente, esto implica la recepción de los datos de voz de ambas partes en la llamada. Estos datos son utilizados luego para volver a reproducir la conversación y utilizar los contenidos con fines ilícitos. No sólo las conversaciones de voz son objeto de escuchas, también las conversaciones de tipos de datos que son transportados por el sistema telefónico.
Alteración de la voz – Stream	Es un ataque de sustitución o ***man-in-the-middle***, el atacante es capaz de escuchar la conversación entre las dos víctimas y también alteran la comunicación. Esto incluye la reproducción de voz previamente capturado para que el receptor escuche un mensaje diferente al que el remitente a enviado. Esto podría ser utilizado con mayor facilidad para cambiar porciones muy pequeñas de una conversación.
SPIT	Es el SPAM de la telefonía IP. Es un ataque que puede usar paquetes de datos o de voz. Ya sea enviando mensajes SMS para promocionar productos a los diferentes terminales, o enviando grabaciones promocionales a los buzones de voz de los usuarios.
VISHING	Es el término usado para referirse a VoIP ***phishing***. Es un ataque con las mismas características del phishing pero adoptado a las posibilidades de VoIP.

Realizado por: Arellano Karina, 2016
Fuente: (Endler & Collier, 2007)

Los atacantes han descubierto que la ***disponibilidad*** de los servicios es el factor más importante para los usuarios de las redes VoIP, puesto que si el sistema de VoIP no se encuentra disponible el impacto de afectación es elevado tanto para los usuarios como para las organizaciones que basan su comunicación en redes VoIP. Los ataques de DoS tienden a ser de fácil ejecución, es por ello que el atacante novato o inexperto en el tema, no necesita más que poseer las herramientas y ejecutarlas. (Jouravlev, 2008)

2.7. Amenazas de denegación de servicio (DoS) en VOIP

Los ataques de DoS son intentos que un atacante realiza para evitar que el servicio telefónico opere dentro de las especificaciones normales de funcionamiento, es decir que comprometen la ***disponibilidad*** del servicio. (Butcher, Li, & Guo, 2007). El objetivo de esta amenaza, es disminuir gravemente el rendimiento de la red o un sistema llegando incluso hasta el punto de impedir del servicio por parte de usuarios legítimos, a través de llamadas falsas que generan tráfico excesivo, envíos de gran cantidad de paquetes o la confección de paquetes para explotar debilidades de servicio; de esta manera, las llamadas legítimas no pueden realizarse o se interrumpen. Según (Al-Allouni, Rohiem, Hashem, El-moghazy, & Ahmed, 2009), VoIP está expuesto a tres tipos de amenazas de DoS, que se detallan en la Tabla 7-2.

Tabla 7-2: Tipos de Amenazas de DoS en VoIP

Amenaza de DoS	Descripción	Característica en VoIP
DENEGACIÓN DE SERVICIO DISTRIBUIDO (DDOS)	Son ataques de DoS generados desde múltiples sistemas, todos coordinados para inhabilitar un sistema de red. Los atacantes generalmente usan troyanos y backdoors, logrando así crear miles de robots listos para realizar sus ataques de DDos.	Tienen como objetivo causar la denegación del servicio de VoIP en varios puntos de la red, de manera simultánea, colapsando el sistema por completo. Además logran generar tráfico en grandes cantidades que ningún dispositivo podría soportar.
FUZZING	Hace uso de paquetes malformados, provocando un mal funcionamiento del sistema debido al desbordamiento de buffer, cuelgues o reinicios en los dispositivos,	En particular el protocolo SIP, envía mensajes en texto plano, por lo tanto, es muy fácil realizar el cambio de los campos del mensaje. Esto puede llevar a un error de un dispositivo VoIP. Además este ataque se utiliza en VoIP para realizar testeos funcionales y verificar cómo se comporta el protocolo. Es uno de los mejores métodos para encontrar errores y agujeros de seguridad
INUNDACIONES (FLOODERS)	Consiste en enviar mucha información en un corto tiempo a un dispositivo con la finalidad de saturarlo.	Su objetivo son los servicios y puertos de telefonía IP, es así que al bloquear los puertos de comunicación, deniegan el servicio a los usuarios legítimos.

Realizado por: Arellano Karina, 2016

2.8. Amenazas de seguridad de SIP

Los sistemas de VoIP son susceptibles a una variedad de ataques, la mayoría de estos ataques se realizan utilizando el protocolo SIP, debido a que dentro del estándar de este protocolo no se consideraron medidas de seguridad suficiente como para protegerlo. Según (Rehman & Abbasi, 2014), (Deng, 2008) y (Sisalem et al., 2006), concuerdan en que los ataques comúnmente usados en redes de VoIP, contra la seguridad específica de SIP, que afectan tanto a la disponibilidad, como a la integridad y confidencialidad, son:

2.8.1. *Suplantación de identidad (registration hijacking)*

Es una amenaza del tipo fraude telefónico, que hace uso de una vulnerabilidad en el mensaje REGISTER. Este ataque utiliza el registro de usuario, que es la primera comunicación que se establece en el entorno VoIP, puede realizarse con o sin autenticación. Si un servidor no autentica las peticiones cualquiera puede registrar cualquier dirección de contacto para cualquier usuario. Es así como el atacante podrá secuestrar la identidad del usuario y sus llamadas. Esto se realiza a través de los mensajes **REGISTER**, donde se modifica la dirección IP actual de la

víctima, de manera que el servidor cambie la dirección IP y envíe las peticiones posteriores hacia el atacante. Cuando existe autenticación, el atacante aún puede realizar una suplantación de identidad capturando mensajes de registros previos. Con estos mensajes legítimos alterados, se cambia la localización y las llamadas pueden seguir siendo direccionadas al atacante.

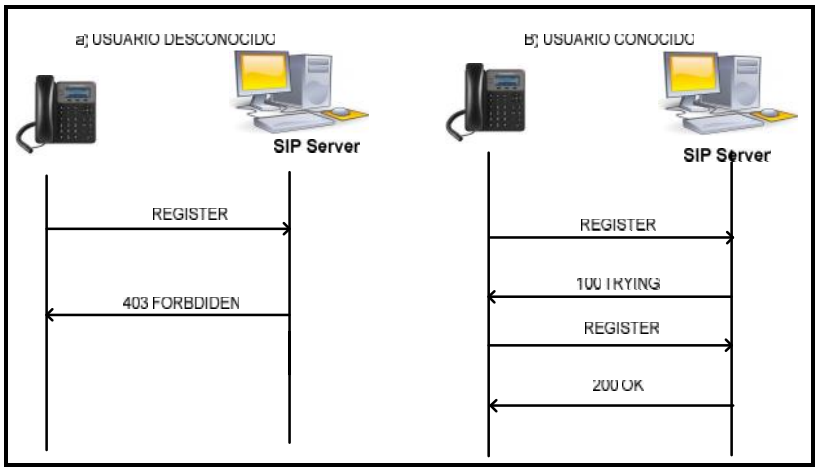


Figura 6-2: Registro SIP
Fuente:(Deng, 2008)

La Figura 6-2 muestra el intercambio de mensajes REGISTER, entre un terminal y una central telefónica en el caso de ser un usuario conocido y desconocido. Par el caso de que el nombre de usuario exista, contesta con un mensaje ***100 TRYING***, luego el terminal debe enviar un mensaje ***REGISTER*** con la respuesta y con la autenticación. Si esta fase concluye exitosamente, el servidor responde un mensaje ***200 OK.*** Ahora si no existe el nombre de usuario, contesta con un mensaje ***403 FORBIDDEN***, en este caso el servidor no establece un límite para la cantidad de intentos fallidos durante el proceso de registro. Es por ello que se pueden realizar ataques de fuerza bruta.

2.8.2. *Des-registro de usuarios*

Este ataque, si actúa por sí solo, se clasifica como una amenaza de DoS. Si se utiliza en conjunto con otros ataques, puede desencadenar una amenaza de interceptación (eavesdroping), fraudes telefónicos o accesos no autorizados. La vulnerabilidad utilizada en este ataque es la falta de autenticación en el mensaje REGISTER. El ataque de des-registro por sí solo, sin la participación de otros ataques, puede lograrse de tres formas:

a) El atacante bloquea el mensaje REGISTER legítimo transmitido por el usuario y no permite que llegue a destino.

b) El atacante envía repetidamente peticiones REGISTER en un corto espacio de tiempo con el objetivo de superponerse a la petición de registro legítima del usuario.

c) El atacante envía al servidor de registro una petición REGISTER indicando la identidad del usuario, con el campo contacto ***"Contact:*"*** y el valor ***"Expire" a cero***. Esta petición eliminará cualquier otro registro de la dirección del usuario, a este ataque se conoce como ataque de ***Eliminación de Registros.***

Figura 6-2: Eliminación del Registro
Fuente:(Deng, 2008)

El atacante deberá realizar cualquiera de estas variaciones periódicamente, para evitar el re-registro del usuario legítimo o alternativamente provocarle un ataque de DoS para evitar que vuelva a registrarse por el tiempo que necesite realizar el ataque.

2.8.3. *Desconexión de usuarios*

Este ataque es un amenaza de DoS. Esta vulnerabilidad hace uso de la posibilidad de alterar los mensajes BYE y CANCEL, y es por lo tanto, una amenaza de ***fuzzing***. La desconexión de usuarios funciona debido a que muchos de los protocolos de VoIP se utilizan sin alguna encriptación. Por lo tanto, es sencillo interceptar mensajes y obtener la información de la identidad del usuario y los datos de la llamada. De esta manera, para un intruso resulta fácil desconectar las llamadas utilizando el mensaje BYE y simulando ser el usuario al otro lado de la línea. Por otro lado el mensaje CANCEL alterado se debe enviar al momento de establecerse la llamada, es antes que el usuario, receptor de la llamada, conteste el teléfono y la llamada sea establecida. A diferencia del mensaje BYE que se envía cuando la llamada está establecida. Una variación de este ataque es transformarlo en una inundación. Se utilizan programas que van

identificando los datos de las llamadas y enviando mensajes de desconexión (BYE o CANCEL) masivamente, conocidos como Floods BYE y Floods CANCEL.

2.8.4. *Malformación en mensajes invite*

El ataque de malformación es una amenaza de DoS de servicio del tipo ***fuzzing*** que modifica campos en el mensaje INVITE. Este ataque funciona enviando mensajes INVITE con contenidos no previstos por el protocolo, provocando que los terminales funciones mal o dejen de funcionar por completo. Estas vulnerabilidades son generalmente de corta duración y de fácil mitigación a través de parches de software.

2.8.5. *Inundación SIP*

Este ataque de DoS basado en inundaciones, se puede lograr mediante él envió de grandes volúmenes de tráfico inútil para ocupar todos los recursos que de otro modo serían utilizados para atender el tráfico legítimo, dentro de estos ataques, se encuentran:

- **INVITE Flood:** Este ataque envía mensajes ***INVITE*** en grandes cantidades para hacer colapsar al dispositivo SIP receptor. Particularmente, este ataque utiliza los mensajes INVITE porque pueden provenir de múltiples direcciones IP falsificadas. (Rico J, 2013)

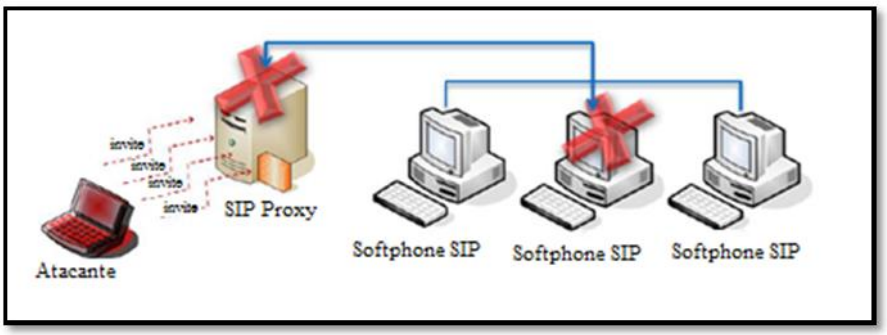


Figura 7-2: Floods INVITE
Fuente: (David Endler, 2007)

- **BYE Flood:** es un ataque que realiza un envío de mensaje BYE falso que incluye el valor apropiado para el campo Call-ID, finalizando la conversación y las llamadas en curso. Este campo se conoce capturando la llamada con un sniffer.

- **CANCEL Flood:** Al igual que el ataque Flood BYE, en éste se envía el mensaje CANCEL falso que incluya el valor apropiado para el campo Call-ID, causando el cierre de la comunicación.

- **REGISTER Flood:** de la misma forma que los ataques anteriores, actúa con el envío masivo de mensajes REGISTER, buscando registrarse como usuario legitimo en la red de VoIP, mediante el mensaje ***REGISTER*** con direcciones IP de origen falsificados, saturando los recursos del servicio de VoIP.

Cabe indicar que a pesar de que hay otras tipos de solicitudes SIP, ***INVITE*** y ***REGISTER*** son los mensajes predominantes utilizados por SIP, y requieren más procesamiento en los componentes SIP que todas las demás solicitudes. Por lo tanto, los sistemas de VoIP basadas en SIP son especialmente vulnerables a los ataques de inundación utilizando estas solicitudes.

Debido a que SIP, puede operar sobre TCP o UDP, también es importante señalar ataques como:

- **SYN Flood:** Es uno de los más comunes debido al funcionamiento las conexiones TCP. Cuando un equipo desea establecer una comunicación con otro, el cliente inicia la comunicación enviando al servidor un paquete TCP SYN, el servidor responde con un SYN+ACK, para luego el cliente enviar un ACK de vuelta y comenzar la transmisión de datos.

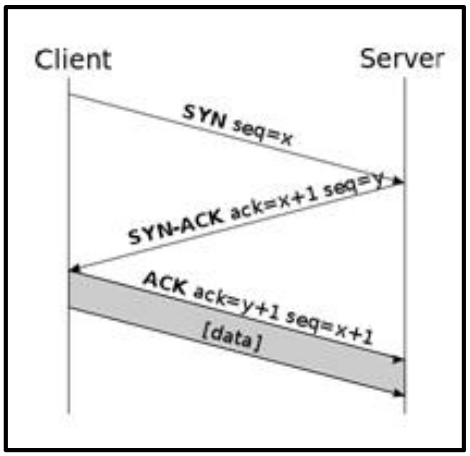


Figura 8-2: Handshske TCP
Fuente: (David Endler, 2007)

En este ataque el cliente envía innumerables paquetes TCP SYN al servidor y estos son respondidos con un SYN+ACK, pero quedan a la espera del ACK final para la

comunicación que nunca va a ser enviado. De esta manera se colapsa la conexión de la víctima logrando un alto consumo de recursos disponibles con solicitudes no válidas y que el servidor o softphone no distinga entre los SYNs legítimos y los SYNs falsos. (Butcher et al., 2007)

Figura 9-2: Ataque SYN Flood
Fuente: (David Endler, 2007)

- **UDP Flood:** es el ataque DoS preferido por los atacantes, ya que las direcciones origen de los paquetes UDP son fácilmente falsificables, además actualmente la gran parte de dispositivos VoIP soportan UDP de manera nativa y transparentemente. (Rico J, 2013)

2.8.6. *Ataque re-invite*

Es una amenaza de fraude telefónico. Este ataque utiliza la vulnerabilidad de la autenticación solicitada a los mensajes INVITE, que se envían cuando una llamada se pone en espera.

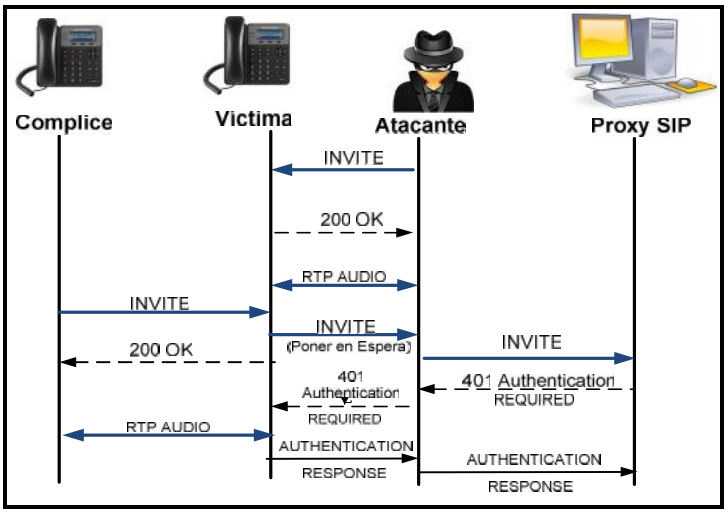


Figura 10-2: Ataque de RE-INVITE
Fuente:(Deng, 2008)

A continuación, se define una matriz que resume los atributos de seguridad que afectan los ataques antes vistos, como la Confidencialidad = C, Integridad = I y Disponibilidad = D.

Tabla 8-2: Impacto de ataques potenciales a VoIP

Protocolo	Ataque	C	I	D
SIP	*Eavesdropping (*Intercepción de mensajes de señalización)	x	x	
	Suplantación de identidad (Registration hijacking)		x	
	Eliminación de Registro de Usuarios	x		x
	Desconexión de usuarios	x		x
	Malformación en mensajes INVITE			x
	Inundación en mensajes INVITE, REGISTER, BYE, CANCEL			x
	Ataque de falsa respuesta (Faked Response)	x	x	
	Ataque de Re-INVITE		x	

Realizado por: Arellano Karina, 2016
Fuente: (Butcher et al., 2007)

2.9. Valoración del riesgo de ataques a SIP

En cualquier tipo de sistema los riesgos son un factor latente dentro del ámbito de la seguridad, lo es aún más en sistemas de voz sobre IP, puesto que siempre están expuestas a situaciones de riesgo; por ello es necesario considerar que todo riesgo se puede minimizar pero nunca eliminar. Para determinar la factibilidad al minimizar el impacto, es necesario identificar a tiempo los riegos y clasificarlos. (Endler & Collier, 2007), en su libro ***Hacking Exposed*** presentan una clasificación del riesgo de los diferentes ataques a VoIP, basado en tres pilares fundamentales que son la ***popularidad*** con la que se efectúan estos ataques, la ***simplicidad*** que representa el esfuerzo necesario para ejecutar el ataque, y el ***impacto*** que produce la ejecución del ataque en el funcionamiento del servicio de VoIP, en la Tabla 9-2, se observa las escalas y definiciones que se proponen.

Tabla 9-2: Clasificación del Riesgo de Ataques VoIP

	Descripción
Popularidad	Es la frecuencia con la que se estima el ataque. Directamente se correlaciona con el campo Simplicidad
Simplicidad	Representa el grado de habilidad necesaria para ejecutar el ataque
Impacto	Es el daño potencial causado por la ejecución del ataque con éxito
Estimación del Riesgo	Este valor se obtiene promediando los tres valores anteriores.

Realizado por: Arellano Karina, 2016
Fuente: (Endler & Collier, 2007)

Estos pilares se valoran en una escala de 1 a 10 puntos, la popularidad, simplicidad, impacto y estimación del riesgo, como se muestra en las Tablas 10-2, 11-2, 12-2 y 13-2, respectivamente.

- **Popularidad:** Varia de 1 a 10, en donde: **1** es el más raro y **10** se utiliza mucho

Tabla 10-2: Escala de Valoración Cuantitativa y Cualitativa de la *Popularidad*

1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Rara vez	Muy Baja	Medianamente Baja	Baja	Poco Frecuente	Frecuente	Moderadamente Frecuente	Alta	Medianamente Alta	Muy Alta

Realizado por: Arellano Karina, 2016
Fuente: (Endler & Collier, 2007)

- **Simplicidad:** Varia de 1 a 10, en donde: **10** es el uso de una herramienta point-and-click generalizado o un equivalente; **1** desarrollar un nuevo exploit para sí mismo. Los valores comprendidos entre **5** y **6** es probable que indique una herramienta a disposición de línea de comandos.

Tabla 11-2: Escala de Valoración Cuantitativa y Cualitativa de la *Simplicidad*

1	**2**	**3**	**4**	**5**	6	**7**
Extremadamente Complejo	Muy Complejo	Medianamente Complejo	Ligeramente Complejo	Relativamente Complejo	Relativamente Fácil	Ligeramente Fácil

8	**9**	**10**
Medianamente Fácil	Muy Fácil	Extremadamente Fácil

Realizado por: Arellano Karina, 2016
Fuente: (Endler & Collier, 2007)

- **Impacto:** Varia de 1 a 10, en donde: **1** ha revelado algunos datos triviales sobre el dispositivo o red; y **10** es conseguir acceso total sobre el objetivo o ser capaz de redirect, sniff, modificar el tráfico de red y denegar el servicio.

Tabla 12-2: Escala de Valoración Cuantitativa y Cualitativa del *Impacto*

1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
Trivial	Muy Tolerable	Tolerable	Muy Moderado	Moderado	Ligeramente Importante	Importante	Muy Importante	Intolerable

10
Extremadamente Intolerable

Realizado por: Arellano Karina, 2016
Fuente: (Endler & Collier, 2007)

- **Estimación del Riesgo:** Varía de 1 a 10, en donde: **1** implica que el nivel de riesgo es insignificante en el rendimiento del servicio y **10** afecta totalmente al normal funcionamiento del servicio de VoIP.

Tabla 13-2: Escala de Valoración Cuantitativa y Cualitativa de *Estimación del Riesgo*

1	2	3	4	5	6	7	8	9
Trivial	Muy Tolerable	Tolerable	Muy Moderado	Moderado	Ligeramente Importante	Importante	Muy Importante	Intolerable

10
Extremadamente Intolerable

Realizado por: Arellano Karina, 2016
Fuente: (Endler & Collier, 2007)

(Endler & Collier, 2007) clasifican los riesgos para un sistema de voz sobre IP según su popularidad, simplicidad e impacto que debe ser tratados y corregidos en el menor tiempo posible utilizando todos los procedimientos y recursos necesarios para asegurar la continuidad del servicio de VoIP, como se muestra en la Tabla 14-2.

Tabla 14-2: Escala de Valoración de Riesgo en VoIP

Ataque	Popularidad	Simplicidad	Impacto	Estimación del Riesgo
Fuzzing	5	5	9	7
Floods INVITE to SIP Proxies (Usando inviteflood Tool)	7	8	10	8
Floods INVITE to SIP Phone (Usando inviteflood Tool)	9	7	9	8
Desconexión de Usuarios (Floods BYE)	7	6	7	7
Flood Register	7	7	9	7
Call Eavesdropping	5	7	7	6
Call Hijacking	8	8	9	8
Eliminación de Registros	6	8	6	7
Voice Phishing	4	4	10	6
SPIT	6	7	5	6
TCP SynFlood	9	8	9	9
Default Asterisk Passwords	7	8	4	6

Realizado por: Arellano Karina, 2016
Fuente: (Endler & Collier, 2007)

El estudio de esta investigación se enfoca principalmente en ataques DoS que afectan de manera directa a la disponibilidad del servicio como se vio en la Tabla 8-2, considerando aquellos que presentan un impacto potencial en el servicio, y la posibilidad de concurrencia; en la Tabla 15-2 se detallan los ataques de DoS que serán objeto de estudio del presente trabajo de investigación.

Tabla 15-2: Escala de Valoración de Riesgo en VoIP

Ataque	Popularidad	Impacto	Estimación del Riesgo
Fuzzing - Malformación de Mensajes	5	9	7
Floods INVITE to SIP Proxies (Usando inviteflood Tool)	7	10	8
Floods INVITE to SIP Phone (Usando inviteflood Tool)	9	9	8
Eliminación de Registros	6	6	7
TCP SynFlood	9	9	9

Realizado por: Arellano Karina, 2016
Fuente: (Endler & Collier, 2007)

2.10. Recomendaciones de seguridad para redes VOIP

La ejecución de políticas y estándares para la seguridad de la información demanda la normalización y definición de recomendaciones para determinar, implementar y mejorar la seguridad, es por ello, que a nivel internacional se establecen parámetros específicos para la iniciación, implementación y mantenimiento de la seguridad de una organización, considerando que no todos las recomendaciones son aplicables para todas las situaciones, sin embargo, conllevan obligaciones legales para su cumplimiento. En este contexto, el presente trabajo de investigación considera las diferentes recomendaciones, normas y estándares de seguridad de la información aplicables en ambientes de redes de voz sobre IP; todas estas recomendaciones están enfocadas en todo tipo de organización, ya sea pequeña, mediana o grande: empresas comerciales, agencias de gobierno, entidades bancarias, organizaciones sin ánimo de lucro. A continuación se describen ciertas recomendaciones de seguridad obtenidas de estándares, metodologías y buenas prácticas, que han sido estudiadas y evaluadas por expertos a lo largo de los años.

2.10.1. *Recomendaciones UIT-T X.805*

La UIT (Unión Internacional de Telecomunicaciones) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones. El UIT-T (Sector de Normalización de las Telecomunicaciones de la UIT) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica recomendaciones sobre los mismos, con

miras a la normalización de las telecomunicaciones en el plano mundial. La recomendación UIT-T X.805 fue aprobada el 29 de octubre de 2003 por la Comisión de Estudio 17 (2001-2004) del UIT-T por el procedimiento de la Recomendación UIT-T A.8., en esta Recomendación se define el marco para la Arquitectura de Seguridad para Sistemas de Comunicación de Extremo a Extremo, y las dimensiones que garantizan la seguridad extremo a extremo de aplicaciones distribuidas. (UIT-T, 2003). X.805 se basa en algunos conceptos de X.800 y en los marcos de seguridad (X.810-X.816). Las dimensiones de seguridad de las comunicaciones, disponibilidad y privacidad de X.805 ofrecen nuevos tipos de protección para la red. Estas siete dimensiones de seguridad se exponen a continuación:

1. Privacidad y confidencialidad de datos
2. Autenticación
3. Integridad de datos
4. No repudio
5. Control de Acceso
6. Comunicación
7. Disponibilidad

Entre las recomendaciones específicas para VoIP se encuentran:

1. Garantizar la seguridad de operaciones, administración, mantenimiento y configuración (OAM&P) de los servicios de red.
2. Proteger la información de control o señalización que se utiliza en el servicio de red. Por ejemplo, proteger el protocolo SIP que se utiliza para iniciar y mantener las sesiones de VoIP.
3. Proteger los datos y la voz cuando el usuario utiliza el servicio de red. Por ejemplo, proteger la confidencialidad de la conversación de un usuario en un servicio VoIP.

2.10.2. *Recomendaciones de seguridad de NIST*

El NIST (National Institute of Standards and Technology) tiene como misión promover la innovación y la competitividad industrial mediante el avance ciencia de la medición, normas, y la tecnología de forma que mejoren la seguridad económica. En su publicación especial 800-58 (Kuhn & Walsh,2005), propone varias recomendaciones prácticas iniciales para la implementación de una red de VoIP segura, entre las más importantes, están:

1. Desarrollar la arquitectura de red apropiada:

   a. Independizar en lo posible las redes de voz y datos utilizando servidores DHCP separados para facilitar la detección de intrusos y la protección del firewall.

   b. Usar autenticación y control de acceso en el sistema gateway que hace interface con el PSTN de la red de voz y en cualquier componente crítico del sistema deshabilitando además el H.323, SIP o cualquier otro protocolo de VoIP de la red de datos.

   c. Implementar mecanismos para permitir el tráfico de VoIP a través de los firewalls.

   d. Usar filtros de paquetes con estado para monitorear el estado de las conexiones.

   e. Usar IPsec o Secure Shell (SSH) para el manejo remoto y la auditoria de accesos.

   f. Utilizar métodos de inscripción en el router u otro gateway dependiendo del poder computacional de los end-points.
2. Asegurar que la organización ha examinado y puede manejar y mitigar los riesgos relacionados con el manejo de la información, sistemas operativos y la continuidad de sus operaciones esenciales después de implementar el sistema de VoIP.
3. Desarrollar controles físicos apropiados en la red VoIP a menos que se encuentre cifrada.
4. Usar los sistemas de emergencia de energía requeridos para asegurar la operación continua durante apagones o fallas del fluido eléctrico.
5. Utilizar los mecanismos de protección apropiados y firewalls especializados en VoIP.

2.10.3. *Recomendaciones de seguridad de ISO/IEC 27002*

Las normas ISO/IEC 27000, son un conjunto de estándares desarrollados (o en fase de desarrollo), por ISO *(International Organization for Standardization)* e IEC *(International Electrotechnical Commission)*, que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña. La norma ISO/IEC 27002, brindan recomendaciones de las mejores prácticas en la gestión de la seguridad de la información, la cual es considerada como la base para la implementación de medidas de seguridad tras un breve y primer análisis de riesgos dentro de una organización. La versión más reciente es la 27002: 2015, que contiene 35 objetivos de control y 114 controles, agrupados en 14 dominios. Para la gestión de la seguridad en redes, el portal en español de la ISO 27002, indica que el objetivo uno de control del estándar ISO27002 es: "*evitar el acceso físico no autorizado, los daños e interferencias a la información de la organización y las instalaciones de procesamiento de la información.*". Los catorce dominios, son:

1. Política de seguridad
2. Organización de seguridad
3. Seguridad de los recursos humanos
4. Gestión de activos
5. Control de acceso
6. Cifrado
7. Seguridad física y ambiental
8. Seguridad de las operaciones
9. Seguridad de las Comunicaciones
10. Adquisición de sistemas, desarrollo y mantenimiento
11. Relaciones con los Proveedores
12. Gestión de Incidencias que afectan a la Seguridad de la Información
13. Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio
14. Conformidad

En cada sección, se detallan los objetivos de los diferentes controles para la seguridad de la información. En cada control se indica una guía para su implementación. Entre las recomendaciones finales enfocadas a comunicaciones de Voz sobre IP están:

1. Controlar los accesos a servicios internos y externos conectados en red.
2. Proteger tráfico de VoIP
3. Cifrar
4. Aplicar mecanismos de autenticación adecuados se aplican a los usuarios y equipos
5. Llevar un rígido manejo de llaves
6. Segregar el tráfico de datos y de voz
7. Hacer uso de servidores proxy delante de firewalls
8. Resguardar los IP-PBX's
9. Usar controles de seguridad perimetrales Firewall o SBC
10. Implementar herramientas de seguridad de red como IDS/IPS (detección y prevención de intrusiones), gestión de vulnerabilidades, etc.

2.10.4. *Recomendaciones de seguridad para sistemas VOIP basados en Asterisk*

Asterisk es un software libre (bajo licencia GPL) que proporciona funcionalidades de una central telefónica (PBX). Es un sistema de centralita IP utilizado por empresas de todos los

tamaños para mejorar su comunicación, soporta protocolos de señalización como H.323, SIP, MGCP y SCCP. Entre las recomendaciones encontradas en su sitio web oficial, están:

1. Actualizar constantemente a la última versión estable, el software tanto de teléfonos (softphones) y servidores IP.
2. Usar servidores de procesamiento de mensajes, que se encarguen de limitar el número veces que se registra una dirección IP (especifica o en particular) por minuto.
3. Emplear herramientas de software de monitoreo del mapeo del direccionamiento MAC a direcciones IP, como por ejemplo Arpwatch.
4. Eliminar los servicios que permiten el cambio de la dirección IP en las terminales sin la necesidad de una contraseña de administrador.
5. El control de acceso al servidor depende de si éste sirve a usuarios ubicados en cualquier dirección de Internet, o por el contrario sirve únicamente a rangos de red conocidos.
6. Cambiar configuración básica. Parámetros de Configuración relacionados con la seguridad del servicio
7. Monitorear continuamente las llamadas activas y las llamadas realizadas durante el día.
8. Restringir el acceso a los equipos de la red

2.10.5. *Recomendaciones de seguridad para sistemas VOIP basados Cisco Unified Communications Manager*

Cisco Unified Communications Manager (CUCM), antes Cisco Unified Call Manager y Cisco Call Manager (CCM), es un software basado en un sistema de tratamiento de llamadas y telefonía sobre IP, desarrollado por Cisco Systems. CUCM rastrea todos los componentes VoIP activos en la red; esto incluye teléfonos, gateways, puentes para conferencia, recursos para transcodificación, y sistemas de mensajería de voz, entre otros. CallManager a menudo utiliza el SCCP (Skinny) como un protocolo de comunicaciones para la señalización de parámetros de hardware del sistema, tales como teléfonos IP. H.323, MGCP, y SIP son usados para trasferir la señalización de las llamadas a los gateways. Entre las recomendaciones de seguridad que presenta CISCO, tenemos:

1. Usar permanentemente VLANs, para separar los clientes VoIP de los de la red de datos.

2. Asegurar todos los elementos de la red VoIP como servidores, protocolos, dispositivos finales y prioridades entre otros.
3. Aplicar políticas de enrutamiento tanto en routers como en switches, con la finalidad de forzar el flujo de tráfico a través de segmentos de seguridad, como firewalls, IDS, IPS y SBCs para analizar el tráfico e impedir cualquier tipo de ataque.
4. Utilizar filtros IP en los routers de borde y switches Capa3, para contrarrestar cualquier ataque malicioso que se pueda originar dentro de la organización y comprometa la red.
5. Usar túneles IPSec cuando sea necesario el cifrado por WAN y además siempre y cuando el sistema lo permita y soporte.
6. Deshabilitar puertos que no se están usando en los switches corporativos y reforzar las políticas de seguridad.
7. Apagar todos los servicios innecesarios o aplicaciones ejecutándose en servidores VoIP, firewalls, routers y otros dispositivos de la red VoIP.
8. Emplear direccionamiento IP estático en la red, o en el caso de usar IP dinámicas, utilizar un servidor DHCP diferente tanto para redes de VoIP como de datos.
9. Para el manejo de tiempos en la red, emplear un servidor (NTP), Network Time Protocol.
10. Restringir el acceso a la administración de dispositivos, usando ACLs y contraseñas.

2.10.6. *Recomendaciones de VOIPSA*

VOIPSA (Voice over IP Security Alliance) (Voipsa, 2005) es una asociación entre la industria de los individuos y organizaciones de los sectores de las comunicaciones VoIP y seguridad, fue fundada en el año 2005, y es una organización abierta sin fines de lucro, supervisa tres grupos de trabajo:

1. **Amenaza Taxonomía.** busca identificar y definir las amenazas actuales y potenciales de seguridad VoIP y educar a los miembros de la industria, los medios de comunicación y el público en general acerca de esas amenazas.

2. **Requisitos de Seguridad.** busca definir los elementos necesarios de diseño, software y hardware para asegurar las comunicaciones unificadas.

3. **Buenas Prácticas**. Define y recomienda prácticas de seguridad para proteger a la industria de las amenazas identificadas en la taxonomía.

Entre las recomendaciones para asegurar los sistemas de VoIP, se encuentran:

1. Identificar los dispositivos de la red VoIP y la infraestructura de soporte tanto externa como interna utilizando una combinación de técnicas de escaneo de UDP, TCP, SNMP e ICMP.
2. Usar reglas estándar en la implementación de firewalls y switches, para restringir los accesos a los servicios administrativos.
3. Modificar las contraseñas de administrador y nombres de usuario por defecto.
4. Deshabilitar los servicios no usados
5. Realizar periódicamente barridos de seguridad usando escaneos automáticos o manuales.
6. Implementar firewalls y/o IPS orientados específicamente a redes VoIP.
7. Asegurar tanto los dispositivos y servidores de la red VoIP, como la red de datos y su infraestructura de soporte.

CAPÍTULO III

3. METODOLOGÍA DE INVESTIGACIÓN

3.1. Diseño de la investigación

La presente Investigación se enmarca dentro del estudio **CUASI-EXPERIMENTAL**, ya que se trabaja con un grupo puntual elegido e igualmente se manipula una variable independiente. Los ataques que se realizaran en el escenario de pruebas, no serán tomados al azar, ya que se los analizará y definirá con anterioridad.

3.2. Tipo de estudio

Esta investigación es de tipo **Aplicada** puesto que se basa en los conocimientos existentes de la proponente y en material procedente de la investigación. También es de tipo **Descriptiva** ya que se genera un Modelo de Seguridad que permita mitigar ataques de Denegación de Servicio en tráfico SIP en servicios VoIP, para redes LAN corporativas.

3.3. Métodos, técnicas e instrumentos

En este apartado, se da a conocer los métodos, técnicas e instrumentos necesarios para el desarrollo de esta investigación, ya que a través de ellas, se recolectó información relevante para elaborar un proceso investigativo productivo y eficiente, y por consiguiente cumplir con éxito los objetivos planteados al inicio de esta investigación.

3.3.1. *Métodos de investigación*

En este punto, se describe los métodos teóricos-prácticos que se maneja en la investigación, los cuales ayudan a obtener información teórica y deducir la misma:

- **Método Científico**.- Mediante este método en la investigación se pudo buscar información en libros, revistas, artículos científicos e Internet, lo que da lugar a detectar los problemas

fundamentales, para lograr esta investigación, porque a través de estos se transmite las posibles soluciones del caso.

- **Método Analítico:** Este método se aplica durante la etapa de análisis donde se recopiló la información necesaria, para tener una idea clara, de lo que se va a realizar durante la investigación, es decir, se puntualiza que es lo que se debe hacer y cómo hacerlo, para determinar las vulnerabilidades SIP y los ataques a la que está expuesta la red de (VoIP), que comprometen la disponibilidad del servicio

- **Experimental:** Este método consiste en provocar voluntariamente una situación que se requiere estudiar, para modificar o alterar, es decir que se diseñan ambientes de simulación, para realizar las pruebas necesarias, y analizar los resultados obtenidos de modo que permitan determinar los mecanismos de defensa apropiados

3.3.2. *Técnicas*

Para el desarrollo del tema de investigación, el investigador requiere de ciertas técnicas y herramientas que ayuden en el proceso de realización de su estudio, a continuación se detallan las técnicas utilizadas, para acceder a información real y necesaria, para la construcción del presente trabajo de investigación.

- **Revisión de documentación:** Con la búsqueda de información en bibliotecas digitales y buscadores académicos, se obtuvo amplios documentos de aporte, entre los que se analizaron artículos científicos, libros, tesis desarrolladas dentro de la ESPOCH y fuera de ella, sitios web oficiales de herramientas actuales de seguridad, que permitieron obtener la información necesaria acerca del objeto de estudio de esta investigación.

- **Pruebas:** Mediante la simulación de un escenario de pruebas de red VoIP, que permita la ejecución de ataques y la aplicación del modelo de seguridad para su validación.

- **Observación:** Se observaron los resultados de las pruebas ejecutadas en el escenario para determinar un patrón de comportamiento, para posteriormente desarrollar el modelo de seguridad e implementarlo; para finalmente observar los resultados obtenidos con la implementación del modelo de seguridad en el escenario.

- **Encuestas:** A través de ellas se obtuvo información de diferentes instituciones públicas y privadas, con la finalidad de obtener la información de la frecuencia de uso del servicio y la importancia de la seguridad en el mismo (ver Anexo A).

3.3.3. *Instrumentos*

Aquí se detalla, las herramientas de seguridad y hacking, para la explotación de redes y sistemas de información. Los instrumentos para recopilar los datos de los indicadores son los siguientes:

- **Kali Linux:** Es una distribución avanzada de Linux, comúnmente usada para realizar pruebas de penetración y auditorías de seguridad.

- **Elastixs 2.5:** Es una aplicación software para crear sistemas de Telefonía IP, que integra las mejores herramientas disponibles para PBXs basados en Asterisk en una interfaz simple y fácil de usar.

- **SuperScan 7.0:** Es un potente escaner de puertos, realiza pings y resuelve nombres de dominio. Realiza todo tipo de operaciones de escaneo de puertos usando una IP o un fichero de texto del cual extraer las mismas. Es capaz de conectar a cualquier tipo de puerto que se descubra, usando aplicaciones apropiadas (Telnet, FTP, Web).

- **SIPVicious:** Es un conjunto de herramientas basado en Python, generalmente usados para comprobar sí la configuración SIP del servidor VoIP es segura. Esta se compone de:
    - **svmap:** Escanea una dirección IP o una serie de direcciones IP para averiguar si hay dispositivos SIP
    - **svwar:** Escanea una centralita PBX buscando el número de extensiones presentes y si están protegidas con contraseña
    - **svcrack:** Intenta obtener la contraseña de una extensión SIP en un servidor PBX

- **Sivus 1.10:** es una herramienta para Windows que permite crear diferentes tipos de mensajes SIP (INVITE, REGISTER, BYE, CANCEL, ACK, OPTIONS, NOTIFY, INFO, REFER). Sivus requiere JRE1.4 (Java Runtime Environment) y funciona en el sistema operativo Windows XP. Sivus no tiene soporte para otros sistemas operativos, además no es compatible con JREs actuales, sin embargo, su instalación se realiza a través de instrucciones del instalador sin mayor problema.

- **Hping3:** es una aplicación de terminal para Linux que permite analizar y generar fácilmente paquetes TCP/IP. A diferencia de un Ping convencional que se utiliza para enviar paquetes ICMP, esta aplicación permite el envío de paquetes TCP, UDP y RAW-IP.

- **InviteFlood:** Esta herramienta permite inundar un objetivo con peticiones INVITE con el objetivo de colapsarlos.

- **Wireshark 1 .12.7:** Es una herramienta multiplataforma usada para realizar análisis sobre paquetes de red.

3.4. Metodología para análisis de vulnerabilidades en redes VOIP

Todo proceso de investigación, requiere el apoyo de metodologías que guíen y respalden los procesos que se llevan a cabo, razón por la cual, se detallan las metodologías idóneas para esta investigación, por ser las más acordes y que cubren los puntos necesarios para dar cumplimiento a los objetivos de la presente investigación.

En este punto se analiza la metodología abierta de testeo de seguridad OSSTMM 2.1 y las técnicas de reconocimiento propuestas por (Endler & Collier, 2007) en su libro Hacking Exposed VoIP, ya que es un test práctico y eficiente de vulnerabilidades conocidas, filtraciones de información, infracciones de normas, estándares de la industria y prácticas recomendadas; y es ampliamente documentada.

OSSTMM es una metodología de testeo de seguridad que reúne diferentes pruebas y métricas de seguridad, empleadas por expertos durante las auditorías de seguridad; Es un conjunto de reglas y lineamientos para CUANDO, QUE y CUALES eventos son testeados. Se centra en los detalles técnicos de los elementos que deben ser probados, cuenta con seis secciones que son: Seguridad de la Información, Seguridad de los Procesos, Seguridad en las Tecnologías de Internet, Seguridad en las Comunicaciones, Seguridad Inalámbrica, y Seguridad Física. (Herzog P., 2003.).

Por otra parte (Endler & Collier, 2007) proponen tres ***Técnicas de Reconocimiento***, que son:

1. **Footprint a una red de VoIP:** consiste en recopilar toda la información disponible acerca de la red VoIP que se vaya atacar, con el fin de maximizar la eficacia y el impacto del ataque que se pretende realizar.

2. **Scanning a una red de VoIP**: una vez recopilada la información mediante el footprint, se investiga qué dispositivos son accesibles en la red, con el fin de identificar cuales sistemas y puertos se encuentran activos y visualizar todos los servicios que se ejecutan en cada uno.

3. **Enumeration a una red de VoIP**: su objetivo es aprovechar los servicios activos para obtener información sensible que puede ayudar en el lanzamiento de nuevos ataques

En este contexto y para efectos de la presente investigación, se realizó un análisis de la Metodología OSSTMM 2.1 y las Técnicas de Recopilación, explicadas anteriormente, puesto que encajan perfectamente en el estudio que se lleva a cabo, y aportaran en el desarrollo del Modelo de Seguridad; de las seis secciones que contiene dicha metodología, se escogen dos secciones denominadas:

- Seguridad en las Tecnologías de Internet.
- Seguridad en las Comunicaciones.

Puesto que la sección de Seguridad en Comunicaciones es la parte medular del estudio, y Seguridad en las Tecnologías de Internet, es la única sección de la metodología que contempla aspectos de testeo de seguridad para la tecnología de voz sobre IP. Los términos que aplica a los diferentes tipos de sistemas y de testeos de seguridad de redes, para el testeo de Seguridad en las Tecnologías de Internet son:

1. **Búsqueda de Vulnerabilidades:** hace referencia a las comprobaciones automáticas de un sistema o sistemas dentro de una red.

2. **Escaneo de la Seguridad:** generalmente son las búsquedas de vulnerabilidades, estas incluyen la verificación manual de falsos positivos, la identificación de puntos débiles de la red y el análisis profesional especificado.

3. **Test de Intrusión:** son las pruebas orientadas hacia un objetivo, con la finalidad de lograr tener accesos privilegiados con medios pre-condicionales.

4. **Evaluación de Riesgo:** hace referencia a los análisis de seguridad en la organización.

5. **Auditoría de Seguridad:** se refiere al examen manual con privilegios administrativos del sistema operativo y de los programas de aplicación del sistema o sistemas dentro de una red o redes.

6. **Hacking Ético:** generalmente son los tests de intrusión, su objetivo es obtener logros en la red dentro de un tiempo predeterminado de duración del proyecto.

7. **Test de Seguridad y su equivalente militar, Evaluación de Postura,** es una evaluación de riesgo, mediante la aplicación de análisis experto mediante escaneos de seguridad donde la intrusión se usa generalmente para confirmar los falsos positivos y los falsos negativos dentro del tiempo permitido de duración del proyecto.

3.5. Propuesta del modelo de seguridad

En este apartado se define el Modelo de Seguridad contra ataques de Denegación de Servicio (DoS) de tráfico SIP en servicios VoIP, que se lo denominará MODELO DE SEGURIDAD **MS-DoS-SIP**, para lo cual se ha establecido algunos mecanismos de defensa orientados a mitigar las vulnerabilidades SIP identificadas anteriormente, con la finalidad de reducir el riesgo de caer en cualquiera de estos ataques.

Esta guía le proporcionará una introducción sobre las herramientas y técnicas que se deben implementar para brindar seguridad a plataformas de Voz sobre IP, basadas en SIP. El modelo de seguridad establece 4 etapas, que son:

Figura 1-3: Modelo de Seguridad MS-DoS-SIP
Fuente: Arellano Karina, 2016

Como se observa en la Figura 1-3, estas etapas deben desarrollarse en forma cíclica ya que cada etapa dependerá de la anterior, creando un ciclo constante sobre la red VoIP de la organización. El desarrollo de estas etapas dependerá de las tecnologías, protocolos y dispositivos utilizados, ya que no todos los dispositivos cuentan con todos los sistemas de seguridad mencionados en este Modelo de Seguridad. Se detallan cada una de las etapas que componen el Modelo de Seguridad.

3.5.1. *Etapa 1. Reconocer la red de VOIP*

El primer paso para atacar una red de VoIP es investigar el objetivo, utilizando la información que esté disponible. En la mayoría de los casos, el éxito del ataque depende de la cantidad de información reunida acerca del objetivo. Si la información ha sido reunida correctamente y con todo detalle, el acceso los sistemas es garantizado.

Por lo indicado anteriormente es de trascendental importancia conocer a profundidad qué tipo de información puede adquirir el atacante y tomar acciones que permitan minimizar el posible daño. Para conseguir éxito en esta etapa se sugiere:

1. Realizar un **FOOTPRINT** de la red de Voz, para ellos se recomienda:

    a) Identificar todos los recursos de la organización; físicos, lógicos, técnicos, internos y externos que utilizan los servicios de comunicación de VoIP
    b) Implementar un software de descubrimiento y monitoreo de red basado en SNMP.
    c) Documentar y respaldar la información obtenida, mediante un registro detallado.

2. Realizar un **SCANNING** de la red de Voz, mediante:

    a) Uso de herramientas especializadas en escaneo de redes y escaneo de puertos que permitan obtener información sensible sobre los puertos, servicios y sistemas operativos que se están ejecutando.
    b) Listar las vulnerabilidades localizadas, para lo cual se sugiere obtener el puerto, servicio y estados.

3. Realizar un **ENUMERATION** de la red de Voz:

    a) Usar herramientas y comandos que permitan buscar agujeros de seguridad en la red de Voz

Básicamente esta etapa se refiere a sondear la red para determinar sus vulnerabilidades, la identificación del diseño de la red de VoIP (topología, mapa, direccionamiento IP, etc), protocolos señalización, y todos los dispositivos hardware y software que conforman la red de VoIP (softphones, SO, configuración y características de dispositivos), Sistemas Operativos, etc.

3.5.2. *Etapa 2. Identificar vulnerabilidades SIP y valorar el impacto en la disponibilidad*

Se determina las ***vulnerabilidades y fallos de seguridad*** comúnmente usadas para causar daños en la infraestructura de voz sobre IP basada en SIP. En la Tabla 1-3, se observa la lista de vulnerabilidades más relevantes en ambientes VoIP. Asimismo, se visualiza el impacto que causa cada en la infraestructura de voz sobre IP.

Tabla 1-3: Lista de Vulnerabilidades e Impacto en el servicio VoIP

VULNERABILIDADES Y FALLOS DE SEGURIDAD	IMPACTO		
	BAJO (1)	MEDIO (2)	ALTO (3)
Red Homogénea		x	
Falta de Segmentación de la Red		x	
Password débiles			x
Puertos abiertos innecesarios			x
Puertos conocidos			x
Servicios habilitados innecesarios			x
Configuraciones débiles			x
Ancho de banda bajo		x	
Poca disponibilidad de recursos		x	
Falta de Autenticación			x
Ausencia de Firewall SIP			x
Falta de Sistemas de Seguridad (IDS/IPS/SBC)			x
Falta de Actualizaciones y parcheo		x	
Enumeración de dispositivos SIP habilitada			x
Permisos de escaneo de usuarios SIP habilitado			x
Protocolo SSH sin protección			x
Permiso de solicitudes concurrentes ilimitado			x
Teléfonos SIP habilitado TFTP, DCHP, TELNET		x	
Ausencia de Auditorias y Bitácoras		x	

Realizado por: Arellano Karina, 2016
Fuente: Adaptado de (Sisalem et al., 2006)

Puesto que este Modelo de Seguridad, se enfoca solo en amenazas de Denegación de Servicio de sistemas de VoIP basados en *SIP*, se determinan y clasifican las principales ***amenazas*** que afectan con mayor criticidad a la disponibilidad del servicio. La Tabla 2-3, muestra un listado de amenazas que comúnmente atentan contra la disponibilidad de sistemas VoIP, con su respectiva probabilidad de ocurrencia que está dado por la popularidad, es decir la frecuencia con la que se estima que ocurra el ataque, y el grado de severidad en las consecuencias, considerando el daño potencial causado por la ejecución del ataque con éxito.

Tabla 2-3: Amenazas de Seguridad de VoIP-Denegación de Servicio

Amenaza	Ataque	Popularidad	Impacto	Estimación del Riesgo
Fuzzing	Malformación de Mensajes	Poco Frecuente	Intolerable	Importante
Flooding	Floods INVITE to SIP Proxies (Usando inviteflood Tool)	Moderadamente Frecuente	Extremadamente Intolerable	Muy Importante
Flooding	Floods INVITE to SIP Phone (Usando inviteflood Tool)	Medianamente Alta	Intolerable	Muy Importante
Flooding	Flood Register	Moderadamente Frecuente	Intolerable	Importante
Manipulación de la Señalización	Eliminación de Registros	Frecuente	Ligeramente Importante	Importante
TCP SynFlood	SynFlood DoS	Medianamente Alta	Intolerable	Intolerable

Realizado por: Arellano Karina, 2016
Fuente: (Endler & Collier, 2007)

Generalmente las vulnerabilidades que se explotan para llevar a cabo las amenazas de SIP, y por consecuente afectar al normal rendimiento del servicios de VoIP, se detalla en la Tabla 3-3, y se expone su posible solución.

Tabla 3-3: Vulnerabilidades explotadas vs. Amenazas efectuadas

VULNERABILIDAD	POSIBLE ATAQUE A LA SEGURIDAD SIP	POSIBLE SOLUCION
Falta de Autenticación	- *Floods* sobre sentencias *SIP (INVITE, BYE,* REGISTER *y CANCEL)*	TLS
Ausencia de Firewall SIP / Firewall deshabilitado	- Mensajes con formato incorrecto (*fuzzing*) - *Floods* sobre sentencias *SIP (INVITE, BYE, REGISTER y CANCEL)* - Eliminación de Registros - SYN Flood Dos	Configurar Firewall
Puertos conocidos	Ataques pre-diseñados a puertos específicos. - Floods sobre sentencias SIP (INVITE, BYE, REGISTER y CANCEL) - Malformación de Mensajes (Fuzzing) - Eliminación de Registros	Cambiar puertos conocidos
Falta de Segmentación de la Red	- SYN Flood - *Floods* sobre sentencias *SIP (INVITE, BYE, REGISTER y CANCEL)*	Configurar VLANs de Datos y de Voz

	- Eliminación de Registros	
Falta de Sistemas de Seguridad (IDS/IPS/SBC)	- Mensajes con formato incorrecto (*fuzzing*)	Implementar una plataforma de seguridad
Configuraciones Débiles	- Mensajes con formato incorrecto (*fuzzing*)	Autenticación
Enumeración de dispositivos SIP habilitada	- *Floods* sobre sentencias *SIP (INVITE, BYE, REGISTER y CANCEL)* - Mensajes con formato incorrecto (*fuzzing*) - Eliminación de Registros	Configuración de reglas de acceso en Firewall
Permisos de escaneo de usuarios SIP habilitado	- *Floods* sobre sentencias *SIP (INVITE, BYE, REGISTER y CANCEL)* - Eliminación de Registros	Corregir archivo sip.conf
Poca seguridad en terminales (Softphones o Teléfonos)	- SYN Flood - *Floods* sobre sentencias *SIP (INVITE, BYE, REGISTER y CANCEL)}* Mensajes con formato incorrecto (*fuzzing*) - Eliminación de Registros	Deshabilitar TFTP, y TELNET en clientes SIP

Realizado por: Arellano Karina, 2016

Es así que mediante el uso de las Tablas expuestas anteriormente, se podrán identificar con certeza, con que vulnerabilidades cuenta nuestra red, y los posibles ataques de los que probablemente seamos víctimas.

3.5.3. *Etapa 3. Examinar la seguridad de la red VOIP*

Existen interrupciones en el servicio de VoIP que no se producen necesariamente por ataques de intrusos, para ellos hay algunos síntomas a tener en cuenta para la identificación de un ataque de denegación de servicio (DoS). Por ejemplo si la red estuviera funcionando en forma mucho más lenta de lo habitual, el servicio no estuviera disponible, o si se recibe una enorme cantidad de peticiones, probablemente es víctima de un ***ataque de denegación de servicio***.

En este sentido es importante establecer ciertas recomendaciones a la hora de diagnosticar si nuestra red está siendo víctima de un ataque de DoS en el servicio de VoIP, para ello el Modelo de Seguridad recomienda:

1. **Monitorizar Recursos**

Para determinar si se está siendo víctima de un ataque se deben recoger los datos de utilización de recursos como CPU, memoria, tráfico de red, disco, etc, de los equipos implicados en la red VoIP y compararlos con los valores "normales" que suele tener el servicio. Se sugiere:

1. Implementar herramientas de monitoreo de red en tiempo real, que permita monitoreo proactivo tanto de la infraestructura de equipos y servidores así como de la red de datos en tiempo real.
2. Definir un baseline del consumo de recursos en condiciones normales de operación del servidor VOIP, monitoreando el consumo de CPU, memoria y disco.
3. Instalar el agente de SNMP en el servidor de VOIP para monitorear los recursos del host y recolectar los datos de rendimiento.
4. Especificar umbrales y configurar alertas basadas en umbrales para cada monitor de recursos. Cuando estos patrones se superen se debe generar una alarma. Cuando:
    - El porcentaje de uso de CPU alcanza el 70%, cambiar el estado a ***WARNING*** y enviar un correo electrónico.
    - El porcentaje de uso de CPU alcanza entre 80% - 100%, cambiar el estado a ***CRÍTICO*** y enviar un correo electrónico y sms.
    - El porcentaje de uso de la Memoria sea mayor al 90%, generar un ***WARNING*** y enviar un correo electrónico o sms.

Generalmente los ataques por flooding tienden a consumir muchos recursos. Si el consumo de nuestro servidor VoIP recae sobre los umbrales especificados, se podría sospechar de un ataque basado en "inundación".

2. **Supervisar el Tráfico SIP de la red VoIP**

Explorar y analizar el tráfico de la red VoIP permite identificar desde ataques de fuerza bruta dirigidos a usuarios SIP hasta detectar spam de telefonía por Internet (SPIT). Esto es posible, mediante el empleo de sniffers y/o analizadores de protocolos. En esencia, los analizadores de protocolos capturan y almacenan los datos que viajan por la red. Es posible detectar un ataque de ***fuzzing*** por medio de analizadores de protocolos, puesto que el paquete enviado por este tipo de ataque los suele reconocer como paquetes ***"malformed packet".*** También permiten detectar

ataques de ***flooding***, ya que si se observa que la red recibe peticiones masivas de mensajes SIP (INVITE, REGISTER, BYE), posiblemente sea víctima de ataques por fuzzing y flooding.

Se recomienda generar una tarea que permita automatizar el proceso de identificación de anomalías en la red.

1. Generar un Script en el servidor de VoIP que permita capturar paquetes de la red por background, mediante la utilización del comando ***tcpdump***
2. Las capturas deberán actualizarse cada cierto tiempo, de preferencia cada 40 mins
3. Guardar los paquetes capturados, para futuros análisis.
4. El archivo guardado puede ser visto por el mismo comando tcpdump. También se puede utilizar el software de código abierto Wireshark para leer los archivos ***tcpdump pcap.***
5. Buscar la cadena ***"malformed packet"*** y/o identificar si existe más de 1000 mensajes ***"INVITE", "REGISTER" o "TCP SYN"*** en el archivo ***tcpdump pcap.***
6. Configurar una ***alerta***, para ser enviada en cuanto se encuentre dicho parámetro

Así mismo se sugiere:

1. Implementar una herramienta de Monitoreo de tráfico SIP, RTCP y RTCP-XR
2. Obtener capturas actualizadas constantemente
3. Realizar búsquedas de llamadas y paquetes SIP fácilmente aplicando diferentes filtros como tiempos, Call-id, método SIP, IP origen, IP destino, etc
4. Descargar el contenido en un archivo pcap o txt (opcional)
5. Configurar el sistema de alarmas para detectar y alertar de ciertos errores o ataques a SIP (por ejemplo, los paquetes enviados desde SIPVicious).
6. Contabilizar ciertos paquetes (403, 482, *spoofing*…) y configurarlo para que al superar un umbral, sea notificado vía email. Esto nos puede alertar de funcionamientos anómalos de nuestros sistemas, pudiendo detectarlos rápidamente.
7. Presentar reportes gráficos, acelerando el descubrimiento de posibles irregularidades como problemas de audio de una llamada, jitters o pérdidas de paquetes.

3. **Monitorear y Analizar Logs**

El análisis de ***logs*** puede revelar información trascendente para la operación del servicio de telefonía IP, como alertar sobre la posible sospecha de un ataque por Floodig (Invite, Bye, Cancel y Register), Malformación de mensajes, Manipulación de la Señalización SIP, Ataques de fuerza bruta, Enumeración, etc. Con la ayuda de un software que escanea los logs de los equipos en búsqueda de repetidos intentos de autenticación fallida y bloqueando de forma automática dicha IP, de tal forma que la IP del atacante será bloqueada después de cierto número de intentos no permitiéndole así adivinar o descifrar las contraseñas. Para ello se sugiere:

1. Implementar software para escaneo y análisis de logs
2. Configurar parámetros para que analice los logs que se desea y bloque IP,s
3. Enviar notificaciones vía e-mail.

3.5.4. *Etapa 4. Aplicar medidas de seguridad*

En esta etapa del Modelo da seguridad a nivel de la red VoIP, para así mitigar en gran cantidad las vulnerabilidades existentes. Se recomienda ciertos mecanismos de seguridad adecuados, que garantizan la protección de los sistemas de telefonía IP basados en SIP, ante ataques de Denegación de Servicio, específicamente para flooding y fuzzing. Se recomienda:

1. **Segmentar la red**

Diseñar la red de comunicaciones independiente tanto para el servicio de voz como para el servicio de datos a través VLANS. Puesto que es una técnica muy eficiente para prevenir ataques que afectan la disponibilidad de los servicios de VoIP. Es por eso que las VLANs son de gran utilidad para la protección de ataques que afectan comúnmente la red de datos y que influyen directamente en los servicios de telefonía IP, tales como gusanos, virus, denegaciones de servicio, Syn Floods, etc. Además, previene ataques de Secuestro de Sesiones (Call Hijacking) y Espionaje de llamadas (Call Eavesdropping). Incluso en el caso del éxito de un ataque, los daños causados serian mínimos.

2. **Evitar utilizar puertos estándares**

Generalmente, los puertos SIP por defecto de la mayoría de los teléfonos y softphones son el 5060 y 5070. Por esto, muchas herramientas de penetración dirigen sus ataques hacia estos puntos de acceso. De forma que, si se cambia la configuración de los mismos, es posible que muchas de estas aplicaciones no logren su objetivo.

3. **Mantener los sistemas actualizados y parchados**

Es totalmente imprescindible, y no solo en infraestructura VoIP, que el administrador de la red esté al corriente de los nuevos parches y actualizaciones y los aplique en sus sistemas. Es recomendable:

1. Incorporar al sistema organizacional de administración y actualización de parches de seguridad y manejo centralizado de antivirus para todos los equipos y servidores utilizados para la implementación de soluciones VoIP.
2. Habilitar las actualizaciones automáticas de cada aplicación, ya que las mismas cubren nuevos huecos de seguridad que han sido descubiertos por el fabricante.

4. **Implementar TLS para las conexiones SIP**

Hay que tener en cuenta que para que una llamada sea segura, se debe emplear TLS para todas las conexiones entre las terminales SIP que participan en la llamada. Hay que considerar que si algunos teléfonos SIP utilizan TLS, pero otros no lo hacen, entonces el modelo de seguridad se rompe. Se recomienda la Configuración de las características TLS, desactivando los cifrados inseguros. (Ver Anexo 3), entonces el establecimiento de la comunicación segura se da en 3 etapas:

1.- Los extremos al iniciar la comunicación negocian el algoritmo de cifrado que van a ejecutar.

2.- Se realiza el intercambio de llaves y se acuerda los algoritmos de firma.

3.- Una vez establecida la comunicación, se emplean los algoritmos tanto de clave simétrica para cifrar como el de firma.

5. **Utilizar Firewall SIP**

El uso de Firewall SIP, es una práctica muy eficiente para detectar y mitigar varios ataques a los sistemas de VoIP. Esta tecnología permite examinar todas las señales enviadas al proxy SIP

protegiendo las aplicaciones VoIP de ataques específicos al protocolo SIP, tales como mensajes con formato incorrecto (fuzzing), floods sobre sentencias SIP (INVITE, BYE, REGISTER y CANCEL), secuestro de sesiones (hijacking), espionaje (eavesdropping) y redirección de llamadas. Estos tipos de ataques son complicados de manejar, ya que dispositivos de seguridad perimetral como Firewalls, UTMs o IPSs, no pueden repeler estos ataques con bloqueos tradicionales; por el contrario, es necesario usar equipos especializados para desviarlos. Estos dispositivos pueden ser proporcionados por diversos proveedores tales como: SecureLogix, Sipera, Elastix, Ingate, entre otros.

6. **Usar IPTABLES**

Se sugiere Configurar reglas de ingreso y salida de paquetes de voz sobre los equipos de la red VoIP. (Ver Anexo 4).

7. **Implementar un SBC (Session Border Controller)**

El uso de un Firewall en redes VoIP no es suficientes, por esto que se recomienda usar un SBC (Controlador de Borde de Sesión) en la red VoIP, puesto que un SBC diferencia el tráfico de voz al entrar en la red, lo que no hace un firewall ya que no reconoce este tipo de tráfico; cabe indicar que a pesar de que los dos son muy necesarios en una red de datos, el SBC es específicamente para redes Voz sobre IP. Este es un dispositivo de seguridad de borde que generalmente se ubica entre red LAN, y el ISP. Además un SBC vigila el tráfico SIP en tiempo real entre las fronteras de las redes basadas en SIP, lo que garantiza la seguridad de la red privada.

8. **Asegurar Terminales (Softphones o Teléfonos)**

Se recomienda desactivar TFTP y Telnet, ya que generalmente los teléfonos SIP hacen solicitudes TFTP para actualizar archivos de configuración y firmware. TFTP es insegura ya que los archivos se envían sin cifrar. También se debe desactivar NAT en las extensiones que no son remotas y como última recomendación configurar contraseñas robustas.

9. Otras Recomendaciones:

1. No usar nombres por defecto para archivos de configuración
2. Limitar el acceso a la ubicación de los equipos y servidores
3. Cambiar el password por defecto de TODOS los equipos y dispositivos que conforman la red VoIP.
4. No aceptar pedidos de autenticación SIP desde cualquier dirección IP.
5. Rechazar los pedidos de autenticación fallidos utilizando nombres de extensiones válidas con la misma información de un rechazo de usuario inexistente.
6. Utilizar claves SEGURAS para las entidades SIP.
7. Usar nombres de usuarios SIP diferentes que sus extensiones.

CAPITULO IV

4. RESULTADOS Y DISCUSIÓN

En este Capítulo, se analizan y comparan los resultados obtenidos en las pruebas ejecutadas en los escenarios establecidos, con la implementación del Modelo de Seguridad propuesto y sin ella, y se comprueba la hipótesis planteada.

4.1. Ambientes de prueba (arquitectura, hardware, software)

Para efectos de esta investigación se ha simulado la red de Voz sobre IP de una organización, puesto que las pruebas de testeo de la seguridad se las realiza en la red en producción, y no es posible hacerlas debido a políticas internas de la organización de salvaguardar la disponibilidad del servicio; para el diseño de la red simulada usó el software de simulación de redes GNS3 versión 1.4.5; que es una aplicación que permite generar escenarios prácticos muy similares a los reales. La figura 1-4 muestra la red simulada.

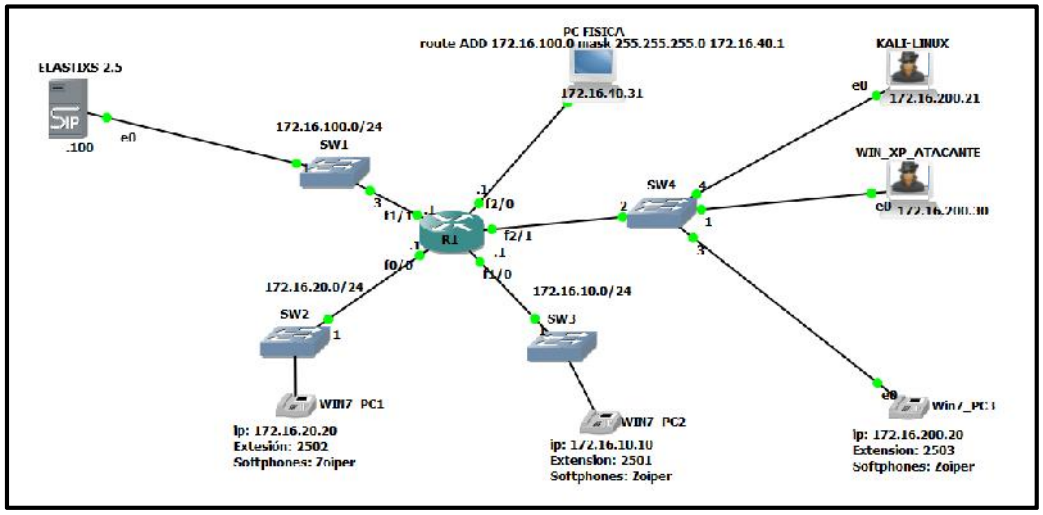


Figura 1-4: Escenario Simulado de pruebas
Realizado por: Arellano Karina, 2016

En la etapa de Reconocimiento de Red es necesario la recopilación de la información del Ambiente de Pruebas, tanto información específica como detallada de algunos componentes

como la topología de la red, mapa de red, direccionamiento IP, softphones, sistemas operativos, configuración y características de cada equipo que conforman la red.

4.1.1. *Footprint*

Se busca obtener la mayor información disponible acerca de la red VoIP que está siendo vulnerable. En este caso mediante el uso de la herramienta de monitoreo ***PRTG Network Monitor***, se obtuvo las características de la infraestructura de comunicaciones de VoIP, presentes en el escenario:

a) 1 central telefónica con Elastixs 2.5 como proveedor de servicio de telefonía IP, ya que es una distribución libre de Servidor de Comunicaciones Unificadas, su servicio es bastante estable y confiable,

b) 4 clientes SIP con Zoiper, que es un softphone gratuito y muy conocido que permite simular teléfonos IP en los computadores, y también Talk Express Softphone en su versión no comercial.

c) 1 router y 4 Switch capa 2.

Se identifica los dispositivos empleados en la red VoIP simulada, como el modelo si es hardware y se identifica la versión en el caso de software. Las características de los equipos y dispositivos de la red de telefonía IP se describen en la Tabla 1-4.

Tabla 1-4: Listado de dispositivos de red Simulada

Hardware	Marca, Modelo y Versión Software
Teléfonos	Sistema Operativo: Microsoft Windows 7 de 64bits, Procesador: Intel® Core™ i5-5200U CPU @ 2.20Ghz, Memoria RAM: 512 Mb
Central Telefónica Virtual PC´s (VirtualBox)	Sistema Operativo: Centos, Elastixs2.5, Memoria RAM: 1024 MB, Procesador: Intel® Core™ i5-5200U CPU @ 2.20Ghz
Switch	Marca: Cisco, Modelo: 2960, Número de Puertos: 8 puertos no administrables, Transferencia: 10/100 Mbps Full Duplex, autodetect.
Router	Cisco, Modelo 7200, Versión del IOS c7200-advipservicesk9-mz.124-4.T1
Zoiper	Zoiper 3.9.32144 32bits, Revisión de la librerai:32121
Express Talk	Version 4.35 Licensed User: Unlicensed Basic Free Version
Elastixs	Versión 2.5

Realizado por: Arellano Karina, 2016

4.1.2. *Scanning*

Ahora una vez obtenida la información acerca de la red, se identifica la información sensible que se encuentran en la red VoIP, como los puertos y servicios habilitados en los componentes de la misma, para esto se hizo uso del software de escaneo de red **NetScan** del cual se obtuvo una lista de los equipos accesibles en la red; concentrándonos en los puertos UDP/TCP 5060 y 5061 debido a SIP permite a los dispositivos a utilizar estos puertos.

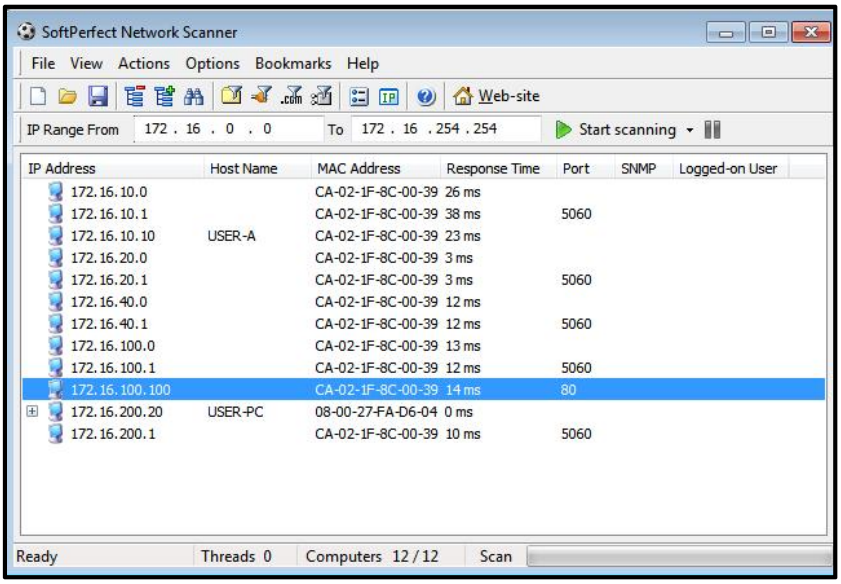


Figura 2-4: Escaneo de IPs con NetScan
Fuente: Arellano Karina, 2016

Se refinó la búsqueda con la herramienta **Nmap**, para obtener mayor información, y se realizó otra exploración intensa para identificar los sistemas operativos que se ejecutan y los servicios; el objetivo es encontrar la información sensible que se muestra en la red.

Figura 3-4: Escaneo con Nmap
Realizado por: Arellano Karina, 2016

En la Figura 4-4, se observa que se ha detectado que el sistema operativo con el que está operando la central telefónica es Linux 2.6.x. y está bajo Elastixs.

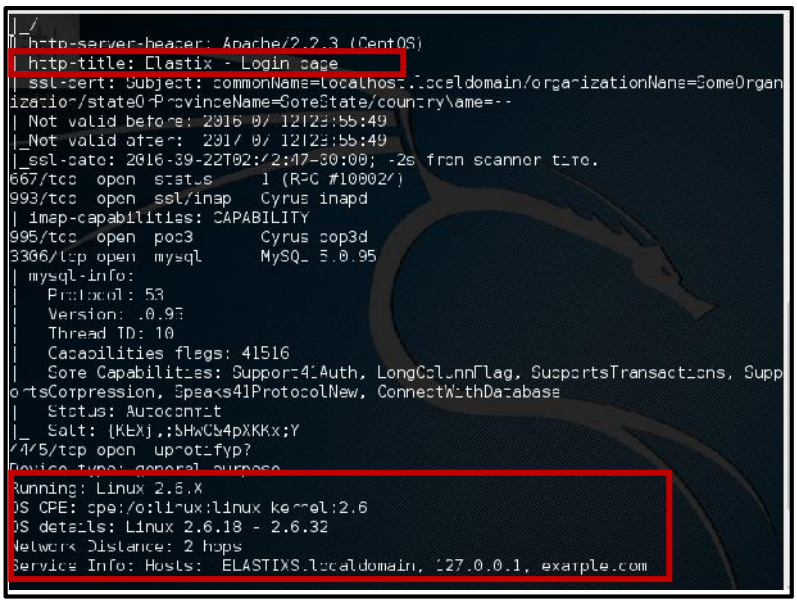


Figura 4-4: Escaneo de puertos y servicios con Nmap
Realizado por: Arellano Karina, 2016

En la Figura 5-4 se observa que los clientes SIP están operando bajo Microsoft Windows 7.

Figura 5-4: Escaneo de puertos y servicios con Nmap
Realizado por: Arellano Karina, 2016

Finalmente se escanea el tráfico y se confirma la información con respecto a los puertos que utilizan el protocolo SIP para cada una de las máquinas del ambiente de pruebas, mediante la ejecución de Wireshark, que es un potente analizador de tráfico.

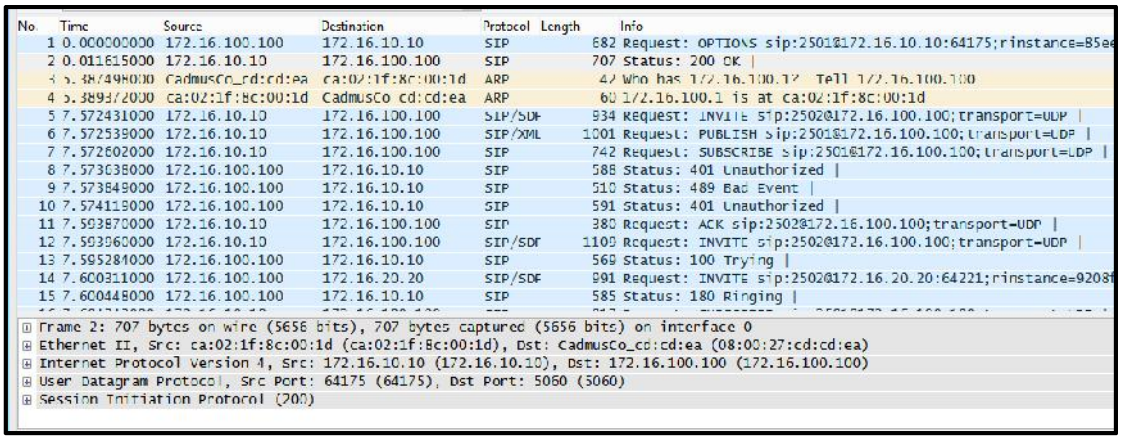


Figura 6-4: Escaneo de puertos con Wireshark
Realizado por: Arellano Karina, 2016

4.1.3. *Enumeración*

En esta etapa se seleccionan los host que probablemente serían atacados mediante la detección de los servicios activos para obtener información sensible que puede ayudar en el lanzamiento de ataques. Hasta el momento, tres máquinas han sido identificadas:

172.16.100.100 (posible servidor SIP)

172.16.10.10 (puede ser cliente SIP, deberá confirmar)

172.16.20.20 (probablemente cliente SIP)

172.16.200.20 (posible cliente SIP)

Pues bien, ahora se ejecuta la herramienta **Svmap** de grupo de herramientas de SIPVicious, ya que esta utilidad permite escanear una dirección IP o una serie de direcciones IP para averiguar si hay dispositivos SIP dentro de la red; comúnmente usada para enumerar servidores VoIP y sus clientes.

La Figura 7-4 muestra la primera enumeración realizada mediante **svmap** al rango de IPs dentro de la red 172.16.0.1-172.16.255.255, en la que se identifica que la IP 172.16.100.100 es el servidor VoIP.

Figura 7-4: Enumeración con svmap
Realizado por: Arellano Karina, 2016

Además mediante el módulo de Metasploit se comprueba que la IP 172.16.100.100, usa SIP por el puerto 5060.

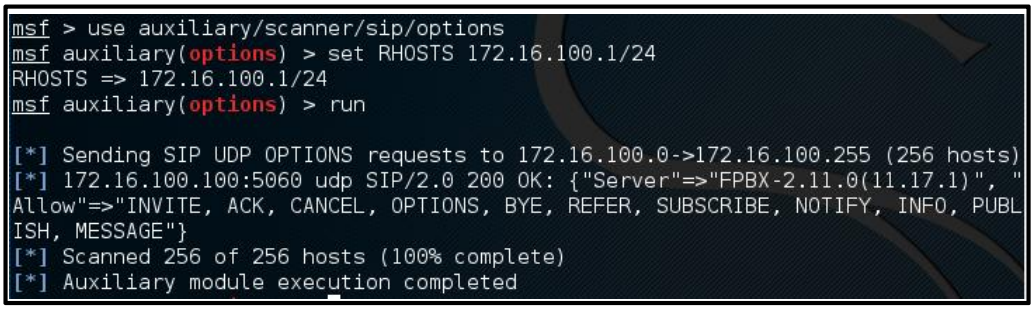


Figura 8-4: Enumeración con Metaexploit
Realizado por: Arellano Karina, 2016

Ahora obtenemos información del software que se ejecuta, su proveedor, y la versión, en la que se confirma que las IPs de los posibles clientes identificados anteriormente, tienen instalado Zoiper Versión 3.9.32144 (softphone) y Express Talk Versión 4.35.

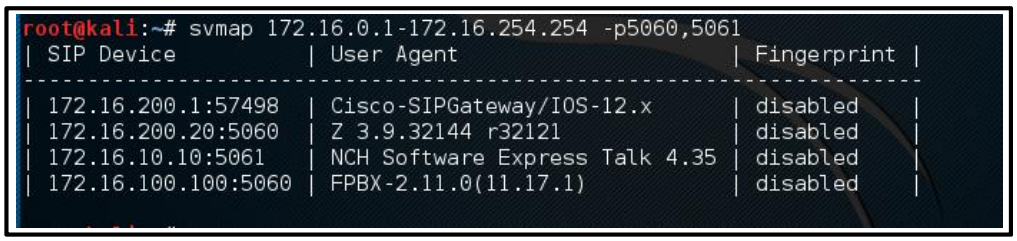


Figura 9-4: Enumeración con SIPVicious
Realizado por: Arellano Karina, 2016

Hasta ahora, se ha confirmado dos IPs (172.16.100.100 | 172.16.10.10), uno es el servidor mientras que el otro es un cliente. Otra máquina sospechosa fue descubierta en el paso anterior, pero no se ha confirmado todavía. Vamos a enviar el paquete INVITE a la máquina:

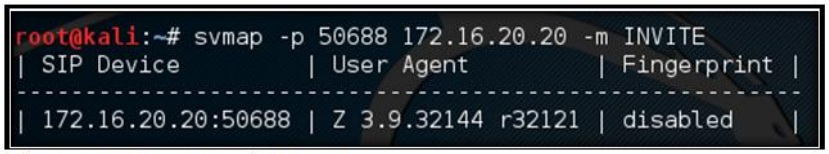


Figura 10-4: Mensaje INVITE
Realizado por: Arellano Karina, 2016

Finalmente se confirma que las máquinas sospechosas son clientes SIP.

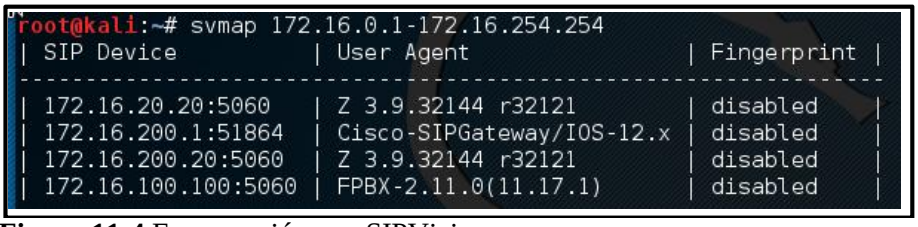


Figura 11-4 Enumeración con SIPVicious
Realizado por: Arellano Karina, 2016

Al finalizar la enumeración con svmap, se obtiene que las direcciones IP, corresponden a:

172.16.100.100 (servidor VoIP)
172.16.10.10 (Cliente, ExpressTalk)
172.16.20.20 (Cliente, Zoiper)
172.16.200.20 (Cliente, Zoiper)

Una vez que se confirma que tipo de información que está al alcance de intrusos, es importante también verificar si es posible obtener las extensiones de usuario o plan de marcación de esta red. La enumeración de usuarios es crucial mientras se ataca a la red de VoIP, para esto se intercepta el tráfico SIP usando el software Wireshark y se analiza los

paquetes para conseguir las extensiones de los usuarios. En la cabecera de cada paquete se muestran las extensiones de emisor y receptor, mediante el análisis de la cabecera, se han identificado dos extensiones: 2501 y 2502.

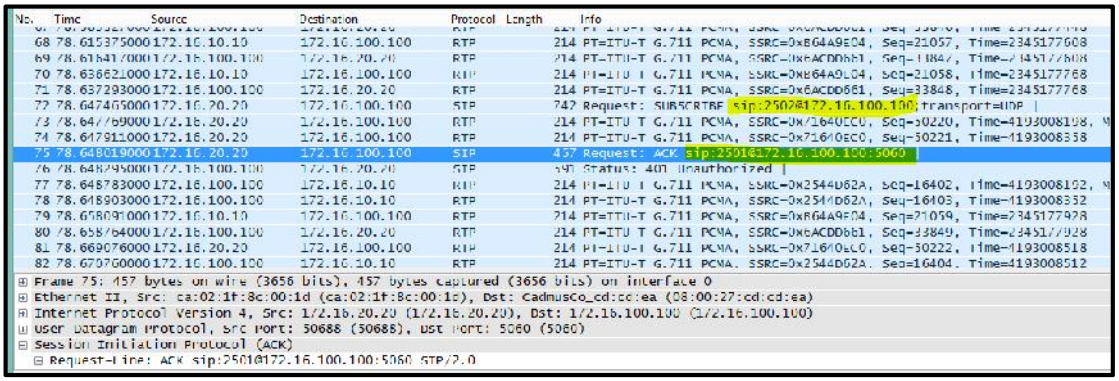


Figura 12-4: Análisis de paquetes SIP
Realizado por: Arellano Karina, 2016

Además se usó la herramienta **Svwar**, puesto que permite mostrar la numeración de las extensiones de una PBX. Como se observa en la Figura 13-4, y se obtiene las extensiones usadas en el escenario de pruebas como se muestra en la Figura 14-4.

```
root@kali:~# svwar -m INVITE --force 172.16.100.100
```

Figura 13-4: Enumeración con Svwar
Realizado por: Arellano Karina, 2016

Extension	Authentication
2503	reqauth
2502	reqauth
2501	reqauth

Figura 14-4: Obtención de Extensiones de un PBX
Realizado por: Arellano Karina, 2016

En la etapa de identificación de vulnerabilidades en el ambiente de pruebas se realiza un breve escaneo de posibles vulnerabilidades, mediante el uso de escáner, herramientas de hacking y exploits actualmente utilizadas. A través de la herramienta ***Zenmap***, se obtuvo información sensible sobre los puertos, servicios y sistemas operativos que se están ejecutando.

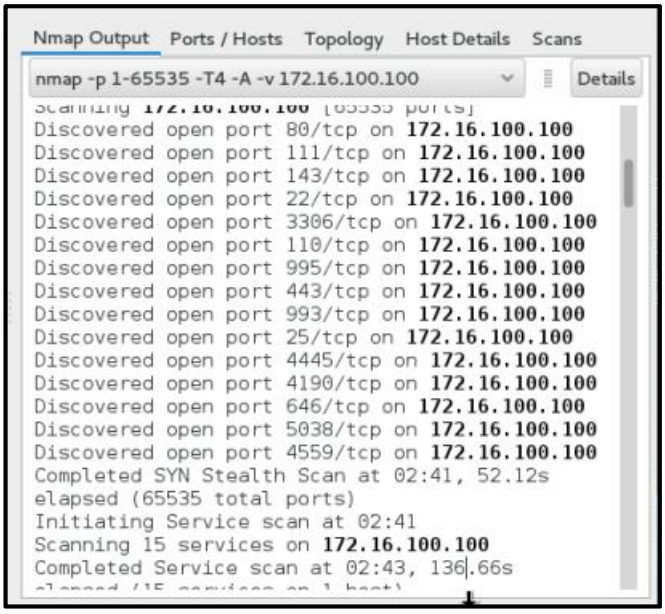


Figura 15-4: Búsqueda de Vulnerabilidades con Zenmap
Realizado por: Arellano Karina, 2016

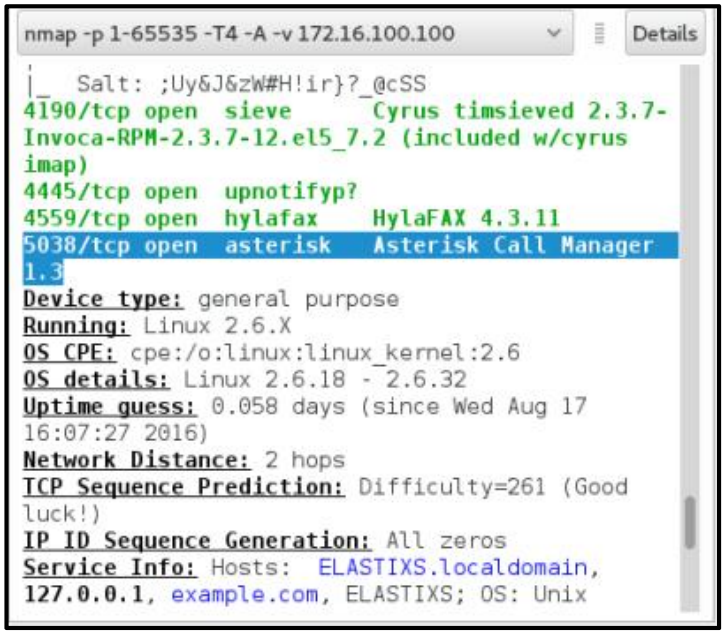


Figura 16-4: Identificación de puerto de Asterisk con Zenmap
Realizado por: Arellano Karina, 2016

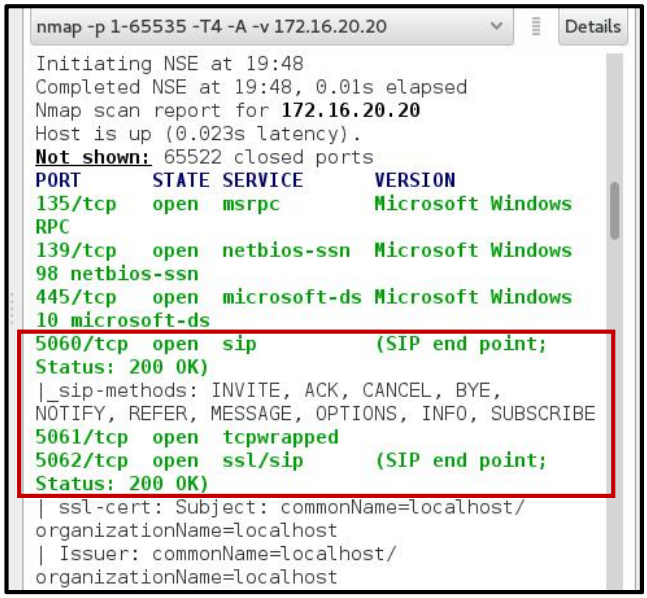


Figura 17-4: Escaneo de puertos SIP en clientes
Realizado por: Arellano Karina, 2016

Finalmente al desarrollar las actividades anteriores se encontraron ciertas vulnerabilidades presentes en el ambiente de pruebas, que se describen en la Tabla 2-4, las mismas que se darán tratamiento con la implementación del Modelo de Seguridad Propuesto.

Tabla 2-4: Vulnerabilidades localizadas en el ambiente de pruebas

N°	Vulnerabilidad
1	Puertos abiertos innecesarios
2	Enumeración de dispositivos SIP habilitada
3	Permisos de escaneo de usuarios SIP habilitado
4	Configuraciones Débiles
5	Falta de Segmentación de la Red
6	Uso de puertos por defecto
7	Servicios habilitados innecesarios
8	Falta de Autenticación
9	Ausencia de Firewall
10	Falta de Sistemas de Seguridad
11	Falta de Actualizaciones y parcheo en sistemas VoIP
12	Terminales SIP Inseguras
13	Protocolo SSH sin protección

Realizado por: Arellano Karina, 2016

De la misma manera en la Tabla 3-4, se listan los ataques que serán objeto de estudio en la presente investigación y que permitirán tomar las correctas medidas de seguridad para mitigarlas.

Tabla 3-4: Ataques a SIP en Ambiente de Pruebas

Amenaza	Ataque
Fuzzing	Malformación de Mensajes
Flooding	Floods INVITE to SIP Proxies (Usando inviteflood Tool)
Flooding	Floods INVITE to SIP Phone (Usando inviteflood Tool)
Manipulación de la Señalización	Eliminación de Registros
TCP SynFlood	SynFlood DoS

Realizado por: Arellano Karina, 2016

4.2. Presentación de resultados

Para el desarrollo de las pruebas, se estableció el número de paquetes enviados en cada ataque, para esto se consideró la recomendación de (Endler & Collier, 2007), de enviar 1.000.000 de paquetes a un objetivo para experimentar ataques de DoS basados en Flooding y Fuzzing. Los valores de 500.000 y 2.000.000 paquetes enviados en las pruebas de penetración son propuestos en esta investigación debido a sus resultados. Excepto en el caso de SYN Flood ya que la herramienta que se usó para su efecto (hping3) tiene configurado por defecto tres parámetros que son: **fast =** 10 paquetes/seg, **faster =** 100 paquetes/seg y **flood =** Envío de paquetes lo más rápido que sea posible, que fueron empleados para las pruebas.

Para determinar el tiempo de interrupción del servicio de VoIP, una vez enviado el ataque, se implementó la herramienta ***PRTG Network Monitor***, que es una herramienta que permite monitorear la red recolectando varias estadísticas de las maquinas, software, y equipos. Soporta múltiples protocolos para recolectar estos datos. Para supervisar los servicios de voz sobre IP (VoIP), es necesario habilitar el sensor de ***opciones de SIP Ping*** ya que supervisa la conectividad para un servidor de Protocolo de Iniciación de Sesión (SIP) utilizando las opciones de SIP "ping".

En la Figura 18-4, se visualiza cuando la herramienta de monitoreo PRTG, detecta que el servicio de SIP no se encuentra disponible.

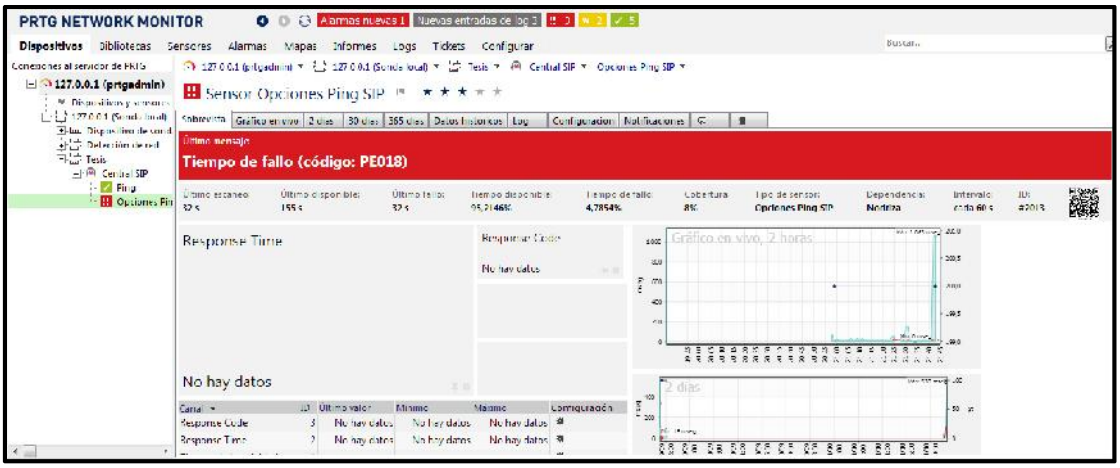


Figura 18-4: Alerta de Disponibilidad de SIP - PRTG
Realizado por: Arellano Karina, 2016

En la figura 19-4, muestra el tiempo en el que el servicio del VoIP no estuvo disponible una vez enviado el ataque de ***Invite Flood***, es de aproximadamente 9 minutos.

Informe para Opciones Ping SIP

Plazo de tiempo de informe:	02/10/2016 0:45:00 - 02/10/2016 1:00:00					
Tipo de sensor:	Opciones Ping SIP (60 s Intervalo)					
Sonda, grupo, dispositivo:	127.0.0.1 > Tesis > Central SIP					
Estadísticas de tiempo disponible:	Disponible:	39 %	[5m47s]	Fallo:	61 %	[9m0s]
Estadísticas de petición:	Bueno:	12 %	[2]	Fallo:	88 %	[15]
Promedio (Response Time):	No hay datos					

Figura 19-4: Informe para opciones de SIP Ping -PRTG
Realizado por: Arellano Karina, 2016

Para este ataque, se envió 1.000.000 de paquetes a un objetivo, tomó alrededor de 9 minutos (540 segundos) para ejecutar, lo que significa que aproximadamente 1851 paquetes fueron puestos en la red por segundo.

Generalmente los ataques por ***Flooding*** consumen recursos del servidor de VoIP como CPU y memoria hasta que se hayan agotado y sea incapaz de proporcionar servicio incluso para los usuarios legítimos. Por otra parte, SIP también es propenso a ataques mensaje incorrecto ***(Fuzzing)*** en el que los atacantes generan mensajes SIP no estándar, que se hacen a mano de forma inteligente para aprovechar las vulnerabilidades en el analizador SIP o en la mala

implementación de un servidor SIP. Un atacante puede, usando un paquete mal formado, desbordar las memorias intermedias de cadena específica, y modificar los campos de manera ilegal. Como resultado, un servidor es engañado para llegar a un estado indefinido, que puede conducir a llamar a los retrasos de procesamiento, un acceso no autorizado y una completa negación de servicio.

Para un posterior análisis y comparación, se han obtenido valores iniciales del servidor de VoIP, es decir como los recursos se comportan en un ambiente en reposo (sin que los clientes hayan tenido acceso al servicio). Estos valores iniciales fueron obtenidos con la ayuda del protocolo SNMP y la herramienta de Monitoreo PRTG, y además cotejados con la información de la propia interfaz web de Elastixs.

Tabla 4-4: Estados Iniciales del Servidor de VoIP

CONSUMO DE RECURSOS DEL SERVIDOR VoIP			**PARAMETROS DE QoS DE VOZ**		
CPU (%)	**Memoria (%)**	**Tráfico de la Red (kB/s)**	**Latencia (ms)**	**Jitter promedio (ms)**	**Paquetes perdidos (%)**
18.1%	21.1%	Sin llamadas: RX= 0.60kB/s TX= 0.44kB/s	-------	------	------
20.8%	23,8%	Con 1 llamada: RX=22.20kB/s TX= 21.94kB/s	7.63	7.26	0%
21.7%	24.1%	Con 2 llamadas (simultaneas): RX= 42.92kB/s TX= 42.76kB/s	8.96	11.29	0%

Realizado por: Arellano Karina, 2016

Las condiciones que afectan en la calidad del servicio de VoIP son la ***latencia, jitter y pérdida de paquetes***. La latencia es el tiempo que tarda un paquete para viajar del punto A al punto B. Jitter es la variación de la latencia a través de una serie de paquetes. La pérdida es el número de paquetes enviados desde el punto A que nunca llegan al punto B. Los resultados esperados de acuerdo a la teoría investigada son:

- **Latencia:** menor a 150ms
- **Jitter:** menor a 50ms
- **Perdida de paquetes:** menor o igual al 3% del volumen de datos transmitido

Para el análisis de estos parámetros de voz se utilizó la herramienta Wireshark en la se obtuvo el Jitter, paquetes perdidos y Latencia (Delta), como se muestra en la Figura 20-4.

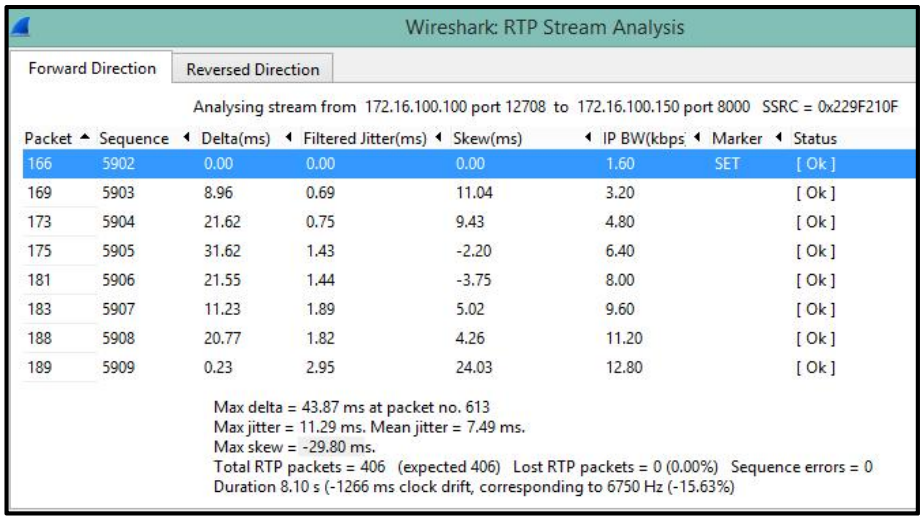


Figura 20-4: Jitter, Latencia y Paquetes Perdidos con Wireshark
Realizado por: Arellano Karina, 2016

Se aplicó una encuesta a diez (10) instituciones públicas y privadas de la provincia de Chimborazo y Tungurahua (ver Anexo A), con el objetivo de recoger información acerca del Servicio de VoIP en cada una de ellas. La cual arrojo resultados relevantes frente al uso del servicio de VoIP y la importancia de mantener siempre disponible el mismo, ya que al 100% de las instituciones encuestadas calificaron como **ALTO** el impacto que produciría la pérdida de disponibilidad del servicio de VoIP en su Institución. Así mismo un 90% de las instituciones dijeron que el tiempo promedio que dura una llamada telefónica IP se encuentra en el intervalo de 1 a 10 minutos. (Ver Anexo B).

En razón de lo expuesto, para las experimentaciones de esta investigación se estableció tres tiempos, referente a la duración de llamadas IP para cada escenario, considerando llamadas de 3, 5 y 8 minutos, respectivamente. Finalmente se ejecutaron los ataques establecidos, con la cantidad de paquetes y tiempo de duración de las llamadas de: 500.000, 1.000.000 y 2.000.000; y 3, 5, 8 minutos, respectivamente.

A continuación, se muestran los resultados de la ejecución de los ataques de DoS a tráfico SIP realizados en el escenario de prueba, dado en dos momentos, que son:

1. Escenario SIN implementación del Modelo de Seguridad (MS-DoS-SIP)
2. Escenario CON implementación del Modelo de Seguridad (MS-DoS-SIP)

En estos dos escenarios los pasos que se siguen para la realización de las pruebas de vulnerabilidades son exactamente los mismos.

4.2.1. *Resultados de pruebas en escenario sin implementación del modelo de seguridad (MS-DOS-SIP)*

Se comenzará a explicar el escenario sin la implementación del Modelo de Seguridad (MS-DOS-SIP), ya que posteriormente se requiere comparar los resultados obtenidos con la implementación del Modelo. Este escenario no cuenta con ningún mecanismo de seguridad que trate de garantizar la disponibilidad ni calidad del servicio de VoIP.

Este primer ataque permite la enumerar dispositivos SIP, mediante el escaneo de un rango de direcciones IP, como muestra la Figura 4-21.

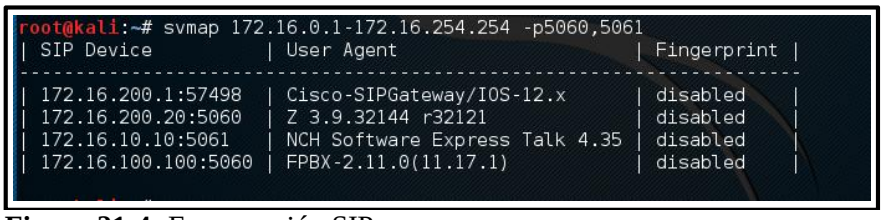


Figura 21-4: Enumeración SIP
Realizado por: Arellano Karina, 2016

También permite listar extensiones (usuarios) en el servidor se VoIP.

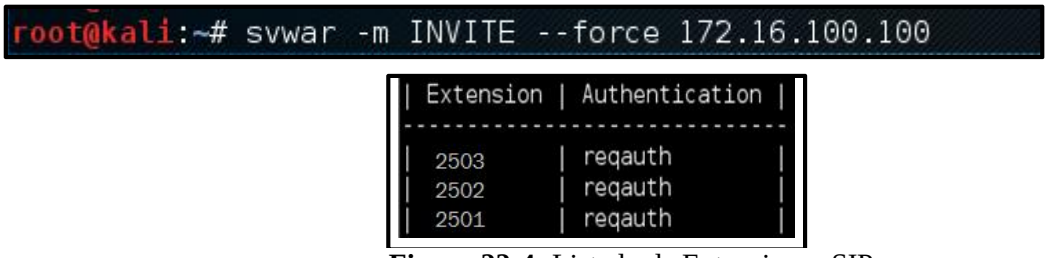


Figura 22-4: Listado de Extensiones SIP
Realizado por: Arellano Karina, 2016

Se aprovechó ciertas vulnerabilidades para la ejecución de los ataques estudiados anteriormente. Y se obtuvo resultados, referente al consumo de recursos del servidor de VoIP y la cantidad de tiempo en el que el servicio de VoIP fue interrumpido.

Las tablas 5-4 y 6-4, muestran los resultados obtenidos en la ejecución del ataque ***Invite Flood to SIP Proxies,*** con un SIP Phone inexistente. Debido a que este ataque consume el porcentaje de CPU al límite y gran cantidad de memoria, los recursos del servidor VoIP tienden a agotarse rápidamente, provocando el colapso del mismo y en cierto punto es necesario reiniciarlo físicamente para que reanude su servicio y se vuelvan a registrar los clientes SIP.

Tabla 5-4: Ataque Invite Flood to SIP Proxies-Consumo de Recursos

PAQUETES ENVIADOS (Número)	CONSUMO DE RECURSOS DEL SERVIDOR			TIEMPO DE INTERRUPCIÓN DEL SERVICIO DE VoIP (mins, seg)
	CPU (%)	Memoria (%)	Tráfico de la Red (kB/s)	
500.000	100	75.3	RX=1,268.76 TX=1,097.33	5 mins 1seg
1.000.000	100	79.9	RX=1,223.15 TX=1,104.86	9 mins 0 seg
2.000.000	100	96.6	RX=1,254.35 TX=1,740.48	12 mins 0 seg

Realizado por: Arellano Karina, 2016

Si el ataque se genera en el momento en que se encuentren llamadas establecidas, la comunicación se torna escasamente clara y molesta, hasta el punto de ser intolerable, conllevando a la ruptura de la comunicación y denegando el servicio total de VoIP.

Tabla 6-4: Ataque Invite Flood to SIP Proxies- Parámetros de Llamada

DURACIÓN DE LA LLAMADA (mins)	PAQUETES ENVIADOS (Número)	PARAMETROS DE QoS DE VOZ		
		Paquetes perdidos (%)	Jitter promedio (ms)	Latencia (ms)
3 MINUTOS	500.000	31.1	64.47	745.13
	1.000.000	40.9	88.61	803.94
	2.000.000	49.6	93.07	978.62
5 MINUTOS	500.000	36.3	105.11	870,62
	1.000.000	45.2	108.03	1172.58
	2.000.000	58.4	114.08	772.95

8 MINUTOS	500.000	28.7	61.53	777.86
	1.000.000	49.9	204.30	2175.29
	2.000.000	86.3	373.06	1948.69

Realizado por: Arellano Karina, 2016

La Tabla 7-4 muestra el resumen de los resultados del ataque:

Tabla 7-4: Resumen de Resultados Ataque Invite Flood to SIP Proxies

	Recibe / Realiza Llamadas?	**Códigos de Respuesta**
Asterisk SIP proxy	No	100 Trying 180 Ringing 408 Request Timeout

Realizado por: Arellano Karina, 2016

El servidor proxy SIP responde con “404 Not Found”. Debido a que el servidor proxy SIP, sabe que el objetivo "666" no existe y, por lo tanto, devolver la respuesta 404. Mientras tanto si un usuario legítimo quiere conectarse, existe tono de marcado pero cualquier intento para iniciar la conexión FALLA. El servicio deja de estar disponible fácilmente.

El segundo ataque ejecutado es ***Invite Flood to SIP Phones***, mediante el envío de una corriente de peticiones SIP INVITE. Puesto que este ataque es enviado específicamente a los clientes SIP, el alto consumo de recursos afecta directamente en los dispositivos que residen los softphone atacados. Como se observa en la Tabla 8-4 y Figura 9-4.

Tabla 8-4: Invite Flood to SIP Phones- Consumo de Recursos

PAQUETES ENVIADOS (Número)	**CONSUMO DE RECURSOS DEL SOFTPHONE**			**TIEMPO DE INTERRUPCIÓN DEL SERVICIO DE VoIP (mins, seg)**
	CPU (%)	**Memoria (%)**	**Tráfico de la Red (kB/s)**	
500.000	100	81.1	RX=1,347.26 TX=26.212	9 mins 0 seg
1.000.000	100	87.0	RX=1,467.10 TX=32.95	13 mins 5 seg
2.000.000	100	92.4	RX=1,379.62 TX=30.56	20 mins 1 seg

Realizado por: Arellano Karina, 2016

Como resultado del ataque, se interrumpe el servicio de un teléfono SIP, este no será capaz de recibir llamadas, hasta que se recupere del ataque o que la aplicación e incluso la PC sea reiniciada. Se debe tener en cuenta que no es aplicable para probar si el teléfono SIP puede hacer llamadas, ya que está constantemente sonando con llamadas entrantes.

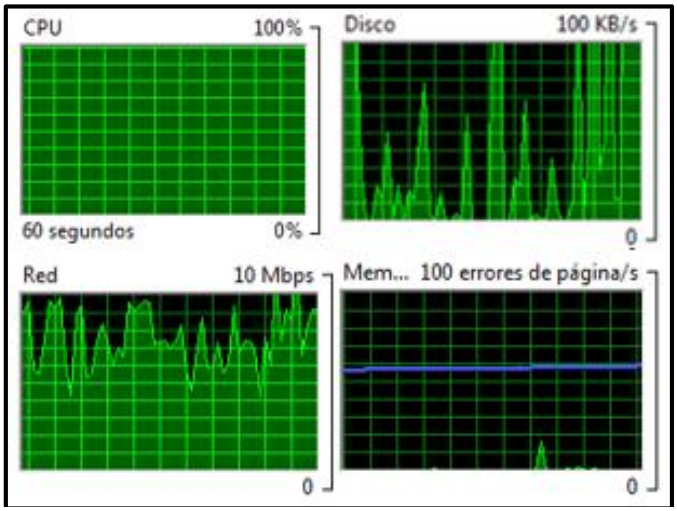


Figura 23-4: Consumo de Recursos en Softphone
Realizado por: Arellano Karina, 2016

Los softphones Express Talk, y Zoiper, son fáciles de engañar para aceptar las solicitudes INVITE; una vez recibidas las peticiones inmediatamente comienzan a sonar ("timbrar").

Se atacó tanto con los teléfonos SIP colgados y descolgados. Por cada ataque, se ha probado la capacidad del teléfono SIP para realizar las siguientes funciones:

- **Comportamiento básico:** Indica si el teléfono SIP, timbra o está completamente muerto.
- **Interfaz de usuario utilizable:** Indica si los botones/interfaz de usuario del teléfono SIP son utilizables. Durante algunos ataques, el teléfono SIP apareció "muerto".
- **Recibir llamadas:** Indica si el teléfono SIP podría recibir llamadas.
- **Recuperado después de un ataque:** Indica si el teléfono SIP se recuperó después que el ataque se detuvo.

La tabla 9-4 resume los resultados para cada softphone SIP probado:

Tabla 9-4: Invite Flood to SIP Phones- Consumo de Recursos

Softphone	Comportamiento básico	Interfaz de usuario utilizable	Recibir llamadas	Recuperado después de un ataque
Express Talk	Ambas líneas suenan. Cuando se responde, no hay ningún audio. Cuando el teléfono está colgado, las líneas empiezan a de sonar.	Sí, pero lento	No	Si
Zoiper	Ambas líneas suenan. Cuando se responde, no hay ningún audio. Cuando el teléfono está colgado, las líneas empiezan a de sonar.	Sí, pero lento	No	No. Deber ser reiniciada la aplicación.

Realizado por: Arellano Karina, 2016

Si el ataque ocurre durante una llamada, la comunicación se vuelve escasamente clara y molesta, ya que constantemente se recibirá peticiones INVITE, experimentando retardos y cortes en la llamada, provocando indisponer el servicio. La Tabla 10-4, muestra los datos encontrados:

Tabla 10-4: Invite Flood to SIP Phones-Parámetros de Llamada

DURACIÓN DE LA LLAMADA (mins)	PAQUETES ENVIADOS (Número)	PARAMETROS DE QoS DE VOZ		
		Paquetes perdidos (%)	Jitter promedio (ms)	Latencia (ms)
3 MINUTOS	500.000	38.9	66.9	372.11
	1.000.000	46.3	433.65	1422.78
	2.000.000	51.1	252.54	1045.26
5 MINUTOS	500.000	45.2	75.31	742.90
	1.000.000	59.1	443.84	1984.77
	2.000.000	62.0	489.20	967.22
8 MINUTOS	500.000	29.1	95.31	726.18
	1.000.000	61.7	510.98	1790.67
	2.000.000	90.3	243.12	972.01

Realizado por: Arellano Karina, 2016

Puesto que este ataque es directamente al teléfono SIP es más interesante porque el proxy SIP no es consciente de los ataques.

El tercer ataque ejecutado es ***SYN Flood DoS***, para el cuál se envió una cantidad de paquetes mediante el parámetro ***flood*** (envía paquetes lo más rápido que sea posible) de la herramienta, y con tiempo de duración del ataque de 2, 4 y 6 minutos.

Tabla 11-4: SYN Flood - Consumo de Recursos

TIEMPO DE DURACIÓN ATAQUE (mins, seg)	PAQUETES ENVIADOS (Aproximadamente)	CONSUMO DE RECURSOS DEL SERVIDOR			TIEMPO DE INTERRUPCIÓN DEL SERVICIO DE VoIP (mins, seg)
		CPU (%)	Memoria (%)	Tráfico de la Red (kB/s)	
2 MINUTOS	500.000	98.4	39.2	RX=747.80 TX=63.23	Es proporcional al tiempo de duración del ataque. Durante el ataque existe tono de marcado pero cualquier intento para iniciar la conexión FALLA.
4 MINUTOS	1.000.000	100	48.3	RX=747.13 TX=65.41	
6 MINUTOS	2.000.000	100	77.3	RX= 732.46 TX=68.64	

Realizado por: Arellano Karina, 2016

Una vez realizado este ataque SYN Flood DoS, el servidor queda colapsado de peticiones SYN, sin poder identificar las peticiones de usuarios reales, hasta el punto que no acepta nuevas peticiones quedando a la espera del ACK final que nunca llegara de las IPs falsas. Al quedar a la espera del ACK final, el servidor rechazó las nuevas conexiones de usuarios reales, logrando con esto la denegación del servicio de VoIP. Si logra establecerse una llamada durante la ejecución del ataque, la comunicación experimentará lo siguiente:

Tabla 12-4: SYN Flood-Parámetros de Llamada

DURACIÓN DE LA LLAMADA (mins)	PAQUETES ENVIADOS (Aproximadamente)	PARAMETROS DE QoS DE VOZ		
		Paquetes perdidos (%)	Jitter promedio (ms)	Latencia (ms)
3 MINUTOS	500.000	73.7	64.17	639.50
	1.000.000	66.6	27.83	607.05
	2.000.000	61.3	93.30	522.79
5 MINUTOS	500.000	43.8	32.99	614.28
	1.000.000	73.8	87.22	813.35
	2.000.000	53.5	38.46	713.57
8 MINUTOS	500.000	52.4	42.02	803.78
	1.000.000	63.6	18.11	560.47
	2.000.000	73.1	75.58	979.72

Realizado por: Arellano Karina, 2016

La cuarta amenaza estudiada es de ***Malformación en mensajes INVITE (Fuzzing)***, mediante la herramienta ***Sivus***, provocó el desbordamiento de la memoria del servidor atacado (Ver Tabla 13-4), puesto que necesita procesar una gran cantidad de paquetes con formatos extraños. Llevando a que los agentes de usuario funcionen mal o incluso dejen de funcionar completamente.

Tabla 13-4: Malformación en mensajes INVITE (Fuzzing) - Consumo de Recursos

PAQUETES ENVIADOS (Número)	CONSUMO DE RECURSOS DEL SERVIDOR			TIEMPO DE INTERRUPCIÓN DEL SERVICIO DE VoIP (mins, seg)
	CPU (%)	Memoria (%)	Tráfico de la Red (kB/s)	
500.000	28.3	58.1	RX=1453.59 TX=828.21	9 mins 0 seg Aún es posible realizar llamadas
1.000.000	35.6	76.5	RX= 1987.45 TX=453.12	13 mins 5 seg En este punto cualquier intento de llamada FALLA
2.000.000	42.1	98.9	RX=1989.16 TX=653.01	20 mins 1 seg En este punto cualquier intento de llamada FALLA

Realizado por: Arellano Karina, 2016

Los efectos del ataque durante una llamada, son altamente impactantes. Como muestra la Tabla 14-4.

Tabla 14-4: Malformación en mensajes INVITE (Fuzzing)

DURACIÓN DE LA LLAMADA (mins)	PAQUETES ENVIADOS (Número)	PARAMETROS DE QoS DE VOZ		
		Paquetes perdidos (%)	Jitter promedio (ms)	Latencia (ms)
3 MINUTOS	500.000	13.6	241.66	109.99
	1.000.000	9.01	333.64	719.82
	2.000.000	10.78	102.56	867.34
5 MINUTOS	500.000	3.01	68.92	502.27
	1.000.000	23.78	167.09	435.89
	2.000.000	11.09	85.87	298.54
8 MINUTOS	500.000	7.03	65.75	124.03
	1.000.000	9.98	235.09	856.09
	2.000.000	32.20	417.78	345.87

Realizado por: Arellano Karina, 2016

Finalmente se ejecutó el ataque de ***Eliminación de Registro de Usuarios SIP***, para ello antes se primero se identificó los usuarios registrados en el servidor SIP antes del ataque.

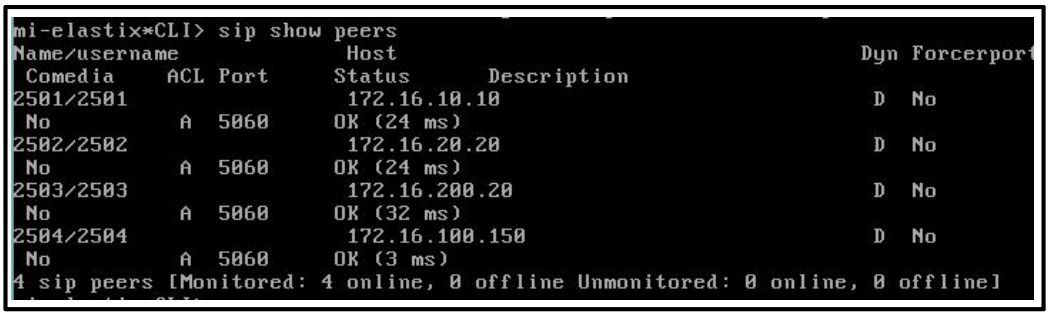


Figura 24-4: Usuarios Registrados en Servidor SIP
Realizado por: Arellano Karina, 2016

En la Figura 25-4, se observa que se eliminó los registros para los usuarios SIP (2501 y 2504) en el proxy SIP.

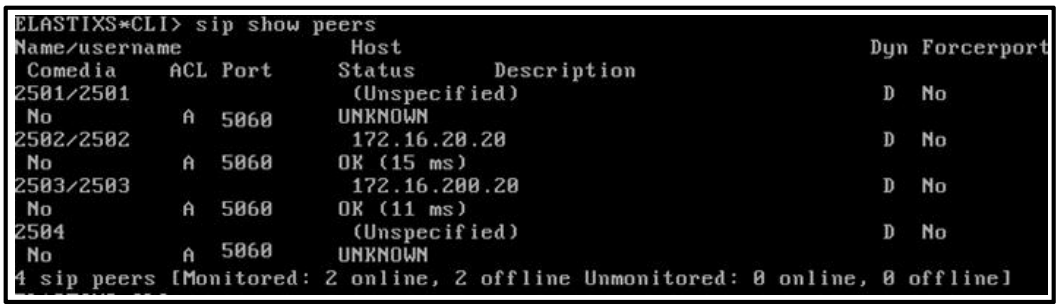


Figura 25-4: Elimina Registro de Usuario
Realizado por: Arellano Karina, 2016

Debido a que el ataque de eliminación de registro de usuarios provoca que el usuario no pueda realizar llamadas pero sí recibirlas, se obtuvo los siguientes resultados:

Tabla 15-4: Eliminación de Registro - Consumo de Recursos

PAQUETES ENVIADOS (Número)	CONSUMO DE RECURSOS DEL SERVIDOR			TIEMPO DE INTERRUPCIÓN DEL SERVICIO DE VoIP (mins, seg)
	CPU (%)	Memoria (%)	Tráfico de la Red (kB/s)	
500.000	26.7	63.7	RX=1453.59 TX=828.21	5 mins 0 seg Es posible realizar llamadas
1.000.000	32.4	70.2	RX= 1987.45 TX=453.12	8 mins 0 seg Es posible realizar llamadas
2.000.000	50.34	88.24	RX=1989.16 TX=653.01	15 mins 1 seg Es posible realizar llamadas

Realizado por: Arellano Karina, 2016

Cuando se elimina un registro, el teléfono SIP no puede recibir ninguna llamada entrante, hasta que se recupere del ataque y/o se registre manualmente con el servidor SIP. Sin embargo este ataque, no afecta a la capacidad del teléfono SIP para realizar llamadas, y los parámetros de QoS no son afectados.

4.2.2. *Resultados de pruebas en escenario con implementación del modelo de seguridad (MS-DOS-SIP)*

En este escenario se implementó el Modelo de Seguridad propuesto, y se ejecutaron las mismas pruebas de vulnerabilidades aplicadas en el apartado anterior. Ciertas herramientas aplicadas ayudaron a identificar ataques de DoS e impedir el acceso de paquetes desde la dirección IP causante de saturación del servidor. Y se obtuvo los siguientes resultados:

En primera instancia no es posible enumerar dispositivos SIP que conforman la red. (Ver Figura 26-4).

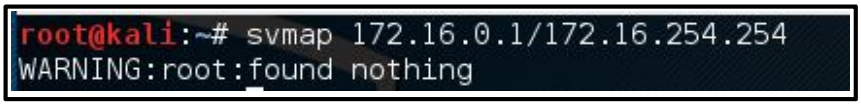
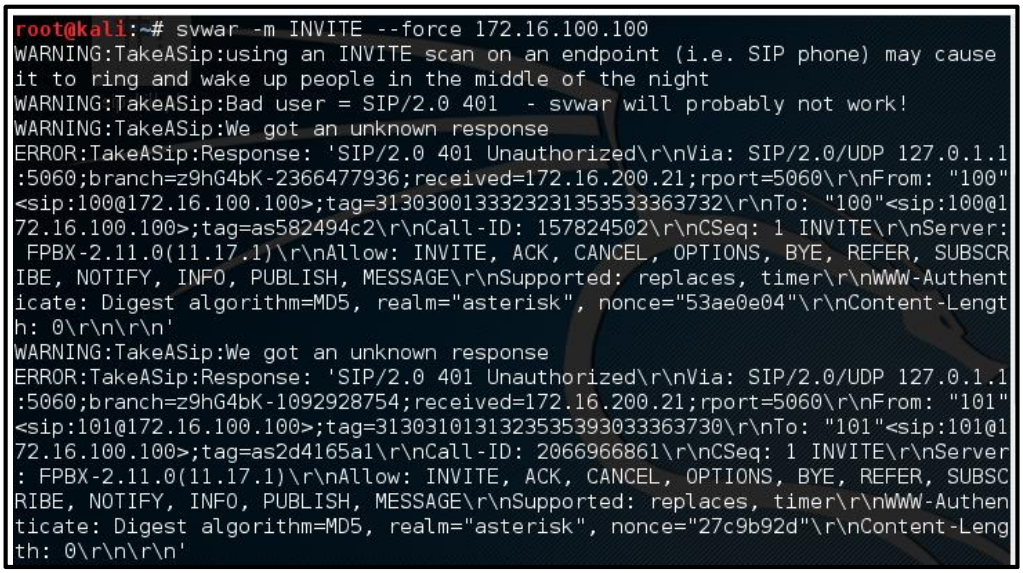


Figura 26-4: NO permite Enumeración SIP
Realizado por: Arellano Karina, 2016

Así mismo momento de intentar listar extensiones (usuarios) en el servidor VoIP, luego de una búsqueda fallida, finalmente no encuentra nada, como se observa en la Figura 27-4.



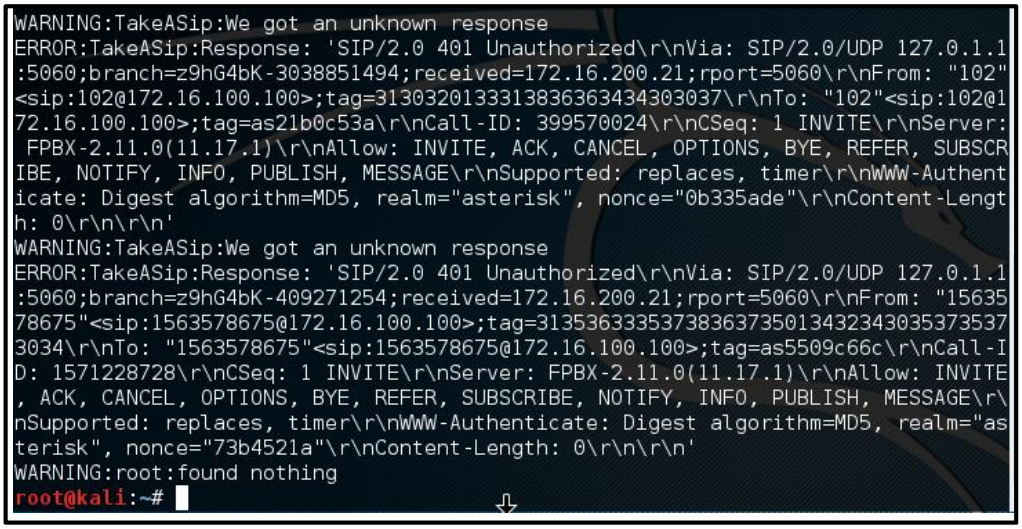


Figura 27-4: Listado de Extensiones SIP- Fallido
Realizado por: Arellano Karina, 2016

Para el caso de ataques ***Flooding***, las herramientas implementadas y protocolos, pudieron identificar estos excesivos flujos de mensajes y bloquearlos. Logrando proteger la central VoIP de un ataque directo si se configura para rechazar estos mensajes.

Las tablas 16-4 y 1-47, muestran los resultados obtenidos en la ejecución del ataque ***Invite Flood to SIP Proxies,*** con un SIP Phone inexistente.

Tabla 16-4: Ataque Invite Flood to SIP Proxies-Consumo de Recursos

PAQUETES ENVIADOS (Número)	CONSUMO DE RECURSOS DEL SERVIDOR			TIEMPO DE INTERRUPCIÓN DEL SERVICIO DE VoIP (mins, seg)
	CPU (%)	Memoria (%)	Tráfico de la Red (kB/s)	
500.000	20.4	23.40	RX=0.58 TX=0.46	0 mins 30 segundos
1.000.000	21.5	22.02	RX=22.20 TX=21.94	
2.000.000	21.7	23.60	RX=34.01 TX=42.76	

Realizado por: Arellano Karina, 2016

El tiempo de indisponibilidad que muestra la herramienta PRTG, no es percibida por el servicio de VoIP, puesto que es el tiempo en que las contramedidas detectan estar en un ataque y lo bloquean, es así que se puede decir que el servicio se muestra 100% disponible.

Al rechazar estas peticiones masivas, las comunicaciones no perciben cambio alguno, como así se muestra en la Tabla 17-4.

Tabla 17-4: Ataque Invite Flood to SIP Proxies- Parámetros de Llamada

DURACIÓN DE LA LLAMADA (mins)	PAQUETES ENVIADOS (Número)	PARAMETROS DE QoS DE VOZ		
		Paquetes perdidos (%)	Jitter promedio (ms)	Latencia (ms)
3 MINUTOS	500.000	0.0	13.33	75.30
	1.000.000	0.1	25.70	59.42
	2.000.000	0.0	39.22	75.34
5 MINUTOS	500.000	0.0	27.19	80.60
	1.000.000	0.0	13.22	68.43
	2.000.000	0.1	18.72	75.02
8 MINUTOS	500.000	0.0	16.42	80.81
	1.000.000	0.0	24.67	65.13
	2.000.000	0.1	32.72	52.10

Realizado por: Arellano Karina, 2016

En resumen este ataque, no tiene efecto en el ambiente VoIP.

Tabla 18-4: Resumen de Resultados Ataque Invite Flood to SIP Proxies

	Recibe / Realiza Llamadas?	Códigos de Respuesta
Asterisk SIP proxy	SI, Totalmente	100 Trying 180 Ringing 200 OK

Realizado por: Arellano Karina, 2016

Los resultados frente a un ataque ***Invite Flood to SIP Phones***, se muestran a continuación:

Tabla 19-4: Invite Flood to SIP Phones- Consumo de Recursos

PAQUETES ENVIADOS (Número)	CONSUMO DE RECURSOS DEL SOFTPHONE			TIEMPO DE INTERRUPCIÓN DEL SERVICIO DE VoIP (mins, seg)
	CPU (%)	Memoria (%)	Tráfico de la Red (kB/s)	
500.000	10	50	RX=0.4 TX=8.58	0 mins 0 segundos Los terminales SIP, funcionan con total normalidad, al 100%.
1.000.000	10	50	RX=13.7 TX=8.62	
2.000.000	10	50	RX=7.56 TX=9.19	

Realizado por: Arellano Karina, 2016

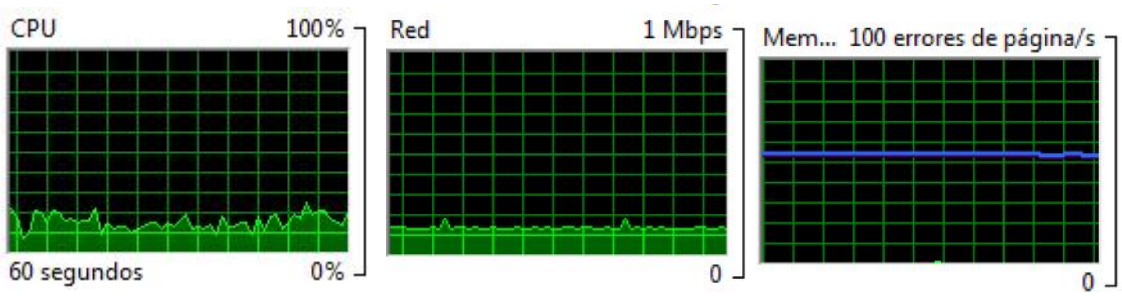


Figura 28-4: Consumo de Recursos Softphone
Realizado por: Arellano Karina, 2016

Tabla 20-4: Invite Flood to SIP Phones- Resultados Softphone

Softphone	Comportamiento básico	Interfaz de usuario utilizable	Recibir llamadas	Realizar llamadas	Recuperado después de un ataque
Express Talk	Se realizan llamadas con normalidad	Sí	Si	Si	No percibe el ataque
Zoiper	Se realizan llamadas con normalidad.	Sí	Si	Si	No percibe el ataque

Realizado por: Arellano Karina, 2016

Así mismo, las llamadas se realizan sin ningún problema.

Tabla 21-4: Invite Flood to SIP Phones-Parámetros de llamada

DURACIÓN DE LA LLAMADA (mins)	PAQUETES ENVIADOS (Número)	PARAMETROS DE QoS DE VOZ		
		Paquetes perdidos (%)	Jitter promedio (ms)	Latencia (ms)
3 MINUTOS	500.000	0.1	30.34	149.01
	1.000.000	0.0	30.28	108.02
	2.000.000	0.1	28.20	98.13
5 MINUTOS	500.000	0.0	27.94	135.66
	1.000.000	0.1	19.99	176.02
	2.000.000	0.0	21.47	92.28
8 MINUTOS	500.000	0.0	12.76	87.46
	1.000.000	0.0	21.57	114.70
	2.000.000	0.01	31.28	89.03

Realizado por: Arellano Karina, 2016

En cuanto al ataque ***SYN Flood DoS***, esta vez no tiene impacto en la disponibilidad y calidad del servicio de VoIP. Presentando los siguientes resultados:

Tabla 22-4: SYN Flood - Consumo de Recursos

TIEMPO DE DURACIÓN ATAQUE (mins, seg)	PAQUETES ENVIADOS (Aproximadamente)	CONSUMO DE RECURSOS DEL SERVIDOR			TIEMPO DE INTERRUPCIÓN DEL SERVICIO DE VoIP (mins, seg)
		CPU (%)	Memoria (%)	Tráfico de la Red (kB/s)	
2.0	500.000	24.4	26.0	RX=120.9 TX=64.21	0 minutos 30 segundos El servicio de VoIP, funciona con total normalidad, al 100%.
4.0	1.000.000	24.0	25.7	RX=47.13 TX=56.41	
6.0	2.000.000	25.3	26.01	RX= 132.20 TX=38.64	

Realizado por: Arellano Karina, 2016

Tabla 23-4: SYN Flood-Parámetros de Llamada

DURACIÓN DE LA LLAMADA (mins)	PAQUETES ENVIADOS (Número)	PARAMETROS DE QoS DE VOZ		
		Paquetes perdidos (%)	Jitter promedio (ms)	Latencia (ms)
3 MINUTOS	500.000	0.0	15.88	67.92
	1.000.000	0.0	16.33	79.67
	2.000.000	0.0	12.23	65.49
5 MINUTOS	500.000	0.0	9.18	75.91
	1.000.000	0.0	14.45	59.50
	2.000.000	0.0	8.87	21.65
8 MINUTOS	500.000	0.0	7.95	76.10
	1.000.000	0.0	9.15	32.30
	2.000.000	0.0	11.18	68.43

Realizado por: Arellano Karina, 2016

Una alternativa frente ataques de ***Malformación en mensajes INVITE (Fuzzing),*** son los dispositivos de seguridad, como SBC. El SBC BLOX implementado en la aplicación práctica identifica el flujo de mensajes SIP inválidos, mediante la configuración de reglas para inspección de paquetes SIP. Las posibles acciones que FreeBlox puede ejecutar frente a un ataque, es mostrar los logs de alerta y el bloqueo de los paquetes que contienen un vector de ataque y la lista negra de la IP atacante para la bloquearla en un tiempo de duración dado por categoría. Blox hace uso de un DPI que examina el tráfico SIP bajo normas de seguridad.

Los resultados obtenidos en este escenario de pruebas al lanzar el ataque se muestra en la Tabla 24-4 y 25-4.

Tabla 24-4: Malformación en mensajes INVITE (Fuzzing) - Consumo de Recursos

PAQUETES ENVIADOS (Número)	CONSUMO DE RECURSOS DEL SERVIDOR			TIEMPO DE INTERRUPCIÓN DEL SERVICIO DE VoIP (mins, seg)
	CPU (%)	Memoria (%)	Tráfico de la Red (kB/s)	
500.000	24.3	26.0	RX= 43.65 TX=38.21	1 minutos 5 segundos
1.000.000	25.2	24.3	RX= 68.45 TX=43.24	
2.000.000	25.1	24.6	RX=89.10 TX=53.0	

Realizado por: Arellano Karina, 2016

Tabla 25-4: Malformación en mensajes INVITE (Fuzzing)

DURACIÓN DE LA LLAMADA (mins)	PAQUETES ENVIADOS (Número)	PARAMETROS DE QoS DE VOZ		
		Paquetes perdidos (%)	Jitter promedio (ms)	Latencia (ms)
3 MINUTOS	500.000	0.0	32.72	80.34
	1.000.000	1.30	38.54	98.02
	2.000.000	0.0	42.65	46.43
5 MINUTOS	500.000	0.0	35.22	67.87
	1.000.000	0.10	23.45	32.08
	2.000.000	2.01	12.67	76.40
8 MINUTOS	500.000	0.0	9.34	96.42
	1.000.000	0.10	19.01	71.63
	2.000.000	2.70	20.07	98.75

Realizado por: Arellano Karina, 2016

Es así que el SBC identificó paquetes con formato incorrecto y bloqueo, impidiendo que llegara a la central telefónica, de esta forma se mitigó el ataque.

En la Figura 29-4 se muestra como el ataque de ***Eliminación de Registro*** no tiene efecto en extensiones que utilizan TLS (extensión 2502 y 2503). Debido a que el puerto utilizado para TLS es 5061, la herramienta no funciona. Esto es posible porque no en todos los usuarios se utilizó TLS.

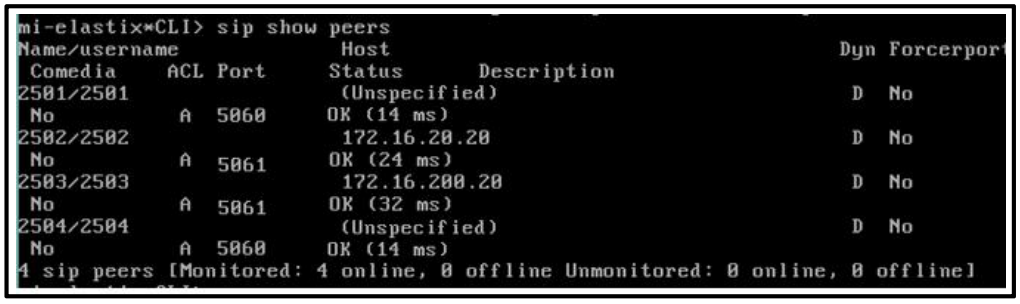


Figura 29-4: Usuarios Registrados en Servidor SIP
Realizado por: Arellano Karina, 2016

Cuando una central telefónica acepta ambas conexiones (SIP y SIP con TLS), también es posible realizar este ataque en usuarios que utilizan TLS, por lo tanto, se debe configurar la central telefónica para que ***sólo*** se acepten conexiones TLS.

Tabla 26-4: Eliminación de Registro - Consumo de Recursos

PAQUETES ENVIADOS (Número)	CONSUMO DE RECURSOS DEL SERVIDOR			TIEMPO DE INTERRUPCIÓN DEL SERVICIO DE VoIP (mins, seg)
	CPU (%)	Memoria (%)	Tráfico de la Red (kB/s)	
500.000	24.1	25.4	RX=153.59 TX=28.21	0 mins 0 seg
1.000.000	23.4	25.01	RX= 197.14 TX=53.20	
2.000.000	25.2	24.3	RX=89.16 TX=65.21	

Realizado por: Arellano Karina, 2016

Debe considerarse que este ataque no tendría efecto si el atacante no se encontrara en la misma red o no tuviera acceso directo a la central VoIP. En este sentido, impedir el acceso a la central telefónica evita el ataque de eliminación de registros de usuarios SIP.

Se pueden emplear varias contramedidas para hacer frente a ataques de DoS contra ambientes de VoIP basados en SIP. La Tabla 27-4, resume las contramedidas aplicadas en este escenario en base al Modelo de Seguridad propuesto.

Tabla 27-4: Resumen de Contramedidas Aplicadas

VULNERABILIDAD	CONTRAMEDIDA
Flooding - INVITE Proxy - INVITE Phones - REGISTER	- Usar TCP y TLS para conexiones SIP - Usar VLANs para separar la Voz y Datos - Cambiar Puertos Conocidos - Usar Firewalls SIP - Usar Iptables - Usar Session Border Controller (SBC BLOX)
Fuzzing - Malformación de Mensajes INVITE	- Usar Session Border Controller (SBC BLOX) - Usar Firewalls SIP - Cambiar Puertos Conocidos
SYN Flood Dos	- Usar VLANs para separar la Voz y Datos - Cambiar Puertos Conocidos - Usar Firewalls SIP - Iptables
Manipulación de la Señalización **Eliminación de Registro**	- Usar TCP para conexines SIP - Usar VLANs para separar la Voz y Datos - Disminuir el interval de tiempo para el Registro - Cambiar Puertos Conocidos - Usar Firewalls SIP - Usar Session Border Controller (SBC BLOX)
Ataques de Enumeración	- Usar Fail2ban - Asegurar el archivo sip.conf - Usar Session Border Controller (SBC BLOX)

Realizado por: Arellano Karina, 2016

4.3. Análisis e interpretación de resultados

Luego de realizar las pruebas en los escenarios establecidos con y sin la Implementación del Modelo de Seguridad MS-DoS-SIP, se procede a realizar el análisis, comparación e interpretación de los resultados obtenido en cada uno de ellos:

4.3.1. *Ataque de enumeración*

Se realiza una comparación de los resultados obtenidos al ejecutar el ataque de enumeración, tanto en el escenario sin la implementación del Modelo MS-DOS-SIP y con él.

Tabla 28-4: Resultados de Ataque de Enumeración con y sin Modelo MS-DOS-SIP

Ataque de Enumeración		
Modelo de Seguridad	**Muestra Dispositivos SIP**	**Lista Extensiones SIP**
Sin Implementación	Si	Si
Con Implementación	No	No

Realizado por: Arellano Karina, 2016

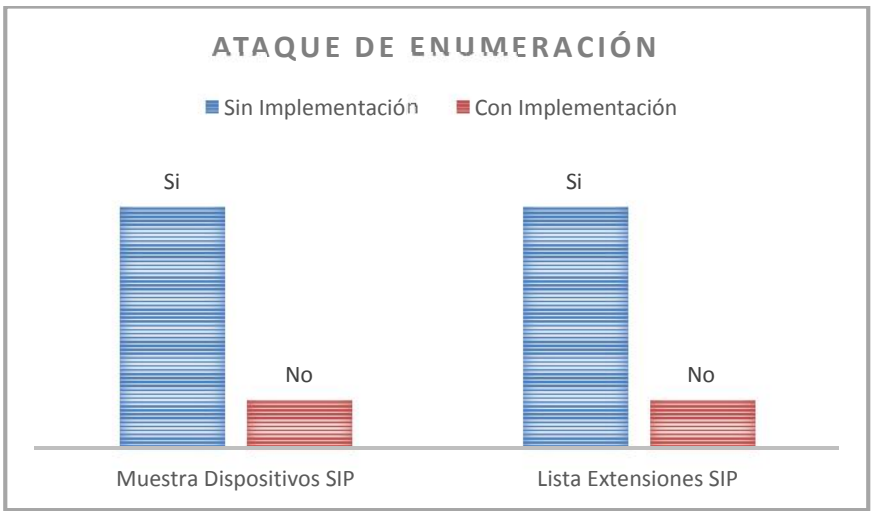


Gráfico 1-4: Resultados de Ataque de Enumeración con y sin Modelo MS-DOS-SIP
Realizado por: Arellano Karina, 2016

De acuerdo a los resultados obtenidos al ejecutar el ataque de enumeración en el escenario que contiene la implementación del Modelo de seguridad, específicamente asegurando el archivo sip.conf, y aplicando la herramienta Fail2ban, se contrarresta estas vulnerabilidades, en contraste a los resultados obtenidos en el escenario SIN la implementación del Modelo de Seguridad.

4.3.2. *Ataque invite flood to SIP proxies*

Se comparan los resultados obtenidos al ejecutar el ataque Invite Flood al Proxy SIP, tanto en el escenario sin la implementación del Modelo MS-DOS-SIP y con él.

Tabla 29-4: Resultados de Ataque Invite Flood to SIP Proxies – Consumo de Recursos

Ataque Invite Flood to SIP Proxies Consumo de Recursos del Servidor VoIP						
Modelo de Seguridad	**500.000 Paquetes Enviados**		**1.000.000 Paquetes Enviados**		**2.000.000 Paquetes Enviados**	
	CPU (%)	**Memoria (%)**	**CPU (%)**	**Memoria (%)**	**CPU (%)**	**Memoria (%)**
Sin Implementación	100%	75.30%	100%	79.90%	100%	96.60%
Con Implementación	20.40%	23.40%	21.50%	22.02%	21.70%	23.60%

Realizado por: Arellano Karina, 2016

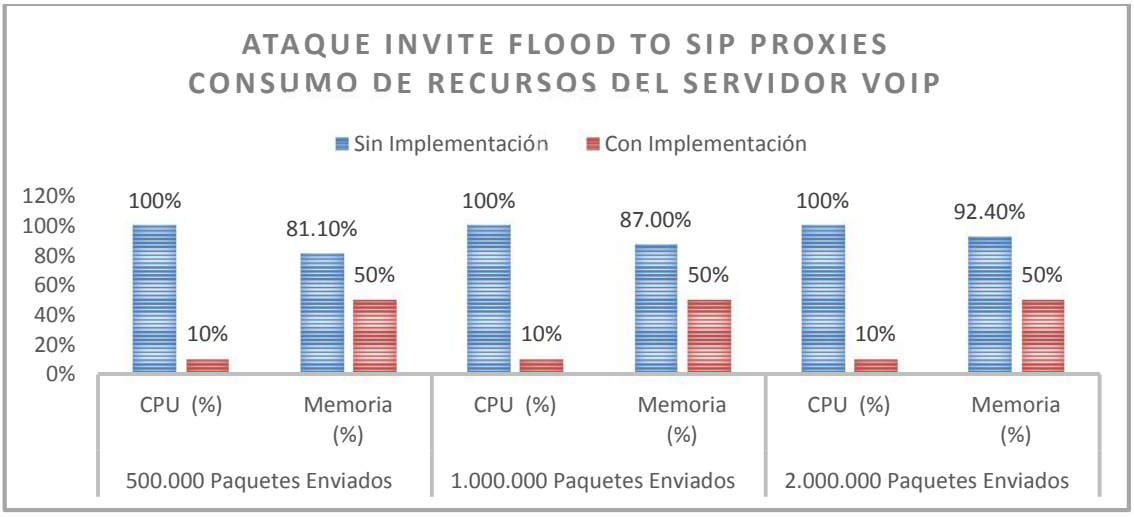


Gráfico 2-4: Resultados de Ataque Invite Flood to Proxy SIP – Consumo de Recursos
Realizado por: Arellano Karina, 2016

Como podemos observar en la Gráfico 4-2, una vez implementado el Modelo de Seguridad en nuestro ambiente VoIP, el consumo de recursos frente a este ataque se reduce considerablemente, puesto que actúan herramientas como el Firewall y SBC BLOX, resguardando la disponibilidad del servicio.

Tabla 30-4: Resultados de Ataque Invite Flood to SIP Proxies – Paquetes perdidos

Ataque Invite Flood to SIP Proxies Parámetros de QoS de la llamada - Paquete Perdidos (%)									
Modelo de Seguridad	**Duración de la Llamada = 3 minutos**			**Duración de la Llamada = 5 minutos**			**Duración de la Llamada = 8 minutos**		
	500.000 Paquetes	**1.000.000 Paquetes**	**2.000.000 Paquetes**	**500.000 Paquetes**	**1.000.000 Paquetes**	**2.000.000 Paquetes**	**500.000 Paquetes**	**1.000.000 Paquetes**	**2.000.000 Paquetes**
Sin Implementación	31.10%	40.90%	49.60%	36.30%	45.20%	58.40%	28.70%	49.90%	86.30%
Con Implementación	0.00%	0.10%	0.00%	0.00%	0.00%	0.10%	0.00%	0.00%	0.10%

Realizado por: Arellano Karina, 2016

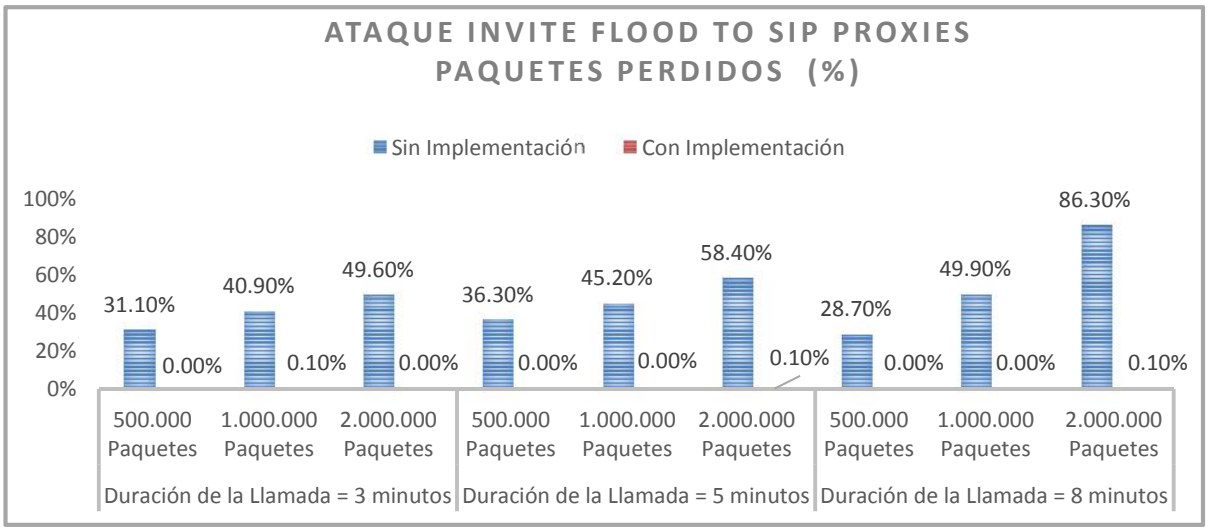


Gráfico 3-4: Resultados de Ataque Invite Flood to Proxy SIP – Paquetes Perdidos
Realizado por: Arellano Karina, 2016

De la misma forma se puede verificar que la cantidad de paquetes perdidos en una llamada establecida disminuye notablemente, una vez aplicado el Modelo de Seguridad permitiendo que la llamada sea clara y sin interrupciones; mientras que sin él la pérdida de paquetes es altamente considerable provocando que la llamada sea escasamente clara.

Tabla 31-4: Resultados de Ataque Invite Flood to SIP Proxies – Jitter

Ataque Invite Flood to SIP Proxies Parámetros de QoS de la llamada - Jitter promedio (ms)									
Modelo de Seguridad	**Duración de la Llamada = 3 minutos**			**Duración de la Llamada = 5 minutos**			**Duración de la Llamada = 8 minutos**		
	500.000 Paquetes	**1.000.000 Paquetes**	**2.000.000 Paquetes**	**500.000 Paquetes**	**1.000.000 Paquetes**	**2.000.000 Paquetes**	**500.000 Paquetes**	**1.000.000 Paquetes**	**2.000.000 Paquetes**
Sin Implementación	64.47	88.61	93.07	105.11	108.03	114.08	61.53	204.00	373.06
Con Implementación	13.33	25.70	39.22	27.19	13.22	18.72	16.42	24.67	32.72

Realizado por: Arellano Karina, 2016

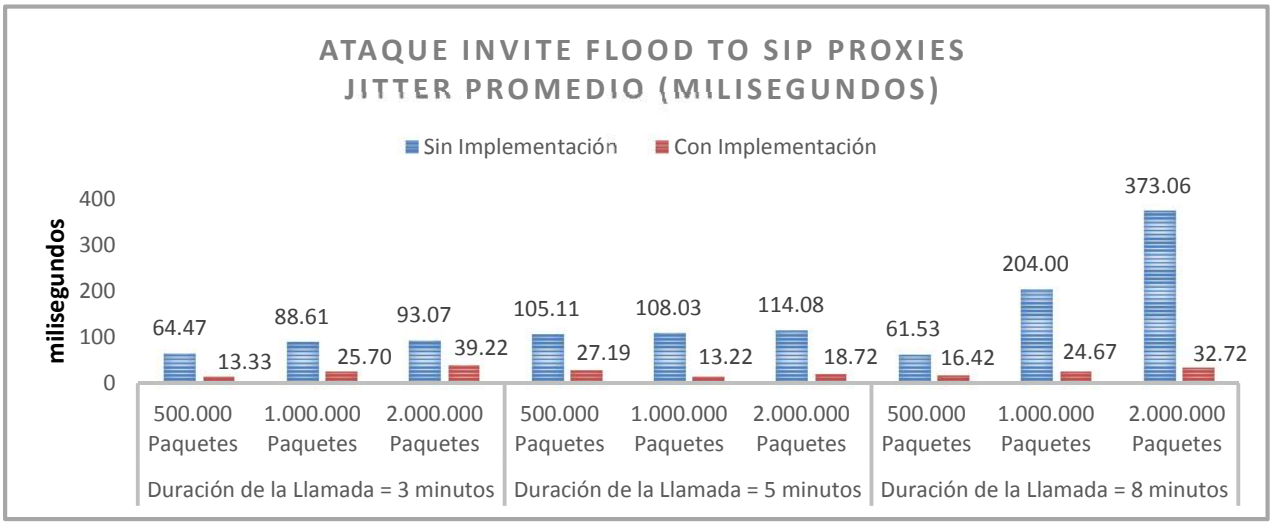


Gráfico 4-4: Resultados de Ataque Invite Flood to Proxy SIP – Jitter
Realizado por: Arellano Karina, 2016

Tabla 32-4: Resultados de Ataque Invite Flood to SIP Proxies – Latencia

Ataque Invite Flood to SIP Proxies Parámetros de QoS de la llamada - Latencia (ms)									
Modelo de Seguridad	**Duración de la Llamada = 3 minutos**			**Duración de la Llamada = 5 minutos**			**Duración de la Llamada = 8 minutos**		
	500.000 Paquetes	**1.000.000 Paquetes**	**2.000.000 Paquetes**	**500.000 Paquetes**	**1.000.000 Paquetes**	**2.000.000 Paquetes**	**500.000 Paquetes**	**1.000.000 Paquetes**	**2.000.000 Paquetes**
Sin Implementación	745.13	803.94	978.62	870.62	1172.58	772.95	777.86	2175.29	1948.69
Con Implementación	75.30	59.42	75.34	80.60	68.43	75.02	80.81	65.13	52.10

Realizado por: Arellano Karina, 2016

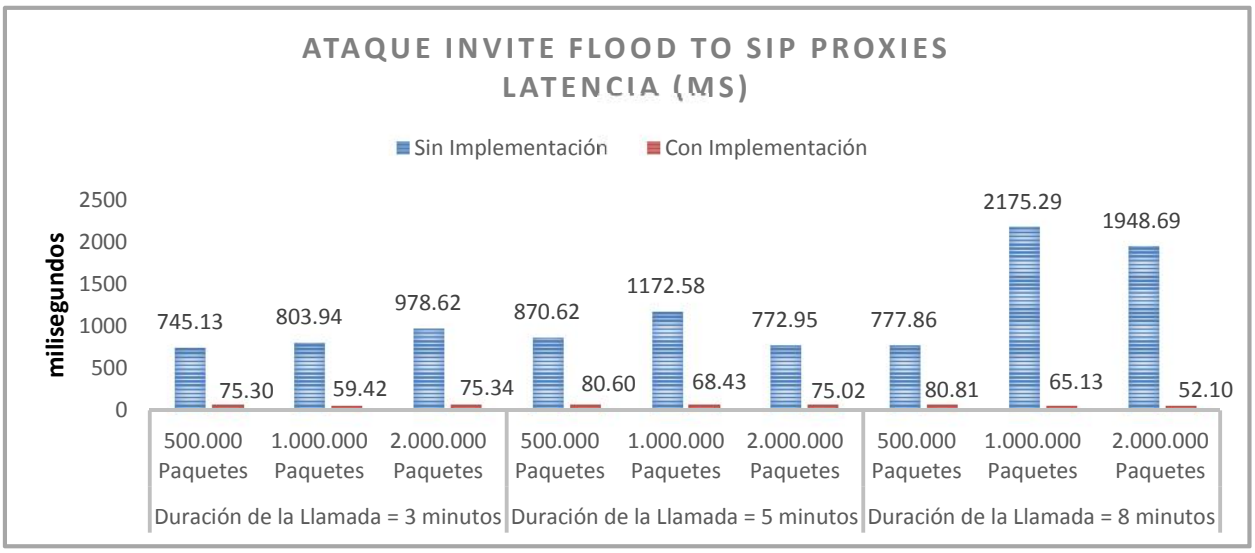


Gráfico 5-4: Resultados de Ataque Invite Flood to Proxy SIP – Latencia
Realizado por: Arellano Karina, 2016

Una vez que se controla el ataque mediante la implementación del Modelo de Seguridad, los valores de Latencia y Jitter se encuentran entre los parámetros permitidos, permitiendo una comunicación de calidad.

Tabla 33-4: Resultados de Ataque Invite Flood to SIP Proxies – No Disponibilidad

Ataque Invite Flood to SIP Proxies Tiempo de Interrupción del Servicio de VoIP (mins)			
Modelo de Seguridad	**500.000 paquetes enviados**	**1.000.000 paquetes enviados**	**2.000.000 paquetes enviados**
Sin Implementación	5.0	9.0	12.0
Con Implementación	0.5	0.5	0.5

Realizado por: Arellano Karina, 2016

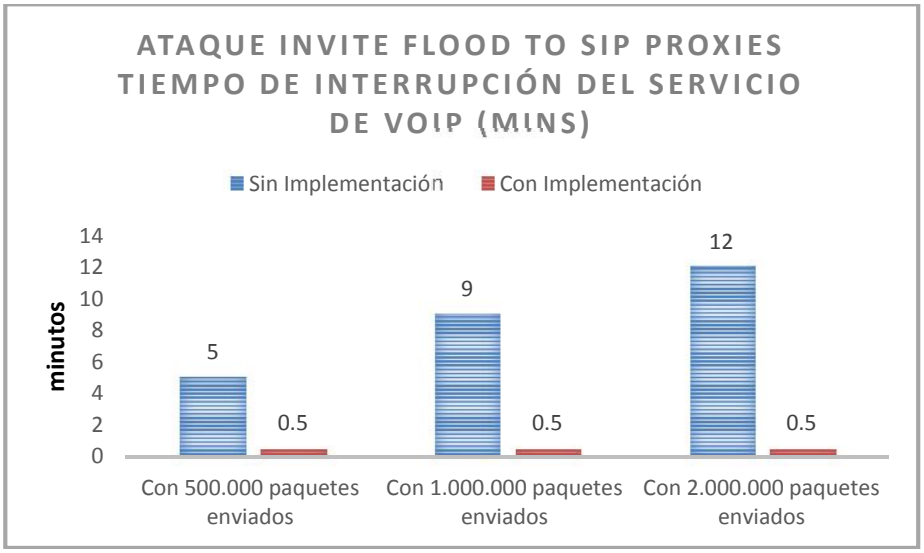


Gráfico 6-4: Resultados de Ataque Invite Flood to Proxy SIP – No Disponibilidad
Realizado por: Arellano Karina, 2016

Como se observa en la Gráfico 6-4, mediante la utilización del Modelo de Seguridad en el ambiente VoIP, se logró proteger la central de telefonía IP, ya que el tiempo de no disponibilidad que experimenta la central VoIP ante esta amenaza es de aproximadamente 0.30 segundos, mismo que muestra la herramienta PRTG, pero no es percibida por el servicio de VoIP, es así que se puede decir que el servicio se muestra 100% disponible, ya que permite recibir como realizar llamadas.

4.3.3. *Ataque invite flood to SIP phones*

Se comparan los resultados obtenidos al ejecutar el ataque Invite Flood específico para teléfonos SIP, en esta investigación se utilizó los softphones Zoiper y Express Talk, tanto en el escenario sin la implementación del Modelo de Seguridad MS-DOS-SIP y con su implementación.

Tabla 34-4: Resultados de Ataque Invite Flood to SIP Phones – Consumo de Recursos

Ataque Invite Flood to SIP Phones Consumo de Recursos del Softphone						
Modelo de Seguridad	**500.000 Paquetes Enviados**		**1.000.000 Paquetes Enviados**		**2.000.000 Paquetes Enviados**	
	CPU (%)	**Memoria (%)**	**CPU (%)**	**Memoria (%)**	**CPU (%)**	**Memoria (%)**
Sin Implementación	100%	81.10%	100%	87.00%	100%	92.40%
Con Implementación	10%	50%	10%	50%	10%	50%

Realizado por: Arellano Karina, 2016

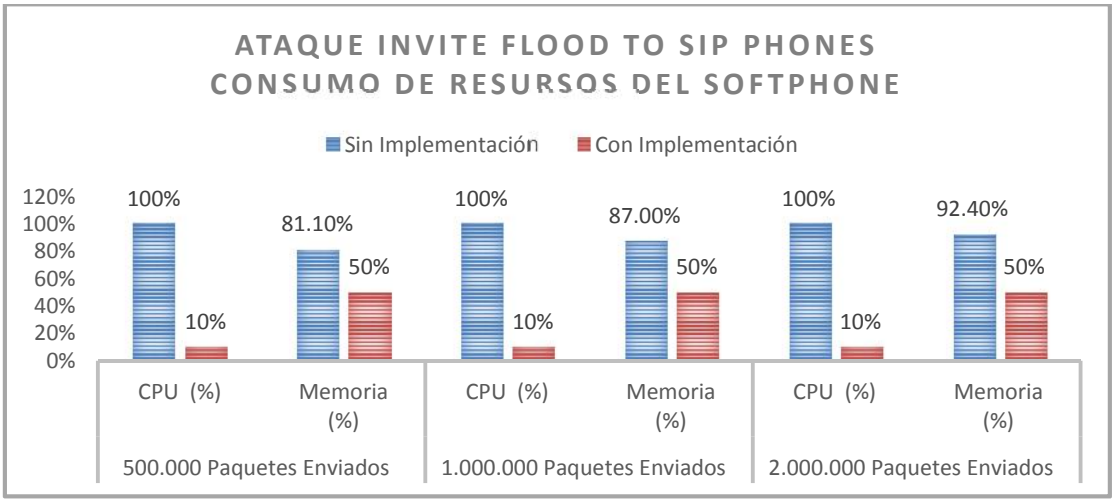


Gráfico 7-4: Resultados de Ataque Invite Flood to SIP Phones – Consumo de Recursos
Realizado por: Arellano Karina, 2016

El consumo de recursos tanto de CPU como de memoria de los dispositivos en que residen los softphone atacados, se minimiza debido a que se ejecutó del Modelo de Seguridad, específicamente al protocolo TLS, tanto en el servidor VoIP como en los clientes SIP.

Tabla 35-4: Resultados de Ataque Invite Flood to SIP Phones – Paquetes Perdidos

Ataque Invite Flood to SIP Phones Parámetros de QoS de la llamada - Paquetes Perdidos (%)									
Modelo de Seguridad	**Duración de la Llamada = 3 minutos**			**Duración de la Llamada = 5 minutos**			**Duración de la Llamada = 8 minutos**		
	500.000 Paquetes	**1.000.000 Paquetes**	**2.000.000 Paquetes**	**500.000 Paquetes**	**1.000.000 Paquetes**	**2.000.000 Paquetes**	**500.000 Paquetes**	**1.000.000 Paquetes**	**2.000.000 Paquetes**
Sin Implementación	38.90%	46.30%	51.10%	45.20%	59.10%	62.00%	29.10%	61.70%	90.30%
Con Implementación	0.10%	0.00%	0.10%	0.00%	0.10%	0.00%	0.00%	0.00%	0.01%

Realizado por: Arellano Karina, 2016

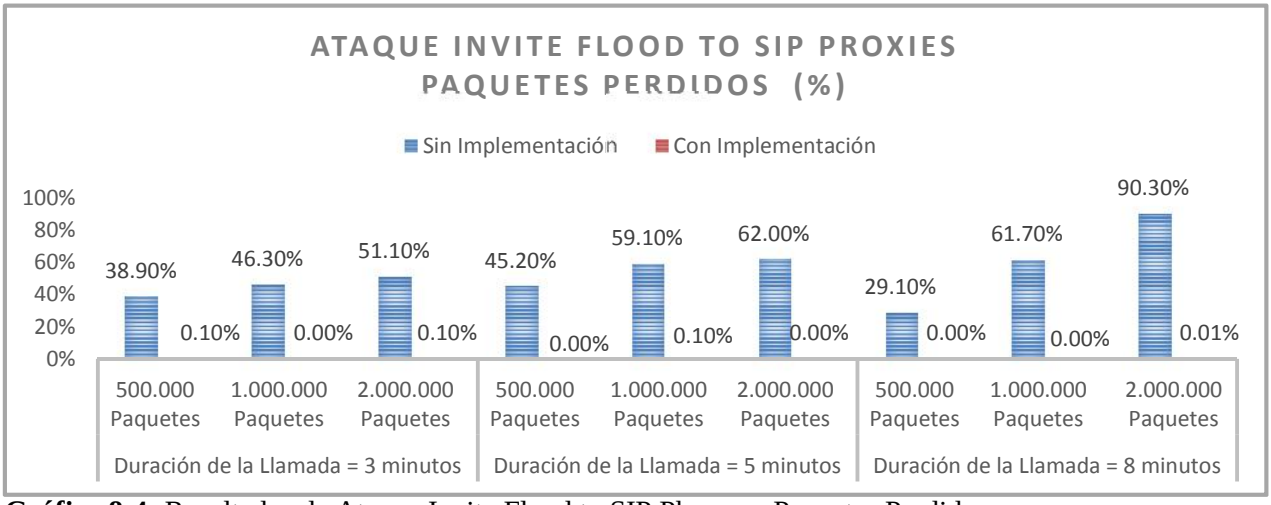


Gráfico 8-4: Resultados de Ataque Invite Flood to SIP Phones – Paquetes Perdidos
Realizado por: Arellano Karina, 2016

Referente al porcentaje de paquetes perdidos, podemos observar en la Gráfico 4-8, que una vez controlado el ataque las comunicaciones se desarrollan bajo los parámetros de calidad, demostrando que la cantidad de paquetes perdidos se minimiza al máximo.

Tabla 36-4: Resultados de Ataque Invite Flood to SIP Phones – Jitter

Ataque Invite Flood to SIP Phones Parámetros de QoS de la llamada - Jitter promedio (ms)									
Modelo de Seguridad	**Duración de la Llamada = 3 minutos**			**Duración de la Llamada = 5 minutos**			**Duración de la Llamada = 8 minutos**		
	500.000 Paquetes	**1.000.000 Paquetes**	**2.000.000 Paquetes**	**500.000 Paquetes**	**1.000.000 Paquetes**	**2.000.000 Paquetes**	**500.000 Paquetes**	**1.000.000 Paquetes**	**2.000.000 Paquetes**
Sin Implementación	66.90	433.65	252.54	75.31	443.84	489.20	95.31	510.98	243.12
Con Implementación	30.34	30.28	28.20	27.20	19.99	21.57	12.76	21.57	31.28

Realizado por: Arellano Karina, 2016

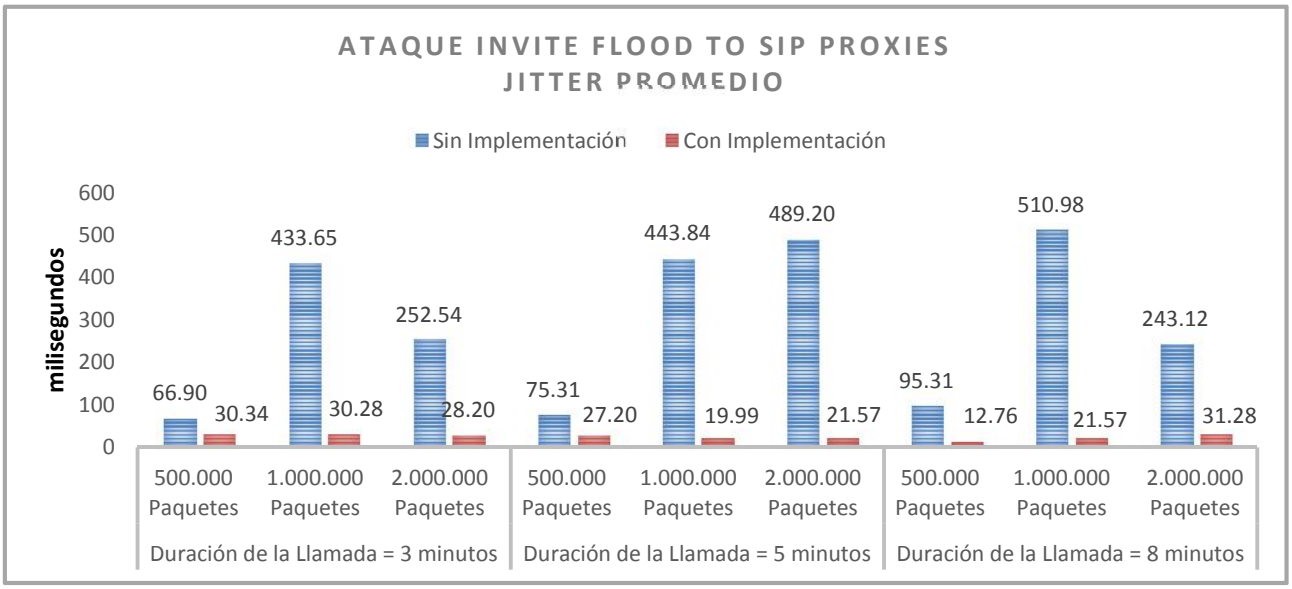


Gráfico 9-4: Resultados de Ataque Invite Flood to SIP Phones – Jitter
Realizado por: Arellano Karina, 2016

Tabla 37-4: Resultados de Ataque Invite Flood to SIP Phones – Latencia

Ataque Invite Flood to SIP Proxies Parámetros de QoS de la llamada - Latencia (ms)									
Modelo de Seguridad	**Duración de la Llamada = 3 minutos**			**Duración de la Llamada = 5 minutos**			**Duración de la Llamada = 8 minutos**		
	500.000 Paquetes	**1.000.000 Paquetes**	**2.000.000 Paquetes**	**500.000 Paquetes**	**1.000.000 Paquetes**	**2.000.000 Paquetes**	**500.000 Paquetes**	**1.000.000 Paquetes**	**2.000.000 Paquetes**
Sin Implementación	372.11	1422.78	1045.26	742.90	1984.77	967.22	726.18	1790.67	972.01
Con Implementación	149.01	108.02	98.13	135.66	176.02	92.28	87.46	114.70	89.03

Realizado por: Arellano Karina, 2016

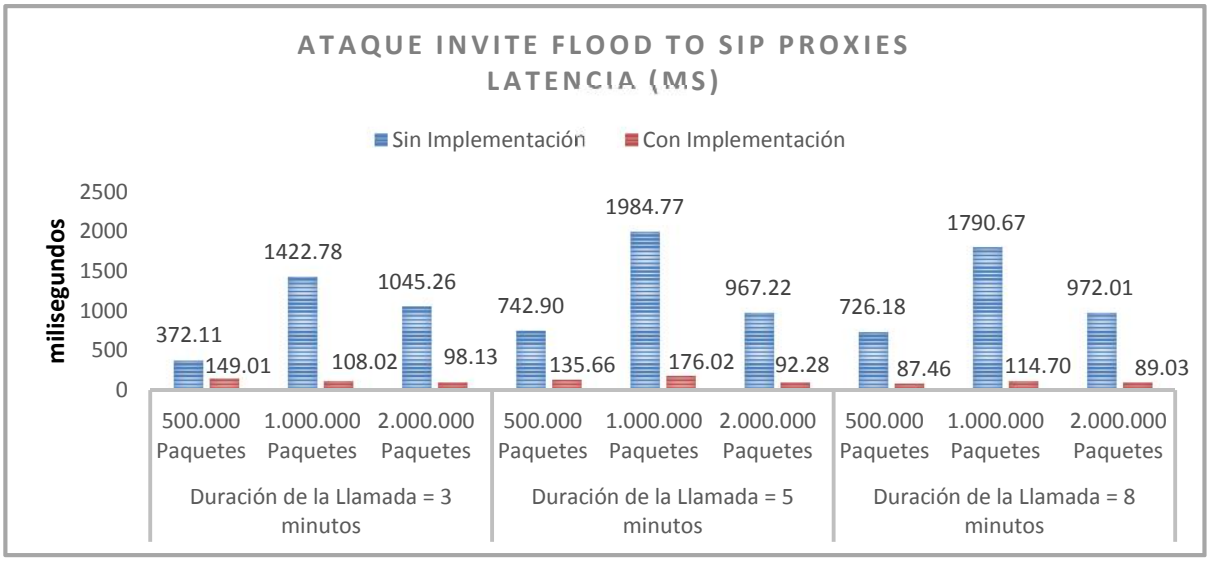


Gráfico 10-4: Resultados de Ataque Invite Flood to SIP Phones – Latencia
Realizado por: Arellano Karina, 2016

Así mismo los valores de Jitter y Latencia se disminuyen considerablemente, dentro de los parámetros permitidos en cada uno de ellos, brindando una comunicación de estable y disponibilidad del servicio de VoIP.

Tabla 38-4: Resultados de Ataque Invite Flood to SIP Phones – No Disponibilidad

Ataque Invite Flood to SIP Phones Tiempo de Interrupción del Servicio de VoIP (mins)			
Modelo de Seguridad	**500.000 paquetes enviados**	**1.000.000 paquetes enviados**	**2.000.000 paquetes enviados**
Sin Implementación	9	13	20
Con Implementación	0	0	0

Realizado por: Arellano Karina, 2016

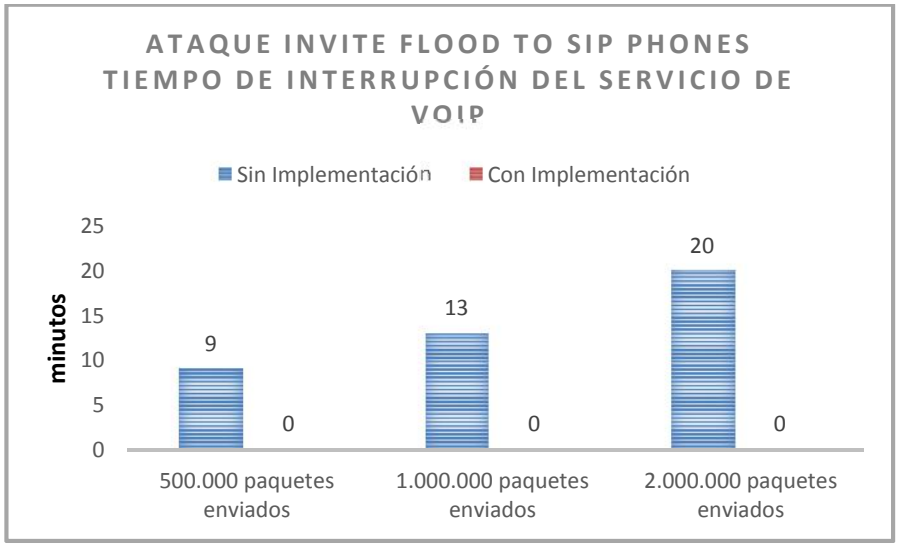


Gráfico 11-4: Resultados de Ataque Invite Flood to SIP Phones – No Disponibilidad
Realizado por: Arellano Karina, 2016

Como resultado de la implementación del Modelo de Seguridad para esta vulnerabilidad, el servicio de un teléfono SIP NO es interrumpido, siendo capaz de recibir y hacer llamadas, dentro de su correcto funcionamiento. Evidentemente incrementa la disponibilidad del servicio a 100%.

4.3.4. *Ataque SYN flood DoS*

Se comparan los resultados obtenidos al ejecutar el ataque SYN Flood DoS, tanto en el escenario sin la implementación del Modelo de Seguridad MS-DOS-SIP, como con su implementación.

Tabla 39-4: Resultados de Ataque SYN Flood DoS – Consumo de Recursos

Ataque SYN Flood DoS Consumo de Recursos del Servidor						
Modelo de Seguridad	**500.000 Paquetes Enviados**		**1.000.000 Paquetes Enviados**		**2.000.000 Paquetes Enviados**	
	CPU (%)	**Memoria (%)**	**CPU (%)**	**Memoria (%)**	**CPU (%)**	**Memoria (%)**
Sin Implementación	98.40%	39.20%	100.00%	48.30%	100.00%	77.30%
Con Implementación	24.40%	26.00%	24.00%	25.70%	25.30%	26.01%

Realizado por: Arellano Karina, 2016

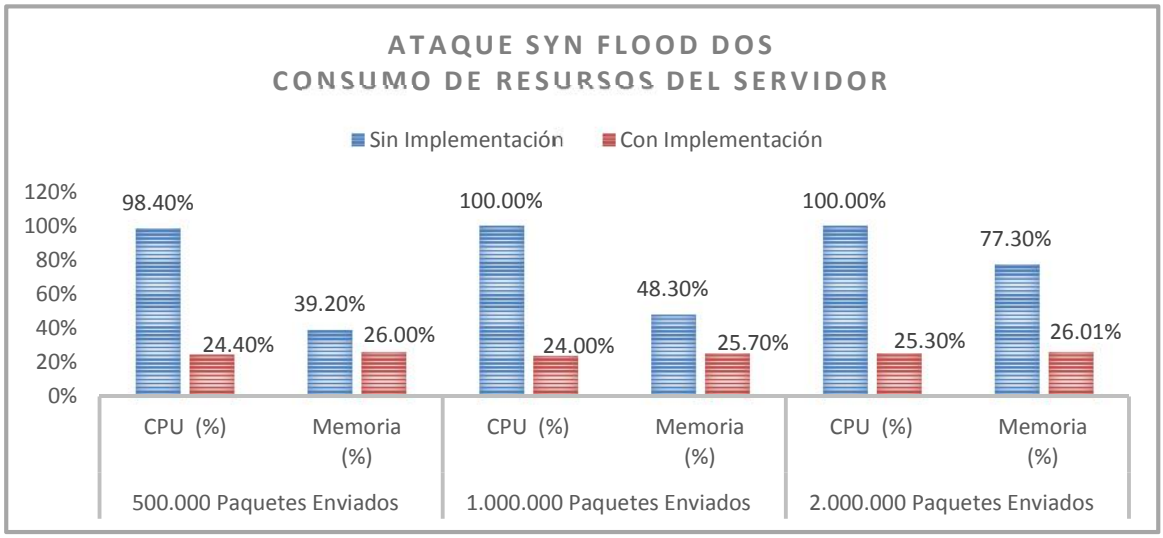


Gráfico 12-4: Resultados de Ataque SYN Flood DoS – Consumo de Recursos
Realizado por: Arellano Karina, 2016

De acuerdo a los resultados obtenidos con la aplicación del Modelo de Seguridad, se disminuye notablemente el consumo de recursos del Servidor VoIP, permitiendo su correcto funcionamiento.

Tabla 40-4: Resultados de Ataque SYN Flood DoS – Paquetes Perdidos

Ataque SYN Flood DoS Parámetros de QoS de la llamada - Paquetes Perdidos (%)									
Modelo de Seguridad	**Duración de la Llamada = 3 minutos**			**Duración de la Llamada = 5 minutos**			**Duración de la Llamada = 8 minutos**		
	500.000 Paquetes	**1.000.000 Paquetes**	**2.000.000 Paquetes**	**500.000 Paquetes**	**1.000.000 Paquetes**	**2.000.000 Paquetes**	**500.000 Paquetes**	**1.000.000 Paquetes**	**2.000.000 Paquetes**
Sin Implementación	73.70%	66.60%	61.60%	43.80%	73.80%	53.50%	52.40%	63.60%	73.10%
Con Implementación	0.00%	0.00%	1.00%	0.00%	0.00%	1.00%	0.01%	0.00%	0.00%

Realizado por: Arellano Karina, 2016

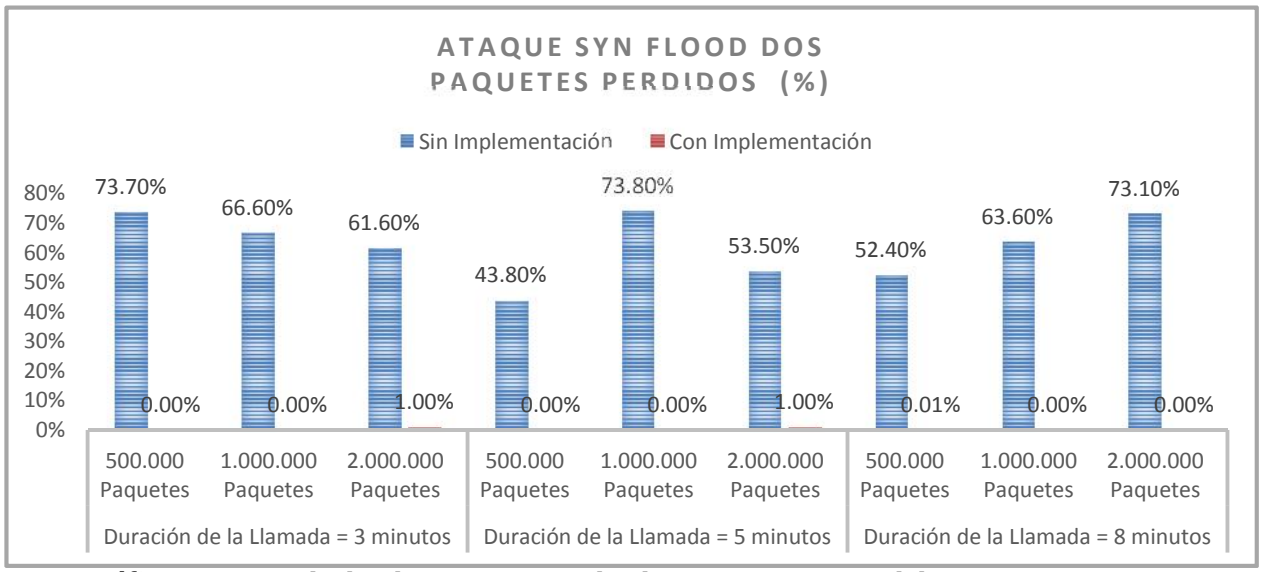


Gráfico 13-4: Resultados de Ataque SYN Flood DoS – Paquetes Perdidos
Realizado por: Arellano Karina, 2016

Así mismo se determina que la cantidad de paquetes perdidos desciende considerablemente, en diferencia con los resultados obtenidos sin la implementación del Modelo de Seguridad, que llegaban has aproximadamente el 80% de paquetes perdidos.

Tabla 41-4: Resultados de Ataque SYN Flood DoS – Jitter

Ataque SYN Flood DoS Parámetros de QoS de la llamada - Jitter promedio (ms)									
Modelo de Seguridad	**Duración de la Llamada = 3 minutos**			**Duración de la Llamada = 5 minutos**			**Duración de la Llamada = 8 minutos**		
	600.000 Paquetes	**1.500.000 Paquetes**	**2.500.000 Paquetes**	**600.000 Paquetes**	**1.500.000 Paquetes**	**2.500.000 Paquetes**	**600.000 Paquetes**	**1.500.000 Paquetes**	**2.500.000 Paquetes**
Sin Implementación	64.17	27.83	93.30	32.99	87.22	38.46	42.02	18.11	75.68
Con Implementación	15.88	16.33	12.23	9.18	14.45	8.87	7.95	9.15	11.18

Realizado por: Arellano Karina, 2016

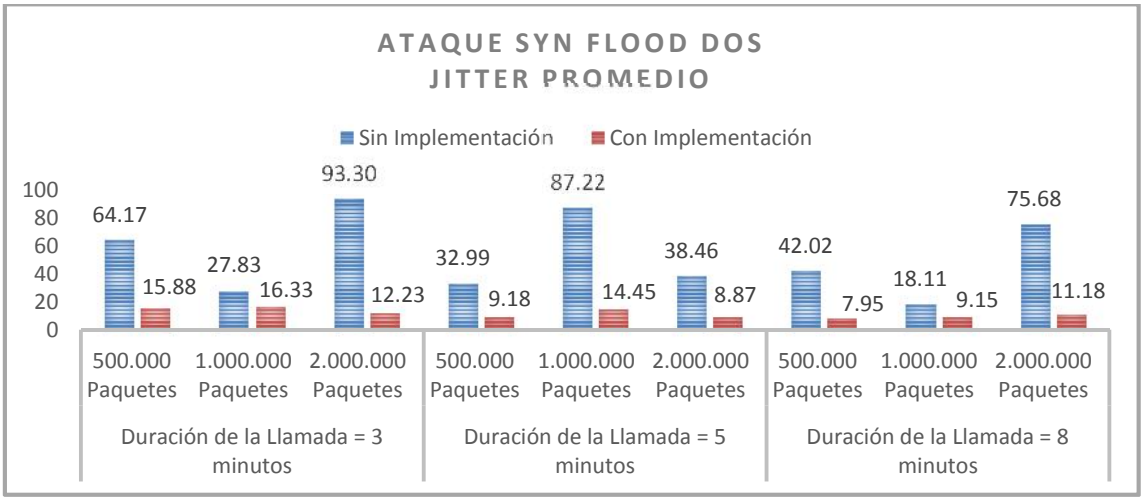


Gráfico 14-4: Resultados de Ataque SYN Flood DoS – Jitter
Realizado por: Arellano Karina, 2016

Tabla 42-4: Resultados de Ataque SYN Flood DoS – Latencia

Ataque SYN Flood DoS Parámetros de QoS de la llamada - Latencia (ms)									
Modelo de Seguridad	**Duración de la Llamada = 3 minutos**			**Duración de la Llamada = 5 minutos**			**Duración de la Llamada = 8 minutos**		
	600.000 Paquetes	**1.500.000 Paquetes**	**2.500.000 Paquetes**	**600.000 Paquetes**	**1.500.000 Paquetes**	**2.500.000 Paquetes**	**600.000 Paquetes**	**1.500.000 Paquetes**	**2.500.000 Paquetes**
Sin Implementación	639.50	607.05	522.79	614.28	813.35	713.57	803.78	560.47	979.72
Con Implementación	67.92	79.67	65.49	75.91	59.50	21.65	76.10	32.30	68.43

Realizado por: Arellano Karina, 2016

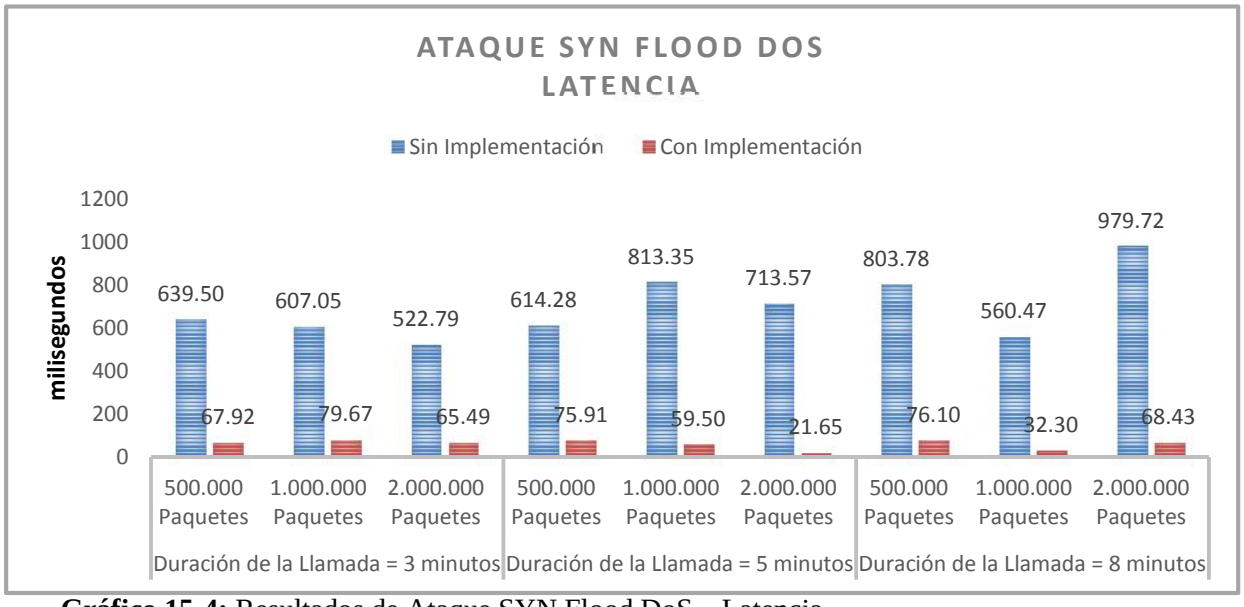


Gráfico 15-4: Resultados de Ataque SYN Flood DoS – Latencia
Realizado por: Arellano Karina, 2016

Los valores tanto de Jitter como Latencia también disminuyen, manteniéndose dentro de los intervalos permitidos en cada uno de ellos, contrastando con los valores obtenidos anteriormente sin la presencia del Modelo de Seguridad.

Tabla 43-4: Resultados de Ataque SYN Flood DoS – No Disponibilidad

Ataque SYN Flood DoS Tiempo de Interrupción del Servicio de VoIP (mins)			
Modelo de Seguridad	**500.000 paquetes enviados**	**1.000.000 paquetes enviados**	**2.000.000 paquetes enviados**
Sin Implementación	3	5	8
Con Implementación	0.5	0.5	0.5

Realizado por: Arellano Karina, 2016

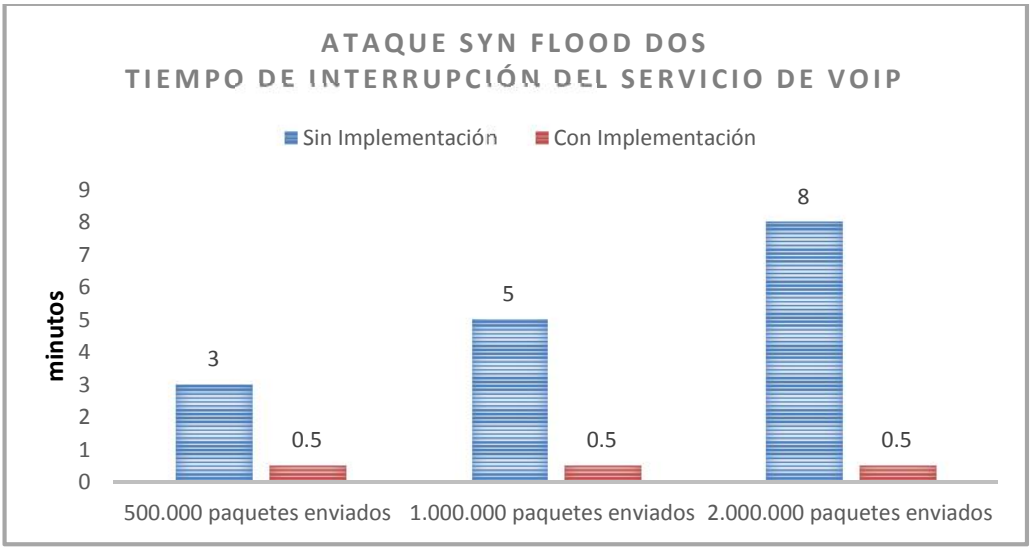


Gráfico 16-4: Resultados de Ataque SYN Flood DoS – No Disponibilidad
Realizado por: Arellano Karina, 2016

Como resultado de aplicar del Modelo de Seguridad, se consigue resguardar la central de telefonía IP, ya que el tiempo de no disponibilidad que experimenta la central VoIP ante esta amenaza es de aproximadamente 0.30 segundos es decir 0.5 minutos, que se observa en la herramienta PRTG, al ser una pequeña cantidad de no tiene impacto en la disponibilidad y calidad del servicio de VoIP, es así que se puede decir que el servicio se muestra 100% disponible.

4.3.5. *Ataque fuzzing – malformación de mensajes INVITE*

Se comparan los resultados obtenidos al ejecutar el ataque Fuzzing específicamente Malformación de Mensajes INVITE, tanto en el escenario sin la implementación del Modelo de Seguridad MS-DOS-SIP, como con su implementación.

Tabla 44-4: Resultados de Ataque Fuzzing – Consumo de Recursos

Ataque Fuzzing - Malformación en mensajes INVITE Consumo de Recursos del Servidor						
Modelo de Seguridad	**500.000 Paquetes Enviados**		**1.000.000 Paquetes Enviados**		**2.000.000 Paquetes Enviados**	
	CPU (%)	**Memoria (%)**	**CPU (%)**	**Memoria (%)**	**CPU (%)**	**Memoria (%)**
Sin Implementación	28.30%	58.10%	35.60%	76.50%	42.10%	98.90%
Con Implementación	24.30%	26.00%	25.20%	24.30%	25.10%	24.60%

Realizado por: Arellano Karina, 2016

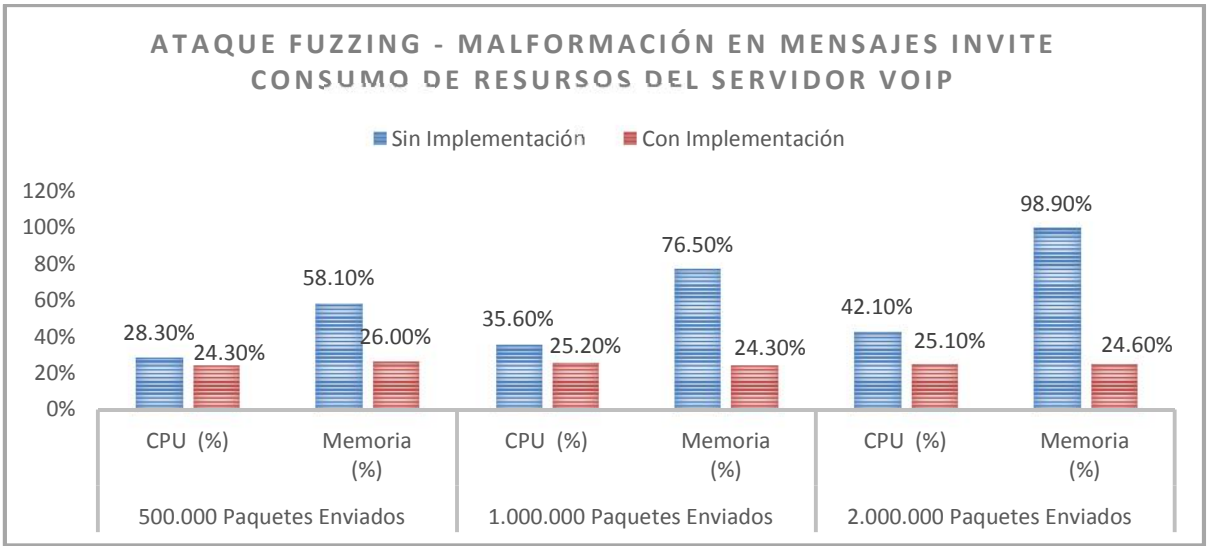


Gráfico 17-4: Resultados de Ataque Fuzzing– Consumo de Recursos
Realizado por: Arellano Karina, 2016

Como se observa en la Gráfico 17-4, este tipo de ataques provoca el desbordamiento de la memoria del servidor atacado, puesto que necesita procesar una gran cantidad de paquetes con formatos extraños. Pero al aplicar el Modelo de Seguridad, se logra combatir estas amenazas, y disminuir el procesamiento del servidor VoIP, ya que estos paquetes malformados son detectados por el SBC y bloqueados, no permitiendo que lleguen hasta la central.

Tabla 45-4: Resultados de Ataque Fuzzing – Paquetes Perdidos

Ataque Fuzzing - Malformación en mensajes INVITE Parámetros de QoS de la llamada - Paquetes Perdidos (%)									
Modelo de Seguridad	**Duración de la Llamada = 3 minutos**			**Duración de la Llamada = 5 minutos**			**Duración de la Llamada = 8 minutos**		
	500.000 Paquetes	**1.000.000 Paquetes**	**2.000.000 Paquetes**	**500.000 Paquetes**	**1.000.000 Paquetes**	**2.000.000 Paquetes**	**500.000 Paquetes**	**1.000.000 Paquetes**	**2.000.000 Paquetes**
Sin Implementación	13.60%	9.01%	10.78%	3.01%	23.78%	11.09%	7.03%	9.98%	32.20%
Con Implementación	0.00%	1.30%	0.00%	0.00%	0.10%	2.01%	0.00%	0.10%	2.70%

Realizado por: Arellano Karina, 2016

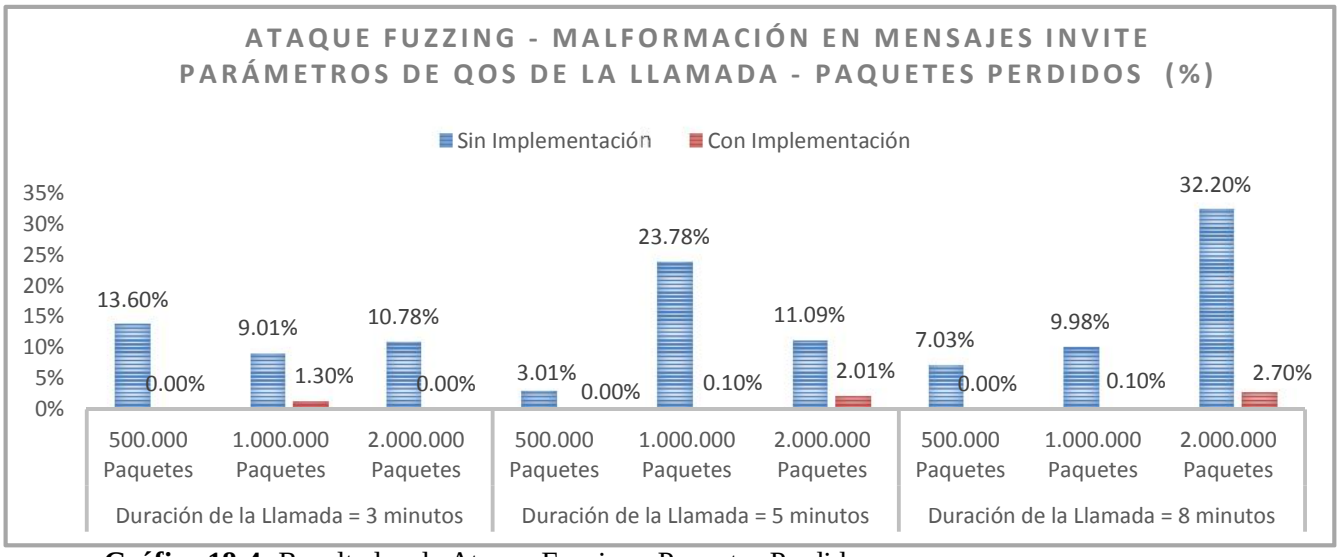


Gráfico 18-4: Resultados de Ataque Fuzzing– Paquetes Perdidos
Realizado por: Arellano Karina, 2016

Al combatir esta amenaza con la ayuda del Modelo de Seguridad, también permite reducir altamente el porcentaje de paquetes perdidos dentro de una comunicación, haciendo que esta sea clara y agradable para los usuarios de VoIP.

Tabla 46-4: Resultados de Ataque Fuzzing – Jitter

Ataque Fuzzing - Malformación en mensajes INVITE Parámetros de QoS de la llamada - Jitter promedio (ms)									
Modelo de Seguridad	**Duración de la Llamada = 3 minutos**			**Duración de la Llamada = 5 minutos**			**Duración de la Llamada = 8 minutos**		
	500.000 Paquetes	**1.000.000 Paquetes**	**2.000.000 Paquetes**	**500.000 Paquetes**	**1.000.000 Paquetes**	**2.000.000 Paquetes**	**500.000 Paquetes**	**1.000.000 Paquetes**	**2.000.000 Paquetes**
Sin Implementación	241.66	333.64	102.56	68.92	167.09	85.87	65.75	235.09	417.78
Con Implementación	32.72	38.54	42.65	35.22	23.45	12.67	9.34	19.01	20.07

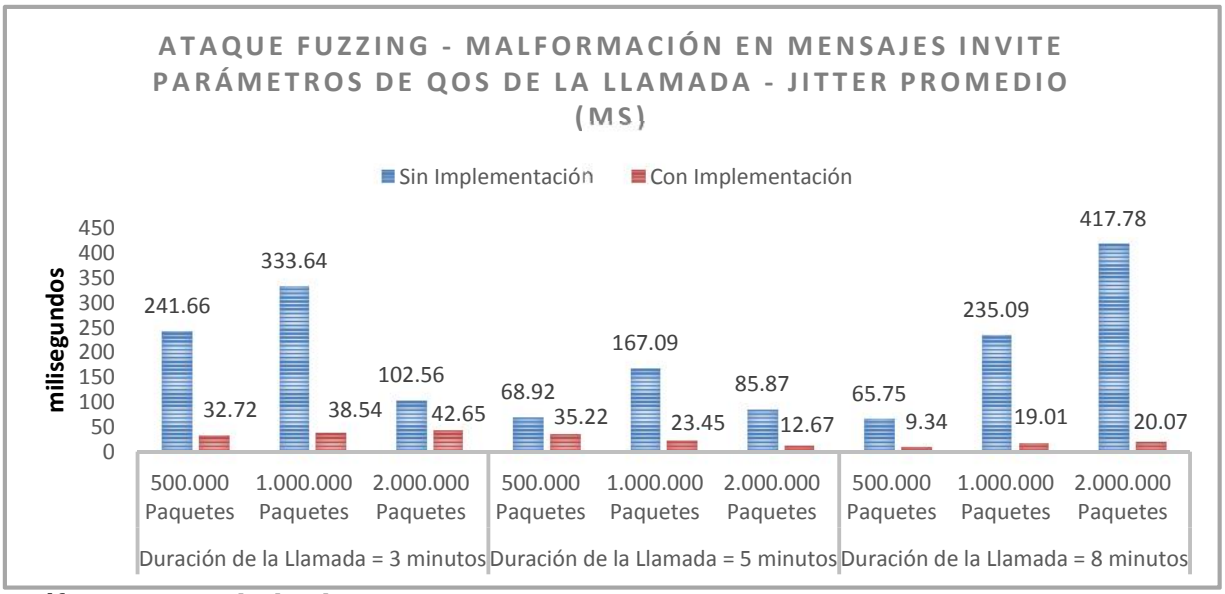


Gráfico 19-4: Resultados de Ataque Fuzzing– Jitter
Realizado por: Arellano Karina, 2016

Tabla 47-4: Resultados de Ataque Fuzzing – Latencia

Ataque Fuzzing - Malformación en mensajes INVITE Parámetros de QoS de la llamada - Latencia (ms)									
Modelo de Seguridad	**Duración de la Llamada = 3 minutos**			**Duración de la Llamada = 5 minutos**			**Duración de la Llamada = 8 minutos**		
	500.000 Paquetes	**1.000.000 Paquetes**	**2.000.000 Paquetes**	**500.000 Paquetes**	**1.000.000 Paquetes**	**2.000.000 Paquetes**	**500.000 Paquetes**	**1.000.000 Paquetes**	**2.000.000 Paquetes**
Sin Implementación	109.99	719.82	867.34	502.27	435.89	298.54	124.03	856.09	345.87
Con Implementación	80.34	98.02	46.43	67.87	32.08	76.40	96.42	71.63	98.75

Realizado por: Arellano Karina, 2016

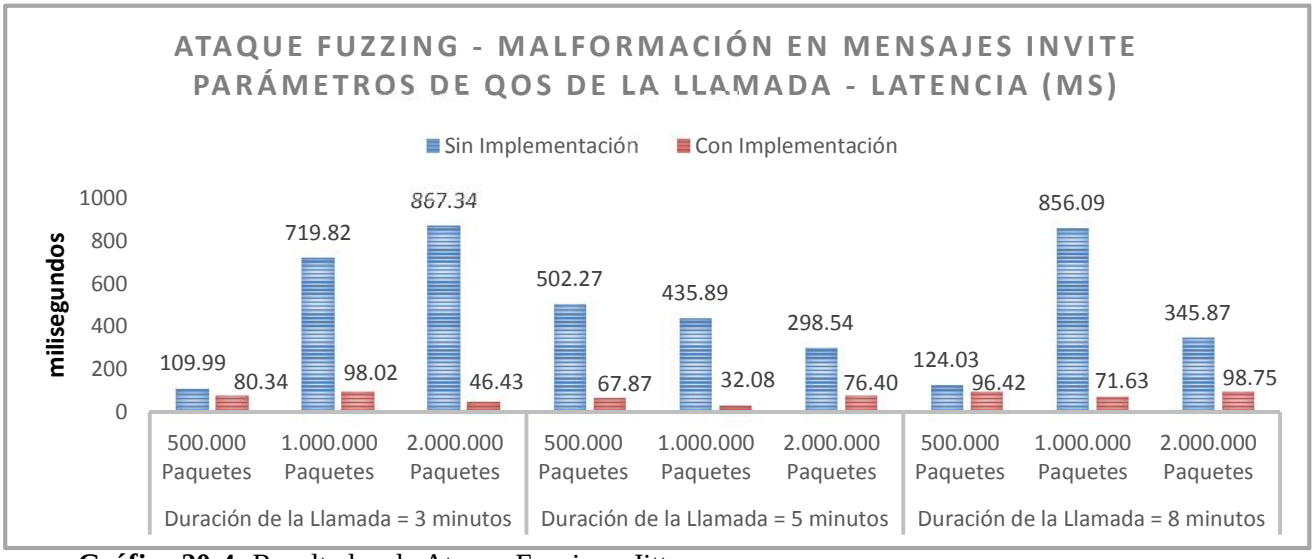


Gráfico 20-4: Resultados de Ataque Fuzzing– Jitter
Realizado por: Arellano Karina, 2016

Los valores de Jitter y Latencia también son afectados al ejecutarse con éxito esta amenaza, indisponiendo el servicio o a su vez impidiendo su correcto funcionamiento, en cambio en el ambiente VoIP con mecanismo de seguridad del Modelo de Seguridad MS-DOS-SIP estos valores se mantienen dentro de lo permitido.

Tabla 48-4: Resultados de Ataque Fuzzing – No Disponibilidad

Ataque Fuzzing - Malformación en mensajes INVITE Tiempo de Interrupción del Servicio de VoIP (mins)			
Modelo de Seguridad	**500.000 paquetes enviados**	**1.000.000 paquetes enviados**	**2.000.000 paquetes enviados**
Sin Implementación	9.0	13.0	20.0
Con Implementación	1.0	1.0	1.0

Realizado por: Arellano Karina, 2016:

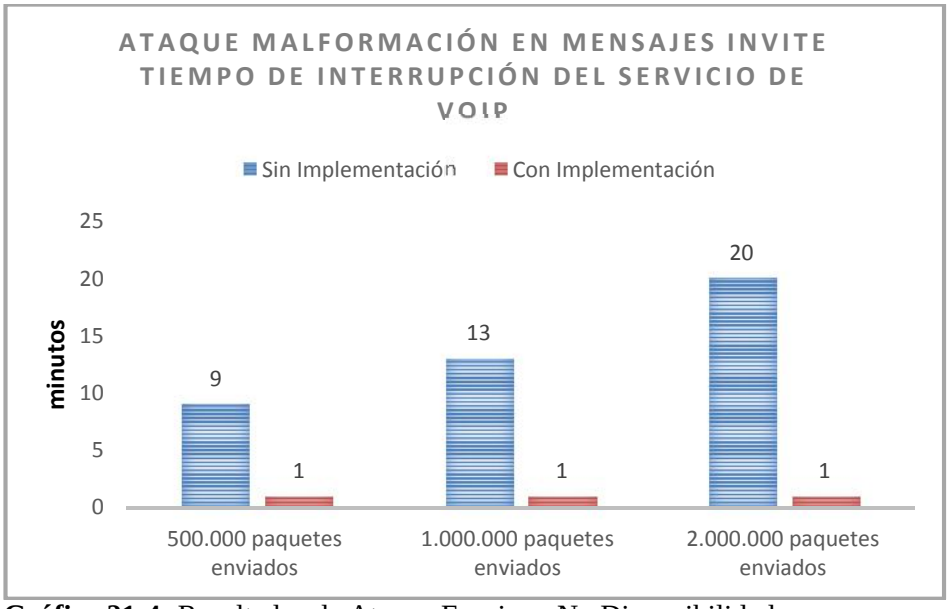


Gráfico 21-4: Resultados de Ataque Fuzzing– No Disponibilidad
Realizado por: Arellano Karina, 2016

Como resultado de emplear del Modelo de Seguridad, se obtiene mayor disponibilidad del servicio de VoIP, puesto que el tiempo de no disponibilidad que experimenta la central VoIP ante esta amenaza es de aproximadamente 1 minuto, que se observa en la herramienta PRTG.

4.3.6. *Ataque de eliminación de registro de usuarios SIP*

Se comparan los resultados obtenidos al ejecutar el ataque de Eliminación de Registro de Usuarios SIP, tanto en el escenario sin la implementación del Modelo de Seguridad MS-DOS-SIP, como con su implementación.

Tabla 49-4: Resultados de Ataque Eliminación de Registro de Usuarios SIP – Consumo de Recursos

Ataque Eliminación de Registro de Usuarios SIP Consumo de Recursos del Servidor						
Modelo de Seguridad	**500.000 Paquetes Enviados**		**1.000.000 Paquetes Enviados**		**2.000.000 Paquetes Enviados**	
	CPU (%)	**Memoria (%)**	**CPU (%)**	**Memoria (%)**	**CPU (%)**	**Memoria (%)**
Sin Implementación	26.70%	63.70%	32.40%	70.20%	50.34%	88.24%
Con Implementación	24.10%	25.40%	23.40%	25.01%	25.20%	24.30%

Realizado por: Arellano Karina, 2016

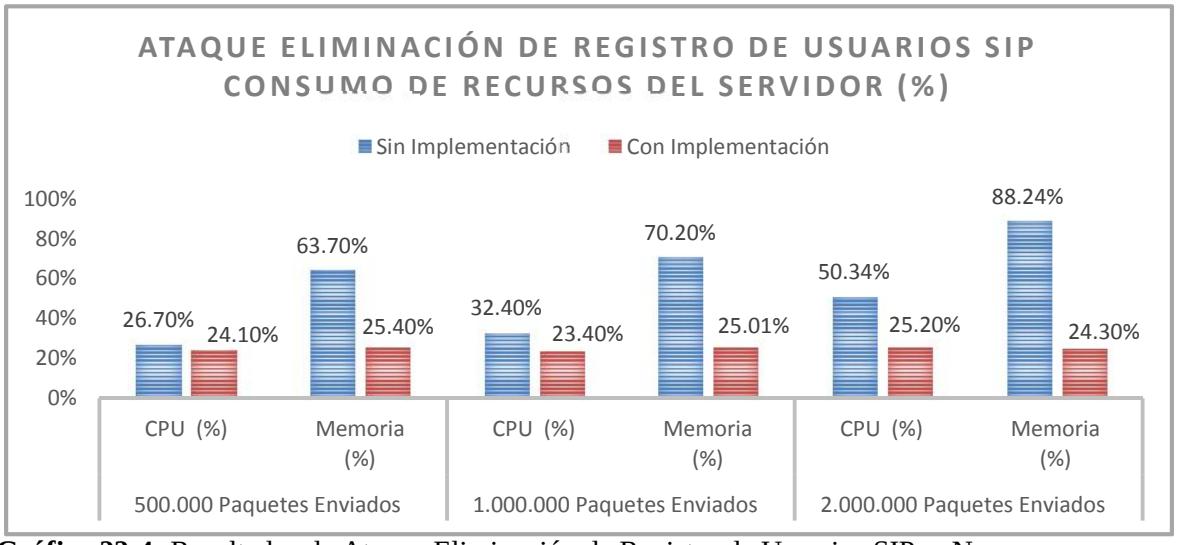


Gráfico 22-4: Resultados de Ataque Eliminación de Registro de Usuarios SIP – No Disponibilidad

Realizado por: Arellano Karina, 2016

Finalmente se puede observar que el consumo de recursos (CPU y Memoria) que invierte la central telefónica una vez aplicado el Modelo de Seguridad es inferior a los valores presentados en el ambiente VoIP siendo víctima de un ataque de Eliminación de Registros sin contar con ninguna medida de seguridad.

Tabla 50-4: Resultados de Ataque Eliminación de Registro de Usuarios SIP – Consumo de Recursos

Ataque Eliminación de Registro de Usuarios SIP Tiempo de Interrupción del Servicio de VoIP (mins)			
Modelo de Seguridad	**500.000 paquetes enviados**	**1.000.000 paquetes enviados**	**2.000.000 paquetes enviados**
Sin Implementación	5	8	15
Con Implementación	0	0	0

Realizado por: Arellano Karina, 2016

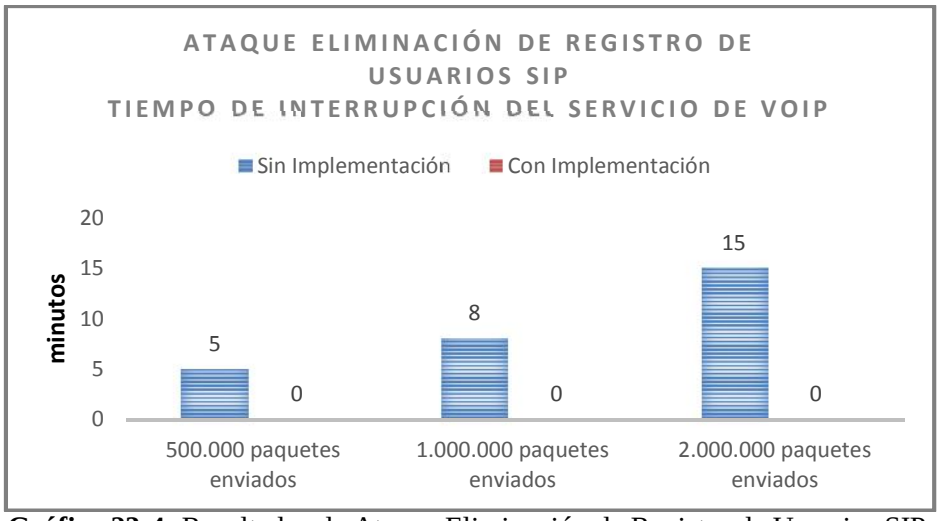


Gráfico 23-4: Resultados de Ataque Eliminación de Registro de Usuarios SIP – No Disponibilidad

Realizado por: Arellano Karina, 2016

Como resultado de la implementación del Modelo de Seguridad, permite incrementar el tiempo de disponibilidad del servicio de VoIP, al mitigar esta amenaza, llevándolo a estar 100% disponible.

4.4. Prueba de la hipótesis de investigación

4.4.1 *Hipótesis*

El Modelo de Seguridad para mitigar ataques de Denegación de Servicio en tráfico SIP en servicios VoIP, reduce las vulnerabilidades ante ataques de DoS incrementando la disponibilidad del servicio de VoIP en redes LAN Corporativas.

4.4.2. *Tipo de hipótesis*

La Hipótesis del presente trabajo es de Tipo Investigación

4.4.3. *Población y muestra*

4.4.3.1. *Población*

En la presente investigación, la población está representada por el conjunto de ataques a la seguridad específica del protocolo de señalización SIP, debido a que el tema investigado se centra en ataques SIP en servicios VOIP, como se muestra en la Tabla 4-51.

Tabla 51-4: Población de la investigación

Amenaza/Ataques	**Confidencialidad**	**Integridad**	**Disponibilidad**
*Eavesdropping (*Intercepción de mensajes de señalización)	x	x	
Suplantación de identidad (Registration hijacking)		x	
Eliminación de Registro de Usuarios	x	x	x
Desconexión de usuarios	x	x	
Malformación en mensajes INVITE			x
Inundación en mensajes INVITE, REGISTER, BYE, CANCEL			x
Ataque de falsa respuesta (Faked Response)	x	x	
Ataque de Re-INVITE		x	
Ataque de Enumeración SIP	x	x	

Realizado por: Arellano Karina, 2016

4.4.3.2. *Muestra*

El tipo de muestra usada en esta investigación es NO ALEATRORIA, ya que se seleccionaron simplemente los ataques que comprometan la disponibilidad del servicio VoIP o impidan su correcto funcionamiento, debido a que el presente tema de investigación se enfoca en ataques de Denegación de Servicio. Es así que se obtuvo una muestra de 5 ataques, que se detallan en la Tabla 4-52.

Tabla 52-4: Muestra de la Investigación

N°	ATAQUE
1	INVITEFlood to SIP Proxy
2	INVITEFlood to SIP Phones
3	Fuzzing (Malformación de Mensajes INVITE)
4	Eliminación de Registro de Usuarios SIP
5	SYN Flood Dos

Realizado por: Arellano Karina, 2016

4.4.4. *Determinación de variables*

De acuerdo a la hipótesis planteada, se determinan las siguientes variables:

Tabla 53-4: Operacionalización Conceptual

VARIABLE	TIPO
Modelo de Seguridad para mitigar ataques de Denegación de Servicio en tráfico SIP en servicios VoIP	Independiente
Vulnerabilidad	Dependiente
Disponibilidad	Dependiente

Realizado por: Arellano Karina, 2016

4.4.5. *Operacionalización conceptual de variables*

La Tabla 54-4, muestra la operacionalización conceptual de las variables determinadas.

Tabla 54-4: Operacionalización Conceptual

VARIABLE	TIPO	CONCEPTO
Modelo de Seguridad para mitigar ataques de Denegación de Servicio en tráfico SIP en servicios VoIP	Simple Cualitativa Independiente	Es el conjunto de medidas que se pueden tomar para contrarrestar o minimizar los impactos. El propósito de la mitigación es la reducción de la vulnerabilidad
Vulnerabilidad	Compleja Cuantitativa Dependiente	Son errores que permiten realizar desde afuera actos sin permiso del administrador del equipo, incluso se puede suplantar al usuario

Disponibilidad	Compleja Cuantitativa Dependiente	Es el porcentaje de tiempo que un sistema es capaz de realizar las funciones para las que está diseñado

Realizado por: Arellano Karina, 2016

4.4.6. *Operacionalización metodológica de variables*

La Tabla 55-4, muestra la operacionalización metodológica de las variables determinadas.

Tabla 55-4: Operacionalización metodológica

VARIABLE	INDICADOR	TÉCNICA	INSTRUMENTO/ FUENTE
Modelo de Seguridad para mitigar ataques de Denegación de Servicio en tráfico SIP en servicios VoIP	-Nivel de Complejidad -Número de Herramientas Usadas - Recursos usados	-Búsqueda de Información - Revisión de papers, journal, etc -Observación -Pruebas -Análisis con Software	- Firewall Iptables - SBC Blox - File2ban - TLS
Vulnerabilidad	-Número de Vulnerabilidades Identificadas	-Observación -Pruebas de Penetración -Análisis	- Kali Linux - Nmap, Zenmap - Servidor de VoIP - Sivus - Wireshark
Disponibilidad	-Porcentaje de recursos usados (CPU, RAM, etc) -Porcentaje del Trafico de la Red -Tiempo de no disponibilidad del Servicio VoIP -Porcentaje de Paquetes Perdidos - Jitter - Latencia	-Observación -Análisis con Software -Pruebas	- Escenarios de Pruebas - PRTG Monitor - Wireshark - Cacti

Realizado por: Arellano Karina, 2016

4.4.7. *Resultados de la medición de indicadores*

El resultado de la medición del ***Indicador: Número de Vulnerabilidades identificadas***, se muestra en la Tabla 56-4, en la que se lista las vulnerabilidades encontradas en el escenario de pruebas simulado, y se identifican las que han sido posibles mitigar mediante la implementación del Modelo de Seguridad propuesto y las que no han sido posibles.

Tabla 56-4: Resultados de Análisis de Vulnerabilidades en Escenario con Implementación del Modelo de Seguridad

N°	Vulnerabilidad	Mitigada	No Mitigada
1	Puertos abiertos innecesarios	si	---
2	Enumeración de dispositivos SIP habilitada	si	---
3	Permisos de escaneo de usuarios SIP habilitado	si	---
4	Configuraciones Débiles	si	---
5	Falta de Segmentación de la Red	si	---
6	Uso de puertos por defecto	si	---
7	Servicios habilitados innecesarios	si	---
8	Falta de Autenticación	si	---
9	Ausencia de Firewall	si	---
10	Falta de Sistemas de Seguridad	si	---
11	Falta de Actualizaciones y parcheo en sistemas VoIP	si	---
12	Terminales SIP Inseguras	si	---
13	Protocolo SSH sin protección	--	no
TOTAL		**12**	**1**

Realizado por: Arellano Karina, 2016

Tabla 57-4: Resultados Final del Análisis de Vulnerabilidades

Modelo de Seguridad	Número de Vulnerabilidades encontradas
Sin Implementación	13
Con Implementación	1

Realizado por: Arellano Karina, 2016

Se puede observar que aún existe una vulnerabilidad que no se ha sido solucionada, esto se debe a que en la guía no se ha considerado la recomendación para solución a dicho problema, ya que no es específico de SIP.

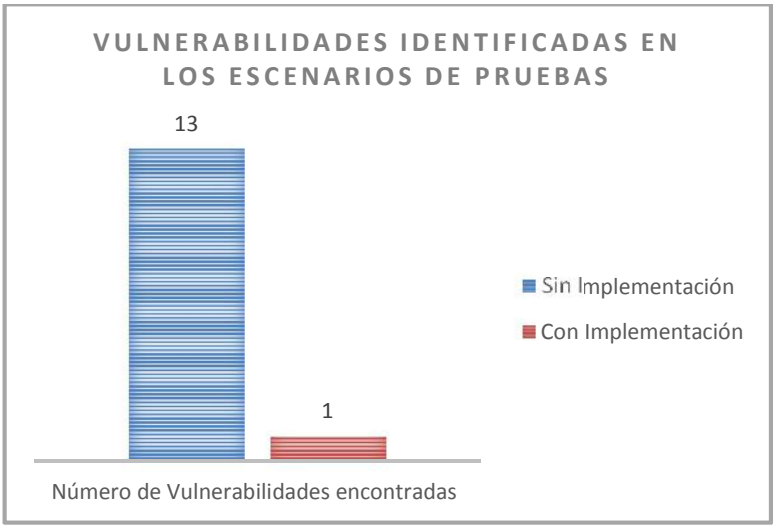


Gráfico 24-4: Resultado final de Análisis de Vulnerabilidades
Realizado por: Arellano Karina, 2016

De esta manera se concluye que mediante la implementación del Modelo de Seguridad MS-DOS-SIP, se reduce en un 92% las vulnerabilidades de DoS en ambientes VOIP basados en SIP, considerando que las 13 vulnerabilidades es el 100%.

Con respecto al ***Indicador: Tiempo de no disponibilidad del servicio VoIP***, se observa en la Tabla 4-58, que con la implementación del Modelo de Seguridad MS-DoS-SIP, se incrementa considerablemente el tiempo de ***disponibilidad*** del servicio de VoIP; de tal manera que los usuarios podrán hacer uso del mismo sin ningún contratiempo, como se observa en la Gráfico 25-4.

Tabla 58-4: Resultados Final del Tiempo de Interrupción del Servicio VoIP

Tiempo de Interrupción del Servicio de VoIP (mins)															
Modelo de Seguridad	**Ataque Invite Flood to SIP Proxies**			**Ataque Invite Flood to SIP Phones**			**Ataque SYN Flood DoS**			**Ataque Fuzzing - Malformación en mensajes INVITE**			**Eliminación de Registro de Usuarios SIP**		
	500.000 pe	**1.000.000 pe**	**2.000.000 pe**	**500.000 pe**	**1.000.000 pe**	**2.000.000 pe**	**500.000 pe**	**1.000.000 pe**	**2.000.000 pe**	**500.000 pe**	**1.000.000 pe**	**2.000.000 pe**	**500.000 pe**	**1.000.000 pe**	**2.000.000 pe**
Sin Implementación	5	9	12	9	13	20	3	5	8	9	13	20	5	8	15
Con Implementación	0.5	0.5	0.5	0	0	0	0.5	0.5	0.5	1	1	1	0	0	0

Realizado por: Arellano Karina, 2016
NOTA: pe:*paquetes enviados*

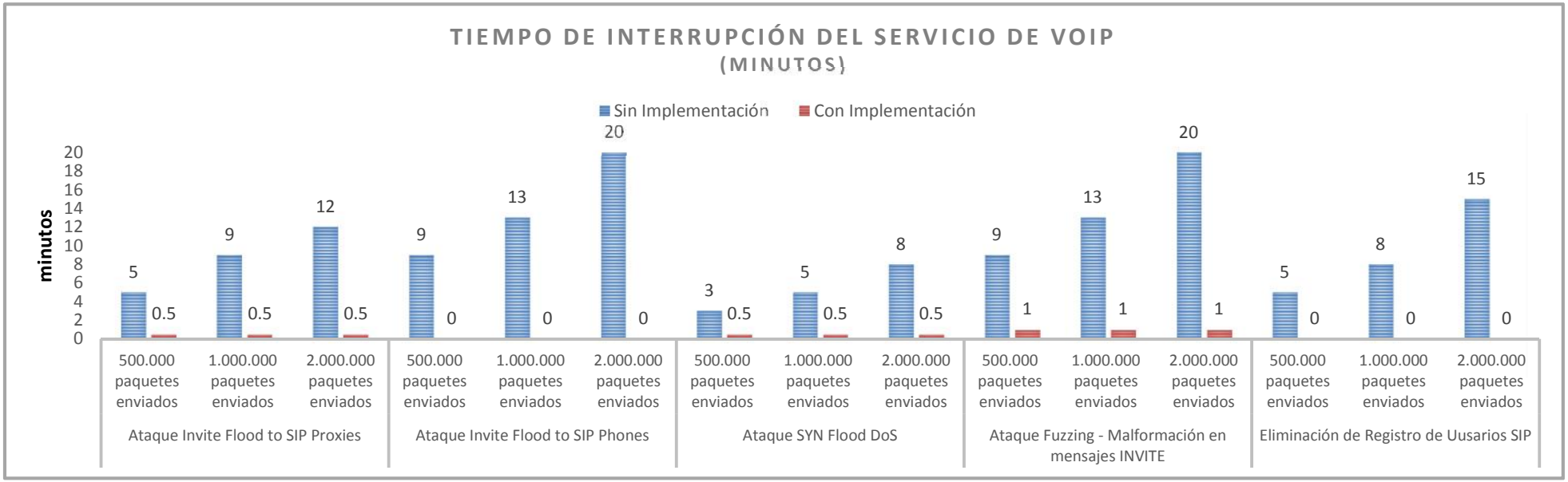


Gráfico 25-4: Incremento del Tiempo de Disponibilidad del Servicio VoIP
Realizado por: Arellano Karina, 2016

4.4.8. *Comprobación estadística de la hipótesis*

De acuerdo al análisis desarrollado en la presente investigación, se ha seleccionado como estadístico de prueba de hipótesis la técnica ***"chi-cuadrado",*** puesto que es una prueba NO paramétrica, que permite medir la relación entre la variable dependiente e independiente.

4.4.8.1. *Planteamiento de las hipótesis*

Se considera la hipótesis nula Ho y la hipótesis de investigación Hi.

Ho: "El Modelo de Seguridad para mitigar ataques de Denegación de Servicio en tráfico SIP en servicios VoIP, no reduce las vulnerabilidades ante ataques de DoS incrementando la disponibilidad del servicio de VoIP en redes LAN Corporativas."

Hi: "El Modelo de Seguridad para mitigar ataques de Denegación de Servicio en tráfico SIP en servicios VoIP, reduce las vulnerabilidades ante ataques de DoS incrementando la disponibilidad del servicio de VoIP en redes LAN Corporativas."

Para crear la tabla de contingencia, se ha considerado una escala para la interpretación de los tiempos en los que el servicio de VoIP no está disponible, frente a las pruebas realizadas, esta escala se basada en la Escala de Likert.

Tabla 59-4: Escala de Tiempo de Interrupción del Servicio VoIP

Tiempo de Interrupción del Servicio VoIP	Valor Cuantitativo	Criterio Cualitativo
0 - 0.5	1	Muy bajo
0.6 – 1	2	Bajo
2 – 6	3	Medio
7 -10	4	Alto
11 - 14	5	Muy Alto
---	0	No aplica

Realizado por: Arellano Karina, 2016

La Tabla 60-4, muestra la relación entre el valor del tiempo promedio de interrupción del servicio de VoIP obtenidos de las diferentes pruebas, con el valor correspondiente de la escala definida en la Tabla 59-4.

Tabla 60-4: Tiempos Promedio de Interrupción del Servicio y Valores de Escala

Ataques	**Tiempo de Interrupción del Servicio de VoIP**			
	Sin Modelo		**Con Modelo**	
	Valor Promedio	**Valor Escala**	**Valor Promedio**	**Valor Escala**
Ataque 1 (Invite Flood to SIP Proxies)	8.67	4	0.5	1
Ataque 2 (Invite Flood to SIP Phones)	14.0	5	0	1
Ataque 3 (SYN Flood DoS)	5.33	3	0.5	1
Ataque 4 (Fuzzing - Malformación en mensajes INVITE)	14.0	5	1.0	2
Ataque 5 (Eliminación de Registro de Usuarios SIP)	9.33	4	0	1

Realizado por: Arellano Karina, 2016

En base a lo ya descrito, se crea la tabla de contingencia para el cálculo de ***chi-cuadrado***, en la que se ubican las frecuencias observadas de cada indicador.

Tabla 61-4: Tabla de Frecuencias Observadas

	Ataques	**Sin Modelo**	**Con Modelo**	**TOTAL**
Reduce el Tiempo de Interrupción del Servicio VoIP	Ataque 1 (Invite Flood to SIP Proxies)	0	1	1
	Ataque 2 (Invite Flood to SIP Phones)	0	1	1
	Ataque 3 (SYN Flood DoS)	0	1	1
	Ataque 4 (Fuzzing - Malformación en mensajes INVITE)	0	2	2
	Ataque 5 (Eliminación de Registro de Usuarios SIP)	0	1	1
NO Reduce el Tiempo de Interrupción del Servicio VoIP	Ataque 1 (Invite Flood to SIP Proxies)	4	0	4
	Ataque 2 (Invite Flood to SIP Phones)	5	0	5
	Ataque 3 (SYN Flood DoS)	3	0	3
	Ataque 4 (Fuzzing - Malformación en mensajes INVITE)	5	0	5
	Ataque 5 (Eliminación de Registro de Usuarios SIP)	4	0	4
	TOTAL	**21**	**6**	**27**

Realizado por: Arellano Karina, 2016

Los valores que se esperan encontrar si las variables no estuvieran relacionadas, se refleja en la tabla de contingencia de frecuencias esperadas, su cálculo se realiza mediante la fórmula aplicada a la tabla de frecuencias observadas.

$$fe = \frac{(total\ del\ renglón) * (total\ de\ la\ columna)}{Total\ de\ Frecuencias\ Observadas}$$

Aplicando la fórmula a los valores de la Tabla de valores observados (Tabla 62-4), se obtiene la tabla de contingencia de valores esperados (Tabla 63-4).

Tabla 62-4: Tabla de Frecuencias Esperadas

	Ataques	Sin Modelo	Con Modelo	TOTAL
Reduce el Tiempo de Interrupción del Servicio VoIP	Ataque 1 (Invite Flood to SIP Proxies)	0.78	0.22	1.00
	Ataque 2 (Invite Flood to SIP Phones)	0.78	0.22	1.00
	Ataque 3 (SYN Flood DoS)	0.78	0.22	1.00
	Ataque 4 (Fuzzing - Malformación en mensajes INVITE)	1.56	0.44	2.00
	Ataque 5 (Eliminación de Registro de Usuarios SIP)	0.78	0.22	1.00
NO Reduce el Tiempo de Interrupción del Servicio VoIP	Ataque 1 (Invite Flood to SIP Proxies)	3.11	0.89	1.22
	Ataque 2 (Invite Flood to SIP Phones)	3.89	1.11	1.22
	Ataque 3 (SYN Flood DoS)	2.33	0.67	3.00
	Ataque 4 (Fuzzing - Malformación en mensajes INVITE)	3.89	1.11	5.00
	Ataque 5 (Eliminación de Registro de Usuarios SIP)	3.11	0.89	4.00
	TOTAL	**21.00**	**6.00**	**20.44**

Realizado por: Arellano Karina, 2016

Ahora, se aplica la siguiente fórmula de ***chi cuadrado:***

$$x^2 = \sum_i \frac{(o_i - e_i)^2}{e_i}$$

La Tabla 63-4, muestra el cálculo para hallar el valor de **X²**.

Tabla 63-4: Cálculo de Chi-Cuadrado

	Indicadores	*O*	*E*	*O-E*	*(O-E)²*	*(O-E)² /E*
SIN MODELO	Reduce/Ataque 1	0.00	0.78	-0.78	0.60	0.78
	Reduce/Ataque 2	0.00	0.78	-0.78	0.60	0.00
	Reduce/Ataque 3	0.00	0.78	-0.78	0.60	0.78
	Reduce/Ataque 4	0.00	1.56	-1.56	2.42	1.56
	Reduce/Ataque 5	0.00	0.78	-0.78	0.60	0.00
CON MODELO	Reduce/Ataque 1	1.00	0.22	0.78	0.60	2.72
	Reduce/Ataque 2	1.00	0.22	0.78	0.60	0.00
	Reduce/Ataque 3	1.00	0.22	0.78	0.60	2.72
	Reduce/Ataque 4	2.00	0.44	1.56	2.42	5.44
	Reduce/Ataque 5	1.00	0.22	0.78	0.60	0.00
SIN MODELO	No Reduce/Ataque 1	4.00	3.11	0.89	0.79	0.25
	No Reduce/Ataque 2	5.00	3.89	1.11	1.23	0.32
	No Reduce/Ataque 3	3.00	2.33	0.67	0.44	0.19
	No Reduce/Ataque 4	5.00	3.89	1.11	1.23	0.32
	No Reduce/Ataque 5	4.00	3.11	0.89	0.79	0.25
CON MODELO	No Reduce/Ataque 1	0.00	0.89	-0.89	0.79	0.89
	No Reduce/Ataque 2	0.00	1.11	-1.11	1.23	1.11
	No Reduce/Ataque 3	0.00	0.67	-0.67	0.44	0.67
	No Reduce/Ataque 4	0.00	1.11	-1.11	1.23	1.11
	No Reduce/Ataque 5	0.00	0.89	-0.89	0.79	0.89
X² Calculado						**20.00**

Realizado por: Arellano Karina, 2016

4.4.8.2. *Criterio*

Es necesario determinar el ***criterio de decisión***. Entonces se acepta ***Ho*** cuando:

$\mathbf{x^2_{calculado} < x^2_{tabla;}}$ caso contrario se rechaza ***Ho*** y se acepta la ***Hi***

Donde el valor de x^2_{tabla} representa el valor proporcionado por la tabla de ***"distribución x^2",*** según el nivel de significación elegido y los grados de libertad.

4.4.8.3. *Nivel de significancia*

Se determina el nivel de significancia, que para el caso del presente análisis se utilizará un nivel de significación estadística de **α = 0,05.**

4.4.8.4. *Interpretación*

Ahora bien, para determinar si el valor de **X^2 Calculado** es o no significativo, se debe establecer los grados de libertad **(gl)**, a través de la siguiente fórmula:

$$gl = (r - 1) * (k-1)$$

Donde:

r: el número de filas o renglones de la tabla de contingencia

k: el de columnas de la tabla de contingencia

La investigación generó una matriz de 10r x 2k. Entonces:

$$gl = (10-1) * (2-1)$$

$$gl = (9) * (1)$$

$$gl = 9 \text{ grado de libertad}$$

De acuerdo a la tabla estadística de distribución de chi-cuadrado que se muestra en la Tabla 4-64, con un nivel de significancia 0,05 a 9 grado de libertad, genera un valor de $\mathbf{x^2_{tabla} = 16.919}$

Tabla 64-4: Tabla Distribución de X

Degrees of Freedom	Possibility of Chance Occurrence in Percentage (5% or Less Considered Significant)								
	90%	80%	70%	50%	30%	20%	10%	5%	1%
1	0.016	0.064	0.148	0.455	1.074	1.642	2.706	3.841	6.635
2	0.211	0.446	0.713	1.386	2.408	3.219	4.605	5.991	9.210
3	0.584	1.005	1.424	2.366	3.665	4.642	6.251	7.815	11.341
4	1.064	1.649	2.195	3.357	4.878	5.989	7.779	9.488	13.277
5	1.610	2.343	3.000	4.351	6.064	7.289	9.236	11.070	15.086
6	2.204	3.070	3.828	5.348	7.231	8.558	10.645	12.592	16.812
7	2.833	3.822	4.671	6.346	8.383	9.083	12.017	14.067	18.475
8	3.490	4.594	5.527	7.344	9.524	11.030	13.362	15.507	20.090
9	4.168	5.380	6.393	8.343	10.656	12.242	17.684	**16.919**	21.666

Realizado por: Arellano Karina, 2016
Fuente: Estadística A - Distribución Chi-Cuadrado. Ing. José Manuel García.

Resultados de la investigación el valor $\mathbf{X^2_{calculado}}$ es de **20.00**, observando que es superior al valor de $\mathbf{x^2_{tabla}}$ **16.919**, como se muestra en la Figura 30-4.

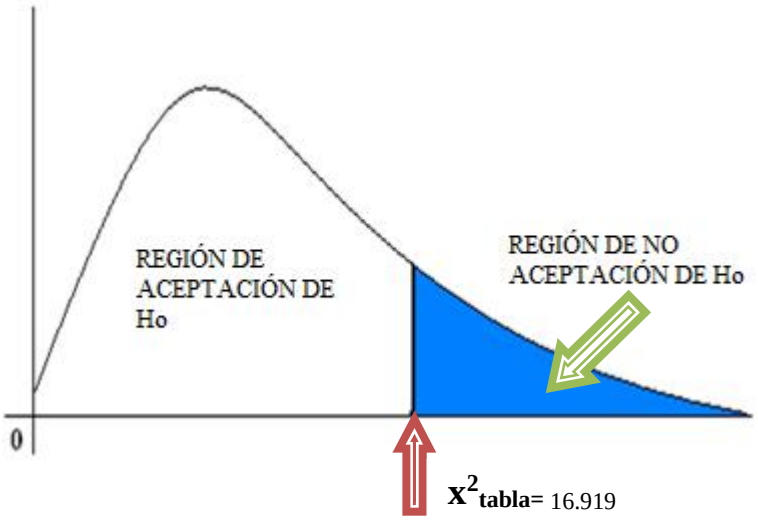


Figura 30-4: Demostración de la Hipótesis
Realizado por: Arellano Karina, 2016

La regla de decisión es entonces:

En consecuencia como el valor de $X^2_{calculado}$ se encuentra en la región de no aceptación de la Hipótesis Nula (***Ho),*** se acepta la Hipótesis de Investigación (***Hi)*** con un nivel de significancia del 5% = 0.05 para obtener un nivel de confianza del 95%.

Quedando demostrado que:

Hi: "El Modelo de Seguridad para mitigar ataques de Denegación de Servicio en tráfico SIP en servicios VoIP, reduce las vulnerabilidades ante ataques de DoS incrementando la disponibilidad del servicio de VoIP en redes LAN Corporativas."

CONCLUSIONES

- En el escenario propuesto de red VoIP basado en SIP para el modelo de seguridad al aplicar herramientas de escaneo como NetScan, Nmap, Zenmap, herramientas de análisis de tráfico Wireshark y herramientas específicas para SIP como la suite de SIPVicious: Svwar, y Svmap se identificaron trece vulnerabilidades; permitiendo la ejecución de los ataques *INVITE Flood para Proxies SIP y Phones, Malformación de Mensajes INVITE, Eliminación de Registro de Usuarios* y S*YN Flood DoS,* con mayor impacto en la disponibilidad del servicio VoIP.

- Se desarrolló un Modelo de Seguridad denominado MS-DoS-SIP, que contiene cuatro etapas: a) Reconocer la red VoIP, b) Identificar Vulnerabilidades SIP y Valorar su Impacto en la Disponibilidad, c) Examinar la Seguridad de la Red VoIP y d) Aplicar las medidas de seguridad; considerando las recomendaciones de seguridad de los estándares y normas internacionales ISO/IEC 2702, UIT-T X.805 y NIST, y mejores prácticas de Asterisk, Cisco y VOIPSA, así como también metodologías como OSSTMM 2.1 y las Técnicas de Reconocimiento (Hacked Exposed VoIP) que permiten tener una idea clara y una referencia de trabajo estándar que facilita las tareas de elaboración del Modelo de Seguridad.

- Mediante la implementación del Modelo de Seguridad MS-DoS-SIP, en un ambiente de red de VoIP simulado se logró minimizar en un 92% las vulnerabilidades en relación del mismo escenario sin mecanismos de seguridad implementados. Al reducir notablemente las vulnerabilidades se consiguió alcanzar tiempos de interrupción del servicio hasta de 0 minutos 0 segundos, garantizando así la continuidad del negocio.

- Con el empleo de la estadística inferencial *chi-cuadrado* y un nivel de significancia de 0.05, de acuerdo a la tabla de distribución se obtiene que $\mathbf{x^2_{tabla}}$ 16.919 y el valor calculado $\mathbf{X^2_{calculado}}$ en esta investigación es de 20.00, notando que es superior al valor de la tabla de distribución, por lo que el valor de $\mathbf{X^2_{calculado}}$ se encuentra en el sector de NO Aceptación de Ho y resulta estadísticamente significativa, Aceptando la hipótesis de investigación Hi.

RECOMENDACIONES

- Tomar en consideración el uso de un sistema de correlación de eventos en las redes de VoIP, y las nuevas recomendaciones de seguridad con la finalidad de estar un paso al frente en la aparición de futuras amenazas y vulnerabilidades que atenten contra la disponibilidad de servicios VoIP, específicamente basados en SIP.

- Se recomienda profundizar la investigación en cuanto a las técnicas y herramientas que usan los atacantes en la actualidad, con el objetivo de ir actualizando el Modelo de Seguridad.

- Se propone para trabajos futuros:
    - Ampliar el número de vulnerabilidades a ser objeto de estudio
    - Investigar Metodologías estándares y herramientas flexibles, que se adapten al cambio continuo.
    - Estudiar otras alternativas, como mecanismos de seguridad que permitan resguardar la disponibilidad del servicio de VoIP basados en SIP

BIBLIOGRAFÍA

[1] Al-Allouni, H., Rohiem, A. E., Hashem, M., El-moghazy, A., & Ahmed, A. E.-A. (2009). VoIP Denial of service attacks classification and implementation (pp. 1-12).

[2] Butcher, D., Li, X., & Guo, J. (2007). Security Challenge and Defense in VoIP Infrastructures. 1152-1162. Recuperado a partir de https://doi.org/10.1109/TSMCC.2007.905853

[3] Cáceres Guayanlema, J. S. (2014, octubre 29). *Análisis de vulnerabilidades en protocolos utilizados en centrales VoIP con IPv6 utilizando troncales SIP* (Thesis Pregrado). Recuperado a partir de http://dspace.espoch.edu.ec/handle/123456789/3532

[4] Chapalbay Santillán, D. C. (2012, febrero 6). *Protección de Tráfico SIP en Redes de Telefonía IP a través del Análisis de Técnicas de Seguridad en Redes Corporativas.* (Thesis Pregrado). Recuperado a partir de http://dspace.espoch.edu.ec/handle/123456789/1532

[5] Chen, E. Y. (2006). Detecting DoS attacks on SIP systems. En *1st IEEE Workshop on VoIP Management and Security, 2006* (pp. 53-58). https://doi.org/10.1109/VOIPMS.2006.1638123

[6] David Endler, M. C. (2007). Hacking Exposed VoIP: Voice Over IP Security Secrets & Solutions. Recuperado a partir de http://www.r0z.hol.es/arquivos/VOIP/Hacking%20Exposed%202%20-%20VoIP.pdf

[7] Deng, X. (2008). Security of VoIP: Analysis, Testing and Mitigation of SIP-based DDoS attacks on VoIP Networks. Recuperado a partir de http://ir.canterbury.ac.nz/handle/10092/2227

[8] Jouravlev, I. (2008). Mitigating Denial-Of-Service Attacks On VoIP Environment. *International Journal of Applied Management and Technology*. Recuperado a partir de http://scholarworks.waldenu.edu/ijamt/vol6/iss1/8/

[9] Keromytis, A. D. (2010). A look at VoIP vulnerabilities. 41-50. Recuperado a partir de http://dialnet.unirioja.es/servlet/articulo?codigo=4956910

[10] Keromytis, A. D. (2012). A comprehensive survey of voice over IP security research. *Communications Surveys & Tutorials, IEEE*, *14*(2), 514–537.

[11]Kuhn & Walsh. (2013). Recuperado a partir de http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf

[12] Lee, J., Cho, K., Lee, C., & Kim, S. (2014). VoIP-aware network attack detection based on statistics and behavior of SIP traffic. *Peer-to-Peer Networking and Applications*. Recuperado a partir de https://doi.org/10.1007/s12083-014-0289-8

[13] Martin, M. V., & Hung, P. C. K. (2005). Towards a security policy for VoIP applications. En *Canadian Conference on Electrical and Computer Engineering, 2005* (pp. 65-68). Recuperado a partir de https://doi.org/10.1109/CCECE.2005.1556878

[14] Moreno, J. I., Soto, I., & Larrabeiti, D. (2001). Protocolos de Señalización para el transporte de Voz sobre redes IP. Recuperado a partir de http://orff.uc3m.es/handle/10016/4295

[15] Ormazabal, G., Nagpal, S., Yardeni, E., & Schulzrinne, H. (2008). Secure SIP: A Scalable Prevention Mechanism for DoS Attacks on SIP Based VoIP Systems. Recuperado a partir de http://link.springer.com/chapter/10.1007/978-3-540-89054-6_6

[16]OSSTMM.2.1. (2011). Recuperado a partir de http://isecom.securenetltd.com/OSSTMM.es.2.1.pdf

[17] Rafique, M. Z., Akbar, M. A., & Farooq, M. (2009). Evaluating DoS attacks against SIP-based VoIP systems. En *Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE* (pp. 1–6). IEEE. Recuperado a partir de http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5426247

[18] Rehman, U. U., & Abbasi, A. G. (2014a). Security analysis of VoIP architecture for identifying SIP vulnerabilities. En *2014 International Conference on Emerging Technologies (ICET)* (pp. 87-93). https://doi.org/10.1109/ICET.2014.7021022

[19] Rico J. (2013, julio 25). Estado Del Arte De La (In)Seguridad Voip. Recuperado a partir de http://urepublicana.edu.co/ingenieria/wp-content/uploads/2014/04/EstadoInseguridadVoIP.pdf

[20] Shan, L., & Jiang, N. (2009). Research on Security Mechanisms of SIP-Based VoIP System. En *Ninth International Conference on Hybrid Intelligent Systems, 2009. HIS '09* (Vol. 2, pp. 408-410). Recuperado a partir de https://doi.org/10.1109/HIS.2009.196

[21] Sisalem, D., Kuthan, J., Ehlert, S., & others. (2006). Denial of service attacks targeting a SIP VoIP infrastructure: attack scenarios and prevention mechanisms. *IEEE Network*, *20*(5), 26–31.

[22] Sun, L., Mkwawa, I.-H., Jammeh, E., & Ifeachor, E. (2013a). VoIP Signalling—SIP. En *Guide to Voice and Video over IP* (pp. 101-122). Springer London. Recuperado a partir de http://link.springer.com/chapter/10.1007/978-1-4471-4905-7_5

[23] Voipsa. (2005). VOIPSA : Activities : Working Groups : Threat Taxonomy. Recuperado 18 de junio de 2016, a partir de http://www.voipsa.org/Activities/taxonomy.php

ANEXOS

ANEXO A: ENCUESTAS APLICADAS

ESCUELA SUPERIOR POLITECNICA DE CHIMBORAZO
ESCUELA DE POSGRADO Y EDUCACIÓN CONTINUA
MAESTRIA EN SEGURIDAD TELEMATICA

ENCUESTA

El objeto de esta encuesta es recoger información acerca del Servicio de VoIP en su Institución, ya que se está desarrollando la Tesis de Grado, Titulada "MODELO DE SEGURIDAD CONTRA ATAQUES DE DENEGACIÓN DE SERVICIO (DoS) DE TRÁFICO SIP EN SERVICIOS VoIP, PARA REDES LAN CORPORATIVAS". Su opinión es muy relevante y contribuirá al desarrollo del trabajo de investigación. Por lo tanto, es de primordial importancia que usted responda con sinceridad y veracidad.

Nombre de la Institución: H. Gobierno Provincial de Tungurahua
Fecha: 8/Septiembre/2016.

PREGUNTAS.-

1.- El servicio de VoIP se encuentra dentro de la infraestructura?

LAN X WAN ___

2.- Que Protocolo de señalización utiliza su servicio de VoIP?

H.323 X SIP X IAX ___ OTRO ___

3.- Cuántas extensiones en promedio tiene su red de telefonía IP?

110

4.- En promedio. En una hora cuantas extensiones realizan llamadas de VoIP?

25

5.- A su criterio cuál es el tiempo promedio que dura una llamada telefónica IP? (minutos)

1-5 mins X 5-10 mins ___ 10-20 mins ___ más de 30 mins ___

6.- A su juicio cual sería el grado de impacto que produciría la pérdida de disponibilidad del servicio de VoIP en su Institución?

ALTA X MEDIA ___ BAJA ___

FIRMA Y SELLO

GOBIERNO PROVINCIAL DE TUNGURAHUA
DIRECCION DE SISTEMAS

ESCUELA SUPERIOR POLITECNICA DE CHIMBORAZO
ESCUELA DE POSGRADO Y EDUCACIÓN CONTINUA
MAESTRIA EN SEGURIDAD TELEMATICA

ENCUESTA

El objeto de esta encuesta es recoger información acerca del Servicio de VoIP en su Institución, ya que se está desarrollando la Tesis de Grado, Titulada "MODELO DE SEGURIDAD CONTRA ATAQUES DE DENEGACIÓN DE SERVICIO (DoS) DE TRÁFICO SIP EN SERVICIOS VoIP, PARA REDES LAN CORPORATIVAS". Su opinión es muy relevante y contribuirá al desarrollo del trabajo de investigación. Por lo tanto, es de primordial importancia que usted responda con sinceridad y veracidad.

Nombre de la Institución: GAD Municipalidad de Ambato

Fecha: 02- SEPTIEMBRE- 2016

PREGUNTAS.-

1.- El servicio de VoIP se encuentra dentro de la infraestructura?

LAN X WAN ___

2.- Que Protocolo de señalización utiliza su servicio de VoIP?

H.323 ___ SIP X IAX ___ OTRO ___

3.- Cuántas extensiones en promedio tiene su red de telefonía IP?

350

4.- En promedio. En una hora cuantas extensiones realizan llamadas de VoIP?

70

5.- A su criterio cuál es el tiempo promedio que dura una llamada telefónica IP? (minutos)

1-5 mins ___ 5-10 mins X 10-20 mins ___ más de 30 mins ___

6.- A su juicio cual sería el grado de impacto que produciría la pérdida de disponibilidad del servicio de VoIP en su Institución?

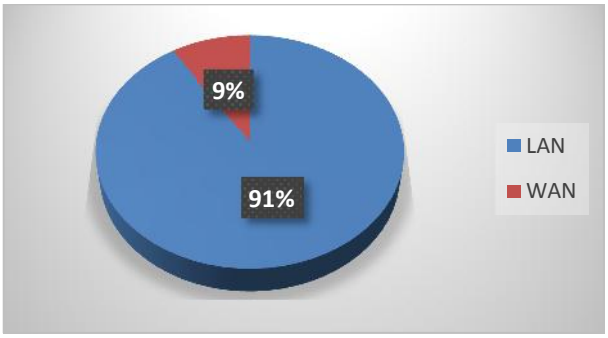
ALTA X MEDIA X BAJA ___

GAD - MUNICIPALIDAD DE AMBATO DIRECCIÓN DE INFORMÁTICA

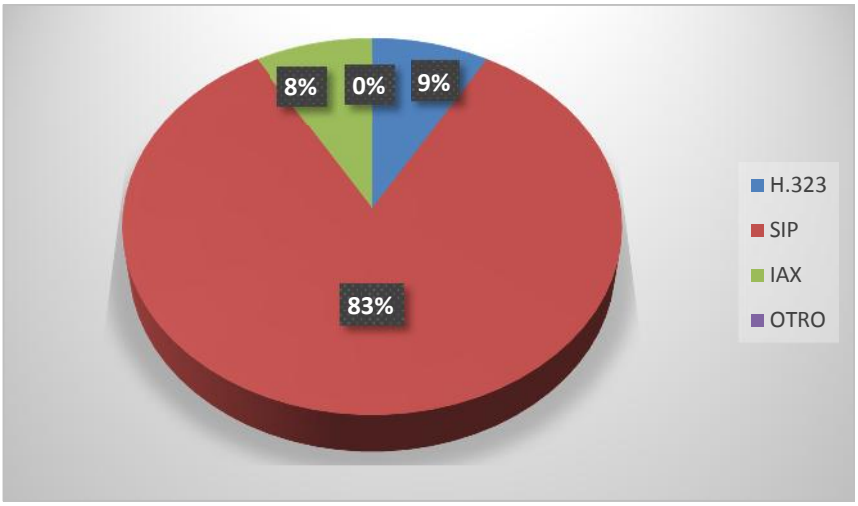
FIRMA Y SELLO

ANEXO B: TABULACIÓN DE LA ENCUESTA

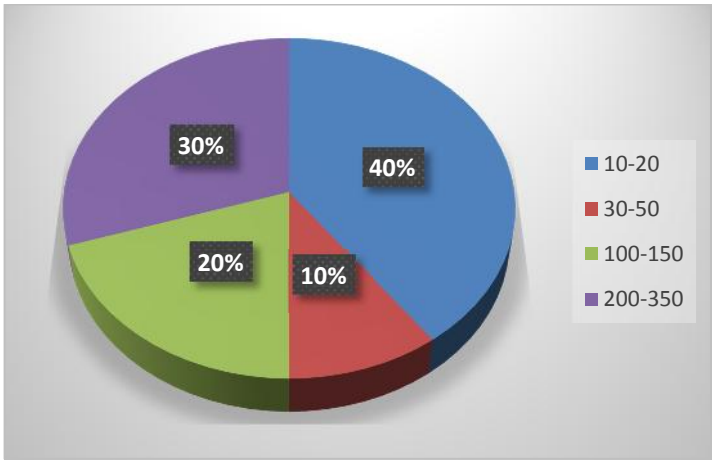
1.- El servicio de VoIP se encuentra dentro de la infraestructura?



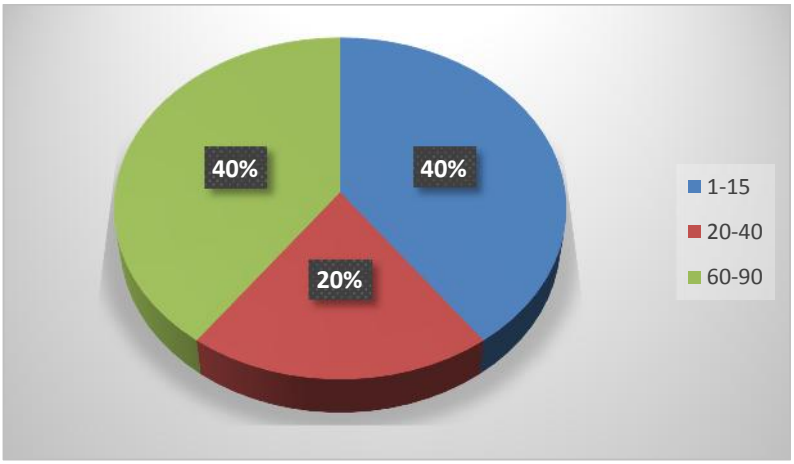
2.- Que Protocolo de señalización utiliza su servicio de VoIP?



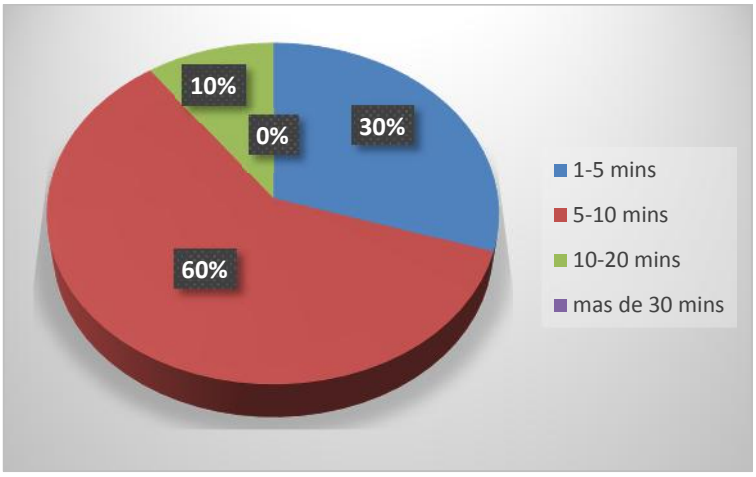
3.- Cuántas extensiones en promedio tienen su red de telefonía IP?



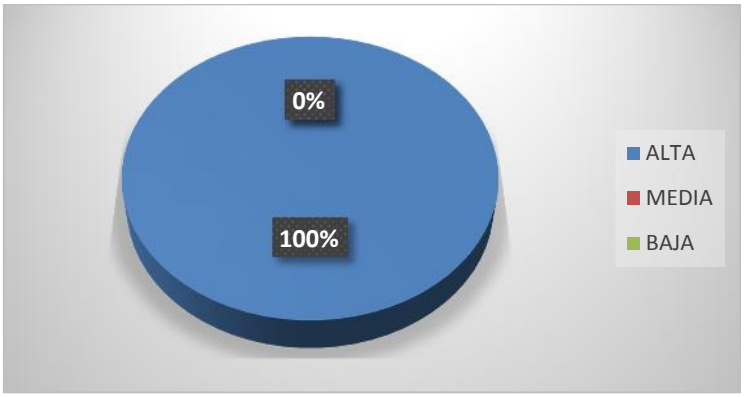
4.- En promedio. En una hora cuantas extensiones realizan llamadas de VoIP?



5.- A su criterio cuál es el tiempo promedio que dura una llamada telefónica IP? (minutos)



6.- A su juicio cual sería el grado de impacto que produciría la pérdida de disponibilidad del servicio de VoIP en su Institución?



ANEXO C: IMPLEMENTACIÓN DE TLS

A continuación se describen los pasos de la implementación del protocolo TLS. La implementación se realizó en Asterisk 11.17.1 y se utilizó los softphone Zoiper.

La siguiente implementación de TLS, está basada en una guía publicada en internet http://juanelojga.blogspot.com/2013/08/srtp-y-tls-en-elastix-actualizado.html y pretende brindar seguridad a la señalización del protocolo SIP.

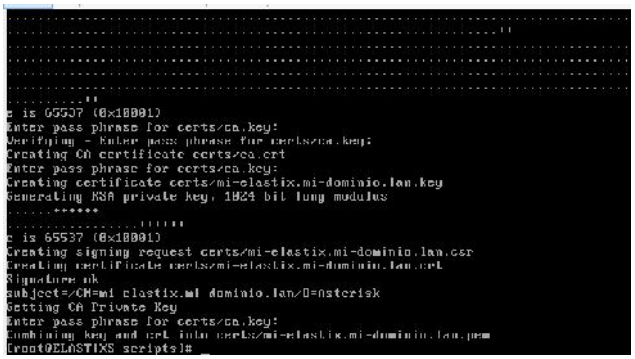
- **Creación certificados**

El primer paso es la creación de una autoridad de certificación y los certificados tanto para el servidor como para el cliente. Para esto se utilizará los scripts que vienen dentro de la documentación de asterisk. Estos scripts están en la carpeta:

/usr/share/doc/asterisk-11.17.1/contrib/scripts

Para generar el certificado de la CA como del servidor se ejecuta lo siguiente (dentro de la carpeta antes mencionada):

 # mkdir certs
./ast_tls_cert -d certs -C mi-elastix.mi-dominio.lan -o mi-elastix.mi-dominio.lan



Una vez generados los certificados tanto para la autoridad de certificación como para el servidor, se copian los siguientes archivos a la carpeta keys de asterisk:

 # cp certs/ca.crt /var/lib/asterisk/keys# cp certs/mi-elastix.mi-dominio.lan.pem /var/lib/asterisk/keys

Se deben dar los permisos de lectura o cambiar de propietario a los archivos copiados a la carpeta keys de asterisk, para que asterisk los pueda cargar:

 # chown -R asterisk:asterisk /var/lib/asterisk/keys/*

- **Configuración en Elastix**

Luego vamos al explorador, ingresamos al Elastix y habilitamos el acceso al FreePBX no embebido, esto se lo hace yendo a la pestaña Security -> Advanced Options -> Enable access to FreePBX -> ON. Luego en una nueva pestaña del explorador se debe poner lo siguiente:

https://ip-del-elastix/admin

Aquí va a solicitar el usuario y contraseña para ingresar.

Una vez adentro de FreePBX no embebido, se debe ir a la sección (ubicada en la esquina superior izquierda) Tools -> Asterisk SIP Settings. Aquí se pueden editar las configuraciones generales para SIP. En la parte final hay una sección que dice Other SIP Settings, ahi ponemos lo siguiente:

tlsenable=yes
tlsbindaddr=0.0.0.0
tlsdontverifyserver=yes
tlscertfile=/var/lib/asterisk/keys/mi-elastix.mi-dominio.lan.pem
tlscafile=/var/lib/asterisk/keys/ca.crt

Y se aplican los cambios.

Para saber si los cambios se aplicaron correctamente se puede ver que asterisk ahora tambien escucha el puerto TCP 5061.

 # netstat -atunp | grep asterisk

- **Configuración de las Extensiones**

Para habilitar el soporte TLS para una extensión, en el campo ***transport*** se debe cambiar "udp" por "tls".

- **Configuración de Softphones**

Por último se debe cambiar la configuración de los terminales.
Para el caso de softphones, se debe cambiar el puerto de registro, en lugar del 5060 el 5061.

ANEXO D: INSTALACIÓN Y CONFIGURACIÓN DE SBC BLOX

A continuación se detalla los pasos para la descarga e instalación necesaria para obtener Blox y acceder a la configuración de FreeBlox.

1.-Descargar **.iso** de Blox desde http://blox.org/download, la imagen ISO de BLOX SBC se compone de un sistema basado en LINUX específicamente CentOS.
2.- Iniciar el p<roceso de instalación, escogiendo la opción **Install,** seleccionar la hora, idioma, idioma del teclado, configurar la contraseña root y comprobar la misma. Configure una contraseña robusta ya que Blox, no permite contraseñas débiles26.
3.- Una vez terminado de instalar, se muestra el login por consola de **BLOX**
4.- Configurar la red. Se necesita configurar 2 interfaces de red y una interfaz virtual para media, y reiniciar el servicio de red mediante el comando **service network restart**

Instalación de FreeBlox

1.- Copiar **freeblox-0.9.0-22.x86_64.rpm** en BLOX server.
2.- Para iniciar sesión con Blox Server, ir a la carpeta FreeBlox-rpm y ejecutar los siguientes comandos:
3.- Reiniciar el sistema usando el comando **reboot**. Y empezar a utilizar la interfaz gráfica FreeBlox para la configuración de Blox SBC.

Configuración de BLOX

1.- Dashboard

Es el primer inicio de sesión, es la interfaz gráfica de usuario Web que proporciona información general del estado de la configuración de FreeBlox presenta:

- El status del sistema, el uso de memoria, uso de flash y el uso de la CPU.

- El panel superior muestra el firmware.
- Status de Red, IP, MAC, LAN, WAN y puerta de enlace del dispositivo.
- Panel de resumen de alertas de seguridad, alarmas.
- Status DPI.

2.- Configuración de red

La interfaz LAN transporta la señalización SIP, que entra y sale de SBC Blox. Las interfaces de Blox son los adaptadores Ethernet, permitiendo al usuario configurar el nombre de host, configuración IP en modo estático, dirección IP/ máscara, puerta de enlace y DNS, permite además activar o desactivar el acceso SSH al dispositivo, permitir o denegar la solicitud ICMP ping.

3.- Señalización

En esta sección de señalización permite configurar perfiles SIP, configuración Trunk, usuarios móviles, Least Cost Routing y TLS.

- **Perfil SIP:** contiene un conjunto de atributos SIP que se asocian a Blox. El perfil SIP utiliza una configuración de los puntos finales externos para conectarse con Blox, enlaza una dirección IP, el puerto y otros parámetros relacionados a SIP. Contiene la configuración SIP UA. FreeBlox puede ser configurado para múltiples UA cada uno con una configuración diferente, por lo tanto un conjunto de diferentes IP y puerto para cada uno.

- **Configuración TLS:**

  En la sección **Device Root CA**, previo a la emisión de certificados se debe realizar los pasos que se detallan a continuación:

  - Configuración de host en los clientes y servidor
  - Configuración de servidor NTP.

  Configurar del servidor, mediante la edición del archivo **/etc/hosts**

Al editar el archivo **/etc/hosts** se procede a realizar la configuración de los clientes, tanto de la PBX como del ISP respectivamente. El usuario puede cargar un archivo CA o generar un certificado digital.

A continuación se muestra la configuración de CA, en el cual se ingresan parámetros como el Common Name que es el hostname que apunta al servidor Blox, configurado previamente, Country Name, en la cual se setea con 2 dígitos el identificador de país, Provincia, Organization Name, Email Address, Encryption Strength y Valid days que son los días de validez del certificado.

Certificado del servidor

Al igual que se puede subir la CA, el usuario de igual manera puede subir el certificado del servidor sin embargo también se puede generar como se muestra a continuación:

Certificado del Cliente

El certificado del cliente, se configura ingresando parámetros como el Common Name que es el hostname que apunta al ISP, configurado previamente, Country Name, en la cual se setea con 2 dígitos el identificador de país, Provincia, Organization Name, Email Address, Encryption Strength y Valid days que son los días de validez del certificado.

Ahora se debe configurar TLS v1.1 en los terminales.

Para realizar la configuración completa se configura los perfiles SIP, por lo general sólo en la WAN agregando el protocolo, puerto TLS y el certificado del servidor previamente generado en este caso **sbcblox.** Como se observa en la Figura

Configuración de la Seguridad

- **Detección de ataques SIP**

Blox cuenta con el módulo de detección de ataques, en el módulo de **Security, SIP ATTACKS DETECTION,** permite configurar reglas para inspección de paquetes SIP.

El usuario puede activar o desactivar la inspección contra determinada categoría, de igual manera se puede tomar medidas al respecto dependiendo del ataque que esté siendo víctima la central VoIP.

FreeBlox muestra logs de alerta y bloqueo de paquetes que contienen un vector de ataque y la lista negra de la IP atacante para la duración dada. La duración del bloqueo en la cual el atacante necesita ser bloqueado se realiza por categoría.

Protocolo Compliance

El DPI usado en Blox inspecciona el tráfico SIP con normas de seguridad. Las anomalías en las cabeceras SIP de mensajes pueden dar lugar a diversas condiciones erróneas, fallas en el análisis SIP y paquetes con formato incorrecto que dará lugar a aplicaciones SIP vulnerables a los ataques.
Los siguientes parámetros serán utilizados por el motor de inspección profunda de paquetes SIP DPI, para la identificación de las diferentes condiciones de anomalías de protocolo y para tomar acciones que son previamente configurados por el administrador. Se recomienda utilizar la configuración por defecto para estos parámetros.

Max Sessions: Una sesión de SIP es la configuración de la conexión de nivel de aplicación que se crea entre el servidor SIP y cliente SIP, para el intercambio de los mensajes de audio / vídeo entre sí.
El parámetro **MAX SESSIONS** define el número máximo de sesiones que el SIP DPI puede analizar. El valor por defecto se ha establecido como 4096.

Max Dialogs per sesión: Especifica el número máximo de mensajes SIP de transacciones que puede pasar entre el servidor y el cliente SIP.

Methods: Este parámetro especifica qué métodos comprobar en cuanto a mensajes SIP se refiere. A continuación se presentan los mensajes SIP que el DPI puede identificar: (1) INVITE, (2) CANCEL, (3) ACK, (4) BYE, (5) REGISTER, (6) OPTIONS, (7) REFER, (8) SUBSCRIBE, (9) UPDATE (10) JOIN (11) INFO (12) MESSAGE (13) NOTIFY (14) PRACK.

Max URI length: El campo **MAX URI LENGTH** identifica al usuario o servicio que se está abordando las peticiones SIP. **MAX URI LENGTH** especifica el tamaño máximo del campo

URI de la solicitud. El valor predeterminado se establece en 256. El intervalo permitido para esta opción es de 1 - 65535.

Max call ID length: El campo **MAX CALL ID LENGHT** en el mensaje SIP actúa como un identificador único y se refiere a la secuencia de mensajes intercambiados entre el cliente SIP y el servidor. **MAX CALL ID LENGHT** especifica el tamaño máximo del campo Call-ID. El valor predeterminado se establece en 256. El intervalo permitido para esta opción es de 1 - 65535.

Max Request name length: Este campo especifica el tamaño máximo de nombre de la petición, que es parte de la ID CSeq. El valor predeterminado se establece en 20. El intervalo permitido para esta opción es de 1 – 65535

Max From length: El campo de la **FROM HEADER** indica la identidad del iniciador de la solicitud SIP. **Max From length** especifica el tamaño máximo del campo. El intervalo permitido para esta opción es de 1 – 65535.

Max To length: El campo **TO HEADER** especifica el destinatario deseado de la petición SIP. **MAX TO LENGTH** especifica el máximo para el tamaño del campo. Por defecto se establece en 256. El intervalo permitido para esta opción es de 1 – 65535

Max Via length: El campo de **VIA HEADER** indica el transporte utilizado para la transacción SIP e identifica la ubicación en la que la respuesta de SIP se va a enviar.
MAX VIA LENGTH especifica el máximo tamaño de campo. El valor predeterminado se establece en 1024. El intervalo permitido para esta opción es de 1 - 65535.

Max Contact length: Identificador utilizado para ponerse en contacto con esa instancia específica del cliente / servidor SIP para posteriores requests. **MAX CONTACT LENGTH** especifica el tamaño máximo de contacto del campo. El valor predeterminado se establece en 256. El intervalo permitido para esta opción es de 1 - 65535.

Max Content length: Especifica la longitud máxima de contenido del cuerpo del mensaje. El valor predeterminado se establece en 1024. El intervalo permitido para esta opción es de 1 - 65535.

ANEXO E. PRUEBAS DE TESTEO DE SEGURIDAD

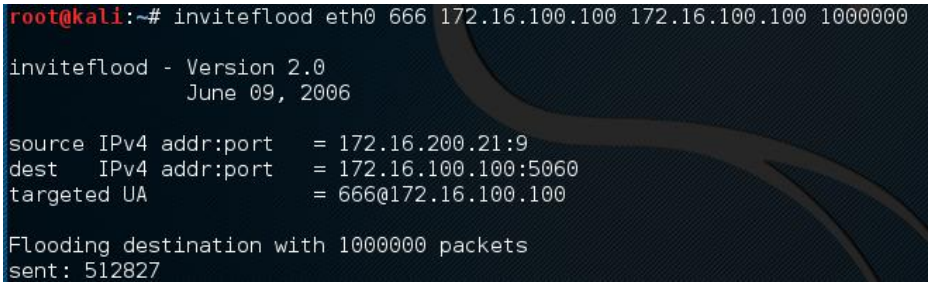
De acuerdo a las vulnerabilidades, amenazas y riesgos identificados en los apartados anteriores, en esta fase se prueban diferentes ataques a la infraestructura VoIP basada en SIP, utilizando herramientas disponibles en Internet.

A continuación se detallan los procedimientos realizados en la experimentación:

PRUEBA 1: INUNDACIÓN DE MENSAJES INVITE (FLOODS INVITE) A SERVIDOR SIP

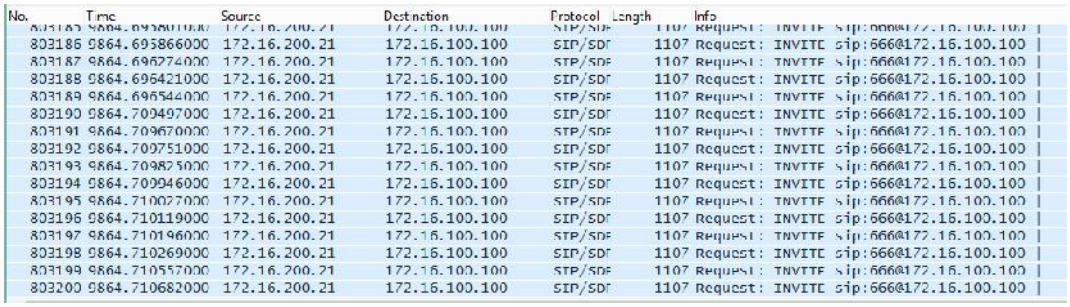
Para realizar este ataque se usó la herramienta ***Inviteflood*** de Kali Linux, ya que confecciona mensajes INVITE y los envía masivamente con la finalidad de colapsarlo. Es una herramienta que va aumentando el número de secuencia de los mensajes INVITE y cambiando los campos ***tag*** y ***Call-ID*** aleatoriamente para que se consideren llamadas independientes.

Para lanzar este ataque es necesario conocer la interfaz que contiene la tarjeta de red, en este caso “eth0”, luego se coloca el nombre de usuario SIP a ser atacado, la dirección IP del servidor, la dirección IP de la víctima y la cantidad de peticiones Invite que se quieren enviar. Este ataque inunda un servidor SIP con las solicitudes INVITE que contienen un teléfono SIP inexistente. Y se envió 1.000.000 de paquetes a un objetivo.



La Figura, muestra el servidor SIP al momento del ataque y como aumenta el uso la carga de la central telefónica. Sin embargo, no registra llamadas entrantes, ya que el servidor autentica los mensajes INVITE, los desecha si no cuenta con autentificación valida.

Se realizó una captura del tráfico que llegaba al Servidor SIP, mediante el software Wireshrak, y lo que se evidencia en el envió masivos de mensajes INVITE.



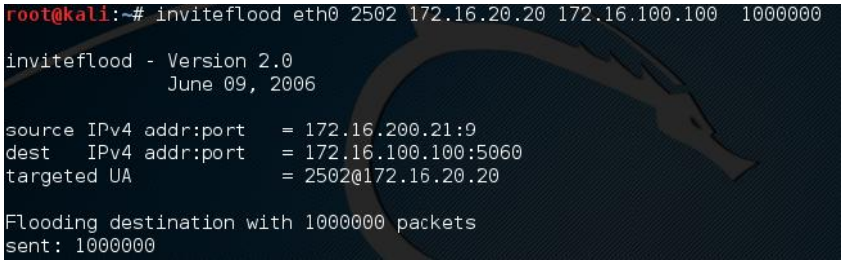
Como respuesta de este ataque, ningún softphone de la red puede realizar llamadas, ya que el servidor se encuentra colapsado de mensajes INVITE.

Se observa como uno de los softphone, no puede ejecutar la llamada ya que el servidor denegó el servicio en su totalidad.

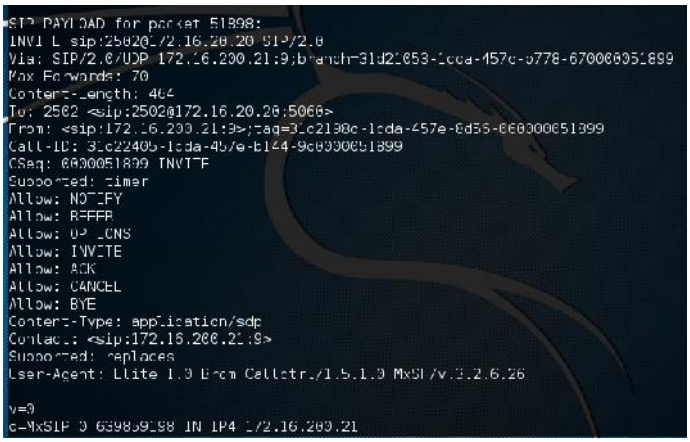
PRUEBA 2: INUNDACIÓN DE MENSAJES INVITE (FLOODS INVITE) A SIP PHONES

Para la ejecución este ataque es necesario identificar las extensiones SIP que se desean atacar, como ya se indicó en el apartado anterior.

La Figura muestra el ataque al UA: 2502, cuya dirección IP era 172.16.20.20, enviándole 1.000.000 peticiones INVITE que lograron colapsar el softphone.



A continuación se observa el envío del paquete número 51898.



Se muestra lo que ocurre con el softphone del UA: 2502, en el momento del ataque.

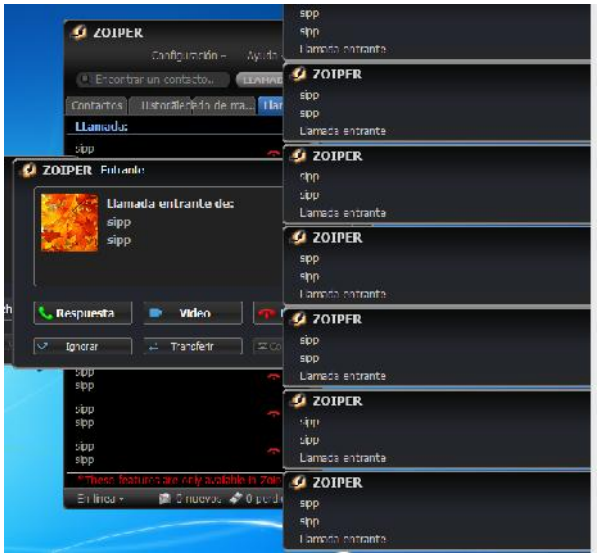
En la Figura muestra el porcentaje de paquetes de audio perdidos en la comunicación, debido a que se encuentra ejecutándose el ataque y se presentan retardos en la misma, volviendo la comunicación escasamente clara y molesta.

También se puede realizar este ataque usando la herramienta SIPp. Ejecutamos el ataque especificando que se realicen 7 llamadas cada 2 segundos (3,5 llamadas por segundo), hacia el usuario con IP 172.16.20.20, que corresponde al UA: 2502.

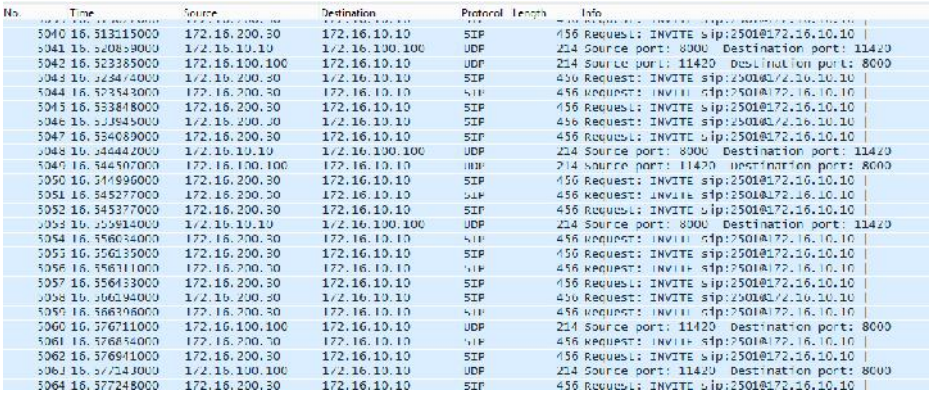
```
root@kali:~# sipp -sn uac -r 7 -rp 2000 172.16.20.20
```

Se muestra la ejecución del ataque de inundación con mensajes INVITE.

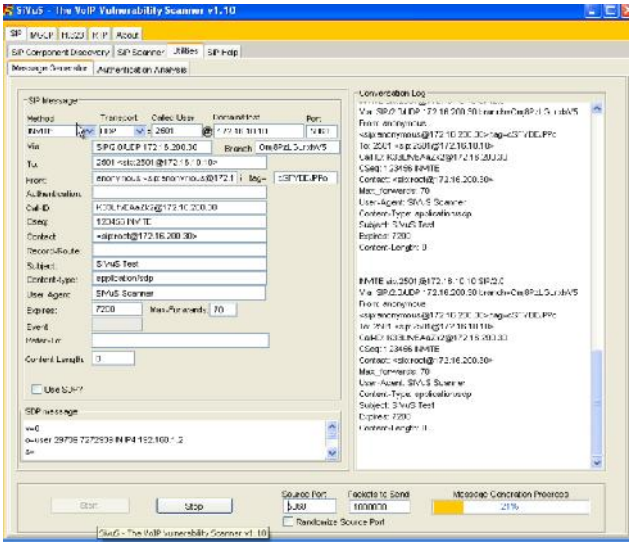
Se muestra que el softphone está colapsado de llamadas del atacante.



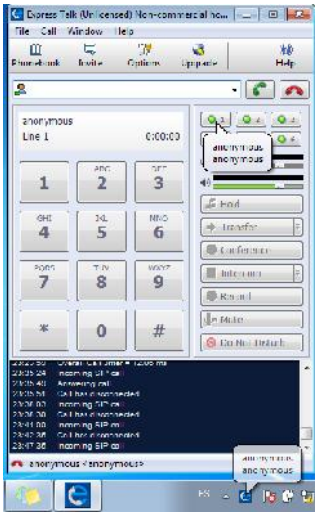
Se capturó el tráfico con ayuda de la herramienta Wireshark, en la que podemos observar las solicitudes de INVITE enviadas hacia el softphone.



Por otra parte, se usó la herramienta Sivus, para la generación de mensajes INVITE, que logró colapsar otro softphone, como se muestra a continuación.



Este tipo de ataque se produce el cuándo un atacante malintencionado envía una corriente de peticiones SIP INVITE para poner fin un dispositivo SIP. El atacante sigue enviando solicitudes SIP INVITE y cuelga una vez que reciba el timbre o 100 mensajes OK desde el dispositivo final. Como resultado, el dispositivo final no será capaz de hacer llamadas ni recibir llamadas legítimas, como se muestra en la Figura0-14.



PRUEBA 3: TCP SYN FLOOD

Para realizar este ataque se utilizó la herramienta ***hping3***, que es una herramienta en línea de comandos que permite crear y analizar paquetes **TCP/IP**, entre sus utilidades tiene la capacidad de provocar un **SYN Flood Attack** mediante denegación de servicio (DoS), mediante inundación de paquetes SYN con direcciones IP origen simuladas, dejando el servidor a la espera del ACK final para la comunicación y dejarlo colapsado para no aceptar verdaderas peticiones.

Lo importante para esta etapa, es la velocidad de tráfico con hping3.

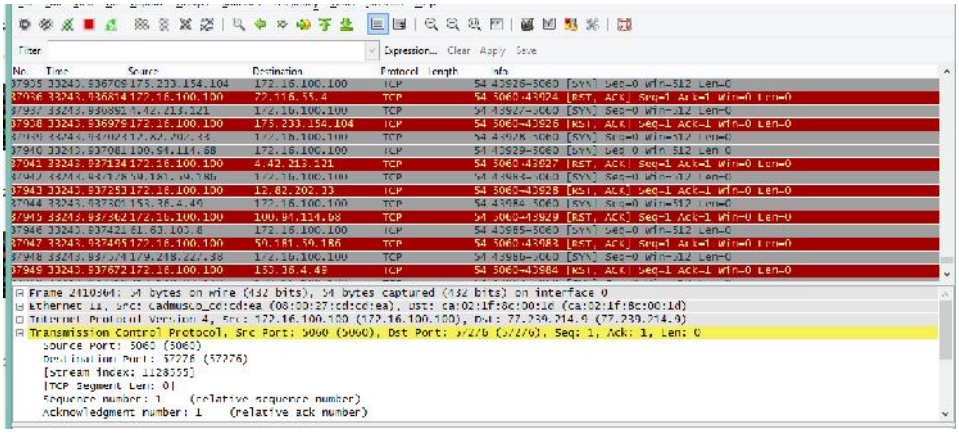
```
-i  --interval  wait (uX for X microseconds, for example -i u1000)
    --fast      alias for -i u10000 (10 packets for second)
    --faster    alias for -i u1000 (100 packets for second)
    --flood      sent packets as fast as possible. Don't show replies.
```

El ***Default*** de un ping es de 1 paquete por segundo, y es el que tiene configurado por defecto hping3, según la documentación de la ayuda de hping3 dice que:

-fast = 10 paquetes por segundo
-faster = 100 paquetes por segundo
-flood = Envío de paquetes lo más rápido que sea posible, y no se muestran respuesta

Para esta experimentación usaremos direcciones IP aleatorias como IPs falsa, -S que activa el flag Syn, -p 5060 el puerto a atacar, --flood para que los paquetes se envíen en tiempo real de forma masiva, y la dirección IP del servidor de VoIP 172.16.100.100 como IP víctima

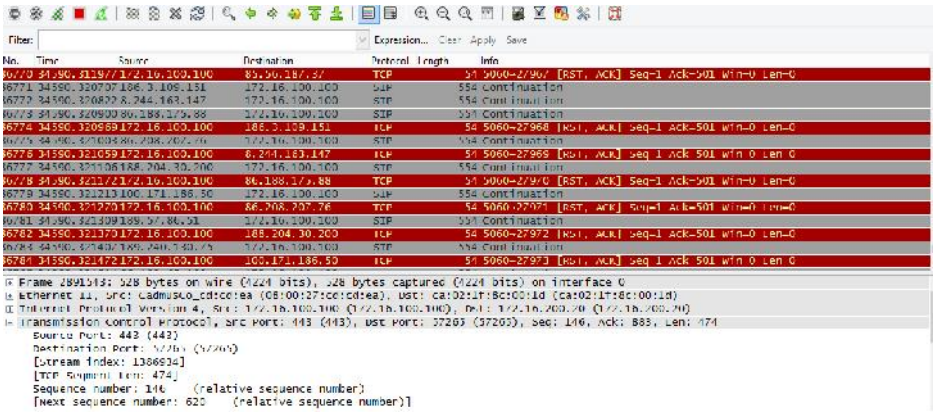
```
root@kali:~# hping3 --rand-source -S -p 5060 --flood 172.16.100.100
HPING 172.16.100.100 (eth0 172.16.100.100): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 172.16.100.100 hping statistic ---
851437 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

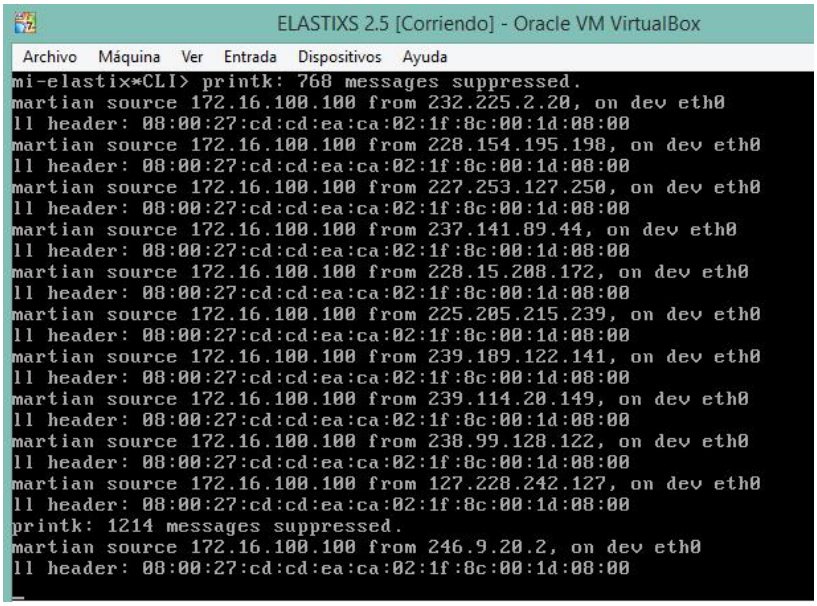


En la Figura, podemos observar que nuestro Kali está enviando peticiones a la víctima con IPs aleatorias. Si bien es cierto el tamaño del paquete TCP es de 54 bytes para colapsar el sistema es poco. Ahora alteramos el tamaño de los paquetes enviados por TCP.

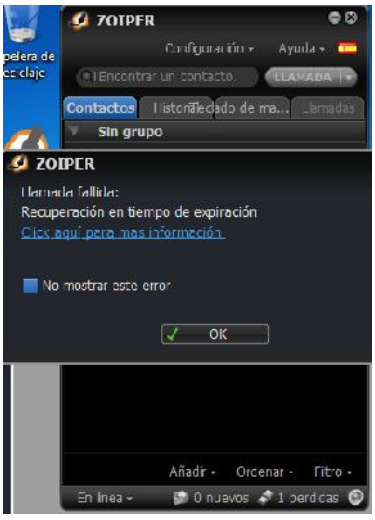
Para ello cambiamos el tamaño del paquete TCP por 500, con la siguiente sentencia.

```
root@kali:~# hping3 --rand-source -d 500 -S -p 5060 --flood 172.16.100.100
HPING 172.16.100.100 (eth0 172.16.100.100): S set, 40 headers + 500 data bytes
hping in flood mode, no replies will be shown
```





Una vez realizado este ataque SYN Flood, el servidor queda colapsado de peticiones SYN, sin poder identificar las peticiones de usuarios reales, hasta el punto que no acepta nuevas peticiones quedando a la espera del ACK final que nunca llegara de las IPs falsas.

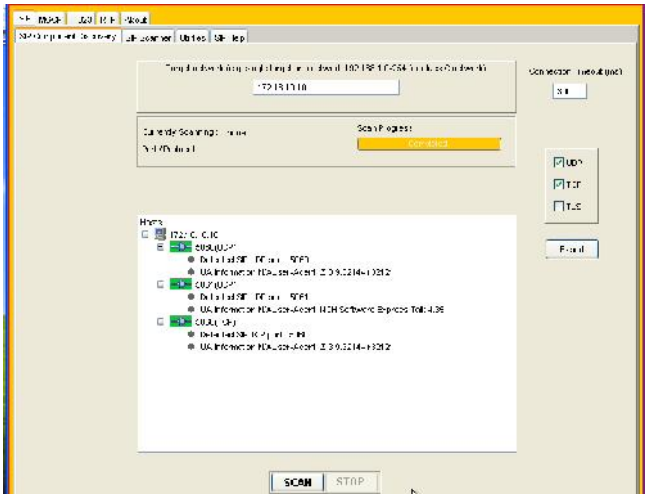


Al quedar a la espera del ACK final, el servidor rechazó las nuevas conexiones de usuarios reales, logrando con esto la denegación del servicio de VoIP.

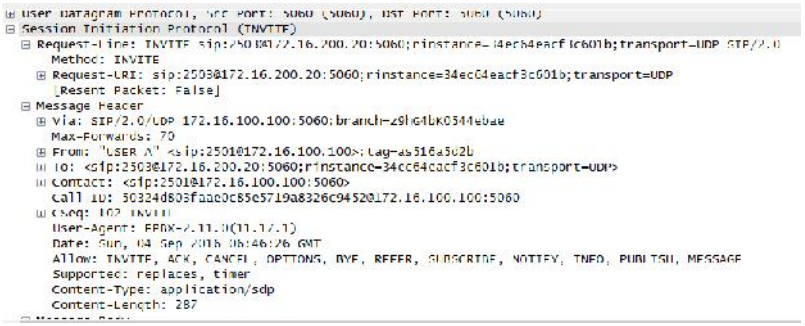
PRUEBA 4: MALFORMACIÓN EN MENSAJES INVITE

Para efectuar este ataque, se utilizó la herramienta Sivus. Esta herramienta además de contar con la funcionalidad de escáner de vulnerabilidades SIP, permite generar mensajes, alterando todos sus parámetros, el envío de mensajes INVITE con contenidos extraños puede hacer que los agentes de usuario funcionen mal o incluso dejen de funcionar completamente.

Antes de iniciar, es importante conocer el puerto por el que está escuchando la víctima.



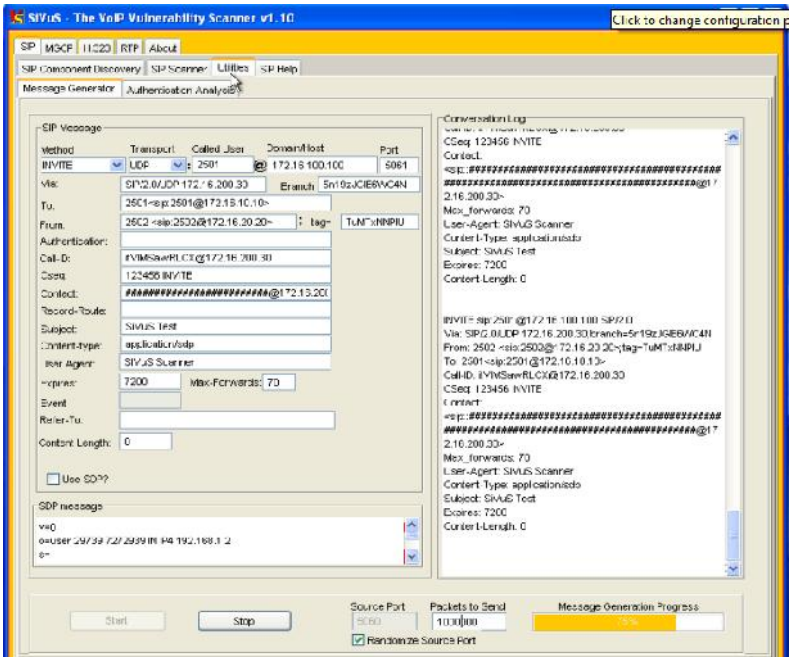
También es importante recordar el típico mensaje INVITE, en la figura se puede observar los URI, a los que se harán referencia en el ataque.

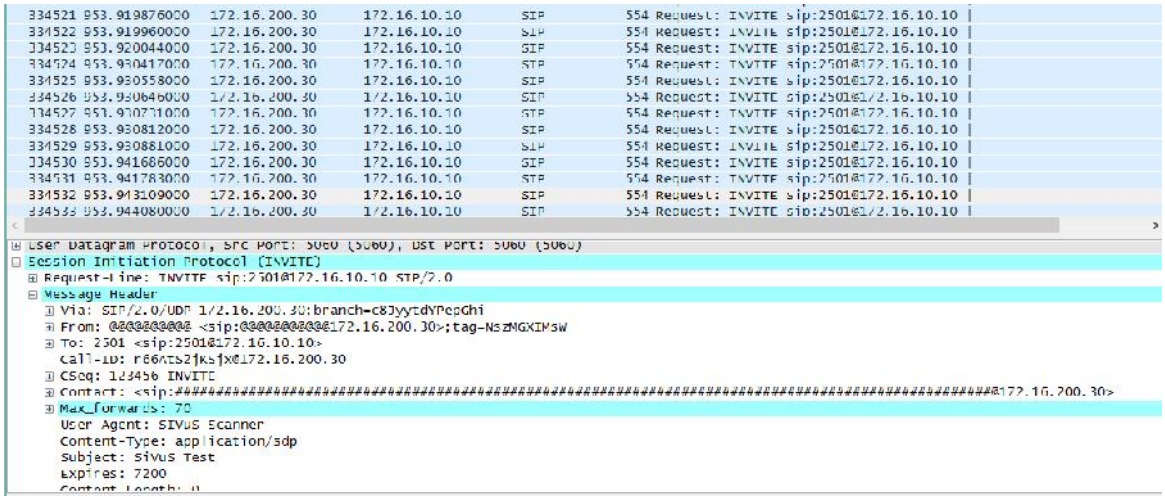


A través de Sivus se identificaron posibles ataques de malformaciones de mensajes INVITE. Es decir, se produce desbordamiento de buffer:

- Al enviar un mensaje INVITE con 100 caracteres, alfanuméricos y especiales, en el campo de despliegue de nombre de usuario (<sip:***usuario***@dominio.com>).
- Cuando se insertan 50 caracteres alfanuméricos y especiales en el campo o= del mensaje SDP inserto en el mensaje INVITE.
- Al enviar un mensaje INVITE con 3000 caracteres NULL.

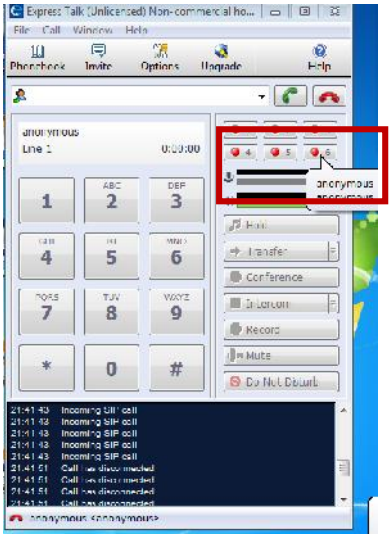
Se realizó el fuzzing al UA 2501, para ejecutar el ataque, ingresamos los parámetros que se observa en la Figura.



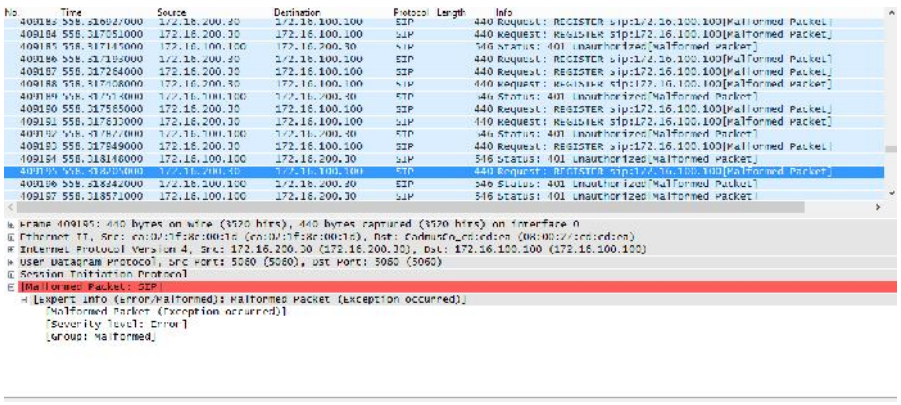


En la Figura se observa lo que sucede con el softphone Zoiper en al momento del ataque.

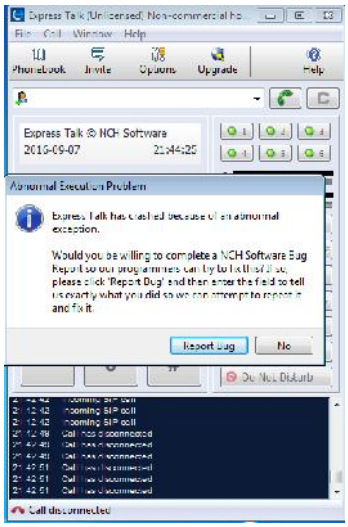
Igualmente, se observa el softphone Express Talk, al momento del fuzzing.



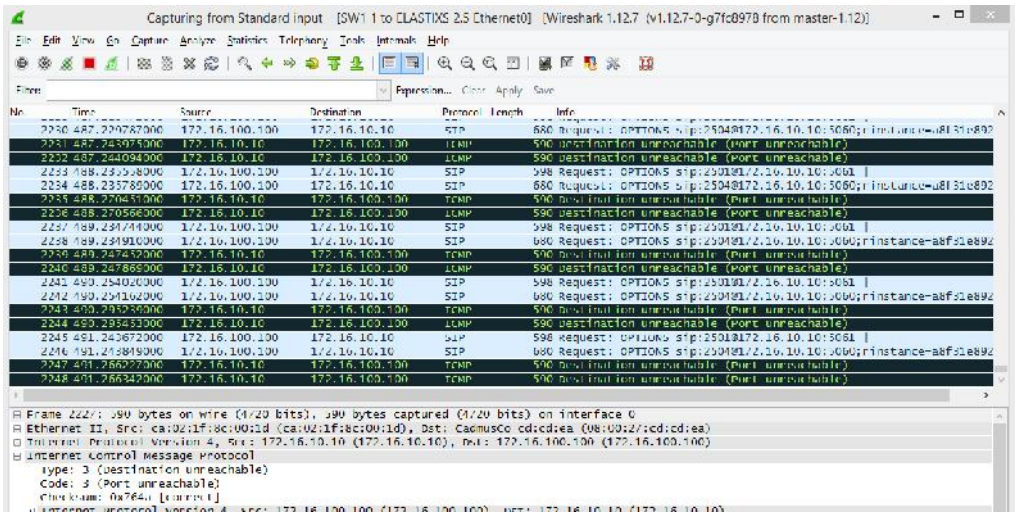
En la Figura se muestra el paquete capturado por el analizador de protocolos Wireshark, reconocido como ***"malformed packet".***



Finalmente, el softphone Express Talk es inundado de paquetes que contienen datos que llevan al protocolo al punto de ruptura, es decir, deja de funcionar.

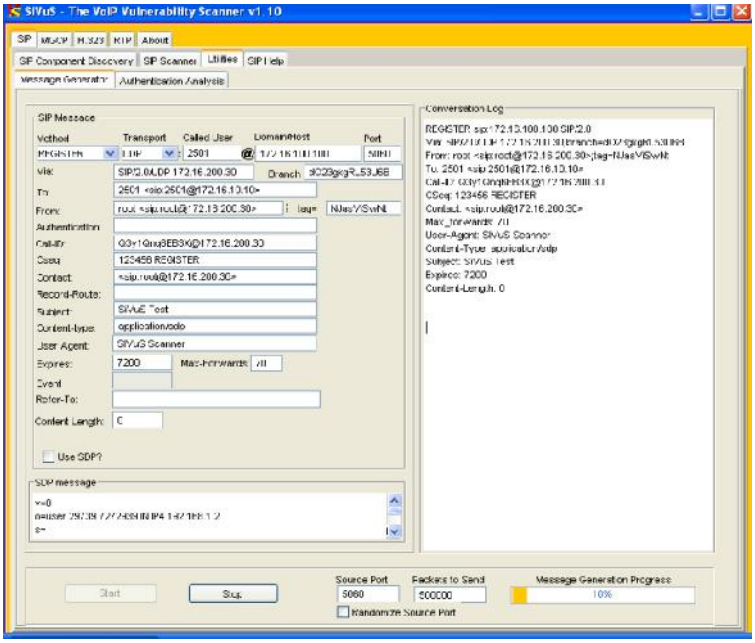


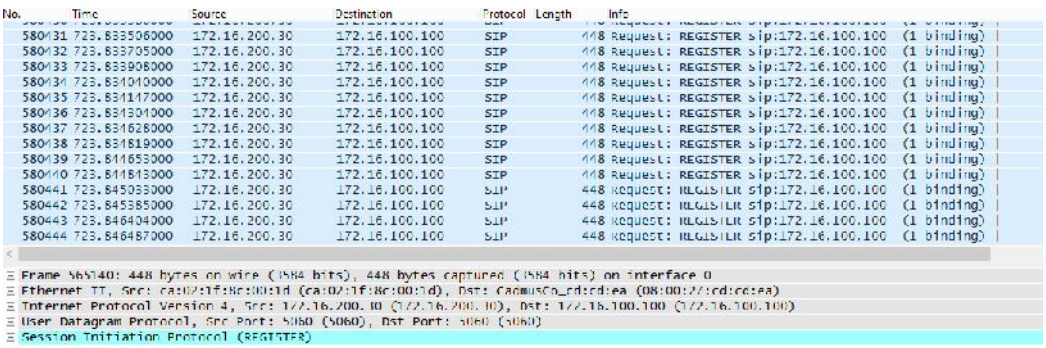
La Figura, muestra el momento en el que el usuario deja de estar disponible



PRUEBA 5: SIP REGISTER FLOODING

El ataque ocurre cuando el atacante envía un flujo de mensajes REGISTER al servidor SIP para agotar sus recursos y obligarlo al punto en el que no puede manejar las llamadas nuevas legítimas.





Las peticiones masivas de ***Register,*** inundan el servidor, hasta colapsarlo, como se muestra en la figura.

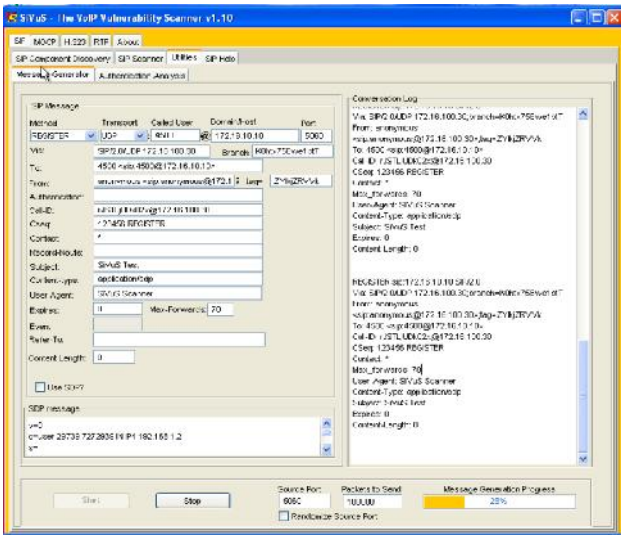
PRUEBA 6: Eliminación de Registro

Los dispositivos SIP tienen que enviar las peticiones REGISTER con el fin de registrarse en el servidor SIP.

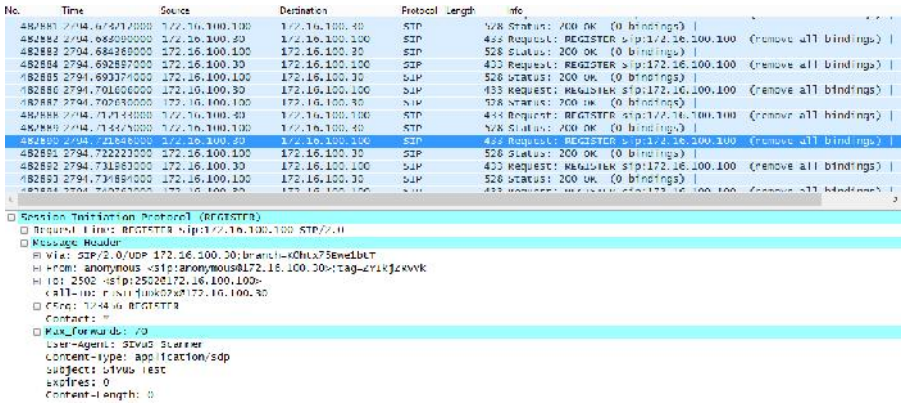
La figura muestra las extensiones que se encuentran registradas en el servidor SIP antes del ataque.

```
ELASTIXS*CLI> sip show peers
Name/username             Host                                    Dyn Forcerport
 Comedia    ACL Port     Status      Description
2501/2501                  172.16.10.10                             D  No
 No         A  5060     OK (16 ms)
2502/2502                  172.16.20.20                             D  No
 No         A  5060     OK (25 ms)
2503/2503                  172.16.200.20                            D  No
 No         A  5060     OK (31 ms)
2504                       (Unspecified)                            D  No
 No         A  0        UNKNOWN
4 sip peers [Monitored: 3 online, 1 offline Unmonitored: 0 online, 0 offline]
```

Este ataque se desarrolló utilizando la herramienta Sivus. Esta herramienta permite confeccionar un mensaje REGISTER. El intruso puede ser capaz de eliminar registros de un usuario fácilmente, enviando al servidor de registro peticiones REGISTER, con los valores clave de ***Contact: **** y ***Expire: 0***, que eliminan todos los registros para un teléfono SIP en el proxy SIP. Cuando se hace esto, el teléfono SIP no puede recibir ninguna llamada entrante.



Mediante el uso de la herramienta wireshark, se puede observar los paquetes RESGITER enviados por la herramienta.



La figura muestra el resultado del ataque de SIP Register Flooding con la herramienta Sivus, en la se puede observar que se elimina el registro de la dirección IP del usuario 2501.

```
ELASTIXS*CLI> sip show peers
Name/username             Host                                    Dyn Forcerport
 Comedia     ACL Port     Status      Description
2501/2501                  (Unspecified)                           D  No
 No          A  0         UNKNOWN
2502/2502                  172.16.20.20                            D  No
 No          A  5060      OK (15 ms)
2503/2503                  172.16.200.20                           D  No
 No          A  5060      OK (11 ms)
2504                       (Unspecified)                           D  No
 No          A  0         UNKNOWN
4 sip peers [Monitored: 2 online, 2 offline Unmonitored: 0 online, 0 offline]
```

Si se elimina un registro el teléfono SIP no puede recibir llamadas. ***El ataque de Eliminación de Registro,*** sin embargo, no afecta a la capacidad del teléfono SIP para realizar llamadas.