Fecha de Realización:	15/09/2021
Programa:	Especialización en Seguridad Informática
Línea de Investigación:	SEGURIDAD EN SISTEMAS VOZ/IP
Título:	MÉTODOS APLICADOS PARA MEJORAR LA SEGURIDAD EN SISTEMAS VOZ/IP
Autor(es):	Pedro Javier Bayter
Palabras Claves:	Riesgos, seguridad, VoIP, Call Manager, Gateways, Protocolo SIP.
Descripción:	La presente monografía tiene como objetivo realizar un estudio sobre los diferentes puntos de falla en la seguridad de las plataformas VoIP, se quiere ahondar en los diferentes ataques que esta plataforma recibe al estar expuesta dentro de una plataforma de datos como la IP, también conocer sus ventajas. Para comprender de una mejor manera los aspectos que se van a tartar en este documento, se hace necesario revisar el panorama de una forma en general sobre la actualidad de las soluciones de VoIP. También se debe estudiar el funcionamiento de la tecnología ya mencionada, describiendo la arquitectura de la red asociada a los protocolos SIP y los demás protocolos que intervienen en la solución. Es necesario realizar una clasificación de las vulnerabilidades que puedan existir en las tecnologías que intervienen en la solución de VoIP y a qué tipo de ataques se está expuesto, todo esto es variable dependiendo del tipo de tecnología que se use dentro de la red.Se trabajará en la investigación y documentación de los diferentes protocolos que ayuden a mejorar la seguridad enfocados a las redes de VoIP y protocolos SIP, estos son protocolos generales que dentro de su funcionamiento está la gestión contraseñas y cifrados, entre otros que pueden ayudar a la seguridad. También se estudian diferentes mecanismos para la detección de intrusiones que puedan generar daños y pérdidas económicas sobre las redes para las empresas, dentro de los cuales se estudiará su funcionamiento y como protegerse. Dentro de los estándares que se analizaran en este trabajo se hará énfasis en los protocolos usados para VoIP (H323, SIP, RTP, MGCP, SCCP e IAX), con la finalidad de entender como los hackers aprovechan las vulnerabilidades existentes en nuestras redes.

Fuentes bibliográficas destacadas:

ALANA B. Johnston. SIP: Understanding the Session Initiation Protocol. 4ª ed. Boston Artech House.2015, 410p

ASLAN S. Vásquez. Consideraciones sobre la seguridad en las redes de telecomunicaciones soportes de voz sobre ip (voip) en cuba. 2007, 40p.

BRYANT R, Madsen L, Van Meggelen Asterisk, the definitive guide, 4ª ed. O'Reilly Media, 2013, 86p.

CARRASCO HIRUELO. Antonio, Documento de la Universidad de Cataluña Seguridad VoIP: ataques y contramedidas en sistemas de código abierto. Cataluña. 2019, 30, 31, 33, 34p.

COLLIER Mark, ENDLER David y HILL Mc Graw. Unified Comunications and VoIP. 2014, 52, 289, 291, 292, 294, 298, 300, 301, 312, 407, 408, 477, 607 p.

GUTIERREZ G. Seguridad en VoIP: Ataques, Amenazas y Riesgos. 2014, 3, 4, 6, 13, 14, 16, 35, 44p.

JHONSON.B. Alan. SIP Understanding the Session Initiation Protocol Fourth Edition. Artechhouse. Boston. 2016, 416p.

KRASHENINNIKOVA E. Seguridad en VoIP: aplicaciones de señuelos. Madrid. 2013, 56p.

LAPSLEY P. Exploding the phone: Thee Untold Story of the Teenagers and Outlaws Who Hacked Ma Bell. New York: Grove Press.2013, 91p.

PIEDRA O. María y SOLORZANO V. Lucia. Análisis comparativo entre alternativas libres y propietarias para la migración de telefonía tradicional a telefonía IP. Cuenca. 2011, 27, 28p.

PORTER T. Practical VoIP Security. Canada: Syngress Publishing. 2016 99p.

REGIS J. Securing VoIP. El Sevier. 2015, 21, 71, 170p.

WALLINGFORD T. VoIP Hacks Beijing: O´REILLY. 2015, 228p.

AUDIOCODECS. Management Product & Solutions. Abril 2020. Disponible en https://www.audiocodes.com/solutions-products/products/management-products-solutions/one-voice-operations-center

AVAYA. Application Server 5300Overview. Marzo 2019. Disponible en https://downloads.avaya.com/css/P8/documents/100174168.

BAUMANN R, Schmid C. Voice Over IP - Security and SPIT. Septiembre 2006. Disponible en http://rainer.baumann.info/public/voip.pdf

COLLIER M. VoIP Vulnerabilities – Registration Hijacking. Junio 2005. Disponible en https://download.securelogix.com/library/Registration_hijacking_060105.pdf

COLLIER M. Basic Vulnerability Issues for SIP Security. Marzo 2005. Disponible en https://download.securelogix.com/library/SIP_Security030105.pdf

CUTILI, Catania, García, Problemas y herramientas en la seguridad de redes de transmisión de datos universitarias. El caso de la Universidad Nacional de Cuyo. 2012, Disponible en http://dspace.redclara.net/bitstream/10786/832/1/10- 2_Problemas_y_herramientas.pdf

DRUID. VoIP-Attacks. 2007. http://druid.caughq.org/presentations/VoIP-Attacks.pdf

GUTIERREZ. Ramírez. Seguridad en VoIP: Ataques, Amenazas y Riesgos, 2020Disponible en http://www.it- docs.net/data/896.pdf

GRANADOS& CARDENAS. Implementación de Voz/IP como solución a obsolescencia del PBX análogo,septiembre2014, Disponible en https://repository.usta.edu.co/bitstream/handle/11634/3586/Cardenasoscar2014.pd f?sequence=1#page=1&zoom=auto-99,792

INCIBE.Glosario de términos de ciberseguridad. Febrero 2017. Disponible en https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf

LIBERONA,M.Seguridad en Voz/IP. noviembre, 2010Disponible enhttp://www.telematica.utfsm.cl/telematica/site/artic/20121011/asocfile/20121011110145/liberonamaria.pdf.

LÓPEZ, A. El portal de ISO 27001 en español. 2020. Disponible en https://www.iso27000.es/glosario.html,

Marco legal que sustenta las TIC en Colombia: marco legal de las TIC en Colombia. [En línea]. 2012. (Recuperado el 12 de abril 2020.) Disponible en http://ticcentroeducativosantateresa.blogspot.com/2012/04/marco-legal-que-sustenta-las-tic-en.html, 2012.

MCAFEE., Las vulnerabilidades de VoIP. 2020. Disponible en http://www.microsa.es/biblioteca/McAfee/McAfee_Vulnerabilidades_de_VoIP.pdf

MCCARRON J. A Brief Overview of VoIP Security. 2020. Disponible en http://www.infosecwriters.com/text_resources/pdf/Voip_JMccarron.pdf,

NETWORK WORLD, Aumentan los ataques cibernéticos a través de VoIP. 2016. Disponible en https://www.networkworld.es/seguridad/aumentan-los-ataques-ciberneticos-a-través-de-voip

SIERRAH. Estado del arte de la seguridad VoIP, 2014, Disponible en http://ojs.urepublicana.edu.co/index.php/ingenieria/issue/view/20/8

SCHOLZ H. SIP Stack Fingerprinting and Stack Difference Attacks. 2020. Disponible en https://www.blackhat.com/presentations/bh-usa-06/BH-US-06-Scholz.pdf.

VOIPSA. VoIP Security and Privacy Threat Taxonomy. Octubre 2005. Disponible en http://www.voipsa.org/Activities/VOIPSA_Threat_Taxonomy_0.1.pdf

Contenido del documento:

Descripción del problema de investigación.	Dada la masificación que ha tenido la Voz sobre IP (VoIP) en el mercado, se presentan muchos problemas de seguridad que los atacantes aprovechan para suplantar o para sacar provechos económicos de la solución a la cual puedan acceder. Uno de los problemas más latentes es la actualización de los sistemas que soportan la solución, de los más reconocidos son Asterisk que corre sobre Linux y que este debe tener un buen robustecimiento en el S.O para evitar que por alguna vulnerabilidad expuesta se puedan filtrar y generar un problema sobre la solución.

	Otro de los problemas tiene que ver con los teléfonos IP que se usan dentro de la solución, estos equipos también tienen un sistema operativo y que estos si no se actualiza el Firmware, también puede ser un punto débil dentro de la solución que terminan afectando el correcto funcionamiento de la solución. Por otro lado, el robustecimiento de las credenciales de usuarios que de una u otra manera tienen acceso a la solución es un punto que se debe mirar con lupa para mitigar una fuga de información o un punto débil dentro de la solución que pueda llegar a afectar el funcionamiento, esto muchas veces es pasado por alto en las organizaciones, pero es algo que realmente ayuda a mitigar cualquier fuga en la solución que llegan a representar problemas económicos
Objetivo general.	Determinar las amenazas dirigidas a los protocolos de Voz sobre IP, basado en metodologías para investigación de vulnerabilidades.
Objetivos específicos.	• Identificar información sobre el uso de sistemas Voz/IP en redes empresariales, que permita evidenciar y documentar posibles fallas de seguridad en la implementación del sistema. • Establecer las posibles amenazas y riesgos asociados a las redes de datos en donde se implementan servicios de Voz sobre IP. • Documentar las mejores prácticas de seguridad informática que permita el aseguramiento de plataformas y/o sistemas de Voz/IP.
Metodología	Por medio de la recolección y análisis de la información asociada al factor humano como riesgo, junto con los diferentes protocolos, puertos y servicios, se pueden identificar problemas asociados a la investigación tanto de las redes LAN como las propias de los sistemas de VoIP que permiten tener información apreciable y fehaciente, sobre las cuales se desarrolla esta monografía, permitiendo identificar factores comunes en los problemas que se presentan debido al factor humano, así como en el entorno sobre el que están y cómo influye en pro o en contra de este en la seguridad de la información, permitiendo identificar los posibles impactos que tienen y posibles soluciones acordes a ellas.
principales referentes teóricos y conceptuales.	La mayor modalidad de ciber crimen es la estafa que se aprovecha de técnicas como la ingeniería social (Centro cibernético Policial, C. C. P. 2017) Tercer sector que más recibe ataques cibernéticos cada día con 83.756 ataques por día, (Dinero, R. 2017) La seguridad de la información ha sido tradicionalmente liderada por la tecnología y como resultado, se ha pasado por alto el rol y el valor de las personas. ASHFORD, W. (2017). Por puertas traseras por infección de malware y la utilización de RAT Remote Access Tool para la ejecución de software malicioso que sirve para la transferencia ilegal y no consentida de Dinero. (Centro cibernético Policial, C. C. P. 2017) Un 95 por ciento de las ataques o incidentes en materia de seguridad se deben a fallos humanos. (CCN-CERT. 2015). La mayoría de estos engaños van mutando con el tiempo, por eso decimos que son difíciles de erradicar porque por más que se eduque a

	los usuarios, los atacantes van cambiando la forma y las técnicas para engañar. (CANCINO, H., 2019)
Conceptos adquiridos:	El factor humano es determinante en los diferentes sistemas como en el de la información donde la falta de compromiso de los empleados a su organización u empresa pone en riesgo no solo la información sino la estabilidad de estas, estos debido a diferentes factores siendo recurrente la falta de conocimiento en los diferentes niveles que componen las organizaciones, principalmente con mayor gravedad los responsables de la toma de decisiones en esta que dirigen los caminos de ellas. El valor que tienen las auditorias por lo que representan debe ser algo que este implementado en todas las organizaciones.
Resultados y Conclusiones:	La investigación y documentación de esta monografía nos lleva a entender que las redes de datos por sí solas no son tan vulnerables o las vulnerabilidades propias son bajas, el problema radica en que estas soluciones de Voz son soportadas por redes de datos, redes ya existentes que en muchas ocasiones son mal configuradas y no son actualizadas de forma correcta, es cuando entendemos que la Voz sobre IP es un conjunto de protocolos que se unen para hacer posible una solución con muchas bondades. Dentro de este trabajo se detallaron los protocolos, puertos, equipos activos y pasivos que juegan un papel importante dentro de las redes de datos apalancando la solución VoIP. Dentro del alcance y como finalidad este trabajo busca documentar las fallas asociadas a la solución de VoIP, pero también es necesario investigar y documentar las posibles soluciones, cuáles son las mejores prácticas al momento de implementar estas soluciones, es por esto que en el desarrollo del objetivo 3 se detalla de forma muy completa las buenas prácticas a tener en cuenta.