Modelo de Seguridad contra ataques de denegación de servicio para tráfico SIP

[a] Diego Fernando Avila Pesantez, [b] Juana Karina Arellano Aucancela, [a] Alberto Leopoldo Arellano Aucancela, [a] Carmen Elena Mantilla

[a] Escuela Superior Politécnica de Chimborazo (ESPOCH)
Chimborazo, Ecuador
davila@espoch.edu.ec, aarellano@espoch.edu.ec, cmantilla@espoch.edu.ec

[b] Universidad Nacional de Chimborazo
Chimborazo, Ecuador
karellano@unach.edu.ec

Resumen. Actualmente, las amenazas de seguridad en redes de Voz sobre IP (VoIP), son una preocupación importante y latente para las personas encargadas de la seguridad en redes corporativas, ya que cada día, se desarrollan nuevos ataques de Denegación de Servicio (DoS). Estos afectan la continuidad del negocio de una organización, en términos de confidencialidad, disponibilidad e integridad de servicios, provocando innumerables pérdidas tanto de información, como económicas. Esta investigación tiene la finalidad de establecer las medidas de necesarias para mitigar las amenazas de DoS, que afectan a la disponibilidad de los sistemas de VoIP, basados en el protocolo de señalización Session Inicial Protocol (SIP). Se plantea un Modelo de Seguridad denominado MS-DoS-SIP, que se basa en dos enfoques. El primero, analiza las recomendaciones de estándares y normas de seguridad internacionales como ISO/IEC 2702, UIT-T X.805 y NIST, mejores prácticas de Asterisk y de la empresa CISCO SYSTEMS, así como, de VOIPSA. El segundo enfoque, toma en cuenta las vulnerabilidades y amenazas, como: INVITE Flood para proxies SIP y teléfonos, malformación de mensajes INVITE, eliminación de Registro de Usuarios y finalmente SYN Flood DoS. La implementación de este modelo en un ambiente de red de VoIP simulado, logró minimizar en un 92% las vulnerabilidades presentes e incrementar el tiempo de disponibilidad del servicio VoIP.

Palabras Clave: Modelo de Seguridad, Vulnerabilidades VoIP-SIP, Ataques DoS, Seguridad SIP.

1 Introducción

Voz sobre IP (VoIP), es una tecnología que proporciona la comunicación de voz a través de la red de TCP/IP. Esta es una alternativa económica para la comunicación telefónica, comparada con la tradicional red pública telefónica (PSTN) [1]. Una llamada de VoIP utiliza dos fases: la señalización, y la transmisión de datos. El protocolo SIP, es un protocolo de la capa de aplicación, usada para la señalización en tráfico de conexiones de VoIP, implementada en una infraestructura de red de comunicaciones. Según IBM [2], el 51 % de los ataques cibernéticos están dirigidos al protocolo SIP. Se establece que, en el segundo semestre del año 2016, se realizaron el mayor número de estos ataques. La principal causa, se debe a las vulnerabilidades de este protocolo [3], tanto como a la inundación basada en el ataque de denegación de servicios (DoS).

Estos ataques son intentos explícitos para deshabilitar la transmisión de voz dentro de una organización, evitando así a usuarios legítimos hacer uso de sus servicios [4].

Para las buenas prácticas de seguridad en las comunicaciones de VoIP, las empresas pueden implementar modelos de seguridad, que permitan proteger y salvaguardar la información, conservando la confidencialidad, disponibilidad e integridad del servicio. Estos modelos permitirán concienciar a los administradores o encargados del área de seguridad, en precautelar los servicios de VoIP, para en la medida de posible, mitigar este tipo de amenazas y los efectos negativos que causan en los sistemas de comunicación. Actualmente, existe varias propuestas de empresas de tecnologías y estándares de la industria que apoyan a la necesidad de crear un modelo de seguridad, pero pocas se enfocan a la seguridad en protocolos SIP. Según la revisión de la literatura, los trabajos de [5-7], desarrollaron investigaciones para asegurar el servicio de VoIP, y mitigar ataques de DoS, pero no presentan soluciones específicas para el protocolo SIP. En cambio, los estudios de [8-10], analizaron el protocolo de señalización SIP, con un enfoque de mecanismos de seguridad, por lo que constituyen la base para la propuesta de nuestro modelo.

Otras investigaciones, como el trabajo de Ormazabal [4], realizaron estudios de funcionalidad y rendimiento de los sistemas de prevención de DoS, empleando herramientas que genera ataques basados en tráfico SIP. Los resultados experimentales fueron capaces de detectar y mitigar los ataques de spoofing y request, response y floods. También, Jouravlev et al [5], analizaron 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 mejorar la seguridad en el entorno de VoIP.

También Keromytis [3], presentó un estudio exhaustivo de la seguridad de voz sobre IP, utilizando un conjunto de 245 publicaciones de investigación académica sobre el tema, los clasificó de acuerdo con una versión extendida de la VOIPSA, según la taxonomía de amenazas. Además, Keromytis proporcionó una hoja de ruta, para los investigadores que buscan entender las capacidades existentes, e identificó las deficiencias en el tratamiento de las numerosas amenazas y vulnerabilidades, presentes en los sistemas de VoIP. Estableció dos áreas problemáticas específicas de denegación de servicio, y el abuso de servicio que exigen más atención por parte la comunidad de investigación.

Para la propuesta, varios componentes fueron analizados, y se fundamentaron en la norma ISO/IEC 27002, que ofrece 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 [11]. Además, con la UIT-T X.805, se definieron el marco de la arquitectura de seguridad, para sistemas de comunicación de extremo a extremo, así como las dimensiones que garantizan la seguridad de aplicaciones distribuidas [12]. Finalmente, se revisó las mejores prácticas propuestas por empresas, que lideran el mercado como Asterisk, Cisco, y Alianza de Seguridad de VoIP (VOIPSA).

Complementando la estructura del modelo propuesto, se consideró la metodología OSSTMM 2.1 compuesta por seis secciones, pero únicamente la sección de Seguridad

en Comunicaciones y Seguridad en las Tecnologías de Internet, se enmarcan en el enfoque del presente estudio [13]. Finalmente, se apoyó en las técnicas de recopilación propuestas en el libro "Hacking exposed VoIP", donde se identifican las fases de hacking ético [14].

Para el análisis de resultados de dicho modelo, se utilizó la metodología de caso de estudio, donde se simuló una red VoIP de una organización utilizando GNS3 versión 1.4.5 [15]. En el ambiente de pruebas, se ejecutaron los ataques más comúnmente utilizados con DoS, y se determinó parámetros de rendimiento de calidad voz y disponibilidad. Además, se registraron las respuestas a ataques, en un escenario sin implementar mecanismos de seguridad, y también los resultados, al aplicar el modelo propuesto, que garantizaría la disponibilidad del servicio de VoIP.

2 Metodología

El modelo propuesto, se basó en la metodología de OSSTMM 2.1 [13], que incluye las técnicas de reconocimiento *Footprint, Scanning y Enumeration* para una red de VoIP, y las recomendaciones más relevantes de la norma UIT-T X805, el estándar ISO/IEC 2702:2007-2015, el estándar NIST [16], la alianza VOIPSA [17], las plataformas de VoIP ASTERISK [18], y CISCO. Estas permitieron determinar la estructura del modelo, definición de sus fases y generación de las políticas de seguridad.

La metodología OSSTMM 2.1, presenta sus fases en función del costo y tiempo, como se muestra en la Figura 1, por lo que la parte práctica se apoyó de varios factores como: el análisis de las secciones de seguridad, las tecnologías de internet, y seguridad en las comunicaciones. Debido a que la primera es la parte medular, y en la segunda contempla aspectos de testeo de seguridad para la tecnología de VoIP, con lo que se define las etapas del modelo.

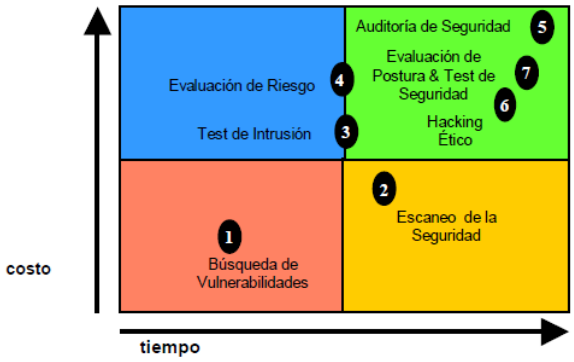

Fig. 1. Fases de OSSTM 2.1 [13].

Mediante la ejecución de las técnicas de reconocimiento *Footprint, Scanning y Enumeration* [13], se identificaron los agujeros de seguridad presentes en la

infraestructura de red. Esto permite emitir políticas de seguridad, para minimizar vulnerabilidades y mitigar amenazas. De las recomendaciones de la UIT-T X805, que hacen referencia a "Proteger la información de control o señalización que se utiliza en el servicio de red", se analizó la protección del protocolo SIP, en el proceso de inicio y mantenimiento de las sesiones de transmisión de VoIP. También, se consideró el estándar ISO/IEC 2702:2007-2015 en su dominio 9, que trata de la Seguridad de las Comunicaciones, haciendo énfasis en la protección del tráfico de VoIP, cifrar, segmentar el tráfico de datos y de voz, asegurar los IP-PBX, emplear controles de seguridad perimetral. En las prácticas iniciales para la implementación de una red VoIP segura, el NIST plantea:
a) Desarrollar una arquitectura apropiada mediante la Independización de la red de voz, usar autenticación y control de acceso, e Implementar Firewalls.
b) Realizar controles físicos en la red VoIP.
c) Utilizar mecanismo de Protección como Firewall especializados en VoIP.

Complementando, con las mejores prácticas propuestas por ASTERISK y CISCO, que recomienda realizar actualizaciones constantes, emplear herramientas de monitoreo de la red VoIP, eliminar servicios que no están siendo usados, modificar las configuraciones básicas, usar siempre VLANs, asegurar los elementos de la red VoIP, aplicar Firewalls, IDS, IPS, y/o SBC para analizar el tráfico y monitorear cualquier tipo de ataque. Además, se sumaron las recomendaciones más importantes de VOIPSA que propone: identificar dispositivos de la red VoIP mediante el escaneo de puertos y protocolos, realizar barridos periódicos de seguridad usando escaneo automáticos o manuales, e implementar Firewalls y/o IPS, orientados específicamente a redes VoIP.

1.1 Modelo de seguridad propuesto

El Modelo de Seguridad se denominó MS-DoS-SIP, y se enfoca hacia ataques de denegación de servicio (DoS) en tráfico SIP. Propone cuatro etapas de acción, que pueden tomar los administradores o profesionales de la Seguridad Informática. Las etapas se muestran en la Figura 2, y deben desarrollarse en forma cíclica, ya que cada etapa dependerá de la anterior, creando un bucle constante de análisis, sobre la red VoIP de la organización. La ejecución de las fases dependerá de las tecnologías, protocolos y dispositivos utilizados, ya que no todos los dispositivos cuentan con sistemas de seguridad mencionados en este modelo.

Fig. 2. Etapas del Modelo propuesto MS-DoS-SIP

ETAPA 1.- El primer paso es investigar la infraestructura de VoIP, utilizando la información que esté disponible en la red. Si la información ha sido recopilada correctamente, y con detalle, permite el acceso garantizado a los sistemas que utilicen el servicio de VoIP. Por esto, es de trascendental importancia conocer en profundidad qué tipo de información puede adquirir el atacante, y tomar acciones que permitan minimizar el posible daño. En esta etapa, se conoce y analiza con rigor, qué tipo de información puede adquirir el atacante de nuestra infraestructura de red. Mediante la aplicación de herramientas de software, se identifica el diseño de la red de VoIP como: topología, mapa, direccionamiento IP, protocolos de señalización, y todos los dispositivos hardware y software que conforman la red de comunicaciones: softphones, sistemas operativos, configuración, y características de dispositivos. de escaneo de puertos y protocolos, se determina sus vulnerabilidades

ETAPA 2.- Se establecen las vulnerabilidades y fallos de seguridad comúnmente usadas, para causar daños en la infraestructura de VoIP basada en SIP, y el impacto que puede causar. En la Tabla 1, se muestra la lista de vulnerabilidades y el impacto en el servicio de VoIP, que por lo común son identificados en las redes de VOIP y se calificó el impacto en la disponibilidad del servicio. Además, en base del trabajo de Endler & Collier [14], se determinaron y clasificaron las principales amenazas, que afectan con mayor criticidad a la disponibilidad del servicio de VoIP. Se analiza la probabilidad de ocurrencia, y el grado de severidad en las consecuencias, considerando el daño potencial causado por la ejecución perpetrado con éxito. Los datos de la Tabla 1 y 2, permiten en esta etapa identificar con certeza, cuáles son las vulnerabilidades detectadas en la red de comunicación, y los posibles ataques que probablemente puede ser víctima.

Tabla 1. Vulnerabilidades e Impacto en VoIP [14].

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	

Tabla 2. Ataques a la disponibilidad de servicios VoIP [14].

ATAQUE	POPULARIDAD	IMPACTO	ESTIMACIÓN DEL RIESGO
Malformación de Mensajes	Poco Frecuente	Intolerable	Importante
Floods INVITE to SIP Proxies (Usando inviteflood Tool)	Moderadamente Frecuente	Extremadamente Intolerable	Muy Importante
Floods INVITE to SIP Phone (Usando inviteflood Tool)	Medianamente Alta	Intolerable	Muy Importante
Flood Register	Moderadamente Frecuente	Intolerable	Importante
Eliminación de Registros	Frecuente	Ligeramente Importante	Importante
SynFlood DoS	Medianamente Alta	Intolerable	Intolerable

ETAPA 3.- Se consideran interrupciones en el servicio de VoIP, que no se producen necesariamente por ataques de intrusos. Para ello, existen ciertos síntomas a tener en cuenta, en la identificación de un ataque de DoS. Se realiza un examen a la seguridad de la red VoIP, con el objetivo de reconocer indicios, que puedan alertar de un posible ataque de DoS, por ejemplo:

a) la red estuvo funcionando en forma mucho más lenta de lo habitual.
b) el servicio no estuvo disponible.
c) se recibe una enorme cantidad de peticiones. Probablemente, la red es víctima de un ataque de denegación de servicio. El monitoreo de red, se realiza mediante herramientas como PRTG (permiten supervisar el tráfico SIP como HOMER5), así como el monitoreo y análisis de logs a través de File2ban.

ETAPA 4.- Finalmente, una vez identificados los síntomas y vulnerabilidades presentes en la red, se procede a aplicar las medidas de seguridad tales como: segmentar la red, cambiar puertos estándares, actualización y parches de software, implementación de TLS, configuración de Firewalls SIP, Iptables, Session Border Controller (SBC), que permiten mitigar las vulnerabilidades y riesgos que puede sufrir la infraestructura de VoIP dentro de una organización.

3 Caso de estudio

Para el caso de estudio propuesto, se diseñó un escenario simulado de pruebas utilizando GNS3 versión 1.4.5. Este permitió establecer la tecnología e infraestructura de red de VoIP adecuada. Se implementó una central telefónica con Elastixs 2.5 (servidor de VoIP), 4 clientes SIP, donde se instaló el softphone Zoiper, que permiten simular teléfonos IP en los computadores, y Express Talk (versión no comercial). Además, se configuró un router y cuatro switches capa 2. Finalmente, para la ejecución de los ataques se empleó máquinas virtuales con Kali Linux y Windows 10. En la figura 3, se observa el escenario planteado en la simulación.

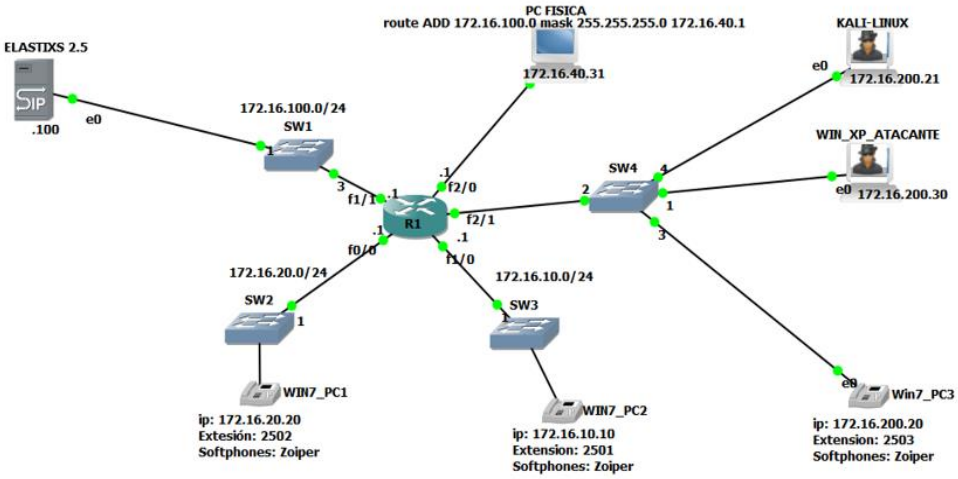

Fig. 3. Diagrama de interconexión establecido para la simulación de pruebas.

Al desarrollar las tres primeras etapas del modelo de seguridad en el escenario de pruebas, se encontraron trece vulnerabilidades, que se describen en la Tabla 3. Luego de establecer estas vulnerabilidades, se dieron tratamiento con la implementación del modelo de seguridad planteado.

Tabla 3. 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

Para esta investigación, se establecieron como objeto de estudio los ataques específicos de SIP que afectan a la disponibilidad de VoIP, tales como los ataques basados en Flooding y Fuzzing: INVITE Flood to Proxy, INVITE Flood to Phones, Malformación

en mensajes INVITE, Eliminación de Registro de Usuarios SIP y SYN flood, como se muestra en la Tabla 4.

Los ataques SIP Flooding, se producen cuando los teléfonos IP generan peticiones o respuestas para enviar a un servidor específico, llamado víctima. Como resultado el servidor está ocupado por la recepción de excesivos mensajes SIP dentro de un corto período de tiempo, afectando a los servicios normales. INVITE Flood, es considerado uno de los ataques más típicos de inundación, tanto para servidores como para terminales. Así como también los ataques de malformación de mensajes son una amenaza del tipo fuzzing que modifica campos en el mensaje INVITE. Este funciona enviando mensajes INVITE con contenidos no previstos por el protocolo, provocando que los terminales funcionen mal o dejen de funcionar por completo.

La vulnerabilidad utilizada en el ataque de Eliminación de Registro de Usuarios SIP, es la falta de autenticación en el mensaje REGISTER. El atacante envía al servidor de registro una petición REGISTER indicando la identidad del usuario, con el campo contacto "Contact:*" y el valor "Expire" = cero. Logrando eliminar cualquier otro registro de la dirección del usuario.

Tabla 4. Ataques a SIP en Ambiente de Pruebas

Amenazas	**Ataque**
Fuzzing	Malformación de mensajes
Flooding	Floods INVITE to SIP Proxies (usando inviteflood Tools)
Flooding	Floods INVITE to SIP Phones (usando inviteflood Tools)
Manipulación de la Señalización	Eliminación de Registros

Para el desarrollo de las pruebas, se estableció el número de paquetes enviados en cada ataque y se consideró la recomendación de Endler & Collier, que establece el envío de 1.000.000 de paquetes a un objetivo para experimentar ataques de DoS basados en Flooding y Fuzzing. En cambio, para las pruebas de penetración los valores propuestos son 500.000 y 2.000.000 paquetes. Además, para establecer parámetros específicos respecto al servicio de VoIP, se aplicó encuestas a instituciones públicas y privadas. La cual estableció resultados relevantes frente al uso del servicio de VoIP y la importancia de mantener siempre disponible el mismo, ya que, el 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. Por 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 con los valores de paquetes establecidos.

Los indicadores que se analizaron en las pruebas son: *latencia*, *jitter* y *pérdida de paquetes*. Puesto que, son los parámetros que afectan directamente a la calidad del servicio VoIP. Se establecieron los valores de latencia: menor a 150ms; Jitter: menor a

50ms; y la pérdida de paquetes: menor o igual al 3% del volumen de datos transmitido. Para este análisis, se utilizó la herramienta Wireshark. Finalmente, el indicador más relevante es el *Tiempo de Interrupción del Servicio de VoIP*, que permitió conocer el tiempo exacto en que el servicio de VoIP dejo de estar disponible en la red, a través de la herramienta PRTG Network Monitor.

Se analizaron y compararon los resultados experimentales obtenidos de las pruebas en cada escenario, permitiendo demostrar la mejora en la prevención de ataques de cada solución propuesta en el Modelo de Seguridad MS-DoS-SIP. Al aplicar el modelo, en número de vulnerabilidades identificadas, se redujo en un 92% con respecto al escenario sin medidas de seguridad, como se muestra en la Figura 4.

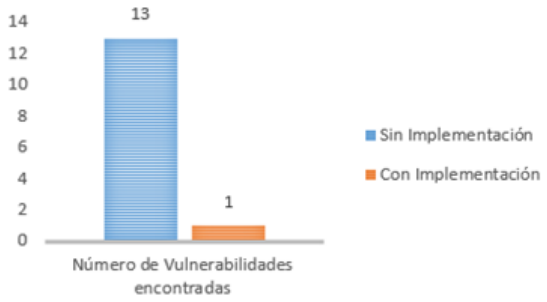

Fig. 4. Vulnerabilidades identificadas en el escenario de pruebas

Para el Indicador: Tiempo de no disponibilidad del servicio VoIP, se establece que con la implementación del Modelo de Seguridad, se incrementa 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 Figura 5.

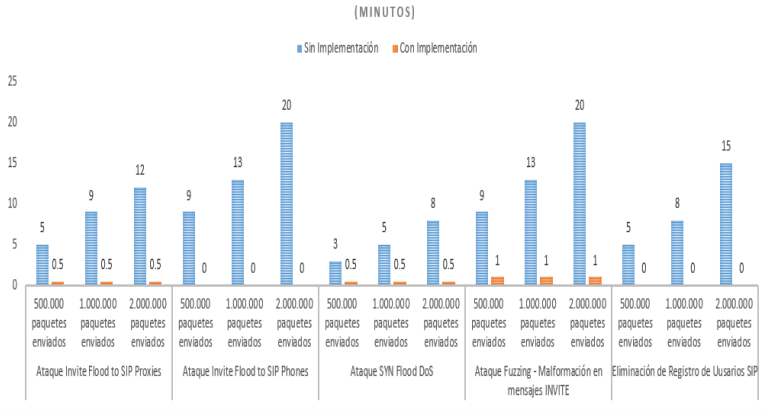

Fig. 5. Tiempo de No Disponibilidad del Servicio VoIP

Finalmente, se demuestra que mediante la aplicación del Modelo de Seguridad MS-DoS-SIP, para mitigar ataques de Denegación de Servicio en tráfico SIP en servicios VoIP, se reduce las vulnerabilidades ante ataques de DoS, incrementando la disponibilidad del servicio de VoIP en redes LAN Corporativas.

4. Conclusiones

La propuesta del Modelo de Seguridad MS-DoS-SIP, orientado a ataques de DoS en tráfico SIP, como soporte al proceso de aplicación de mecanismo de seguridad en una red VoIP, ayuda a asegurar que se apliquen las contramedidas adecuadas, en el momento de buscar mitigar ataques de DoS. Esta metodología, se basa en propuestas como la OSSTMM 2.1 y las Técnicas de Reconocimiento (Hacked Exposed VoIP), que permiten tener una idea clara, y una referencia de trabajo estándar. Además, se consideraron las recomendaciones de seguridad de los estándares y normas internacionales ISO/IEC 2702:2007-2015, en donde se enfatiza la protección de tráfico de VOIP mediante el cifrado, segmentación de tráfico y empleo de controles de seguridad perimetral.

La UIT-T X.805, sugiere que se debe proteger el protocolo SIP con el uso de TLS, NIST; colocar una arquitectura adecuada y emplear firewalls especializados en VOIP. Finalmente, las mejores prácticas de Asterisk, Cisco y VOIPSA, mencionan examinar periódicamente la seguridad de la red, mediante el escaneo de puertos en protocolos.

La aplicación del Modelo MS-DoS-SIP, en un ambiente de red de VoIP simulado, a través de escenarios prácticos, logró minimizar en un 92% las vulnerabilidades establecidas en este trabajo, en comparación con el mismo escenario sin mecanismos de seguridad. Al reducir notablemente las vulnerabilidades, se consiguió alcanzar tiempos de interrupción del servicio de pocos segundos, garantizando así la continuidad de VoIP dentro de una organización.

Es altamente recomendable profundizar la investigación, en cuanto a las técnicas y herramientas que usan los atacantes en la actualidad, con la finalidad de ir actualizando el Modelo de Seguridad propuestos. En trabajos futuros, se aconseja tomar en consideración, el uso de un sistema de correlación de eventos en las redes de VoIP, y las nuevas actualizaciones de seguridad, con objeto 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.

Referencias

[1] D. Golait and N. Hubballi, "Detecting Anomalous Behavior in VoIP Systems: A Discrete Event System Modeling," *IEEE Transactions on Information Forensics and Security,* vol. 12, no. 3, pp. 730-745, 2017.

[2] S. Intelligence, "https://securityintelligence.com/hello-youve-been-compromised-upward-attack-trend-targeting-voip-protocol-sip/."

[3] A. D. Keromytis, "A comprehensive survey of voice over IP security research," *IEEE Communications Surveys & Tutorials,* vol. 14, no. 2, pp. 514-537, 2012.
[4] G. Ormazabal, S. Nagpal, E. Yardeni, and H. Schulzrinne, "Secure sip: A scalable prevention mechanism for dos attacks on sip based voip systems," *Principles, systems and applications of IP telecommunications. Services and security for next generation networks,* pp. 107-132, 2008.
[5] I. Jouravlev, "Mitigating Denial-Of-Service Attacks On VoIP Environment," *International Journal of Applied Management and Technology,* vol. 6, no. 1, 2008.
[6] M. V. Martin and P. C. Hung, "Towards a security policy for VoIP applications," in *Electrical and Computer Engineering, 2005. Canadian Conference on*, 2005, pp. 65-68: IEEE.
[7] L. Shan and N. Jiang, "Research on security mechanisms of SIP-based VoIP system," in *Hybrid Intelligent Systems, 2009. HIS'09. Ninth International Conference on*, 2009, vol. 2, pp. 408-410: IEEE.
[8] J. Lee, K. Cho, C. Lee, and S. Kim, "VoIP-aware network attack detection based on statistics and behavior of SIP traffic," *Peer-to-Peer Networking and Applications,* vol. 8, no. 5, pp. 872-880, 2015.
[9] M. Z. Rafique, M. A. Akbar, and M. Farooq, "Evaluating DoS attacks against SIP-based VoIP systems," in *Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE*, 2009, pp. 1-6: IEEE.
[10] U. U. Rehman and A. G. Abbasi, "Security analysis of VoIP architecture for identifying SIP vulnerabilities," in *Emerging Technologies (ICET), 2014 International Conference on*, 2014, pp. 87-93: IEEE.
[11] ISO, "Glosario de términos."
[12] UIT-T, "X.805 : Arquitectura de seguridad para sistemas de comunicaciones extremo a extremo."
[13] P. Herzog, "Manual de Metodología Abierta de Testeo de Seguridad," ed: INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES, Última versión, 2003.
[14] D. Endler and M. Collier, *Hacking exposed VoIP: voice over IP security secrets & solutions*. McGraw-Hill, Inc., 2006.
[15] GNS3, "https://gns3.com/news/article/gns3-1-4-5-released-2."
[16] NIST, "https://www.nist.gov/publications/security-considerations-voice-over-ip-systems."
[17] VOIPSA, "http://www.voipsa.org/."
[18] ASTERISK, "https://community.asterisk.org/t/asterisk-security-best-practices/."