MEDICIÓN DE LA SEGURIDAD DE LA TELEFONÍA IP ASTERISK EN CREAMIGO MOTUL BAJO TÉCNICAS DE PENTESTING.

CÉSAR AUGUSTO MEJÍA OSORIO

JORGE IVÁN MOSQUERA PALACIOS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SANTIAGO DE CALI, MEDELLÍN.
2017

MEDICIÓN DE LA SEGURIDAD DE LA TELEFONÍA IP ASTERISK EN CREAMIGO MOTUL BAJO TÉCNICAS DE PENTESTING.

CÉSAR AUGUSTO MEJÍA OSORIO

JORGE IVÁN MOSQUERA PALACIOS

Propuesta Proyecto de Grado para optar por el título:
Especialista en Seguridad Informática

Asesor de proyecto: SALOMON GONZÁLEZ GARCÍA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SANTIAGO DE CALI, MEDELLÍN.
2017

Nota de Aceptación

_____
_____
_____
_____
_____
_____
_____
_____
_____

_____
Firma del Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Santiago de Cali, 21 de Septiembre de 2017

TABLA DE CONTENIDO

Pág.

INTRODUCCIÓN 9
1.DESCRIPCIÓN DEL PROBLEMA 11
1.1FORMULACIÓN DEL PROBLEMA 12
2.JUSTIFICACIÓN 13
3.OBJETIVOS 14
3.1.OBJETIVO GENERAL 14
3.2.OBJETIVOS ESPECIFICOS 14
4.MARCO REFERENCIAL 15
4.1.MARCO TEÓRICO 15
4.2.MARCO CONCEPTUAL 20
5.METODOLOGÍA DE INVESTIGACIÓN 22
5.1.TIPO DE ESTUDIO. 22
5.2.NIVEL DE MEDICIÓN Y ANÁLISIS DE LA INFORMACIÓN 23
5.3.FUENTES PRIMARIAS 23
5.4.FASES DE LA METODOLOGÍA 24
6.CRONOGRAMA DE ACTIVIDADES 25
DESARROLLO DEL PROYECTO 26
BIBLIOGRAFÍA Y REFERENCIAS 72
ANEXOS 77

LISTA DE TABLAS

Pág.

Tabla 1. Versiones Asterisk. 16
Tabla 2. Cronograma de actividades 2 25
Tabla 3. Codecs de voz utilizados en Asterisk. 27
Tabla 4. Tasas de procesamiento de la voz en Asterisk. 27
Tabla 5. Características Máquina HOST. 43
Tabla 6. Características Red y recursos de conectividad. 43
Tabla 7. Características Software virtualizador. 43
Tabla 8. Características máquinas virtuales. 44
Tabla 9. Fases del Pentesting. 46
Tabla 10. Resultado escaneo Zenmap Banco de Pruebas. 48
Tabla 11. Nmap – escaneo de puertos y servicios. 49
Tabla 12. Puertos abiertos Servidor Asterisk Creamigo Motul. 50
Tabla 13. Inicio de proceso de Escaneo Servidor telefonía IP. 51
Tabla 14. Clasificación de vulnerabilidades OpenVas. 51
Tabla 15. Clasificación de vulnerabilidades Nessus. 55
Tabla 16. Detalles vulnerabilidades en Servidor telefonía IP mediado por Nessus. 57
Tabla 17. Tratamiento de las vulnerabilidades. 59
Tabla 18. Vulnerabilidades Servidor telefonía IP clase Alta y Media OpenVas Vs. Nessus. 60
Tabla 19. Tratamiento de vulnerabilidades de Alto impacto Servidor de telefonía IP. 64

LISTA DE FIGURAS

Pág.

Fig. 1. Entorno de Trabajo en Asterisk. 17
Fig. 2. Arquitectura de Asterisk. 19
Fig. 3. Teléfono IP Cisco Ref. 8800 29
Fig. 4. Teléfono IP Grandstream GXP2140. 30
Fig. 5. Teléfono IP Yealink T48G 30
Fig. 6. Gateway ATA Cisco SPA232D. 31
Fig. 7. Softphone eyeBeam 31
Fig. 8. Sesión web Registro de cuenta SIP en teléfono IP Grandstream. 32
Fig. 9. Registro cuenta SIP Softphone eyeBeam. 33
Fig. 10. Consola de comandos Asterisk. 35
Fig. 11. Interfaz de Bienvenida Sistema Elastix 2.4 Creamigo Motul S.A. 36
Fig. 12. Dashboard – Recursos del Sistema Elastix 37
Fig. 13. Gestión PBX del Sistema Elastix. 37
Fig. 14. Registro de llamadas Elastix 38
Fig. 15. Servidor Asterisk Creamigo Motul S.A. 39
Fig. 16. Información CPU Servidor Asterisk Creamigo Motul S.A. 40
Fig. 17. Información Memoria RAM Servidor Asterisk Creamigo Motul S.A. 41
Fig. 18. Información Software Servidor Asterisk Creamigo Motul S.A. 42
Fig. 19. Diagrama de red Banco de pruebas. 45
Fig. 20. Máquinas Virtuales Banco de Pruebas. 45
Fig. 21. Topología de red Banco de prueba. 47
Fig. 22. Resultados de escaneo Servidor telefonía IP. 52
Fig. 23. Vulnerabilidades clase Alta Servidor telefonía IP. 52
Fig. 24. Configuración Detalles del Escaneo Nessus. 53
Fig. 25. Activación de Plugin básicos para el Escaneo en Nessus. 53
Fig. 26. Configuración de usuario y credenciales para acceso al servicio de escaneo Nessus. 54
Fig. 27. Escaneo completo Servidor telefonía IP con Nessus. 55
Fig. 28. Vulnerabilidades Críticas y Medias en el Servidor de telefonía IP. 56
Fig. 29. Detalles vulnerabilidad crítica en Nessus. 56
Fig. 30. Banner publicitario empresarial Creamigo Motul S.A. 60
Fig. 31. Solución 4 vulnerabilidad ID 5. 69

LISTA DE ANEXOS

Pág.

Anexo A. Solicitud Autorización desarrollo del proyecto. 77
Anexo B. Aceptación solicitud de autorización para el desarrollo del proyecto. 79
Anexo C. Acta de capacitación Telefonía IP Asterisk. 80
Anexo D. Divulgación del proyecto. 82

TÍTULO DEL PROYECTO

Medición de la seguridad de la telefonía IP Asterisk en Creamigo Motul bajo técnicas de Pentesting.

Tema

El tema para investigación sugerido para los trabajos de grado corresponde al Nº 1 Seguridad en Sistemas VOZ/IP.

Área del Conocimiento

Seguridad en Sistemas de Telefonía IP.

INTRODUCCIÓN

Creamigo es una Sociedad Anónima cuya denominación social es COMERCIALIZADORA DE IMPORTADOS LOS AMIGOS S.A. Sigla CREAMIGO S.A, bajo NIT. 800187910 - 2, es una empresa Caleña con 22 Años de tradición y experiencia en el sector automotriz y de autopartes. Inició en 1993, importando repuestos para motores de Gasolina y Diésel.

Desde hace 10 años se solidifica en una alianza estratégica con MOTUL, empresa francesa global que fabrica, desarrolla y distribuye lubricantes para motores (motos, coches y otros vehículos) y para la industria de alto rendimiento desde hace 160 años.

Importando sus lubricantes a los departamentos colombianos del Valle, Cauca, Nariño, Huila, Cauca, Caldas, Risaralda, Quindío, Caquetá y Putumayo. [1]

En la actualidad, la empresa cuenta con un Servidor Gigabyte Thermaltake de 5ta Generación, el cual es el núcleo de las comunicaciones VozIP, este brinda los servicios de telefonía IP mediado por Asterisk sobre plataforma operativa Linux Centos 5.6, cuenta con un total de 33 usuarios tanto locales como remotos y 5 troncales digitales para el procesamiento de las llamadas a la red PSTN a distancia Local, Nacional, Celular e Internacional. En el mismo, opera la sede Principal ubicada en la ciudad de Santiago de Cali, como también de las sucursales ubicadas en la misma ciudad como también en Yumbo, Neiva y Pasto.

El planteamiento de la propuesta de Proyecto de Grado, surge de la necesidad de poner en práctica los conocimientos aprendidos hasta el momento relacionándolos con las experiencias vividas donde el propósito es solucionar y/o mitigar problemas del entorno en cuanto a aspectos de la seguridad informática se refiere.

El impulso a seleccionar el proyecto de grado como tipo aplicado, radica en la aplicación de conocimientos y prácticas que contribuyan en la solución de problemas focalizados en una organización; Creamigo Motul S.A. es la organización

[1] http://www.creamigo.com/creamigo-es

que dio viabilidad en la gestión y desarrollo de esta propuesta, permitiendo iniciar con un esquema de trabajo, la cual se focaliza en el sistema de telefonía IP - Asterisk, tema que es de gran interés por parte de los autores, el proceso del levantamiento de la información, identificación de problemas y demás aspectos que se relacionan directamente con el sistema en mención.

Finalmente en la estructuración de esta idea de proyecto se logra entender y comprender a partir de la problemática planteada el objetivo del mismo con el fin de satisfacer las dos partes, por un lado y principalmente la empresa previamente mencionada, puesto que se solventará en aspectos que a seguridad informática se refiere y están ligados al sistema de telefonía IP - Asterisk y por el otro lado los autores de la propuesta de proyecto puesto que podrán afianzar sus conocimientos en la aplicación de los mismos obtenidos en el desarrollo de la especialización.

1. DESCRIPCIÓN DEL PROBLEMA

En el momento de la presente investigación CREAMIGO MOTUL S.A no cuenta con una estructura de seguridad informática que proteja ante fraudes o posibles ataques al servidor de telefonía IP Asterisk, hecho que es riesgoso a nivel de seguridad informática, debido que no cuenta con un sistema de seguridad a nivel lógico, que garantice la estabilidad e integridad del servicio de telefonía IP.

En la actualidad no es indiferente saber acerca de los múltiples riesgos que se corren con servicios telemáticos, y ante un servidor de Voz sobre IP no hay excepción; a mediados del año 2016 el servidor Asterisk de la empresa Creamigo Motul S.A. debido a una falla de seguridad por mala configuración en el servicio de Apache, permitió el acceso al servidor de terceros no autorizados, dándoles facultad de poder secuestrar troncales telefónicas, modificar archivos de contextos de configuración del Asterisk y con ello generar miles de llamadas a destinos internacionales, todo a causa de medidas de seguridad mal configuradas o inexistentes, como consecuencia, la empresa se ha visto en la actualidad a aislar de la red pública el servidor de telefonía, imposibilitando la comunicación directa con las demás sedes. Por tal razón es de vital importancia contar con mecanismos y políticas que garanticen la integridad de Información de la organización.

Dicho lo anterior es primordial que la empresa Creamigo Motul S.A. permita evaluar la seguridad informática tanto en aspectos hardware como software del Servidor de Telefonía IP – Asterisk, mediante la práctica de Penetration Testing para determinar la efectividad de las medidas que posiblemente en la actualidad este tenga implementadas y de la misma manera identificar vulnerabilidades y/o fallos de seguridad que pongan en riesgo la información de la empresa, proceso que permitirá establecer nuevos métodos y políticas de seguridad a partir de los resultados obtenidos y contar con mecanismos de detección, identificación y defensa que permitan minimizar los riesgos ante posibles ataques o amenazas a los que se expone la empresa con su servidor de telefonía IP.

1.1 FORMULACIÓN DEL PROBLEMA

¿Cuáles son las herramientas lógicas de seguridad informática garantes de la integridad de la información del servidor de telefonía IP-Asterisk de Creamigo Motul S.A. y de su protección ante posibles ataques informáticos?

2. JUSTIFICACIÓN

Creamigo Motul S.A. es una empresa líder en el sector de lubricantes para motores de vehículos de carga pesada y liviana, este se encarga de la comercialización a distribuidores en los departamentos del Valle, Cauca, Nariño, Huila, Cauca, Caldas, Risaralda, Quindío, Caquetá y Putumayo. El equipo comercial de ventas mantiene una fuerte y estrecha relación con los proveedores y clientes, por tal motivo hacen uso permanente de las comunicaciones que la empresa les brinda, de la misma manera el departamento Administrativo, Cartera, Operativo y Recurso Humano dependen circunstancialmente del servicio de telefonía IP. La empresa en el año 2013 adquirió la mejora del servicio, pasando de la tradicional a la telefonía Voz IP se reflejaron los beneficios en un 50%, como por ejemplo, en la reducción de los costes de la facturación telefónica local. Ante este gran avance, la empresa no tuvo en cuenta los contra que está tecnología trae consigo misma, como por ejemplo, los posibles riesgos o vulnerabilidades informáticas a los que se expone este servicio dejando en evidencia que el proveedor y/o integrador de servicio no tenía conocimiento muy completo sobre las medidas de seguridad en Asterisk o de otro modo no se las exigió o recomendó a la empresa contratante.

Por lo mencionado previamente se hace necesario la ejecución de dicho proyecto para garantizar el servicio de la telefonía IP, puesto que el mismo no se encuentra exento de posibles fallas por la acción de un ataque o amenaza digital, por tal razón y teniendo en cuenta el CONPES 3854 enfocado especialmente en “La Política Nacional De Seguridad Digital” donde se refleja que existe una gran preocupación de la rama Ejecutiva, al reunir al Ministerio de Tecnologías de la información y las comunicaciones (MINTIC), Ministerio de Defensa Nacional, Dirección Nacional de Inteligencia y Departamento Nacional de Planeación, enfocados en la ciber seguridad y los continuos ataques informáticos perpetrados que se han ocasionado a diferentes plataformas operativas, entre ellas servidores con Sistema Operativo Linux, donde corre la plataforma de telefonía IP Asterisk de la empresa en mención y de la misma manera desconociendo el impacto que un ataque pueda provocar en el servidor de Telefonía IP – Asterisk, como justificación se planea la realización de prácticas de Penetration Testing con el fin de analizar, diagnosticar y determinar las pautas de seguridad con el cual el servidor cuenta, con ello una vez se obtengan resultados, se pretende formular un esquema completo de seguridad informática al departamento de sistemas de la compañía para que se ejecute y logren minimizar posibles causales de ataques informáticos.

3. OBJETIVOS

3.1. OBJETIVO GENERAL

- Identificar los mecanismos apropiados de seguridad informática garantes de la integridad de la información y del servidor de telefonía IP-Asterisk de Creamigo Motul S.A. protegiéndolo ante posibles amenazas informáticas.

3.2. OBJETIVOS ESPECIFICOS

- Explicar la funcionalidad y aspectos relacionados con la Telefonía IP mediado por Asterisk.

- Examinar las posibles amenazas informáticas a las que está expuesto el servidor de telefonía IP Asterisk de la empresa Creamigo Motul S.A.

- Determinar las herramientas de Pentesting idóneas para minimizar los riesgos de seguridad a los que se expone el servidor de telefonía IP de la empresa Creamigo Motul S.A.

4. MARCO REFERENCIAL

4.1. MARCO TEÓRICO

Asterisk es una aplicación de funcionalidad destinada a la gestión de PBX sobre protocolo IP, presentada inicialmente como proyecto desarrollado por Mark Spencer el cual era estudiante de ingeniería informática en la Universidad de Auburn, Alabama. En el año 1999 Mark creó la empresa "Linux Support Services" empresa que se caracterizó por brindar soporte a usuarios con plataforma operativa Linux.

Con el paso del tiempo el soporte a S.O. Linux tomó fuerza por lo cual Mark se vio en la necesidad de construir una Central Telefónica con una computadora económica para brindar un mejor servicio a sus clientes, fue entonces cuando nació Asterisk como proyecto desarrollado en lenguaje C y con ello se iniciaron desarrollos de software por parte de terceros y demás desarrollos que se iban integrando a Asterisk para hacer una mejor y completa herramienta.

El principal servicio de los diferentes proveedores de Voz sobre IP es el de hacer de pasarela hacia la red telefónica pública a costes muy reducidos. [2] Con el tiempo, en el año 2002, Linux Support Services se convierte en Digium, puesto que se observa que había más demanda en soporte y desarrollo sobre Asterisk que sobre la misma plataforma operativa Linux con el cual se inició como objetivo inicial.

Asterisk es un software de código abierto que funciona bajo Licenciamiento GPL, por esta gran razón el auge que ha tenido a nivel mundial, puesto que esta gran característica permite que cientos de desarrolladores logren diseñar e implementar aplicaciones que se acoplan e interactúan de una manera óptima con Asterisk.

La primera versión estable de Asterisk surge en el año 2004, desde allí surgen una serie de versiones que van implementando mejoras en cuanto a la extensión de las funcionalidades en el ámbito de operar como Central Telefónica, de la misma manera mejoras en aspectos de seguridad, autenticación de los usuarios en sus diferentes tecnologías (SIP, IAX, H.323) como también compactibilidad con los dispositivos que diseñan los grandes proveedores de telefonía IP.

A continuación se relacionan las versiones de Asterisk que se han desarrollado con sus respectivas fechas:

[2] http://bytecoders.net/content/historia-de-asterisk-pbx.html

Tabla 1. Versiones Asterisk.

N°	Versión	Tipo	Fecha de Lanzamiento	Fecha Actualización de Seguridad	Fecha de Finalización
1	1.2.X		2005/11/21	2007/08/07	2010/11/21
2	1.4.X	LTS	2006/12/23	2011/04/21	2012/04/21
3	1.6.0.X	Standard	2008/10/01	2010/05/01	2010/10/01
4	1.6.1.X	Standard	2009/04/27	2010/05/01	2011/04/27
5	1.6.2.X	Standard	2009/12/18	2011/04/21	2012/04/21
6	1.8.X	LTS	2010/10/21	2011/10/21	2015/10/21
7	10.X	Standard	2011/12/15	2012/12/15	2013/12/15
8	11.X	LTS	2012/10/25	2016/10/25	2017/10/25
9	12.X	Standard	2013/12/20	2014/12/20	2015/12/20
10	13.X	LTS	2014/10/24	2020/10/24	2021/10/24
11	14.X	Standard	2016/09/26	2017/09/26	2018/09/26
12	15.X	Standard	2017/10/03	2018/10/03	2019/10/03

Fuente: Wiki Asterisk.org

Disponible en: https://wiki.asterisk.org/wiki/display/AST/Asterisk+Versions

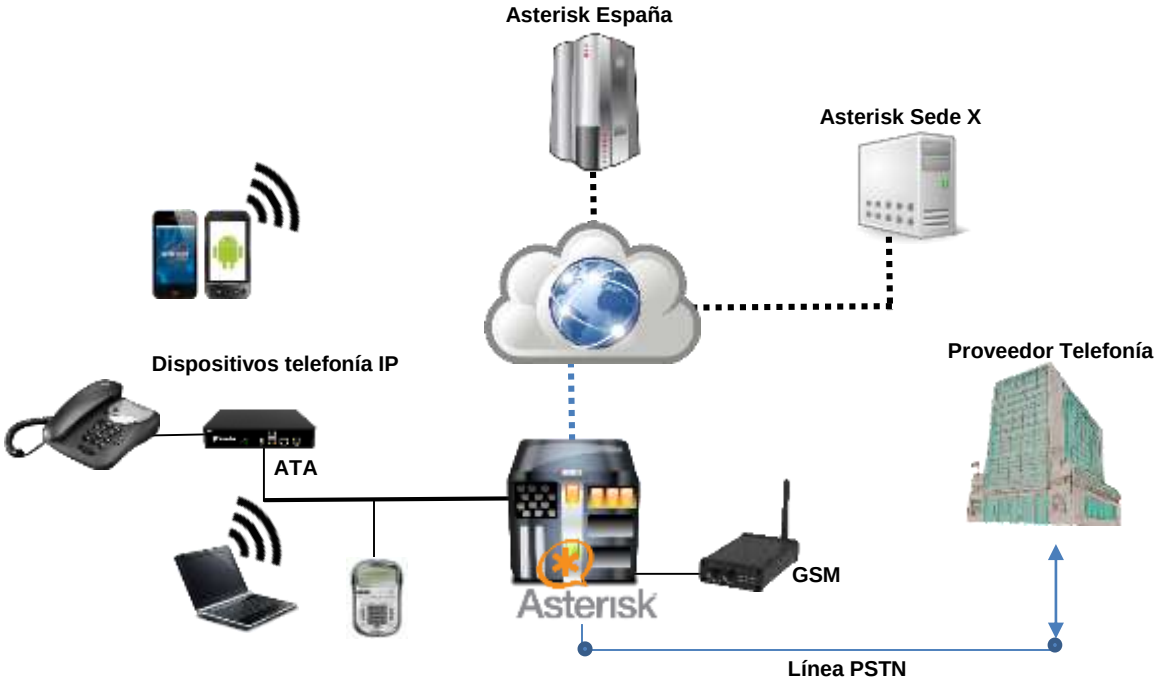
Una PBX (Private Branch eXchage) o Centralita Privada es un servicio ofrecido por proveedores de telefonía, es cual consiste en la administración de las llamadas entrantes y salientes según la cantidad de líneas físicas con el cual cuente el cliente, estas líneas telefónicas son relacionadas directamente a un único numero público el cual recibe las llamadas. En los principios era necesario hacer conexión de cables para lograr establecer comunicación, a este sistema se le conoce como PMBX, Centralita Privada Manual, con el tiempo este dispositivo fue reemplazado por PABX, Centralita Privada Automática, la cual se caracterizaba por gestionar funciones limitadas mediante componentes electrónicos de manera automática.

Una PBX permite la integración de varios teléfonos dentro de un espacio físico permitiendo la comunicación interna entre los usuarios sin necesidad de realizar llamadas hacía la red pública, además este servicio permite la recepción de muchas líneas telefónicas para gestionarlas en operaciones de llamadas entrantes y salientes, estas últimas se generan marcando un número de selección del canal y posteriormente el número telefónico de destino. El gran limitante de las PBX convencionales, es que vienen con funciones predeterminadas y el rango de

expansión entre la interconexión de otras PBX y nuevos dispositivos tiene un límite definido.

Estas, al igual que Asterisk, tienen funciones especiales para realizar en función a las llamadas, incluso funciones exclusivas para un usuario como tal, muchas de estas PBX cuentan con funcionalidades que de manera básica no trae Asterisk, sin embargo la gran ventaja, es que al ser Asterisk un software de código libre, permite el acople de cualquier funcionalidad que sea desarrollada.

Fig. 1. Entorno de Trabajo en Asterisk.



Fuente: El Autor

La Arquitectura con la cual ha sido desarrollada Asterisk permite exclusivamente flexibilidad, definiéndolo como núcleo interno de las comunicaciones y operando de manera eficiente con un conjunto de API´s. Lo fascinante de Asterisk es que permite hacer uso de distintos protocolos, diferentes codecs y cualquier interfaz de hardware o tecnología relacionada con la telefonía IP. Este núcleo administra unas herramientas internamente:

1. **La conmutación de la PBX**; es la tarea ideal de Asterisk puesto que conecta las llamadas entre los usuarios, tanto entrantes como salientes y de la misma manera gestiona las distintas tareas que se pueden realizar con éstas (grabación, transferencias, captura, monitoreo, etc.) de una manera transparente, rápida, efectiva y lo mejor sin importar que tipo de interfaz hardware o tecnología se utilice.

2. **La intencionalidad de operación**; es la gestión de tareas que Asterisk realiza a bajo nivel, permitiendo la ejecución de esta de una manera óptima sin consumir muchos recursos del hardware donde éste interactúe.

3. **La traducción de códecs**; Asterisk es el encargado de utilizar diferentes módulos para codificar o decodificar los distintos formatos de compresión de audio que se puedan utilizar en una llamada bajo protocolo IP, esto con el único objetivo de obtener la máxima calidad de audio haciendo uso de una ancho de banda adecuado.

4. **Lanzamiento de aplicaciones**; se encarga de ejecutar servicios de aplicaciones según se requieran previo a una serie de configuraciones realizadas por el usuario, tales como: música en espera, voz email, transferencias, parqueadero de llamadas, mensaje de bienvenida, condiciones de tiempo o IVR.

Las herramientas que se definen en la arquitectura de Asterisk como núcleo interno de la conmutación de una PBX y se describieron previamente, también se les conoce como módulos API – Interfaz de Programación de Aplicaciones los cuales se identifican y se relacionan respectivamente de la siguiente manera:

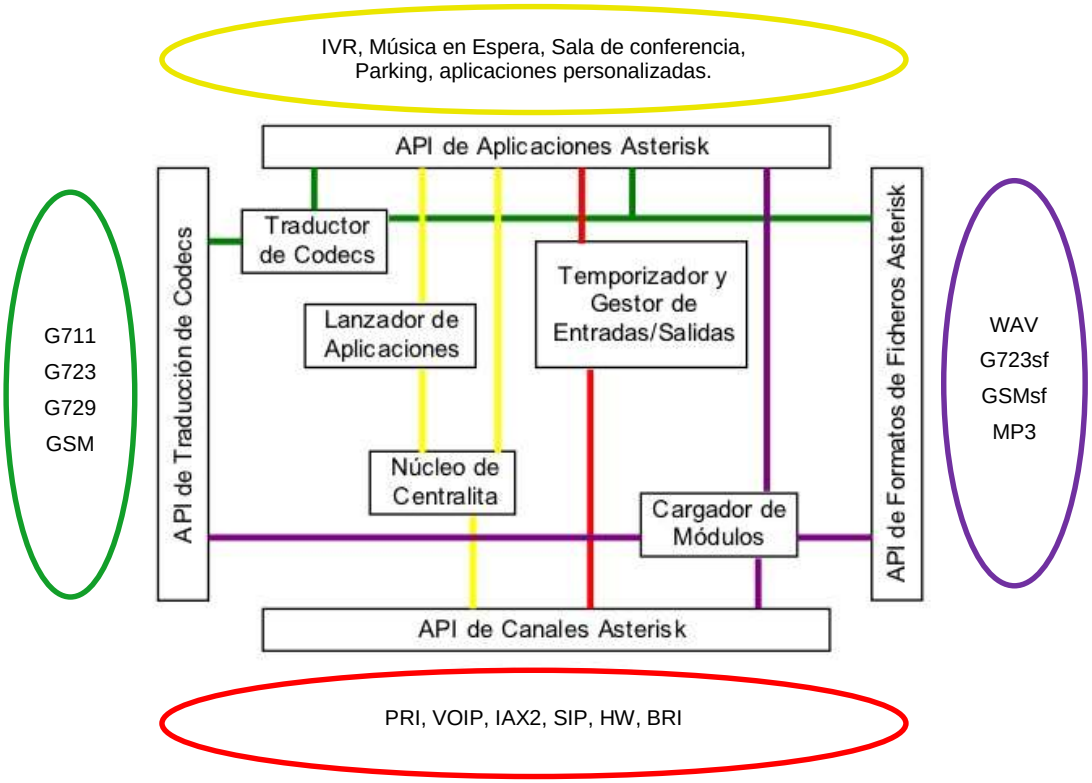
1. **API de canal (Channel API)**, la encargada de manejar el tipo de conexión que se realiza en una llamada entrante sin importar el tipo de conexión o tecnología que se utilice.

2. **API de formato de ficheros (File format API)**, es la encargada de administrar la lectura y escritura de los datos que se almacenan.

3. **API de traducción de códecs (Códec translator API)**, es la encargada de realizar la traducción o interacción entre los códecs, decodificando en diferentes formatos de audio, tales como: WAV, ULaw, GSM hasta MP3.

4. **API de aplicación (Aplication API)**, es la encargada de permitir la ejecución de varias aplicaciones para llevar a cabo diversas funciones.

Fig. 2. Arquitectura de Asterisk.



Fuente: El Autor

Es así como en la actualidad, la telefonía IP ha desplazado casi en su totalidad a la telefonía convencional, permitiendo comunicación de alta calidad sin medir distancias y llegando a solventar cualquier necesidad imaginable por un usuario u empresa.

4.2. MARCO CONCEPTUAL

TRONCALES: Son el medio que permiten comunicar a la PBX-IP Asterisk-Elastix con el mundo exterior o PSTN, son los canales de comunicación de entrada y salida de llamadas, también permiten la comunicación hacia otras PBX, tradicionales, IP o servidores virtualizados.[3]

CODEC: Es la forma de digitalizar la voz humana para ser enviada por las redes de datos. Algunos ejemplos: G.711, G.729, GSM, iLBC, Speex, G.723. Los códec se utilizan para transformar la señal de voz analógica en una versión digital.[4]

PROTOCOLO: Es el 'lenguaje' que se utiliza para negociar y establecer las comunicaciones de voz sobre IP. Los más importantes: SIP, H323, IAX2, MGCP. [5]

INTEGRIDAD: La integridad intenta que los datos almacenados por un usuario no sufran ninguna alteración sin su consentimiento. (Buendía, 2013)

Certificando que tanto la información como sus métodos de proceso son exactos y completos. (Gascó, Serrano, Ramada, & Pérez, 2013)

CONFIDENCIALIDAD: Cualidad de un mensaje, comunicación o datos, para que solo se entiendan de manera comprensible o sean leídos, por la persona o sistema que esté autorizado. Comprende por tanto la privacidad o protección de dicho mensaje y datos que contiene. (Santos, 2011).

DISPONIBILIDAD: La disponibilidad del sistema informático también es una cuestión de especial importancia para garantizar el cumplimiento de sus objetivos, ya que se debe diseñar un sistema lo suficientemente robusto frente a ataques e interferencias como para garantizar su correcto funcionamiento, de manera que pueda estar permanentemente a disposición de los usuarios que deseen acceder a sus servicios. (Vieites, 2014)

VULNERABILIDAD: Una vulnerabilidad es un defecto de una aplicación que puede ser aprovechado por un atacante. Si lo descubre, el atacante programará un software (llamado malware) que utiliza esa vulnerabilidad para tomar el control de la máquina (xploit) o realizar cualquier operación no autorizada. (Buendía, 2013)

---

[3] http://elastixtech.com/troncales-y-rutas-en-elastix/

[4] https://es.slideshare.net/edgarjgonzalezg/curso-asterisk-voz-ip-1introduccionsip

[5] https://es.slideshare.net/edgarjgonzalezg/curso-asterisk-voz-ip-1introduccionsip

AMENAZA: Una amenaza es cualquier entidad o circunstancia que atente contra el buen funcionamiento de un sistema informático. Aunque hay amenazas que afectan a los sistemas de forma involuntaria, como, por ejemplo, un desastre natural, en la mayoría de casos es necesaria una intención de producir daño. (Gascó, Serrano, Ramada, & Pérez, 2013)

PENETRATION TEST: Es una prueba de penetración o una subclase de piratería ética que comprende un conjunto de métodos y procedimientos. El objetivo es probar y proteger la seguridad de una organización. Las pruebas de penetración resultan útiles para encontrar vulnerabilidades en una organización y comprobar si un atacante podría explotar dichas vulnerabilidades para obtener acceso no autorizado a un activo.[6]

ATAQUE: Un ataque es una acción que trata de aprovechar una vulnerabilidad de un sistema informático para provocar un impacto sobre él e incluso tomar el control del mismo. (Gascó, Serrano, Ramada, & Pérez, 2013)

PROTOCOLO SIP: Es un protocolo de señalización de capa de aplicación que usa el puerto bien conocido 5060 para la comunicación. SIP puede ser transportado con los protocolos de capa de transporte ya sea UDP o TCP**.** (Pérez, 2014)

SOFTPHONE: Es un software que hace una simulación de teléfono convencional por computadora. Es decir, permite usar la computadora para hacer llamadas a otros softphones o a otros teléfonos convencionales. (Monografía, diseño de un sistema de voz sobre IP (VozIP) para la empresa Sedenti Ltda, Efraín Ortiz Díaz y William Guillén Chalen). [7]

[6] http://genesis-hs.ru/docs/etnihakipenitra.pdf
[7] http://biblioteca.unitecnologica.edu.co/notas/tesis/0062296.pdf

5. METODOLOGÍA DE INVESTIGACIÓN

Para la ejecución de este proyecto se llevará a cabo el **método inductivo**, teniendo en cuenta cuatro pasos esenciales que son: la clasificación y el estudio de estos hechos; la derivación inductiva que parte de los hechos y permite llegar a una generalización; y la contrastación.

Es un proceso analítico, que parte del estudio del caso y los hechos o eventos que se generan para llegar a lo que se propone como idea principal o finalidad de una ley o principio general. Se utiliza este método puesto que, con las visitas personales al sitio, la creación del escenario de pruebas, las fases de experimentación, comparaciones que permiten conocer los problemas que se presentan en el servidor de telefonía IP – Asterisk de la empresa CREAMIGO MOTUL S.A.

5.1. TIPO DE ESTUDIO.

El presente proyecto se considera de estudio **exploratorio** y **descriptivo** ya que describe lo que es la seguridad informática y los principales riesgos que tiene la carencia de la misma, detalla la situación en un contexto Internacional, Nacional y Empresarial, así como se ubica al objeto de estudio en toda la problemática presentada. No obstante es válido afirmar que su enfoque también ha sido **explicativo;** porque no solo describe hechos, sino que determinan las causas de los fenómenos generando sentido de entendimiento, al igual que soluciones, y sus **fuentes** han sido primarias y de investigación participativa, ya que el estudio está basado en **trabajo de campo**, donde el fenómeno se da realmente, con la intención de ejecutar pruebas de acceso a la información del sistema, para lograr encontrar los mecanismos necesarios que garanticen la seguridad del servidor de telefonía IP-Asterisk de CREAMIGO MOTUL S.A. protegiéndolo ante posibles amenazas informáticas.

5.2. NIVEL DE MEDICIÓN Y ANÁLISIS DE LA INFORMACIÓN

Las herramientas de PENTESTING son los instrumentos de medición que se han elegido para este proyecto investigativo, los cuales reúnen los requisitos esenciales de un instrumento de medición que son:

- **Confiabilidad:** Es el grado de la aplicación de diversos procesos sobre un producto obteniendo en cada aplicación el mismo resultado.

- **Validez:** Valor en el que un instrumento de medición pretende medir una variable.

- **Intervención:** Uso de herramientas informáticas de seguridad, escaneo de puertos, filtrado de paquetes en tráfico de red, administración de consolas operativas y cifrado y descifrado de contraseñas.

5.3. FUENTES PRIMARIAS

- ESCRIVÁ GASCÓ, Gema. ROMERO SERRANO, Rosa Mª. RAMADA, David Jorge. ONRUBIA PÉREZ, Ramón. (2013), Seguridad Informática, GRUPO MACMILLAN, Madrid España.

- COSTAS SANTOS, Jesús. (2011), Seguridad y Alta Disponibilidad, RA-MA, S.A. Editorial y Publicaciones, Madrid España.

- GÓMEZ VIEITES, Álvaro. (2014), Seguridad en Equipos Informáticos, RA-MA, S.A. Editorial y Publicaciones, Madrid España.

- ROA, José Fabián. (2013), Seguridad Informática, McGraw-Hill / Interamericana de España, S. L.

- THERMOS, Peter. TAKANEN, Ari (2008), Securing VoIP Networks: Threats, Vulnerabilities, and Countermeasures.

5.4. FASES DE LA METODOLOGÍA

- Fase 1: Diagnóstico.
- Fase 2: Aplicación de técnicas de recolección de datos.
- Fase 3: Socialización de funcionalidad telefónica IP.
- Fase 4: Análisis de la información.
- Fase 5: Examinar amenazas informáticas.
- Fase 6: Aplicación de herramientas para minimizar el riesgo.
- Fase 7: Presentación de informe.

6. CRONOGRAMA DE ACTIVIDADES

Fecha de Inicio: 24 de agosto de 2017. (Semana 1).

Tabla 2. Cronograma de actividades 2

ACTIVIDAD	FASE 1 24 AGO 6 SEP	FASE 2 7 SEP 4 OCT	FASE 3 5 OCT 29 NOV	FASE 4 30 NOV 10 DIC
Consolidación y presentación final de la propuesta de trabajo de Grado.	X			
Creación de imagen del Servidor de Telefonía IP Asterisk de la Empresa Creamigo Motul S.A.	X			
Explicar la funcionalidad y aspectos relacionados con la Telefonía IP mediado por Asterisk.		X		
Realizar capacitación acerca de la funcionalidad de Asterisk como sistema de telefonía IP al personal administrativo y usuarios del Sistema de Telefonía Asterisk de la empresa Creamigo Motul S.A.		X		
Implementación del banco de trabajo virtual para el desarrollo de las pruebas de Pentesting.		X	X	
Examinar las posibles amenazas informáticas a las que está expuesto el servidor de telefonía IP Asterisk de la empresa Creamigo Motul S.A.			X	
Realizar un informe detallado de las posibles fallas, vulnerabilidades y amenazas a las que se expone un servidor de telefonía IP basado en Asterisk.			X	
Determinar las herramientas de Pentesting idóneas para minimizar los riesgos de seguridad a los que se expone el servidor de telefonía IP de la empresa Creamigo Motul S.A.			X	
Pruebas de Pentesting para la identificación de vulnerabilidades y amenazas del Servidor de Telefonía IP Asterisk de la empresa Creamigo Motul S.A.			X	
Análisis de los resultados obtenidos posterior a los procesos de Pentesting realizados al Servidor de Telefonía IP Asterisk de la empresa Creamigo Motul S.A.			X	X
Conclusiones y recomendaciones.				X
Crear y presentar un informe técnico y gerencial al Jefe Administrativo de la empresa Creamigo Motul S.A. sobre todo el proceso realizado, los resultados obtenidos y las recomendaciones de seguridad propuestas para minimizar los riesgos encontrados en el Servidor de Telefonía IP Asterisk.				X

Fuente: El Autor

DESARROLLO DEL PROYECTO

1. ¿Qué es Asterisk y cómo funciona?

Asterisk es un software diseñado para administrar funciones telefónicas, este es el núcleo utilizado en plataformas operativas Linux, en especial distribuciones CentOS en conceptos de telefonía IP, puesto que proporciona funcionalidades de una centralita telefónica permitiendo la conexión de teléfonos IP y convencionales, convertidores, proveedores de VoIP, redes RDSI, softphone, entre otros.

Este software se puede instalar en modo consola y modo grafico acompañado de una variedad de herramientas que hacen de Asterisk un software muy completo para la gestión de las comunicaciones vía telefónica en cualquier organización sin importar su tamaño. Asterisk es un software de código abierto y es libre (Licencia GNU GPL), lo que permite el diseño y desarrollo de nuevas aplicaciones de comunicaciones utilizando la funcionalidad de su núcleo para operar.

En la actualidad este software es la base de las comunicaciones en millones de empresas a nivel mundial, debido al sin número de ventajas y beneficios que esta otorga a empresas, desarrolladores y clientes. Los requisitos físicos que exige Asterisk son mínimos, teniendo en cuenta factores como el tamaño de la empresa y las aplicaciones que se requieran para administrar de una mejorar manera este software. En la actualidad Asterisk se encuentra en la versión estable 15.1.0.15 de octubre de 2017.

Básicamente Asterisk nos permite de una manera muy simple tener una central telefónica inteligente a muy bajo costo, administrable y con beneficios a gran escala. Cuando se implementa y se integra Asterisk a un servidor Linux y se hace uso de los servicios que el mismo Sistema Operativo ofrece, esto contribuye en los aspectos de seguridad y ergonomía, como por ejemplo, el sistema de seguridad o firewall en Linux mediado por reglas de iptables, al contar con una muy buena configuración de este componente en un sistema Linux, se logra mejorar los aspectos de seguridad de la misma consola de Asterisk.

Asterisk en su forma simple y básica permite la comunicación tradicional entre dos partes sin inconveniente alguno como también permite realizar gestiones de consulta en bases de datos, programación de tareas, como lo es, cobro de cartera, recordatorios de pago, video llamadas, conferencias, envío de mensajes, gestión de campañas telefónicas y diseño de menú inteligentes que permiten el despliegue e interacción con otros sistemas de información.

Teniendo claro lo que Asterisk como software de comunicaciones abiertas, surge una pregunta y es… **¿Cómo funciona Asterisk?** Bien para responder esta pregunta debemos entender que la información que manipula y/o administra Asterisk es la "voz" humana, que es lo que fluye en una llamada, a nivel de informática, la voz viaja por redes de datos, pero en ese proceso de transporte, ésta previamente pasa por un proceso de codificación desde el punto origen y cuando llega al destino se descodifica entregando así el mensaje. Para llevar a cabo este proceso, Asterisk hace uso de una serie de codecs, los cuales hacen posible que la voz humana que se encuentra en estado análogo, se codifique pasando a un estado digital mientras viaja de un lugar a otro y luego vuelva a su estado natural cuando llegue al otro extremo. A continuación presentamos una serie de codecs que utiliza Asterisk para las funciones de codificación y decodificación de la voz en una llamada:

Tabla 3. Codecs de voz utilizados en Asterisk.

NOMBRE	ORGANISMO ESTANDARIZADOR	TIPO DE CODIFICACIÓN	TASA DE BITS	FRECUENCIA DE MUESTREO	MOS
G.711	ITU-T	PCM	64 Kbps	8 KHz	4.1
G.726	ITU-T	ADPCM	32 Kbps	8 KHz	3.85
G.728	ITU-T	CELP	16 Kbps	8 KHz	3.61
G.729A	ITU-T	CELP	8 Kbps	8 KHz	3.9
GSM	ETSI	RPE-LTP	13 Kbps	8 KHz	3.4

Fuente: Sinologic

Disponible en: https://blog.sinologic.net/2015-08/ancho-banda-necesario-hablar-voip.html

Tabla 4. Tasas de procesamiento de la voz en Asterisk.

CÓDEC	ANCHO DE BANDA	INTERVALO DE PAQUETE	BITS DE VOZ POR PAQUETE	PROCESADO
G.711	64 Kbps	20ms	1280 bits	Bajo
G.726	32 Kbps	20ms	640 bits	Medio
G.728	16 Kbps	10ms	160 bits	Alto
G.729A	8 Kbps	20ms	160 bits	Alto
GSM	13 Kbps	20ms	160 bits	Bajo

Fuente: Sinologic

Disponible en: https://blog.sinologic.net/2015-08/ancho-banda-necesario-hablar-voip.html

Las anteriores tablas enlista algunos de los diferentes códecs que son utilizados por Asterisk en las labores de generación de llamadas, estos códecs tienen características especiales como la calidad de la voz que de la misma manera hacen unas exigencias del ancho de banda con el cual se cuente en una red comunicaciones bien sea a nivel local o a nivel de red mundial (Internet), como por ejemplo, una llamada con codecs de comunicación Allaw o Ullaw es decir códec G.711A o G.711U respectivamente tiene mayor calidad y consume más ancho de banda de red que una llamada con códec GSM o el habitual usado G.729A, donde estos últimos hacen un uso de banda de datos más estrecho pero la calidad de la voz no se compara con los codecs inicialmente comparados.

Ahora bien, entendida la parte de la transformación de la voz humana de estado Análogo a Digital mediado por un codificador o códec, surge una segunda pregunta y es… **¿Cómo se lleva a cabo el proceso de registro de los usuarios en Asterisk?** como previamente se mencionó, Asterisk hace uso de una red de datos y se integra como servicio a Sistema Operativo, este software hace uso del protocolo TCP/IP, donde a través de los procesos que maneja este protocolo logra hacer las funciones de telefonía a través de una red de datos, de esta manera se hace referencia al termino de telefonía IP o VoIP (Voz sobre IP). Asterisk además de operar bajo protocolo TCP/IP, utiliza dos protocolos para el registro de los usuarios o canales de comunicaciones en el sistema, estos protocolos los cuales son IAX2, H.323 y SIP, conocidos también como protocolos de señalización.

El protocolo H.323, es el primer protocolo que se recomendó por parte de la ITU (Unión Internacional de Telecomunicación), este protocolo es utilizado para entablar sesiones de comunicación audiovisual haciendo uso de la red, la desventaja se refleja en la calidad y transporte de los datos, puesto que no es muy confiable.

El protocolo de Inicio de Sesión SIP (Session Initiation Protocol), este protocolo es utilizado para el paso de video, datos, voz y mensajería, normalmente utiliza el puerto 5060 para el proceso de registro pero para el transporte de la voz puede hacer uso de puertos que oscilan entre el 10.000 y el 20.000, razón por la cual, este protocolo presenta inconvenientes en muchos casos con los firewall en una red de datos, puesto que estos últimos no logran asimilar la forma de operar de este protocolo, por lo cual se evidencia, que el usuario se registra de manera satisfactoria pero cuando se establece una llamada entre dos partes por medio de una canal, la voz nunca llega a su destino.

El protocolo IAX (Inter-Asterisk Exchange protocol), Protocolo de Intercambio de Asterisk, este protocolo permite la interconexión de dos Asterisk en una red de datos, es utilizado especialmente para evitar inconvenientes con aquellas redes donde hay existencia de un firewall, puesto que este protocolo solo hace uso de un

puerto UPD 4569, lo que permite que todos los paquetes entre los Asterisk conectados viajen por ese solo puerto, haciendo de este, un protocolo mucho más sencillo y fácil de operar, el único inconveniente es que cuando hay muchas llamadas simultaneas se tienen a hacer mucho más uso el ancho de banda. En la actualidad se hace uso de la versión IAX2 la cual tiene características mucho más especiales en cuestión de procesamiento de datos que la anterior versión IAX.

Ahora bien, para lograr el registro en Asterisk, se requiere de una información básica la cual permitirá que se realice la negociación entre el usuario a través de un dispositivo físico o tipo software y el mismo núcleo. Normalmente estos datos corresponde a:

- IP del servidor (Asterisk).
- Usuario
- Contraseña
- Puerto
- Códec
- Protocolo

Los proveedores de telefonía IP a nivel mundial, fabrican dispositivos para operar con plataformas Asterisk haciendo masivo del protocolo SIP debido a las múltiples ventajas que suele otorga por medio de la estructura del mismo protocolo, proveedores tales como GrandStream, Cisco, Avaya, Yealink, Digium, Polycom, GoIP, entre otros. Tambien diseñan gateways ATA, los cuales posibilitan el uso de teléfonos análogos en este tipo de telefonía IP.

Fig. 3. Teléfono IP Cisco Ref. 8800

Fuente: https://www.cisco.com

Fig. 4. Teléfono IP Grandstream GXP2140.

Fuente: http://www.grandstream.com/

Fig. 5. Teléfono IP Yealink T48G

Fuente: http://www.yealink.com/

Fig. 6. Gateway ATA Cisco SPA232D.

Fuente: https://www.cisco.com

Asterisk también permite operar con teléfonos virtuales conocidos como Softphone, entre los más conocidos esta Zoiper, X-lite, Bria y eyeBeam.

Fig. 7. Softphone eyeBeam

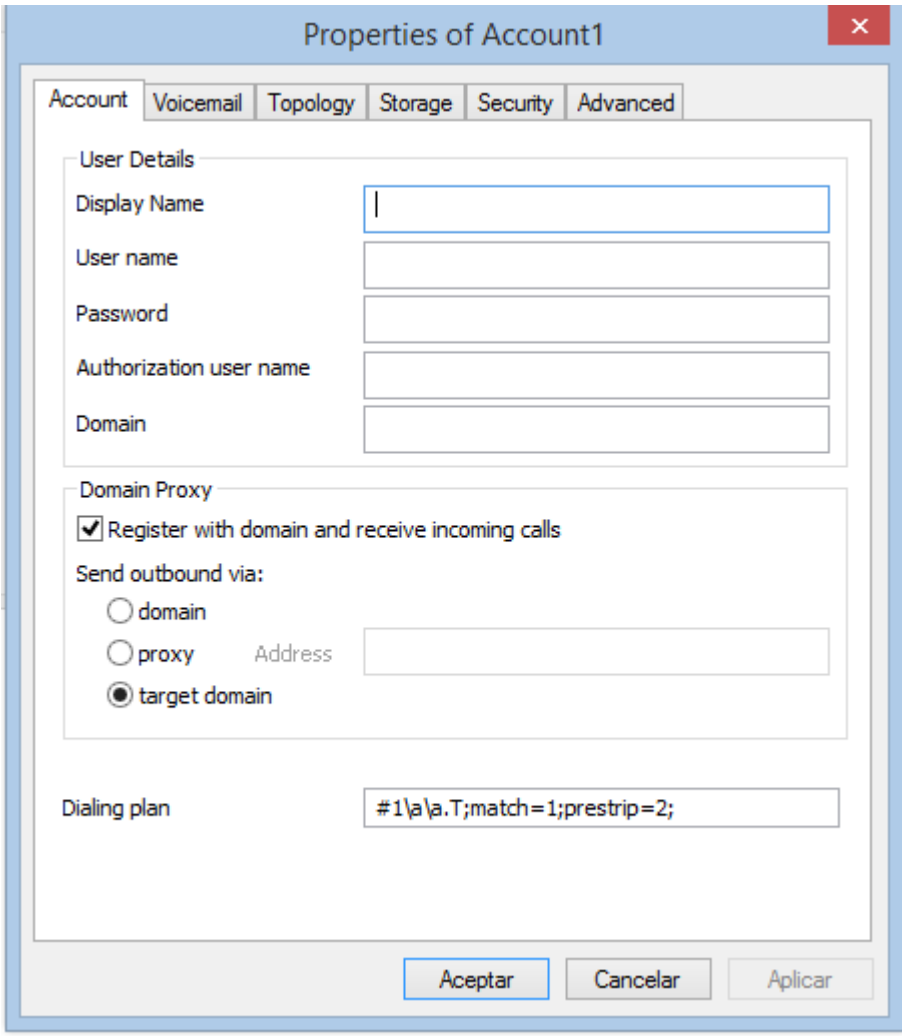
Fuente: www.counterpath.com

Ahora bien echemos un vistazo a la sesión de registro y configuración de un teléfono IP Grandstream y un softphone eyeBeam y Zoiper:

Fig. 8. Sesión web Registro de cuenta SIP en teléfono IP Grandstream.

Fuente: El Autor

Fig. 9. Registro cuenta SIP Softphone eyeBeam.



Fuente: El Autor

Asterisk permite el registro y la configuración de troncales o canales bajo los protocolos de señalización antes mencionados para permitir el acceso de llamadas de la red pública, este se hace mediante recursos físicos y lógicos otorgados por los proveedores de servicio, es decir, en una central Asterisk se pude configurar una planta GSM para generar llamadas a la red celular de una zona o país de la misma manera se pueden agregar líneas telefónicas análogas y digitales para la realización de llamadas desde y hacia la red de telefonía pública conmutada - PSTN, identificando la central IP PBX con números de cabeceras que pueden ser manipulados de diversas maneras, como por ejemplo, al ingresar una llamada

conectarla inmediatamente con un IVR que le permita escoger opciones al llamante o en otros casos puede que al conectar dicha llamada la desvié automáticamente a un destino celular o una derivación de registro SIP ubicada en un espacio geográfico alterno al de la central IP Asterisk, proceso que para el llamante es totalmente transparente.

Entre las ventajas más destacables de Asterisk se encuentra:

1. Operatividad: Asterisk es compactible con diversos dispositivos de diferentes marcas y no solo físicos sino también de nivel software en diversas plataformas operativas.

2. Funcionalidad: Reúne muchas más funciones que las más avanzadas centrales análogas convencionales en la actualidad, permite conferencias, capturas de llamadas, transferencias atendidas y desatendidas, monitoreo en tiempo real, grabación de llamadas detallando origen, destino, canal, duración, fecha, etc., parqueo de llamadas, buzón de voz, voice mail, música de espera, IVR, entre muchas otras funciones que permiten hacer de Asterisk una de las mejores soluciones telefónicas a nivel mundial.

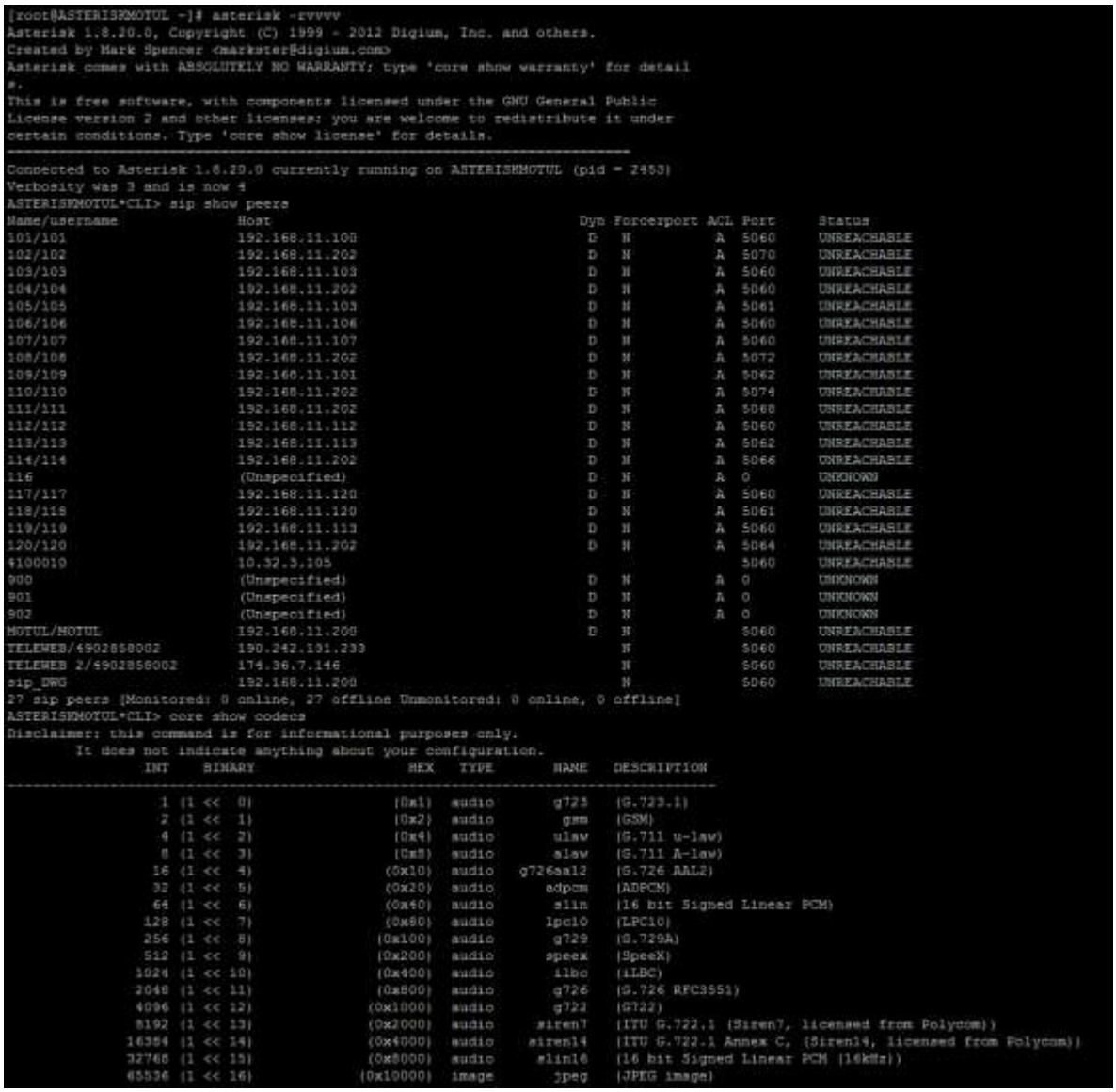
3. Costo: Los costos de Asterisk son bajos, fuera de ser de código abierto, esta utiliza una plataforma servidor lo cual exige solo la compra de interfaces de red para realizar las configuraciones para el registro de usuarios y troncales, las cuales hoy por hoy en el mercado tienen un valor muy económico, en conclusión, se puede resaltar que Asterisk puede hacer uso de hardware genérico, esto abarca desde el equipo donde se desee instalar, bien sea un servidor robusto de marca, hasta un equipo con especificaciones básicas tipo clone.

4. Flexibilidad: Asterisk permite la integración proveedores de telefonía VoIP, telefonía convencional, permite interconexión con planta PBX análogas, interacción con sistemas de monitoreo y vigilancia CCTV y la operatividad con sistemas de información propios de una organización o empresa.

5. Capacidad de Expansión: Asterisk es de fácil expansión tanto en termino lógicos, es decir software como también hardware, debido a que como trabaja sobre protocolo TCP/IP, esta característica posibilita que desde una sola Central Asterisk se interconecten varios dispositivos a nivel local, metropolitano y mundial, eso sí, contar siempre con buena calidad en los recursos de la red de datos.

Por otro lado, en la actualidad muchas compañías hacen uso de Asterisk bajo consola de comandos, donde desde allí operan y configuran todas las funcionalidades de Asterisk, además de observar los procesos y registros que se van generando a medida que se trabaja en ello, para este nivel, se requiere de un personal con conocimientos en Linux y en Asterisk capaz de realizar todo tipo de configuraciones que contribuyan al buen funcionamiento del núcleo. Las siguientes imágenes son de la consola de Asterisk, es decir sin modo gráfico:

Fig. 10. Consola de comandos Asterisk.



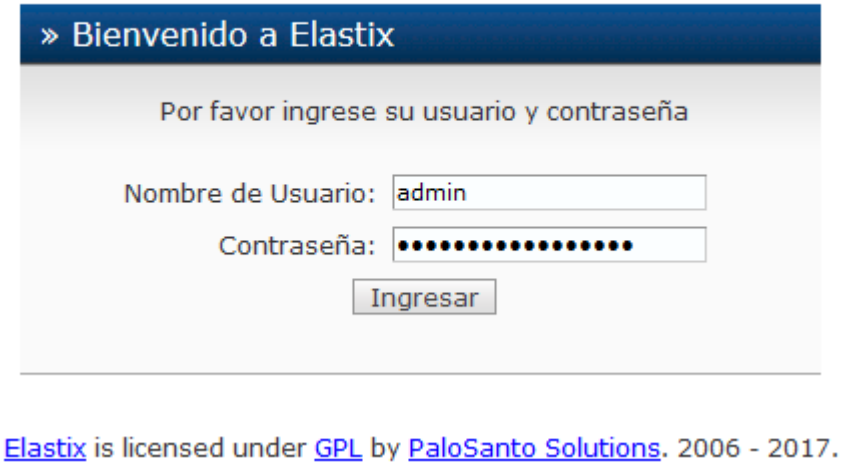
Fuente: El Autor

Como se mencionó al inicio, Asterisk al ser software de código abierto permite que terceros logren desarrollar aplicaciones para operar en conjunto de tal manera que hace mucho más amena la forma de trabajar con Asterisk, para ello, se hace referencia a la interfaz gráfica de usuario Elastix, el cual permite operar todo el núcleo de Asterisk de una manera mucho más amigable desde un entorno totalmente grafico a modo web y multilenguaje.

Elastix es una compilación de scripts diseñados para dar administración al núcleo de las comunicaciones de telefonía IP basado en Asterisk, es totalmente gratis y se resuelve todo mediante acceso web, desde cualquier explorador, Mozilla, IExplorer, Chrome, Safari, etc. Actualmente se encuentra desarrollada y estable la versión 5.0. Este software de código abierto se caracteriza por unificar todas las funciones que reúne un servidor de telefonía PBX IP, Telefonía, Correo Electrónico, Mensajería Instantánea, CRM, Fax, etc.

A continuación se puede apreciar capturas de pantalla de la interfaz de administración Elastix, versión 2.4, la cual es la que tiene implementada la empresa Creamigo Motul S.A.:

Fig. 11. Interfaz de Bienvenida Sistema Elastix 2.4 Creamigo Motul S.A.



Fuente: El Autor

En esta sesión se accede digitando en el explorador web la dirección IP del servidor Asterisk e inmediatamente digitar el nombre de usuario y la contraseña.

Fig. 12. Dashboard – Recursos del Sistema Elastix

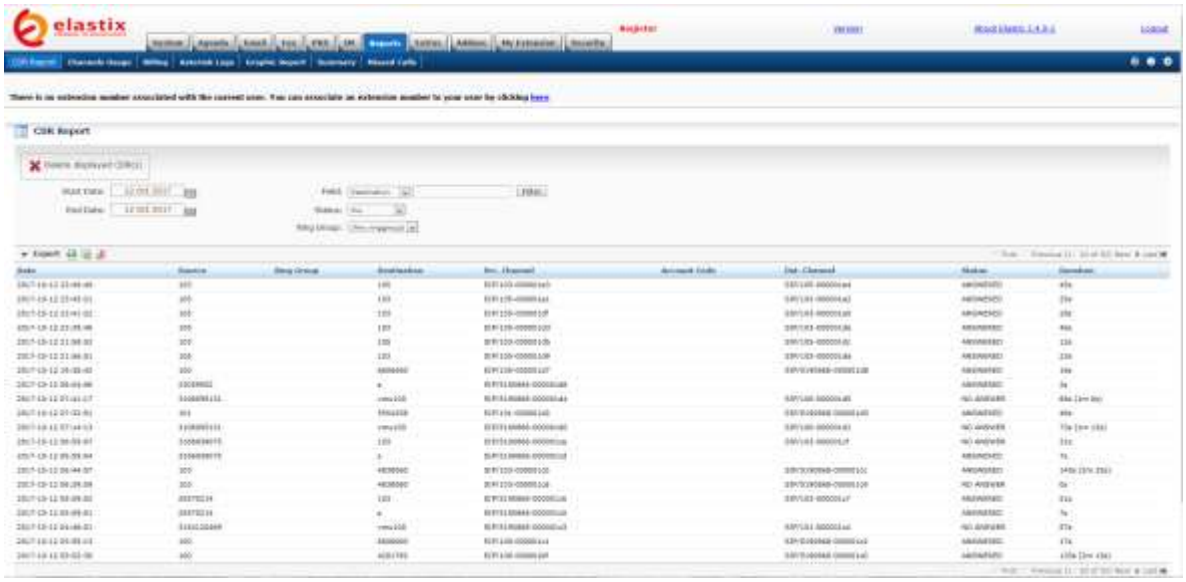
Fuente: El Autor

Esta primera imagen representa el estado de los recursos físicos y registro de actividades del sistema de Telefonía IP Asterisk, en esta sesión se puede apreciar la capacidad en RAM, CPU y disco duro del servidor Asterisk, además de ver los servicios instalados y activos como también registro de actividades relacionadas con el flujo de llamadas en la central PBX-IP.

Fig. 13. Gestión PBX del Sistema Elastix.

Fuente: El Autor

Fig. 14. Registro de llamadas Elastix



Fuente: El Autor

Esta imagen corresponde al registro de llamadas que se originan en Asterisk. Estas pueden ser filtradas por los parámetros de fuente, destino, fecha, canal, conjunto de pines, entre otras y al mismo tiempo exportarlas en formato PDF para presentar un informe o en formato Excel para realizar algún tipo de operación sobre los datos obtenidos.

Estas y muchas otras más funcionalidades y características presenta Elastix como software administrador de Asterisk, es verdaderamente muy útil y permite que un usuario que no tenga conocimientos técnicos en informática logre gestionar la operación y control de la central telefónica IP, desde cualquier lugar del mundo a cualquier hora y desde cualquier dispositivo electrónico con acceso a internet.

Finalmente es bueno resaltar, que Elastix, permite la creación de diversos usuarios con permisos diferentes para realizar administración de la central telefónica.

2. **Examinar las posibles amenazas informáticas a las que está expuesto el servidor de telefonía IP Asterisk de la empresa Creamigo Motul S.A.**

Para el desarrollo de esta fase es muy pertinente citar aspectos físicos y lógicos de la estructura de la empresa Creamigo Motul S.A. relacionados con el servidor de la telefonía IP Asterisk.

A continuación se exponen las características físicas y lógicas del servidor Asterisk que intervienen en el sistema de comunicación telefónica IP.

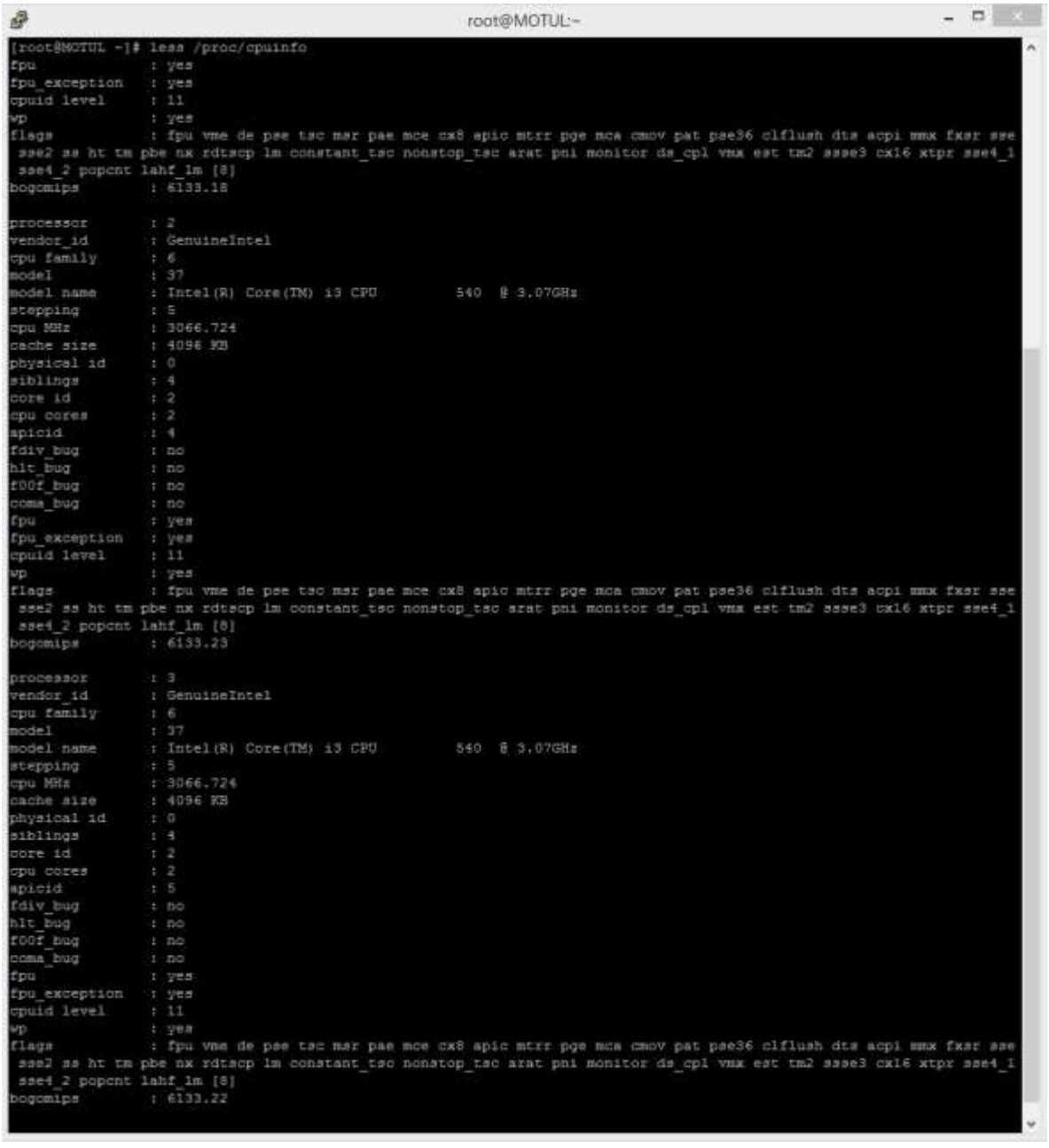
Fig. 15. Servidor Asterisk Creamigo Motul S.A.

Fuente: El Autor.

Las características tipo hardware de este servidor son:

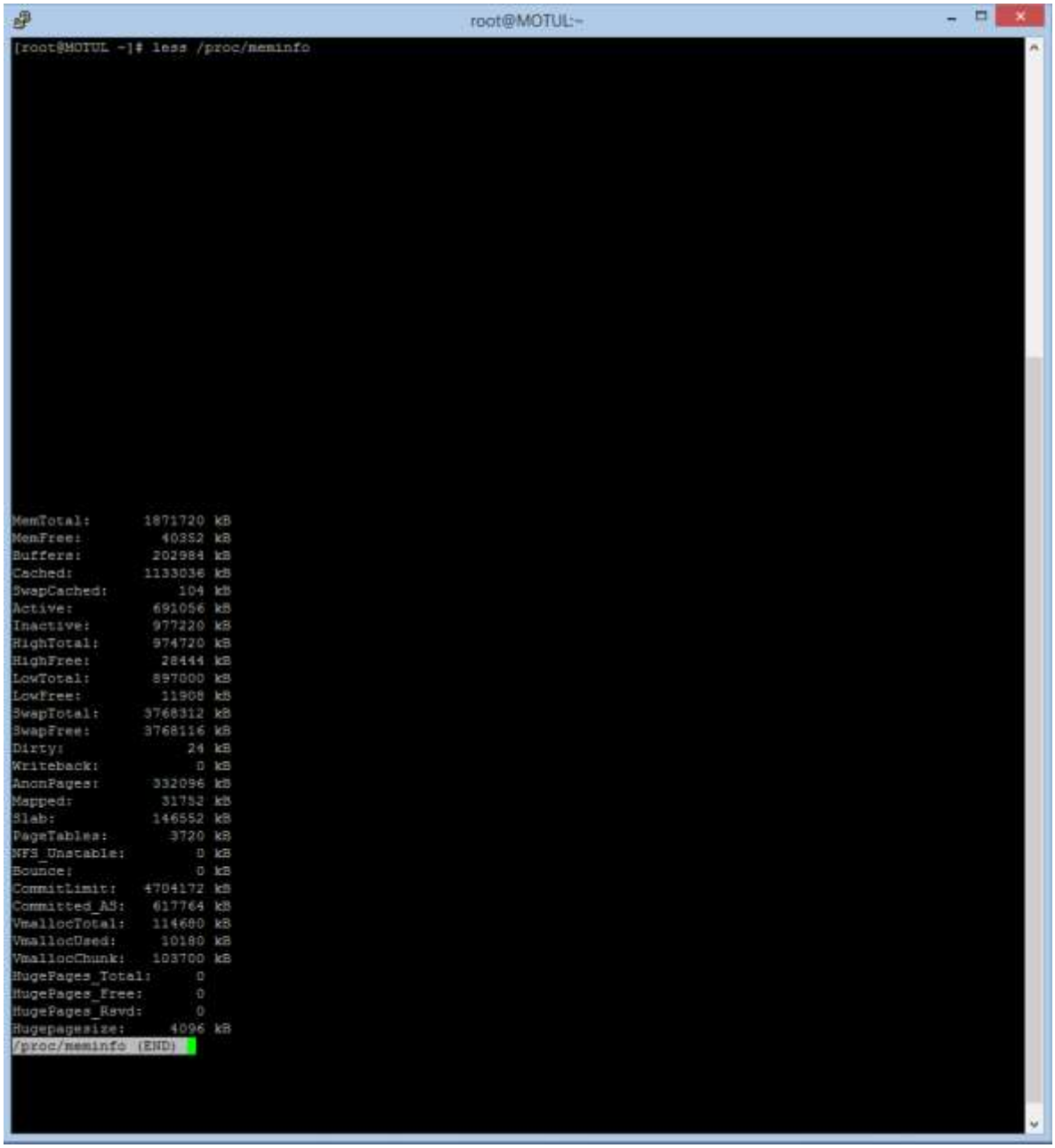
- Servidor tipo Mini Tower para gabinete.
- Marca: Thermaltake A30 VM70001W2Z Black SECC MicroATX.
- CPU Inter ® Core ™ i3 540 @ 3.07 GHz.
- Memoria RAM 4 GB DDRIII x1 modulo.
- 3 Intefaces de red PCI base 1000 Mbps.
- HDD Hitachi HDS7210 500GB SATA 7200 RPM.
- Sistema de ventilación y refrigeración iCooler TT.

Fig. 16. Información CPU Servidor Asterisk Creamigo Motul S.A.



Fuente: El Autor.

Fig. 17. Información Memoria RAM Servidor Asterisk Creamigo Motul S.A.

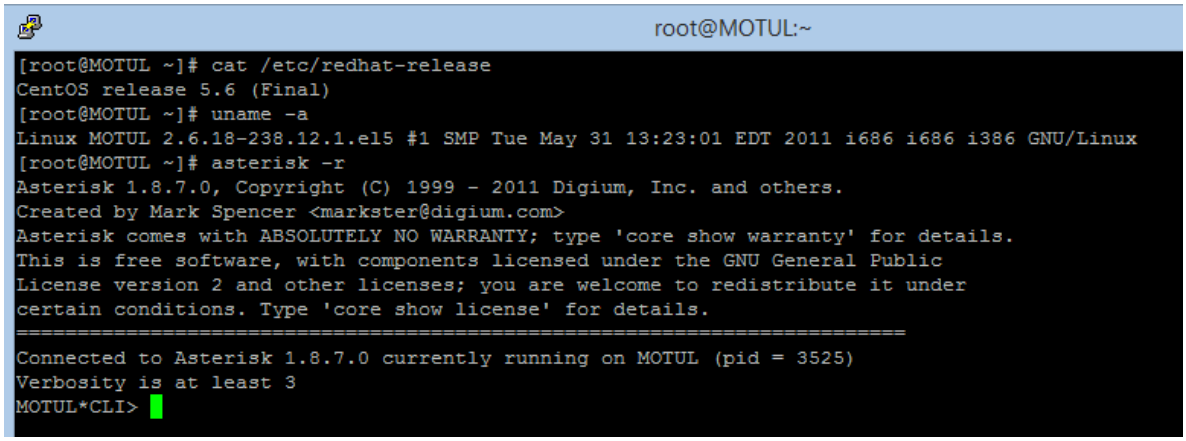


Fuente: El Autor.

Las características tipo software de este servidor son:

- Sistema Operativo Centos 5.6.
- Arquitectura 32 bits.
- Asterisk 1.8.7.0
- Elastix 2.4 (Consola WEB)

Fig. 18. Información Software Servidor Asterisk Creamigo Motul S.A.



Fuente: El Autor.

3. BANCO DE PRUEBAS

a. Implementación.

El objeto de realizar un banco de pruebas, es con el único fin de no afectar la disponibilidad del servidor físico de Asterisk de la empresa Creamigo Motul S.A.

Para llevar a cabo este proceso se realizó una copia exacta de toda la configuración del servidor Asterisk de Motul, con el fin de que sea restaurada en una instalación limpia de Centos 5.6 con aplicativo Asterisk 1.8.7.0 y administración Web Elastix 2.4.

A continuación se detallan las características físicas y recursos de conectividad que se utilizaron para medir la seguridad del servidor de telefonía IP de la empresa Creamigo Motul S.A. mediado por Asterisk.

Tabla 5. Características Máquina HOST.

MARCA	MODELO	OS	CPU	RAM	HDD
Hewlett Packard	Probook 800	Win 10 Pro x 64 bits	Intel ® Core ™ i7 @ 3.4 GHz	8 GB DDR4	750 GB

Fuente: El Autor.

Tabla 6. Características Red y recursos de conectividad.

RED LAN	IP DE ENRUTAMEINTO	RED WAN	EQUIPO DE RED	SERVICIOS DE RED ACTIVOS
192.168.0.0/24	192.168.0.1	Se posee una red dinámica, el proveedor de servicios es Claro, soluciones fijas.	Se posee un Router Technicolor QAM256, provee conexión de red WiFi y Ethernet.	• DHCP. • Puerta de enlace. • Internet. • SSID. • LAN.

Fuente: El Autor.

Tabla 7. Características Software virtualizador.

REFERENCIA	VERSIÓN
Oracle VirtualBox	Versión 5.2.0 r118431 (Qt5.6.2) for Windows

Fuente: El Autor.

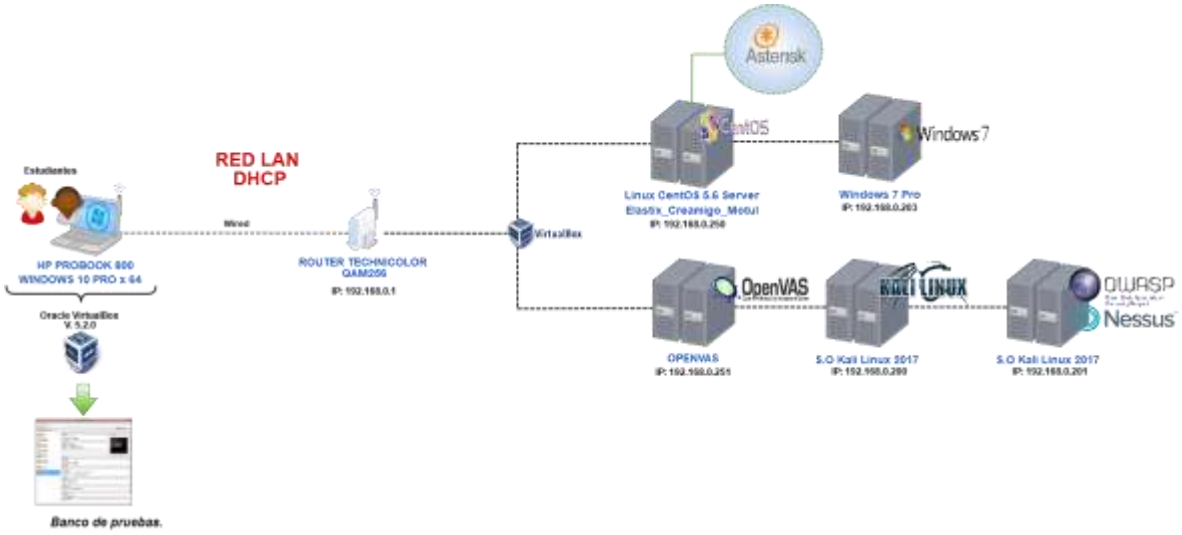
Tabla 8. Características máquinas virtuales.

NOMBRE	OS	RED	NUCLEOS CPU	RAM	HDD	DETALLES
Elastix_Creamigo_Motul	CentOS reléase 5.6 32 bits.	192.168.0.250	1	1024 MB	8 GB	Se configura instancia de prueba de servidor Asterisk de la empresa Creamigo Motul S.A
Elastix_Creamigo_Motul COPIA	CentOS reléase 5.6 32 bits.	192.168.0.250	1	1024 MB	8 GB	Replica de servidor Asterisk, con el fin de tener respaldo en caso de corromperse el sistema por las herramientas de Pentesting utilizadas
KALI LINUX UNAD PRACTICA S.O.	KALI GNU Linux, 64 bits basada en Debian.	192.168.0.200	1	1024 MB	16 GB	Instancia base de KALI LINUX 2017, esta es usada para realizar pruebas de escaneo bajo NMAP y otras herramientas como METASPLOIT, HYDRA y JOHNRIPPER. Se usa para hacer copias de otras máquinas virtuales bajo KALI Linux.
KALI LINUX NESSUS OSWAP METASPLOIT	KALI GNU Linux, 64 bits basada en Debian	192.168.0.201	1	1024 MB	16 GB	Copia de la maquina base de KALI Linux, esta se usará solo para la activación trial de 30 días de NESSUS.
WINDOWS 7 SEGUNDO SEMESTRE	Windows 7 64 bits	192.168.0.203	1	1024 MB	20 GB	Equipo donde se corren aplicaciones como PentestBOX y otros utilitarios que corren solo en Windows.
OPENVAS	Bajo Kernel Debian 3.4, 64 bits	192.168.0.251	1	2048 MB	9GB	Variante de Nessus en versión gratuita. Trabaja en entorno Web.

Fuente: El Autor.

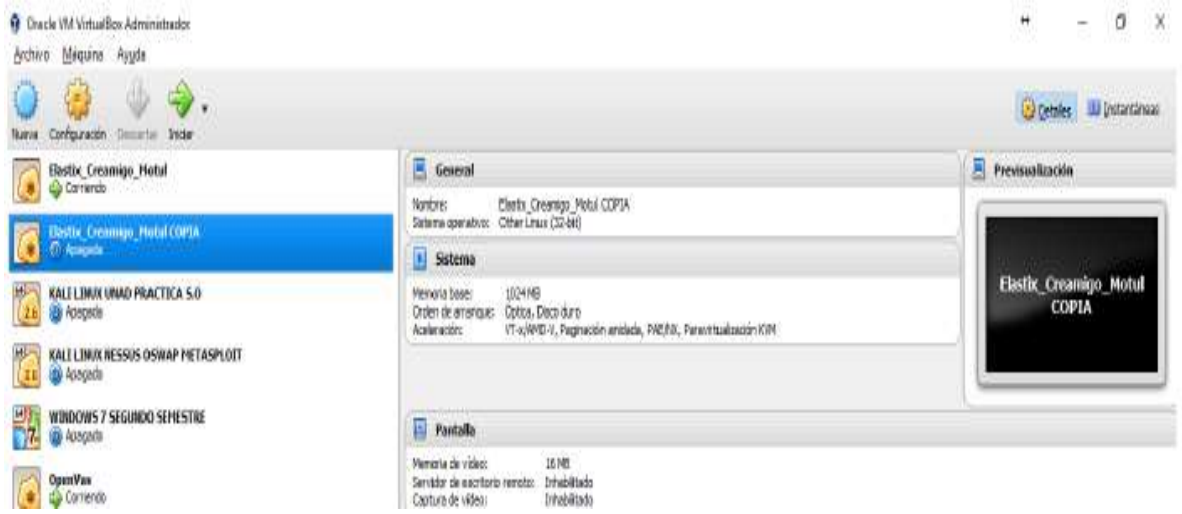
A continuación se representa el diagrama de red del banco de pruebas implementado:

Fig. 19. Diagrama de red Banco de pruebas.



Fuente: El Autor.

Fig. 20. Máquinas Virtuales Banco de Pruebas.



Fuente: El Autor.

b. Cláusula de Pentesting bajo Ethical Hacking para Creamigo Motul S.A. y la UNAD.

El objetivo de realizar pruebas de Pentesting al servidor de telefonía IP Asterisk de la empresa Creamigo Motul S.A., es con el fin de desarrollar el trabajo de la asignatura proyecto y así poder alcanzar el título de posgrado en seguridad informática.

Toda información procesada, recolecta, descifrada, explotada hacia el servidor de PBX de Creamigo Motul S.A. y la copia digitalizada que sirve de insumo en el banco de pruebas es con el fin de mejorar la seguridad actual que posee este equipo en la prestación del servicio básico de telefonía IP. Es así como solo la información que aquí se recolecte será de conocimiento de Creamigo Motul S.A. y de manejo académico de la Universidad Nacional Abierta y a distancia UNAD.

Mediante la presente clausula, se definen los pasos de documentación del proceso de Pentesting.

Tabla 9. Fases del Pentesting.

N°	TÉCNICA	DESCRIPCIÓN
1	**FootPrint**	Técnica de escaneo de red, protocolos, puertos, estructura, arquitectura y máquinas activas.
2	**Escaneo y enumeración de servicios**	Mediante herramientas de escaneo como NMAP, OPENVAS y NESSUS, se revisan y enumeran los servicios activos que posee el equipo objetivo.
3	**Análisis de vulnerabilidades**	Luego de realizar un análisis exhaustivo, se identifican las vulnerabilidades de impacto alto y medio.
4	**Obtención de acceso**	Se explotan las vulnerabilidades de impacto alto, con el fin de obtener acceso al equipo objetivo.
5	**Escalamiento de evidencia**	Se intenta escalar privilegios, sea teniendo copia del archivo Shadow o Passwd de Linux o encontrar acceso a nivel ROOT con la explotación de vulnerabilidades de impacto alto.
6	**Obtención de evidencia**	Luego de obtener acceso, se obtiene evidencia que sirva para demostrar que se pude tener acceso a recursos protegidos.

Fuente: El Autor.

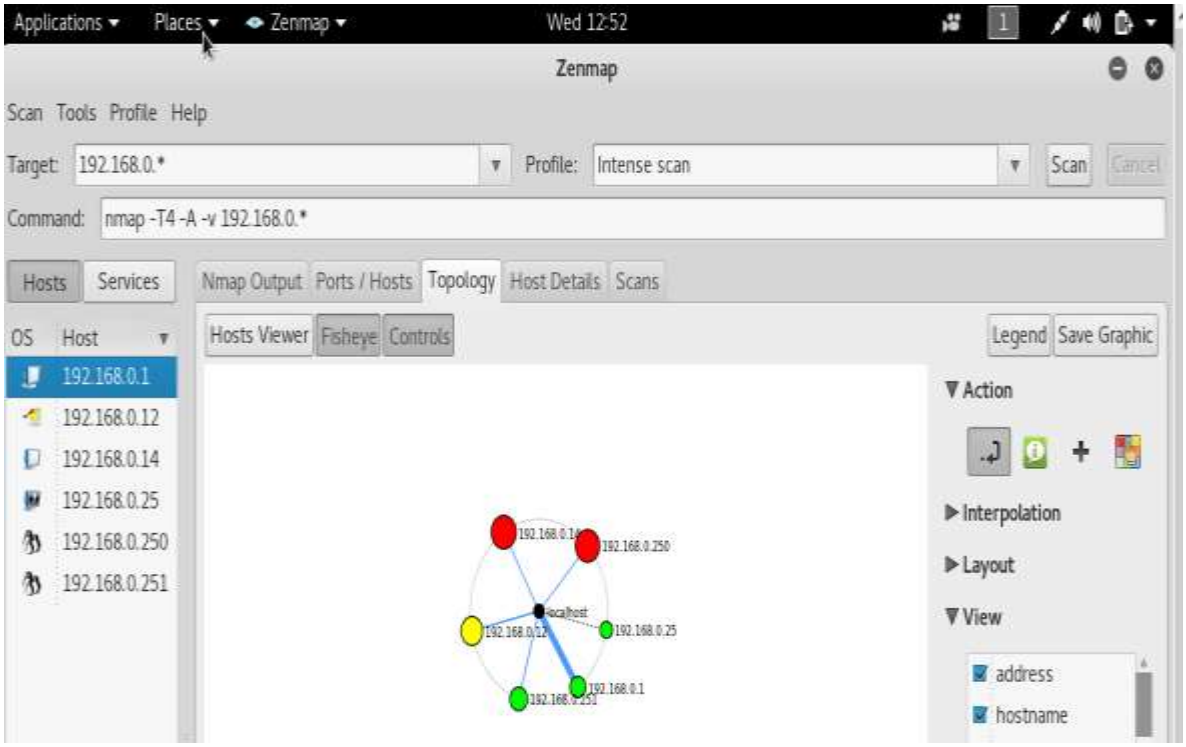
4. INICIO PENTESTING

a. FASE 1: FootPrint

Se procede a revisar toda la subred 192.168.0.0/24, con el fin de detectar que equipos se encuentran activos dentro de este rango.

Usando ZENMAP, mediante el comando “nmap –T4 _a -v 192.168.0.*” se realiza la búsqueda por toda la subred especificada.

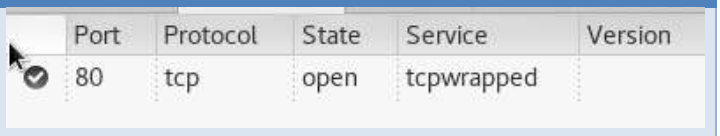
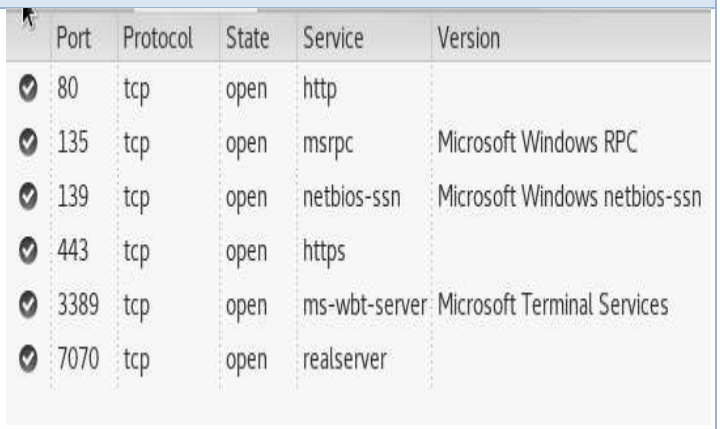
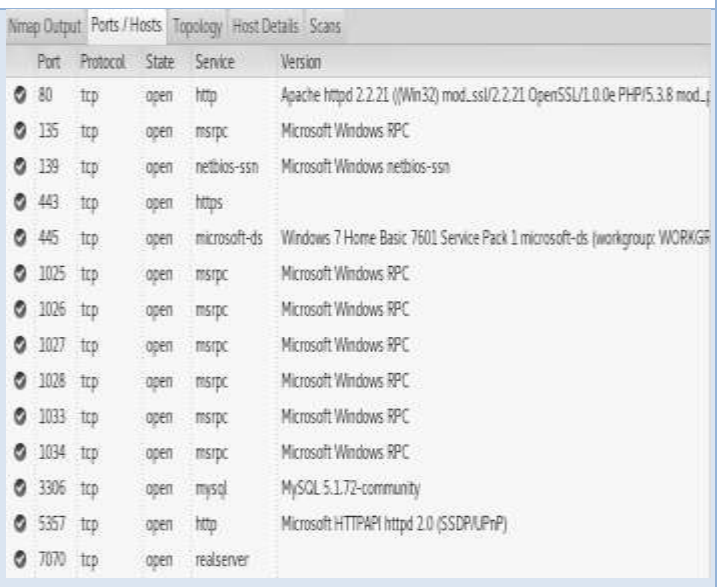
Fig. 21. Topología de red Banco de prueba.



Fuente: El Autor.

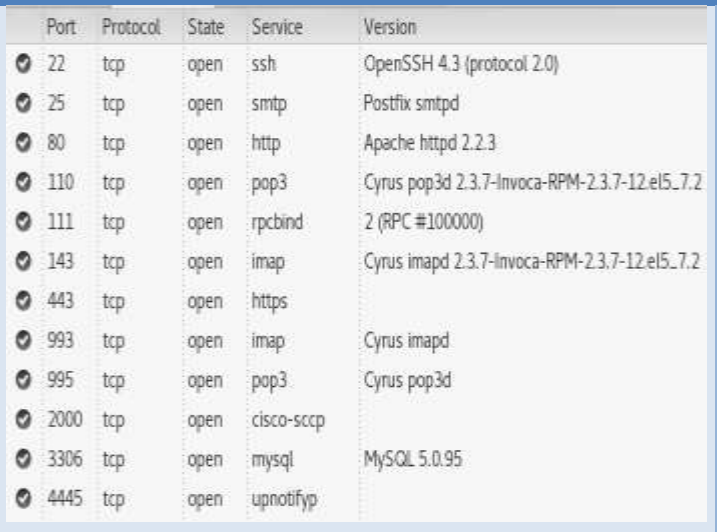
Se puede observar que se detectan los siguientes hosts:

Tabla 10. Resultado escaneo Zenmap Banco de Pruebas.

Host	Estado	IP	Servicios abiertos
Router	Físico	192.168.0.1	
Win. 10 Pro	Físico	192.168.0.12	
Win. 7 home	Virtual	192.168.0.14	

Kali Linux	Virtual	192.168.0.25	No detecta ningún puerto abierto.
			`Nmap scan report for 192.168.0.25`
			`Host is up (0.000024s latency).`
			`All 1000 scanned ports on 192.168.0.25 are closed`
			`Too many fingerprints match this host to give specific OS details`
			`Network Distance: 0 hops`

Tabla 10. (Continuación)

Host	Estado	IP	Servicios abiertos
Elastix PBX	Virtual	192.168.0.250	
OpenVas	Virtual	192.168.0.251	

Fuente: El Autor.

b. FASE 2: Escaneo y enumeración de servicios.

Tabla 11. Nmap – escaneo de puertos y servicios.

UTILIDAD	DESCRIPCIÓN	OBSERVACIÓN
NMAP	Utilidad para escaneo de puertos y servicios	Se realiza mediante el comando del escaneo de todos los puertos TCP y UDP del servidor Elastix PBX, Nmap **-p 1-65535 -T4 -A -v 192.168.0.250**

Fuente: El Autor.

HALLAZGOS

Tabla 12. Puertos abiertos Servidor Asterisk Creamigo Motul.

RESULTADOS ESCANEO		
PUERTOS ABIERTOS	**IDENTIFICACIÓN**	**DESCRIPCIÓN**
22	SSH	Puerto seguro de SSH.
25	SMTP	Puesto recepción de correo electrónico.
80	HTTP	Puerto de acceso a servidor web.
110	POP3	Puerto de envió de correo.
111	RPC	Puerto RPC CentOS.
143	IMAP	Puerto de correo bajo IMAP.
443	HTTPS	Puerto de acceso seguro a servidor web
993	IMAP / SSL	Puerto SSL de correo bajo IMAP.
995	RPC	Puerto RPC CentOS.
2000	Cisco	Puerto SCCP
3306	MySQL	Puerto de base de datos MySQL.
4190	Cyrus IMAP Client	Cliente de correo Cyrus
4445	Upnotifyp	Puerto UPN
4559	IAX2	Puerto para el servicio IAX2
5038	Asterisk	Asterisk Call Manager 1.1
5060	SIP	Puerto SIP

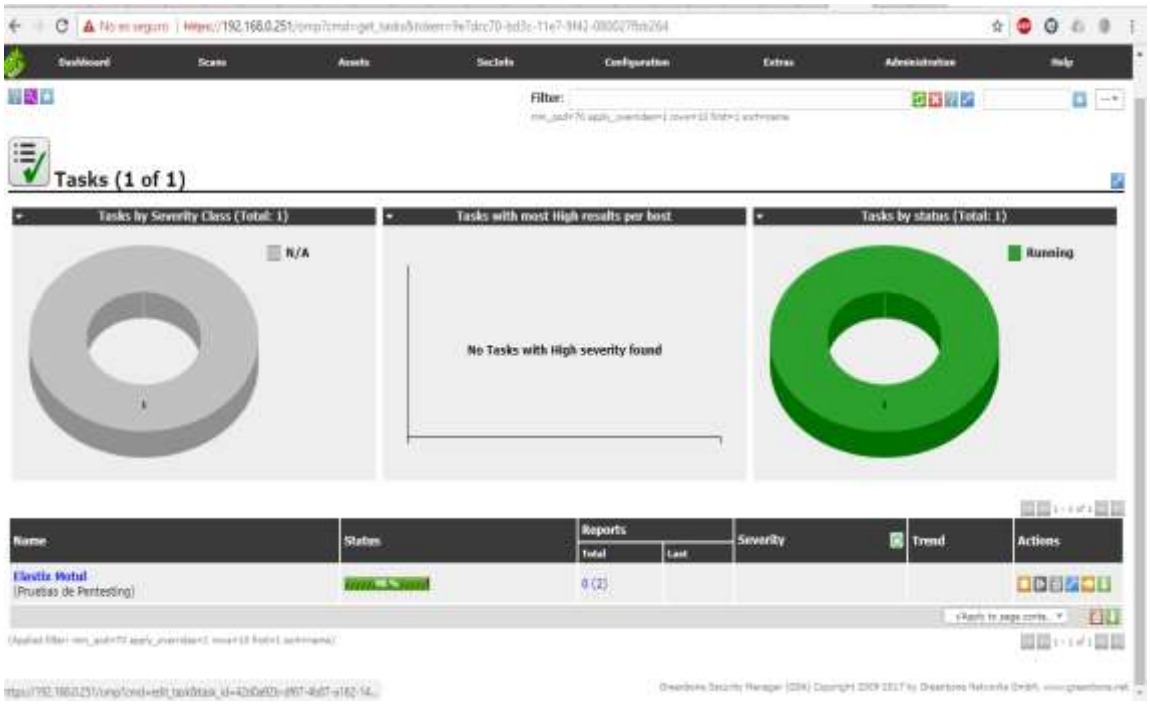
Fuente: El Autor.

c. FASE 3: Análisis de Vulnerabilidades.

Para llevar a cabo esta fase se realizó dicho proceso haciendo uso de dos herramientas de escaneo de vulnerabilidades, OpenVas y Nessus.

Se realizó inicialmente un escaneo profundo del servidor de telefonía IP de la empresa Creamigo con **OpenVas.**

Tabla 13. Inicio de proceso de Escaneo Servidor telefonía IP.



Fuente: El Autor.

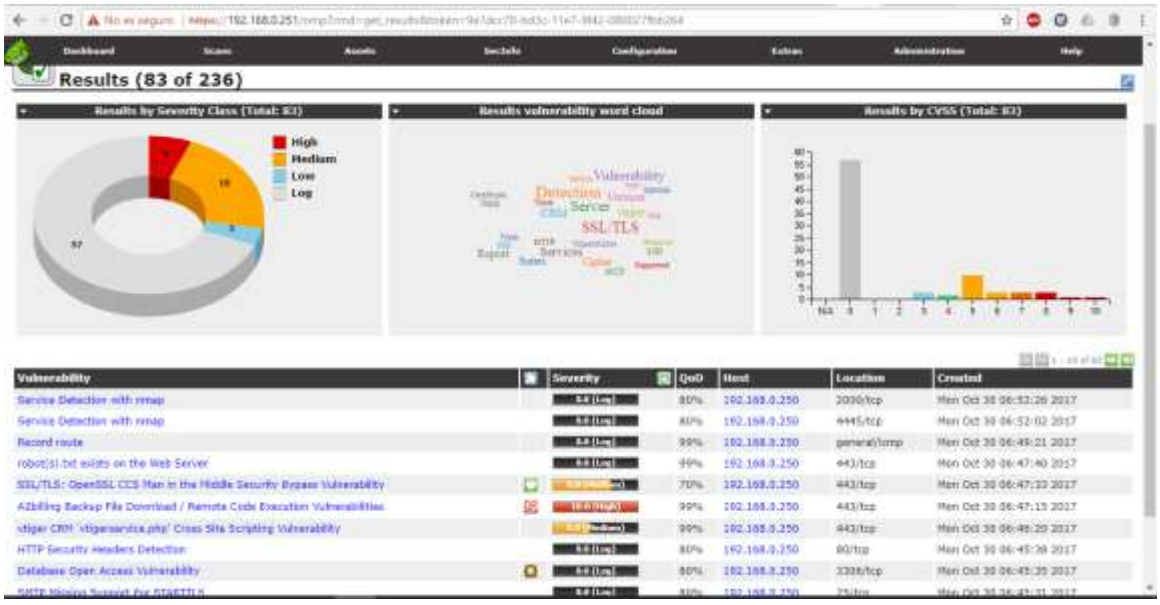
Se puede apreciar a continuación en la Fig. 22, que la herramienta OpenVas arroja un reporte completo donde se logra evidenciar un total de 83 de 236 vulnerabilidades. Los colores identifican la clase de vulnerabilidad. OpenVas clasifica las vulnerabilidades de la siguiente manera:

Tabla 14. Clasificación de vulnerabilidades OpenVas.

N°	COLOR	CLASS	DEFINICIÓN
1	ROJO	High	Alta o Crítica
2	NARANJA	Medium	Media
3	AZUL	Low	Baja
4	GRIS	Log	Registro

Fuente: El Autor.

Fig. 22. Resultados de escaneo Servidor telefonía IP.



Fuente: El Autor.

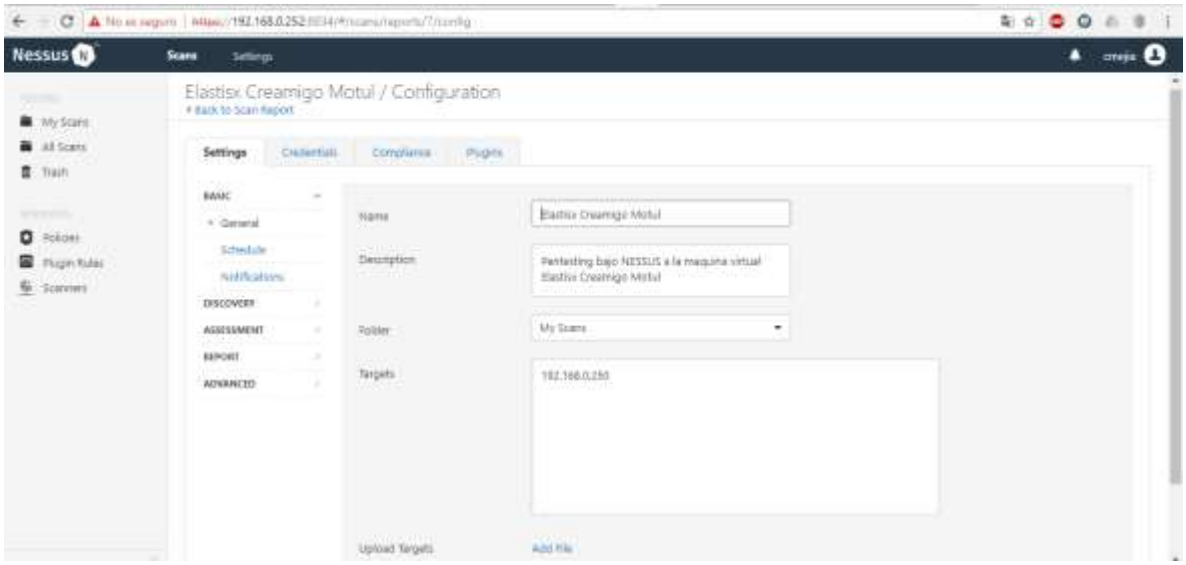
En el escaneo profundo con OpenVas se obtuvieron 5 de 236 vulnerabilidades de clase Alta – Crítica.

Fig. 23. Vulnerabilidades clase Alta Servidor telefonía IP.

Fuente: El Autor.

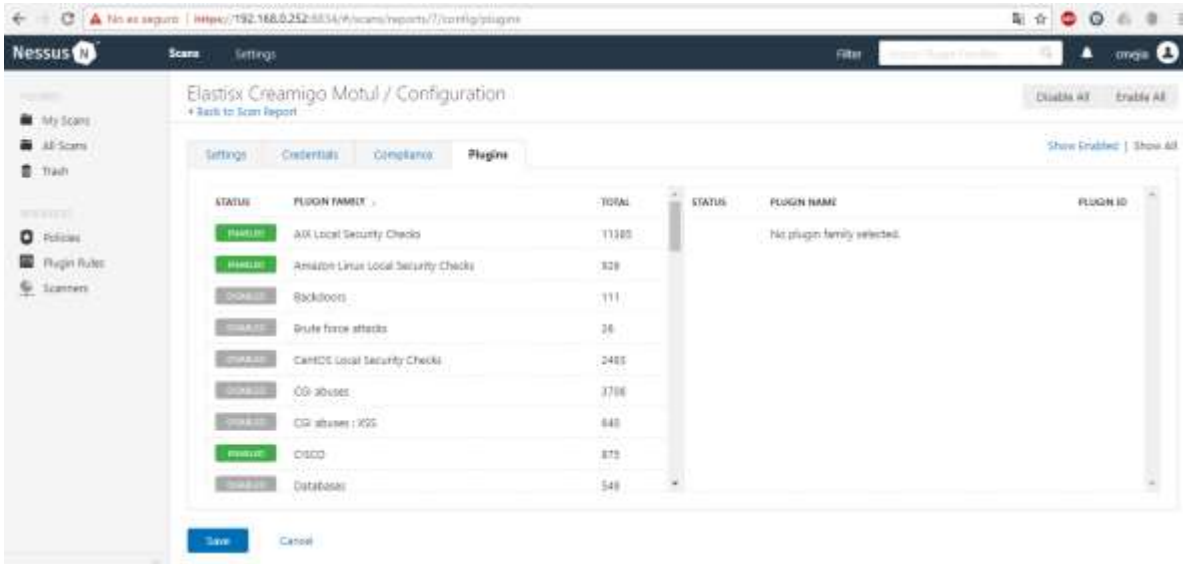
A continuación se exponen las evidencias encontradas tras realizar el proceso de escaneo de vulnerabilidades mediado por **Nessus.** En las siguientes imágenes podremos observar la parte inicial de configuración del proceso de escaneo que Nessus como software de escaneo de vulnerabilidades solicita como primera instancia.

Fig. 24. Configuración Detalles del Escaneo Nessus.



Fuente: El Autor.

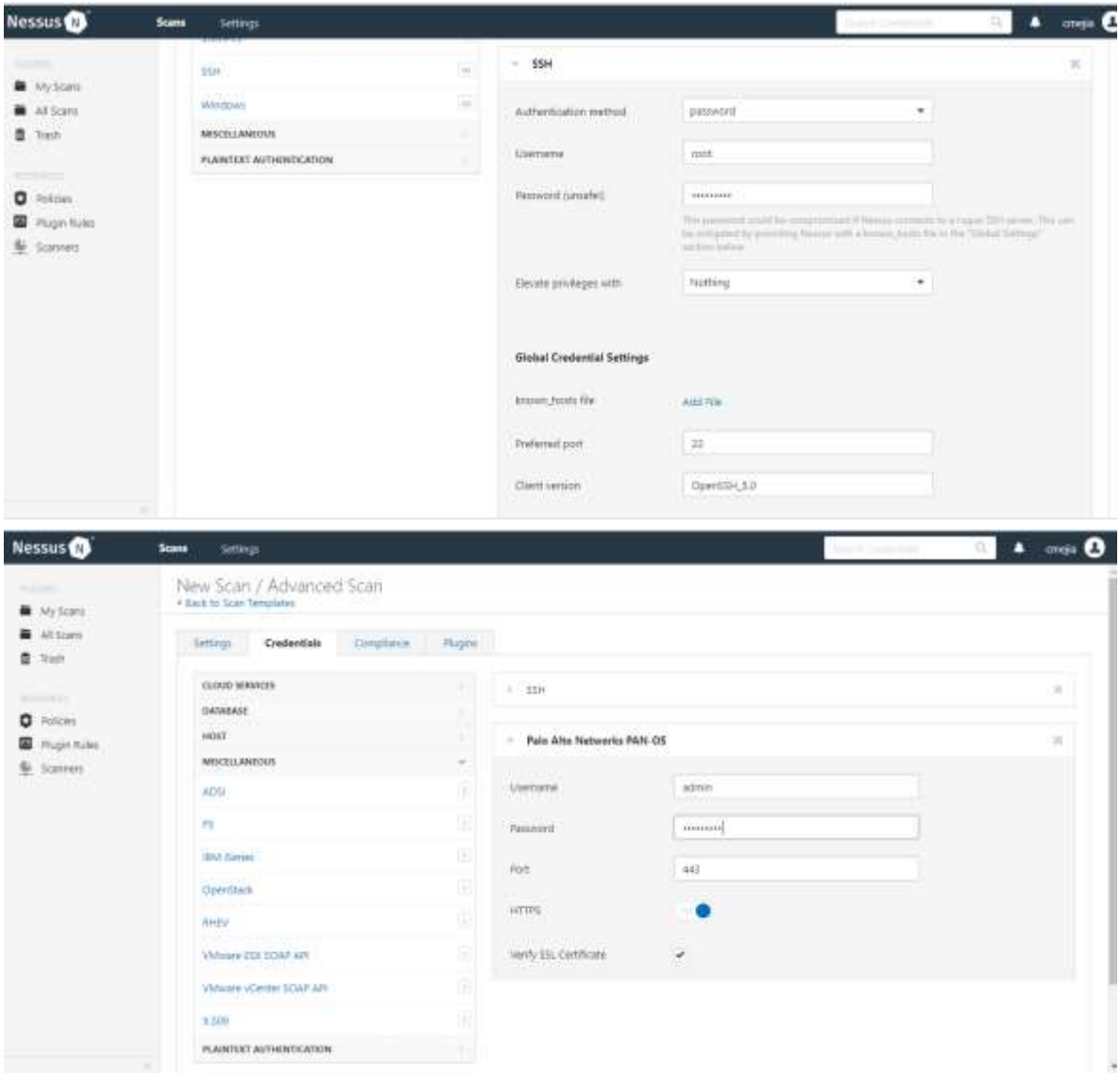
Fig. 25. Activación de Plugin básicos para el Escaneo en Nessus.



Fuente: El Autor.

Se debe tener en cuenta que Nessus genera una licencia gratis con funcionalidades básicas y limitadas para poder llevar a cabo un proceso de escaneo profundo sobre un objetivo como tal. Para este caso se logran cargar los Plugin básicos que Nessus ofrece el cual permitirá obtener información real sobre las posibles vulnerabilidades que el objetivo presente. La ventaja de contar con una licencia de pago, es obtener un sin número de plugin que además de contribuir en identificar las vulnerabilidades permite obtener información puntual y efectiva sobre la manera de explorar dichas vulnerabilidades. No obstante, el objetivo de esta fase como se ha definido previamente es identificar las vulnerabilidades que pueda tener el servidor de telefonía IP Asterisk de la empresa Creamigo Motul S.A.

Fig. 26. Configuración de usuario y credenciales para acceso al servicio de escaneo Nessus.



Fuente: El Autor.

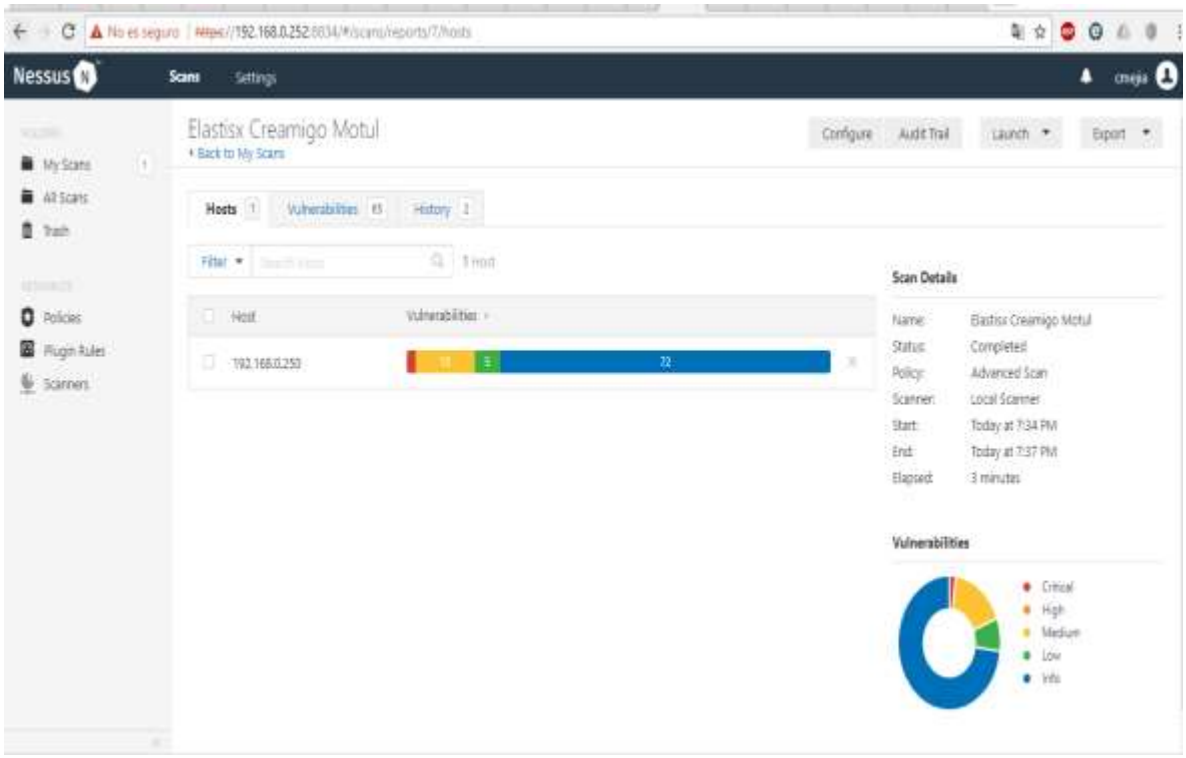
A continuación se inicia el proceso de escaneo una vez definidas las configuraciones solicitadas por Nessus y OpenVas se clasifican las vulnerabilidades de la siguiente manera:

Tabla 15. Clasificación de vulnerabilidades Nessus.

N°	COLOR	CLASS	DEFINICIÓN
1	ROJO	Critical	Crítica
2	NARANJA	Hight	Alta
3	AMARILLA	Medium	Media
4	VERDE	Low	Baja
5	AZUL	Info	Información

Fuente: El Autor.

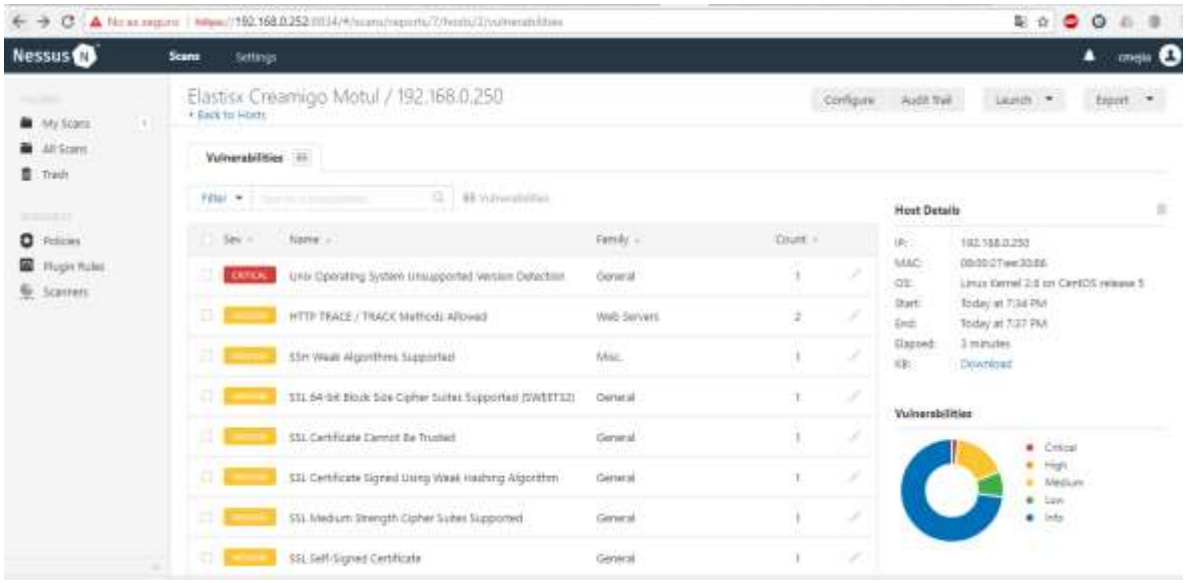
Fig. 27. Escaneo completo Servidor telefonía IP con Nessus.



Fuente: El Autor.

Obtuvimos tras el escaneo avanzado con Nessus un total de 65 vulnerabilidades.

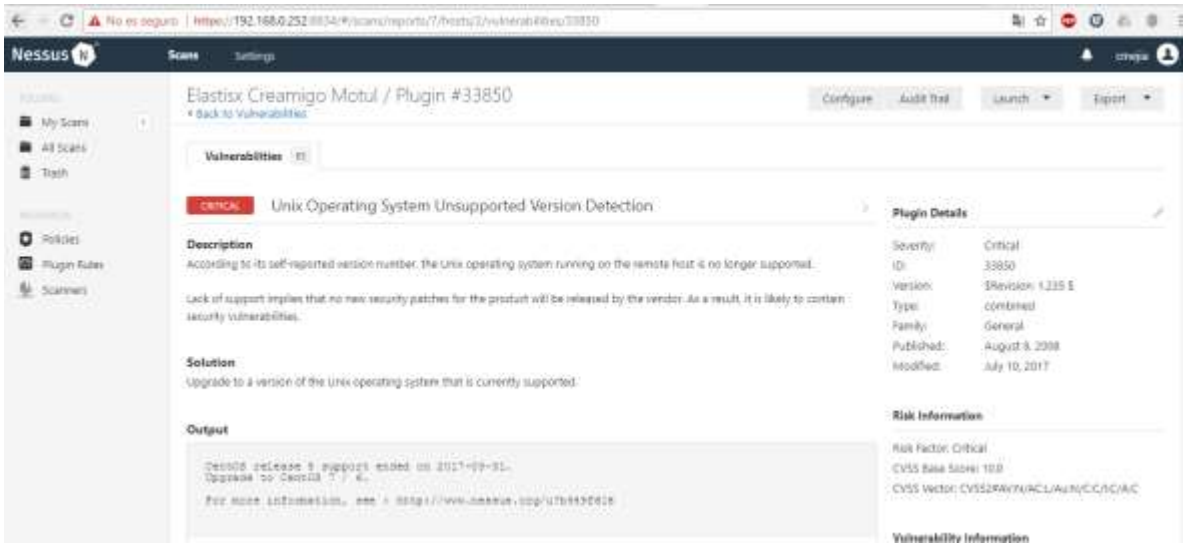
Fig. 28. Vulnerabilidades Críticas y Medias en el Servidor de telefonía IP.



Fuente: El Autor.

Para la vulnerabilidad Crítica que se obtuvo con Nessus, al seleccionarla se detalla la descripción de la misma, el plugin que se utilizó, el código de la vulnerabilidad y los detalles relacionados a la solución.

Fig. 29. Detalles vulnerabilidad crítica en Nessus.



Fuente: El Autor.

De la misma manera es posible obtener un reporte más detallado de todas las vulnerabilidades encontradas en el escáner de vulnerabilidades del Servidor de Telefonía IP Asterisk de la empresa Creamigo Motul S.A. donde se puede apreciar la clasificación de la vulnerabilidad, el plugin utilizado, el nombre además de identificarse con su respectivo color y el valor cuantitativo que se le asigna a cada una.

Tabla 16. Detalles vulnerabilidades en Servidor telefonía IP mediado por Nessus.

SUMMARY					
Critical	**High**	**Medium**	**Low**	**Info**	**Total**
1	0	11	5	48	65

DETAILS		
Severity	**Plugin Id**	**Name**
Critical (10.0)	33850	Unix Operating System Unsupported Version Detection
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium (5.0)	11213	HTTP TRACE / TRACK Methods Allowed
Medium (5.0)	20007	SSL Version 2 and 3 Protocol Detection
Medium (5.0)	42873	SSL Medium Strength Cipher Suites Supported
Medium (5.0)	94437	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
Medium (4.3)	26928	SSL Weak Cipher Suites Supported
Medium (4.3)	62565	Transport Layer Security (TLS) Protocol CRIME Vulnerability
Medium (4.3)	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
Medium (4.3)	90317	SSH Weak Algorithms Supported
Medium (4.0)	35291	SSL Certificate Signed Using Weak Hashing Algorithm
Low (2.6)	15855	POP3 Cleartext Logins Permitted
Low (2.6)	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
Low (2.6)	70658	SSH Server CBC Mode Ciphers Enabled
Low (2.6)	71049	SSH Weak MAC Algorithms Enabled
Low	69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
Info	10107	HTTP Server Type and Version
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10185	POP Server Detection

Tabla 16. (Continuación)

Severity	Plugin Id	Name
Info	10223	RPC portmapper Service Detection
Info	10263	SMTP Server Detection
Info	10267	SSH Server Type and Version Information
Info	10287	Traceroute Information
Info	10302	Web Server robots.txt Information Disclosure
Info	10386	Web Server No 404 Error Code Check
Info	10719	MySQL Server Detection
Info	10863	SSL Certificate Information
Info	10881	SSH Protocol Versions Supported
Info	10884	Network Time Protocol (NTP) Server Detection
Info	11111	RPC Services Enumeration
Info	11153	Service Detection (HELP Request)
Info	11154	Unknown Service Detection: Banner Retrieval
Info	11219	Nessus SYN scanner
Info	11414	IMAP Service Banner Retrieval
Info	11819	TFTP Daemon Detection
Info	11936	OS Identification
Info	14773	Service Detection: 3 ASCII Digit Code Responses
Info	18261	Apache Banner Linux Distribution Disclosure
Info	19506	Nessus Scan Information
Info	20834	Inter-Asterisk eXchange Protocol Detection
Info	21642	Session Initiation Protocol Detection
Info	21643	SSL Cipher Suites Supported
Info	22877	Skinny Server Detection
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	25220	TCP/IP Timestamps Supported
Info	35716	Ethernet Card Manufacturer Detection
Info	39520	Backported Security Patch Detection (SSH)
Info	39521	Backported Security Patch Detection (WWW)
Info	45590	Common Platform Enumeration (CPE)
Info	48243	PHP Version Detection

Tabla 16. (Continuación)

Severity	Plugin Id	Name
Info	51891	SSL Session Resume Supported
Info	53335	RPC portmapper (TCP)
Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	62563	SSL Compression Methods Supported
Info	63202	Asterisk Detection
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported
Info	70657	SSH Algorithms and Languages Supported
Info	76347	HylaFAX Installed
Info	84574	Backported Security Patch Detection (PHP)
Info	94761	SSL Root Certification Authority Certificate Information

Fuente: El Autor.

Los análisis realizados por OpenVas y Nessus, muestran varias vulnerabilidades, para el presente proyecto se documentarán y analizarán las vulnerabilidades de clase Alta y Media de impacto, en la siguiente tabla se hace un análisis de los resultados que se encontraron, en donde se puede observar que producto se usó y cuál fue el primer hallazgo arrojado, pero se debe tener en cuenta los siguientes criterios:

Tabla 17. Tratamiento de las vulnerabilidades.

Tipo de solución	
Tratamiento	**Descripción**
Parche ofrecido por el fabricante.	Actualización o fix del fabricante para dar solución al bug reportado.
Mitigar	Cambios en la configuración que ayudan a dar solución.
Solución alternativa	Cambio en configuración que ayudan a mitigar hasta que se genere algún fix pro el proveedor.
No existe parche	Por el momento no hay solución.
Migrar	Cambio de versión de software.
Actividades de log	Actividad que puede indicar información sobre un puerto específico, revelando versión del software que escucha en ese puerto.

Fuente: El Autor.

Fig. 30. Banner publicitario empresarial Creamigo Motul S.A.

Fuente: Creamigo Motul S.A.
Disponible en: www.creamigo.com

Fecha de Pruebas	Objetivo de las pruebas	Autorización Previa	Servidor de Producción	Servidor de Pruebas
3 de Noviembre de 2017	Pentesting Servidor PBX	SI	NO	SI (Virtual)

A continuación se relacionan y se exponen las vulnerabilidades encontradas tras los procesos de escaneo de vulnerabilidades al Servidor de telefonía IP – Asterisk de la empresa Creamigo Motul S.A. mediado por OpenVas y Nessus. En esta se detallan aspectos técnicos de las vulnerabilidades y se le da prioridad solo a las que se clasifican como clase Alta y Media como se mencionaba previamente.

Tabla 18. Vulnerabilidades Servidor telefonía IP clase Alta y Media OpenVas Vs. Nessus.

ID	Escáner	Vulnerabilidades	Tipo de solucion	Impacto	QoD	IP	Puerto
1	OPENVAS	A2billing Backup File Download / Remote Code Execution Vulnerabilities	Solución alternativa	10.0 (High)	99%	192.168.0.250	443/tcp
2	OPENVAS	VTiger CRM Privilege Escalation and Unrestricted File Upload Vulnerability	Parche ofrecido por el fabricante	8.5 (High)	80%	192.168.0.250	443/tcp
3	OPENVAS	Vtiger CRM Multiple SQL Injection Vulnerabilities April-14	Parche ofrecido por el fabricante	7.5 (High)	80%	192.168.0.250	443/tcp

ID	Escáner	Vulnerabilidades	Tipo de solucion	Impacto	QoD	IP	Puerto
4	OPENVAS	vtiger CRM 'onlyforuser' Parameter SQL Injection Vulnerability	Parche ofrecido por el fabricante	7.5 (High)	80%	192.168.0.250	443/tcp
5	OPENVAS	vtiger CRM 'class.phpmailer.php' Remote Code Execution Vulnerability	Parche ofrecido por el fabricante	7.5 (High)	80%	192.168.0.250	443/tcp
6	OPENVAS	SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability	Parche ofrecido por el fabricante	6.8 (Medium)	70%	192.168.0.250	443/tcp
7	OPENVAS	vTiger CRM Cross Site Scripting and SQL Injection Vulnerabilities	Solución alternativa	6.5 (Medium)	80%	192.168.0.250	general/ tcp
8	OPENVAS	SSL/TLS: Missing `secure` Cookie Attribute	Mitigar	6.4 (Medium)	99%	192.168.0.250	443/tcp
9	OPENVAS	http TRACE XSS attack	Solución alternativa	5.8 (Medium)	99%	192.168.0.250	80/tcp
10	OPENVAS	http TRACE XSS attack	Solución alternativa	5.8 (Medium)	99%	192.168.0.250	443/tcp
11	OPENVAS	Vtiger CRM Access Control Vulnerability	Parche ofrecido por el fabricante	5.5 (Medium)	80%	192.168.0.250	443/tcp
12	OPENVAS	SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	Mitigar	5.0 (Medium)	98%	192.168.0.250	443/tcp
13	OPENVAS	Check if Mailserver answer to VRFY and EXPN requests	Solución alternativa	5.0 (Medium)	99%	192.168.0.250	25/tcp
14	OPENVAS	Missing `httpOnly` Cookie Attribute	Mitigar	5.0 (Medium)	80%	192.168.0.250	443/tcp
15	OPENVAS	vTiger CRM PHP Code Injection Vulnerability	Parche ofrecido por el fabricante	4.9 (Medium)	80%	192.168.0.250	443/tcp
16	OPENVAS	SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection	Mitigar	4.3 (Medium)	98%	192.168.0.250	443/tcp
17	OPENVAS	SSL/TLS: Report Weak Cipher Suites	Mitigar	4.3 (Medium)	98%	192.168.0.250	443/tcp
18	OPENVAS	Elastix Multiple Cross-Site Scripting Vulnerabilities	no existe parche	4.3 (Medium)	98%	192.168.0.250	443/tcp
19	OPENVAS	vtiger CRM 'vtigerservice.php' Cross Site Scripting Vulnerability	Solución alternativa	4.3 (Medium)	99%	192.168.0.250	443/tcp
20	OPENVAS	SSH Weak Encryption Algorithms Supported	Mitigar	4.3 (Medium)	95%	192.168.0.250	22/tcp

ID	Escáner	Vulnerabilidades	Tipo de solucion	Impacto	QoD	IP	Puerto
21	OPENVAS	SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)	Mitigar	4.3 (Medium)	80%	192.168.0.250	443/tcp
22	OPENVAS	SSL/TLS: Certificate Signed Using A Weak Signature Algorithm	Mitigar	4.0 (Medium)	80%	192.168.0.250	443/tcp
23	OPENVAS	SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability	Solución alternativa	4.0 (Medium)	80%	192.168.0.250	443/tcp
24	OPENVAS	SSL/TLS: TLS/SPDY Protocol Information Disclosure Vulnerability (CRIME)	Mitigar	2.6 (Low)	98%	192.168.0.250	443/tcp
25	OPENVAS	SSH Weak MAC Algorithms Supported	Mitigar	2.6 (Low)	95%	192.168.0.250	22/tcp
26	OPENVAS	TCP timestamps	Mitigar	2.6 (Low)	80%	192.168.0.250	general/ tcp
27	NESSUS	Unix Operating System Unsupported Version Detection	Mitigar	10.0 (High)	99%	192.168.0.251	general/ tcp
28	NESSUS	SSL Certificate Cannot Be Trusted	Mitigar	6.4 (Medium)	80%	192.168.0.252	443/tcp
29	NESSUS	SSL Self-Signed Certificate	Mitigar	6.4 (Medium)	80%	192.168.0.253	443/tcp
30	NESSUS	HTTP TRACE / TRACK Methods Allowed	Mitigar	6.4 (Medium)	80%	192.168.0.254	443/tcp
31	NESSUS	SSL Version 2 and 3 Protocol Detection	Mitigar	6.4 (Medium)	80%	192.168.0.255	443/tcp
32	NESSUS	SSL Medium Strength Cipher Suites Supported	Mitigar	6.4 (Medium)	80%	192.168.0.256	443/tcp
33	NESSUS	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)	Mitigar	6.4 (Medium)	80%	192.168.0.257	443/tcp
34	NESSUS	SSL Weak Cipher Suites Supported	Mitigar	6.4 (Medium)	80%	192.168.0.258	443/tcp
35	NESSUS	Transport Layer Security (TLS) Protocol CRIME Vulnerability	Mitigar	6.4 (Medium)	80%	192.168.0.259	443/tcp
36	NESSUS	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability	Mitigar	6.4 (Medium)	80%	192.168.0.260	443/tcp
37	NESSUS	SSH Weak Algorithms Supported	Mitigar	6.4 (Medium)	80%	192.168.0.261	443/tcp
38	NESSUS	SSL Certificate Signed Using Weak Hashing Algorithm	Mitigar	6.4 (Medium)	80%	192.168.0.262	443/tcp
39	NESSUS	POP3 Cleartext Logins Permitted	Actividad de log	2.6 (Low)	70%	192.168.0.263	110/tcp
40	NESSUS	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Actividad de log	2.6 (Low)	70%	192.168.0.264	443/tcp

Tabla 18. (Continuación)

ID	Escáner	Vulnerabilidades	Tipo de solucion	Impacto	QoD	IP	Puerto
41	NESSUS	SSH Server CBC Mode Ciphers Enabled	Actividad de log	2.6 (Low)	70%	192.168.0.265	22/tcp
42	NESSUS	SSH Weak MAC Algorithms Enabled	Actividad de log	2.6 (Low)	70%	192.168.0.266	22/tcp
43	NESSUS	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits	actividades de log	2.6 (Low)	70%	192.168.0.267	22/tcp
44	NESSUS	HTTP Server Type and Version	actividades de log	2.6 (Low)	70%	192.168.0.268	443/tcp
45	NESSUS	ICMP Timestamp Request Remote Date Disclosure	actividades de log	2.6 (Low)	70%	192.168.0.269	general/ tcp
46	NESSUS	POP Server Detection	actividades de log	2.6 (Low)	70%	192.168.0.270	110/tcp
47	NESSUS	RPC portmapper Service Detection	actividades de log	2.6 (Low)	70%	192.168.0.271	general/ tcp
48	NESSUS	SMTP Server Detection	actividades de log	2.6 (Low)	65%	192.168.0.272	25/tcp
49	NESSUS	SSH Server Type and Version Information	actividades de log	2.6 (Low)	65%	192.168.0.273	22/tcp
50	NESSUS	Traceroute Information	actividades de log	2.6 (Low)	65%	192.168.0.274	general/ tcp
51	NESSUS	Web Server robots.txt Information Disclosure	actividades de log	2.6 (Low)	65%	192.168.0.275	80/tcp
52	NESSUS	Web Server No 404 Error Code Check	actividades de log	2.6 (Low)	65%	192.168.0.276	80/tcp

Fuente: El Autor.

5. Descripción de las vulnerabilidades de impacto Alto y soluciones.

Los hallazgos de nivel alto, serán tratados con el fin de dar corrección a estos, se debe tener en cuenta que solucionarlos mejora en algunos casos las vulnerabilidades de nivel medio. En la siguiente tabla se muestran discriminadas las vulnerabilidades alto impacto, las cuales se describirán y se propondrán las posibles soluciones.

Tabla 19. Tratamiento de vulnerabilidades de Alto impacto Servidor de telefonía IP.

Id	Escáner	Vulnerabilidades	Impacto	Descripción	Solución	Programa o modulo afectado
1	OPENVAS	A2billing Backup File Download / Remote Code Execution Vulnerabilities	10.0 (High)	Vulnerabilidad del Módulo A2billing, basada en técnica de inyección SQL blind. Por medio de código remoto.	Configuración de Seguridad mediada en el acceso web de Apache.	A2billing
2	OPENVAS	VTiger CRM Privilege Escalation and Unrestricted File Upload Vulnerability	8.5 (High)	Vulnerabilidad del Módulo VTiger CRM basada en técnica de inyección SQL blind. Por medio de la cual pueden cargar contenido malicioso.	Actualización de versión.	VTiger CRM
3	OPENVAS	Vtiger CRM Multiple SQL Injection Vulnerabilities April-14	7.5 (High)	Vulnerabilidad del Módulo VTiger CRM basada en técnica de inyección SQL, por medio de la cual se inyecta código malicioso.	Actualización de versión.	VTiger CRM
4	OPENVAS	vtiger CRM 'onlyforuser' Parameter SQL Injection Vulnerability	7.5 (High)	Vulnerabilidad del Módulo VTiger CRM basada en técnica de inyección SQL, por medio de la cual se inyecta código malicioso.	Actualización de versión.	VTiger CRM
5	OPENVAS	vtiger CRM 'class.phpmailer.php' Remote Code Execution Vulnerability	7.5 (High)	vulnerabilidad del Módulo VTiger CRM basada en tecnica de inyeccion SQL la cual ataca los archivos 'class.phpmailer.php	Actualización de versión.	VTiger CRM
27	NESSUS	Unix Operating System Unsupported Version Detection	10.0 (High)	Esta vulnerabilidad es por falta de soporte a la versión de Linux Centos.	Cambio de CentOS 5.6 a 7	Centos 5.6

Fuente: El Autor.

5.1 Vulnerabilidad: A2billing Backup File Download / Remote Code Execution Vulnerabilities

ID: 1

Escáner: OPENVAS.

Impacto: 10.0 / Alto

Programa o modulo afectado: A2billing.

Descripción: Vulnerabilidad del Módulo A2billing, basada en técnica de inyección SQL blind. Por medio de código remoto, este directorio contiene un archivo llamado "**iridium_threed.php**" el cual presenta la vulnerabilidad mediante la manipulación del parámetro transactionID permitiendo el ataque de tipo SQL injection, una vez se realiza la inyección de código SQL, se pasa a crear un contexto en el archivo **extensions_custom.conf,** el cual se caracteriza por administrar y controlar los contextos de operación durante una llamada. Esta vulnerabilidad es definida como crítica y es esta la que provocó la falla presentada en el servidor tiempo atrás, porque se creó sin autorización alguna un contexto que permitió realizar miles de llamadas internacionales de manera ilegal haciendo uso de la troncal contratada con el proveedor Emcali y por obvias razones, este fallo de seguridad provoco alzas sorprendentes en la facturación del servicio de la telefonía IP mediado por IP Trunk.

Solución 1: A2billing es un módulo con acceso y administración web, que permite tarificar y facturar las llamadas que se realizan a través del módulo de telefonía IP Asterisk, ante la vulnerabilidad que presenta este módulo, se recomienda eliminar el directorio a2billing, que se encuentra en la ruta "/var/www/html". Se recomienda eliminar como primera instancia, justificando, que dicha herramienta no es de uso, ni importancia para el funcionamiento normal de la telefonía IP de la empresa Creamigo Motul S.A.

Solución 2: Actualizar y/o migrar el módulo A2billing a una versión superior.

Solución 3: Otro aspecto a tener en cuenta es que esta vulnerabilidad se aprovecha de los puertos 80 o 443, por los mencionados, se accede y se realiza la inyección SQL, para evitar esto, se debe configurar un nuevo usuario Apache que valide y autorice el acceso web al módulo de Elastix solicitando nombre de usuario y contraseña. No obstante se recomienda cambiar, los puertos por defecto de acceso web o servidor Apache.

5.2 Vulnerabilidad: VTiger CRM Privilege Escalation and Unrestricted File Upload Vulnerability

ID: 2

Escáner: OPENVAS.

Impacto: 8.5 / Alto

Programa o modulo afectado: VTiger CRM v. 5.2.1

Descripción: Vulnerabilidad del Módulo VTiger CRM basada en técnica de inyección SQL blind. Por medio de la cual pueden cargar contenido malicioso. Esta vulnerabilidad permite al atacante ejecutar código SQL y HTML, hecho el cual permite eludir restricciones de seguridad y manipular datos exponiendo al sistema a un daño general.

Solución 1: VTiger CRM es un módulo con acceso y administración web, que permite implementar un sistema de relación y registro de clientes, automatizar las ventas que ofrezca una compañía, gestiona inventarios, analiza informes y se puede integrar con diversas herramientas como lo son los clientes de correo electrónico; como solución inicial se debe eliminar el directorio VTiger CRM, que se encuentra en la ruta "/var/www/html". Se recomienda eliminar como primera instancia, justificando, que dicha herramienta no es de uso, ni importancia para el funcionamiento normal de la telefonía IP de la empresa Creamigo Motul S.A.

Solución 2: Actualizar y/o migrar el módulo VTiger CRM a una versión superior (6.4.0) de manera manual.

Solución 3: Otro aspecto a tener en cuenta es que esta vulnerabilidad se aprovecha de los puertos 80 o 443, por los mencionados, se accede y se realiza la inyección SQL, para evitar esto, se debe configurar un nuevo usuario Apache que valide y autorice el acceso web al módulo de Elastix solicitando nombre de usuario y contraseña. No obstante se recomienda cambiar, los puertos por defecto de acceso web o servidor Apache.

5.3 Vulnerabilidad: Vtiger CRM Multiple SQL Injection Vulnerabilities April-14

ID: 3

Escáner: OPENVAS.

Impacto: 7.5 / Alto

Programa o modulo afectado: VTiger CRM v. 5.2.1

Descripción: Vulnerabilidad del Módulo VTiger CRM basada en técnica de inyección SQL, por medio de la cual se inyecta código malicioso. Esta vulnerabilidad permite al atacante ejecutar código SQL y HTML, hecho el cual permite eludir restricciones de seguridad y manipular datos exponiendo al sistema a un daño general.

Solución 1: VTiger CRM es un módulo con acceso y administración web, que permite implementar un sistema de relación y registro de clientes, automatizar las ventas que ofrezca una compañía, gestiona inventarios, analiza informes y se puede integrar con diversas herramientas como lo son los clientes de correo electrónico; como solución inicial se debe eliminar el directorio VTiger CRM, que se encuentra en la ruta "/var/www/html". Se recomienda eliminar como primera instancia, justificando, que dicha herramienta no es de uso, ni importancia para el funcionamiento normal de la telefonía IP de la empresa Creamigo Motul S.A.

Solución 2: Actualizar y/o migrar el módulo VTiger CRM a una versión superior (6.4.0) de manera manual.

Solución 3: Otro aspecto a tener en cuenta es que esta vulnerabilidad se aprovecha de los puertos 80 o 443, por los mencionados, se accede y se realiza la inyección SQL, para evitar esto, se debe configurar un nuevo usuario Apache que valide y autorice el acceso web al módulo de Elastix solicitando nombre de usuario y contraseña. No obstante se recomienda cambiar, los puertos por defecto de acceso web o servidor Apache.

Solución 4: Aplicar parche de seguridad **VtigerCRM540_Security_Patch.zip** el cual se podrá descargar de la página oficial de VTiger CRM, esto con el fin de resolver el bug en el módulo.

5.4 Vulnerabilidad: vtiger CRM 'onlyforuser' Parameter SQL Injection Vulnerability

ID: 4

Escáner: OPENVAS.

Impacto: 7.5 / Alto

Programa o modulo afectado: VTiger CRM v. 5.2.1

Descripción: Vulnerabilidad del Módulo VTiger CRM basada en técnica de inyección SQL, por medio de la cual se inyecta código malicioso. Esta vulnerabilidad permite al atacante ejecutar código SQL y HTML, hecho el cual permite eludir restricciones de seguridad y manipular datos exponiendo al sistema a un daño general.

Solución 1: VTiger CRM es un módulo con acceso y administración web, que permite implementar un sistema de relación y registro de clientes, automatizar las ventas que ofrezca una compañía, gestiona inventarios, analiza informes y se puede integrar con diversas herramientas como lo son los clientes de correo electrónico; se recomienda eliminar el directorio VTiger CRM, que se encuentra en la ruta "/var/www/html". Se recomienda eliminar como primera instancia, justificando, que dicha herramienta no es de uso, ni importancia para el funcionamiento normal de la telefonía IP de la empresa Creamigo Motul S.A.

Solución 2: Actualizar y/o migrar el módulo VTiger CRM a una versión superior (6.4.0) de manera manual.

Solución 3: Otro aspecto a tener en cuenta es que esta vulnerabilidad se aprovecha de los puertos 80 o 443, por los mencionados, se accede y se realiza la inyección SQL, para evitar esto, se debe configurar un nuevo usuario Apache que valide y autorice el acceso web al módulo de Elastix solicitando nombre de usuario y contraseña. No obstante se recomienda cambiar, los puertos por defecto de acceso web o servidor Apache.

5.5 Vulnerabilidad: vtiger CRM 'class.phpmailer.php' Remote Code Execution Vulnerability

ID: 5

Escáner: OPENVAS.

Impacto: 7.5 / Alto

Programa o modulo afectado: VTiger CRM v. 5.2.1

Descripción: vulnerabilidad del Módulo VTiger CRM basada en tecnica de inyeccion SQL la cual ataca los archivos 'class.phpmailer.php

Solución 1: VTiger CRM es un módulo con acceso y administración web, que permite implementar un sistema de relación y registro de clientes, automatizar las ventas que ofrezca una compañía, gestiona inventarios, analiza informes y se puede integrar con diversas herramientas como lo son los clientes de correo electrónico; se recomienda eliminar el directorio VTiger CRM, que se encuentra en la ruta "/var/www/html". Se recomienda eliminar como primera instancia, justificando, que dicha herramienta no es de uso, ni importancia para el funcionamiento normal de la telefonía IP de la empresa Creamigo Motul S.A.

Solución 2: Actualizar y/o migrar el módulo VTiger CRM a una versión superior (6.4.0) de manera manual.

Solución 3: Otro aspecto a tener en cuenta es que esta vulnerabilidad se aprovecha de los puertos 80 o 443, por los mencionados, se accede y se realiza la inyección SQL, para evitar esto, se debe configurar un nuevo usuario Apache que valide y autorice el acceso web al módulo de Elastix solicitando nombre de usuario y contraseña. No obstante se recomienda cambiar, los puertos por defecto de acceso web o servidor Apache.

Solución 4: Modificar las líneas 393 y 395 por las siguientes líneas de código:

Fig. 31. Solución 4 vulnerabilidad ID 5.

```
393: $ sendmail = sprintf ("% s -oi -f% s -t",
escapeshellcmd ($ this-> Sendmail), escapeshellarg ($ this-> Sender));
395: $ sendmail = sprintf ("% s -oi -t", escapeshellcmd ($ this-> Sendmail));
```

Fuente: El Autor.

5.6 Vulnerabilidad: Unix Operating System Unsupported Version Detection

ID: 27

Escáner: NESSUS.

Impacto: 10.0 / Alto

Programa o modulo afectado: CentOS 5.6

Descripción: Esta vulnerabilidad es por falta de soporte a la versión de Linux Centos.

Solución 1: Actualizar por completo el Sistema Operativo Linux CentOS 5.6 a CentOS 7.

6. RECOMENDACIONES

- Mantener el Sistema Operativo actualizado, para ello establecer y/o implementar un proceso de mantenimiento lógico con el fin de identificar mejoras por parte del proveedor.

- Mantener actualizadas las aplicaciones o componentes de terceros que interactúan en la plataforma operativa.

- Configurar y revisar regularmente las políticas y/o reglas establecidas en el sistema firewall del sistema operativo.

- Cambiar todas las configuraciones que vengan por defecto o predeterminadas en un sistema operativo, como es el caso de los puertos de acceso, SSH, HTTP, SSL, entre otros como también contraseñas de usuario por default en el sistema.

- Deshabilitar los permisos y la activación de uso del usuario ROOT en un sistema operativo.

- ¡Lo que no se usa, se desecha! Eliminar o deshabilitar todo software, componente o aplicativo que se encuentre activo en el sistema pero que no cumple con ninguna función ni soluciona una necesidad.

- Habilitar controles de acceso y seguridad a servicios primordiales dentro del sistema operativo, como es el caso de habilitar un usuario Apache antes de acceder a la GUI de administración de Elastix.

- Revisar y definir los permisos de los usuarios creados en el sistema como también someter a los usuarios a realizar cambios de contraseñas de alta seguridad y de manera periódica.

- Revisar o definir las políticas de seguridad de la información de la empresa con el fin de garantizar la calidad y seguridad de la operatividad del servicio de telefonía IP mediado por Asterisk.

7. CONCLUSIONES

Se logra satisfactoriamente realizar un proceso practico de Ethical Hacking o Pentesting con objetivos educativos y con la misión de identificar vulnerabilidades en el sistema de telefonía IP de la empresa Creamigo Motul S.A., sistema el cual opera bajo Asterisk; este proceso entrega resultados los cuales se abordaron y posteriormente se le dio tratamiento, concluyendo y recomendando una serie de pautas que de seguro permitirán que el sistema sea mucho más robusto ante las amenazas a las que se exponen actualmente.

La seguridad informática debe ser vista hoy por hoy como un tema de fuerza mayor, puesto que es este el componente que garantiza la disponibilidad, la integridad y confidencialidad de la información de una empresa u organización.

El contar con un sistema flexible como lo es Asterisk también requiere de llevar a cabo una serie de controles y procedimientos que ayudan a que este sistema sea más confiable y seguro, minimizando en un gran porcentaje riegos de ataques por parte de terceros o fallas operativas.

Revisar de manera completa el sistema con un chequeo regulado o periódico son buenas prácticas que permitirán identificar con facilidad el estado del sistema, razón el cual permitirá actuar en el momento preciso y evita vulnerabilidades.

Conocer la estructura del sistema de comunicaciones Asterisk permite identificar de qué manera opera el mismo, factor que evitará que se tenga en operatividad componentes innecesarios que pueden comprometer el sistema.

BIBLIOGRAFÍA Y REFERENCIAS

GÓMEZ, F. L., & Andrés, Á. A. (2012). Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes. España: AENOR - Asociación Española de Normalización y Certificación. {En línea}. {Febrero de 2017} disponible en: (http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=1&docID=10637105&tm=1456691803193)

CANALES, E (1996). Metodología de la investigación. México: Uteha/ NORIEGA.CASTAÑEDA, J. (1995). Métodos de investigación" México: McGrawHill. Castañeda, J. (1996). Métodos de investigación II. México: McGraw-Hill.

C. T. Ester, (2014, Jul). Gestión de incidentes de seguridad informática, IC Editorial. {En línea}. {16 de febrero de 2017} disponible en: (http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/detail.action?docID=11126339)

OREBAUGH, Angela. RAMIREZ Gilbert. BEALE, Jay. (2007), Wireshark & Ethereal Network Protocol Analyzer Toolkit, Published By Syngrees Publishing, Inc.

DOUPÉ, Adam. COVA, Marco. VIGNA, Giovanni. (2010), Why Johnny Can't Pentest: An Analysis of Black-Box Web Vulnerability Scanners, Notes in Computer Science, vol 6201.

ZURITA SÁNCHEZ, Juan Manuel. La ética del hacker y el espíritu de la era de la información, 2002, {En línea}. {16 de febrero de 2017} disponible en: (http://eprints.rclis.org/12851/)

BEALE, Jay. DERAISON, Renaud. MEER, Haroon. TEMMINGH, Roelof. VAN DER WALT, Charl. Nessus Network Auditing, (2004), Syngress Publishing 2004.

MORANT, J. L. Seguridad y protección de la información, Editorial Universitaria Ramón Areces, 1994.

R. Vivek, BackTrack 5 Wireless Penetration Testing Beginner's Guide. 7 ed. United Kingdom: Packt Publishing Ltd, 2011. 220 p. ISBN 978-1-849515-580.
S. Mcclure, J. Scambray, J. Kurtz, Hacking exposed: network security secrets & solutions. 7 ed. United States of America: Osborne/McGraw-Hill, 2012. 768 p. ISBN 978-0071780285.

IANA, {En línea}. {16 de febrero 2017} disponible en: (https://www.iana.org)

SANS, Institute. Security Issues and countermeasure for VoIP. (2007) {En línea}. {18 de febrero de 2017} disponible en: (https://www.sans.org/reading-room/whitepapers/voip/security-issues-countermeasure-voip-1701)

EL TIEMPO. QUÉ ES EL CONPES - Archivo Digital de Noticias de Colombia y el Mundo desde 1.990 - eltiempo.com {En línea}. {18 de febrero de 2017} disponible en: (http://www.eltiempo.com/archivo/documento/MAM-221821)

NETWORK WORLD. ¿Es lo suficientemente segura la telefonía IP? | Seguridad | NetworkWorld {En línea}. {8 de marzo de 2017} disponible en: (http://www.networkworld.es/seguridad/es-lo-suficientemente-segura-la-telefonia-ip)

L, C. María José, SEGURIDAD EN VOZ SOBRE IP, (2007) {En línea}. {8 de marzo de 2017} disponible en: (http://www.telematica.utfsm.cl/telematica/site/artic/20121011/asocfile/20121011110145/liberonamaria.pdf)

MINTIC. Ley 1273 de 2009. {En línea}. {18 de febrero de 2017} disponible en: (http://www.mintic.gov.co/portal/604/w3-article-3705.html.)

VOZTOVOICE. Asterisk 1.6 - empezando a experimentar sip-tls. {En línea}. {8 de marzo de 2017} disponible en: (www.voztovoice.org/?q=node/173)

SAMPIERI, Roberto. COLLADO, Carlos Fernández. BAPTISTA LUCIO, Pilar. Metodología de la investigación. Editorial Presencia Ltda. Bogotá Colombia 1991.

BURGA GUEVARA, Dina. Guía para formular proyectos de investigación e innovación tecnológica (2) {En línea}. {marzo de 2017} disponible en: (https://www.academia.edu/15434288/Gu%C3%ADa_para_formular_prroyectos_de_investigaci%C3%B3n_e_innovaci%C3%B3n_tecnol%C3%B3gica_).

SOBARZO ARTEAGA, Ana. Formulación de Presupuesto y Cronograma en un proyecto. {En línea}. {31 de marzo de 2017} disponible en: (http://bvsper.paho.org/videosdigitales/matedu/2012investigacionsalud/20120627CronogramaPresupuesto_AnaSobarzo.pdf?ua=1)

TORRES, Carrión. HERNÁN Leonardo. BASTIDAS, Moncayo. GONZÁLEZ

GONZÁLEZ, César Augusto. MARIANA, Carmen. Análisis de vulnerabilidades físicas y lógicas de los servidores de la unidad de telecomunicaciones e información de la Universidad Nacional de Loja y construcción de un plan de mitigación de riesgos. (2013), {En línea}. {8 de abril de 2017} disponible en: (http://dspace.unl.edu.ec/jspui/handle/123456789/14271.)

HOWLETT, Tony. Open Source Security Tools Practical Applications for Security, 2002, Prentice Hall.

WILHELM, Thomas. Professional Penetration Testing: Creating and Operating a Formal Hacking Lab, (2009), Syngress Publishing.

NEGUS, Christopher. BORONCZYK, Timothy. CentOS Bible 1st, Wiley Publishing 2009.

GIL, Roberto Gutiérrez. Seguridad en VoIP: Ataques, Amenazas y Riesgos. {En línea}. {abril 2017} disponible en: (http://www.it-docs.net/ddata/896.pdf)

ELASTIX.ORG. Elastix - Your Linux PBX Unified Communications Solution. {En línea}. {12 de mayo de 2017} disponible en: (https://www.elastix.org/)

VÁSQUEZ COSTALES, Pamela. Análisis del protocolo SSL y su aplicación en el aseguramiento de tráfico de VoIP frente a los ataques de Eavesdropping - See more at: {En línea}. {mayo de 2017} disponible en: (http://dspace.espoch.edu.ec/handle/123456789/4030#sthash.RnHkvsdr.dpuf)

COUNTERPATH. eyeBeam 1.5 VoIP Calling Software & Multimedia Communicator | CounterPath {En línea}. {5 de mayo de 2017} disponible en: (http://www.counterpath.com/eyebeam/)

SANTOS, Gustavo Vega. Asterisk - The Open Source PBX Telefonía IP mediante Asterisk PBX, (2008), {En línea}. {12 de mayo de 2017} disponible en: (http://tesis.blanque.com.ar/tesis/Home_files/Tesis_Gustavo_Vega.pdf.)

SERVITUX-VOIP. Softphone Zoiper y Línea VoIP - Servitux® VoIP {En línea}. {13 de mayo de 2017} disponible en: (https://www.servitux-voip.com/2013/05/09/softphone-zoiper-classic-sip-e-iax-y-linea-ip.)

MALDONADO RUIZ, Daniel Alejandro. Diseño e implementación de una red de

telefonía IP mediante Asterisk, con función de Voicemail y transferencia de llamadas y desarrollo de políticas de seguridad y manual de usuario del sistema para SACMIS Cía. Ltda, (2012), QUITO/EPN/2012, {En línea}. {6 de mayo de 2017} disponible en: (http://bibdigital.epn.edu.ec/bitstream/15000/4725/1/CD-4359.pdf.)

SOLÍS SOLÍS, Luis Alberto. CASICANA APUPALÓ, Sandra Verónica. VPN (Red privada virtual) usando software libre para disminuir los ataques Eavesdropping en la red de comunicación Voip en la Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato, Universidad Técnica de Ambato. Facultad de Ingeniería en Sistemas, Electrónica e Industrial. Carrera Ingeniería en Sistemas Informáticos y Computacionales, 2013, {En línea}. {mayo de 2017} disponible en:(http://repositorio.uta.edu.ec/bitstream/123456789/4950/1/Seminario_t817si.pdf)

CHÁVEZ ZAPATA, Jorge Polivio. Simulación y análisis de mecanismos de defensa ante los ataques de denegación de servicios (DoS) en redes de área local convergente, quito/epn/2011, {En línea}. {26 de mayo de 2017} disponible en: (http://bibdigital.epn.edu.ec/bitstream/15000/4282/1/CD-3905.pdf.)

ELASTIXTECH. Troncales y Rutas en Elastix | ElastixTech - Aprende Telefonía IP Asterisk - Elastix. {En línea}. {26 de mayo de 2017} disponible en: (http://elastixtech.com/troncales-y-rutas-en-elastix/.)

CONPES 3854 de 2016, CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL REPÚBLICA DE COLOMBIA DEPARTAMENTO NACIONAL DE PLANEACIÓN “La Política Nacional De Seguridad Digital”.

ESCRIVÁ GASCÓ, Gema. ROMERO SERRANO, Rosa Mª. RAMADA, David Jorge. ONRUBIA PÉREZ, Ramón. (2013), Seguridad Informática, GRUPO MACMILLAN, Madrid España.

COSTAS SANTOS, Jesús. (2011), Seguridad y Alta Disponibilidad, RA-MA, S.A. Editorial y Publicaciones, Madrid España.

GÓMEZ VIEITES, Álvaro. (2014), Seguridad en Equipos Informáticos, RA-MA, S.A. Editorial y Publicaciones, Madrid España.

ROA, José Fabián. (2013), Seguridad Informática, McGraw-Hill/Interamericana de España, S. L.

ORTIZ DÍAZ, Efrain. GUILLÉN CHALEN, William. (2011), Diseño de un Sistema de Voz Sobre IP (voip) para la EMPRESA SEDENTI LTDA, Universidad Tecnológica

de Bolívar facultad de Ingenierías dirección de programas de ingeniería eléctrica y electrónica, {En línea}. {27 de mayo de 2017} disponible en: (http://biblioteca.unitecnologica.edu.co/notas/tesis/0062296.pdf)

DIMAS A., Yanneth. MORALES S., Luis Carlos, (2009), ANALISIS DE REQUERIMEINTO E IMPLEMENTACIÓN DE LA PLATAFORMA ASTERISK UTILIZANDO ESTANDAR H.323/IAX2, {En línea}. {2 de agosto de 2017} disponible en:
(www.konradlorenz.edu.co/images/stories/articulos/Asterisk.pdf)

OSPINA, Walter, (2015), Creamigo - Creamigo es..., {En línea}. {febrero de 2017} disponible en:
(http://www.creamigo.com/creamigo-es)

TELEFONIA VOZIP. Protocolos en la Telefonía IP, Protocolos VoIP {En línea}. {13 de marzo de 2017} disponible en: (http://www.telefoniavozip.com/voip/protocolos-en-la-telefonia-ip.htm)

ELASTIXTECH. Protocolo IAX | ElastixTech - Aprende Telefonía IP Asterisk - Elastix, {En línea}. {13 de marzo de 2017} disponible en: (http://elastixtech.com/protocolo-iax/)

ELASTIXTECH. Características de Elastix | ElastixTech - Aprende Telefonía IP Asterisk - Elastix, {En línea}. {2 de agosto de 2017} disponible en: (http://elastixtech.com/curso-basico-de-elastix/caracteristicas-de-elastix/)

SERVITUX. Softphone Zoiper y Línea VoIP - Servitux® VoIP, {En línea}. {2 de agosto de 2017} disponible en: (https://www.servitux-voip.com/2013/05/09/softphone-zoiper-classic-sip-e-iax-y-linea-ip/)

TELEFACIL. X-Lite - Softphone VoIP Telefacil, {En línea}. {2 de agosto de 2017} disponible en:
(https://www.telefacil.com/wiki/index.php/X-Lite)

ELASTIXTECH. Troncales y Rutas en Elastix | ElastixTech - Aprende Telefonía IP Asterisk - Elastix, {En línea}. {27 de mayo de 2017} disponible en: (http://elastixtech.com/troncales-y-rutas-en-elastix/)

GORKA, Gorrotxategi. Curso Asterisk Voz IP 1-Introduccion-sip, {En línea}. {31 de agosto de 2017} disponible en: (https://es.slideshare.net/edgarjgonzalezg/curso-asterisk-voz-ip-1introduccionsip)

ANEXOS

Anexo A. Solicitud Autorización desarrollo del proyecto.

Santiago de Cali, 21 de Marzo de 2017.

Ing. Oscar Castaño Tangarife.
Jefe Administrativo.
Creamigo Motul S.A.
La ciudad.

Asunto: Solicitud autorización desarrollo de proyecto aplicado "Medición de la seguridad de la telefonía Ip Asterisk".

Mediante la presente, como actual estudiante de la Universidad Nacional Abierta y a Distancia – UNAD, del programa de especialización Seguridad Informática, solicito de manera muy respetuosa yo Jorge Iván Mosquera Palacios identificado con número de cedula 1.130.659.879 de Cali – Valle, Ingeniero de Soporte Servicios Telemáticos de la empresa Creamigo Motul S.A. y César Augusto Mejía Osorio identificado con número de cedula 8.105.269 de Sabaneta – Antioquia, compañero de estudio de la especialización en mención, se nos autorice la ejecución y aplicabilidad del desarrollo de la propuesta de Grado para optar por el título de Especialista en Seguridad Informática, dicha propuesta o proyecto de grado tiene como objetivo principal Medir la Seguridad del servidor de Telefonía IP Asterisk el cual interactúa en la empresa y suple las necesidades de comunicación telefónica entre las sedes y de la misma manera la comunicación a nivel nacional e internacional, esto con el fin de aplicar los conocimientos adquiridos a lo largo de la especialización y además contribuir en aspectos de seguridad y calidad a los servicios en mención propios de la empresa.

Para el desarrollo de este proyecto es necesario realizar una imagen o copia de todo el servidor de telefonía IP Asterisk como también levantar información técnica del mismo, para realizar los procesos técnicos y de seguridad sin poner en riesgo el estado del servidor físico y demás servicios de la empresa, para ello se tiene en cuenta la siguiente **Cláusula de confidencialidad:** el presente proyecto aplicado "**Medición de la seguridad de la telefonía Ip Asterisk**" solo será con fines académicos, los datos y mediciones recolectados, serán de conocimiento de la Universidad Nacional a Distancia "UNAD" con fines evaluativos para alcanzar el grado de Profesionales Especializados en Seguridad Informática. El producto final resultante del proyecto aplicado, será entregado a CREAMIGO Motul con el fin de contextualizar los hallazgos y mejoras en aras de optimizar la seguridad del servidor Ip Asterisk.

No siendo más agradezco la atención brindada y espero se haga efectiva mi solicitud en el menor tiempo posible.

Me despido deseándole éxitos en sus labores

Atentamente.

JORGE IVAN MOSQUERA PALACIOS.
Ing. Informático
Soporte Telemático Creamigo Motul.
Cali – Valle.

Contacto:
Cel: 312 750 24 67
Email: ivannetce@hotmail.com
Skype: iv3041

Anexo B. Aceptación solicitud de autorización para el desarrollo del proyecto.

Creamigo MOTUL

Santiago de Cali, 30 de Marzo de 2017.

Ing. Jorge Iván Mosquera Palacios.
Ingeniero Soporte Telemático.
Creamigo Motul S.A.
La ciudad.

Asunto: Respuesta solicitud autorización desarrollo de proyecto aplicado presentada el día 21 de marzo de 2017.

El pasado viernes 24 de marzo del presente año, se socializó con el Gerente General Walter Ospina, la solicitud presentada por usted para el desarrollo y aplicación del proyecto educativo universitario **"Medición de la seguridad de la telefonía Ip Asterisk bajo técnicas de Pentesting"** el cual usted y su compañero de estudio sustentaron con claridad, y se llegó a la conclusión de **conceder la autorización** de dicha solicitud durante el tiempo de ejecución y desarrollo del mismo, con la única sugerencia, de mantenerme informado con antelación de cada uno de los procesos que se requieran para llevar a cabo la aplicación del proyecto y dejando claro que los recursos que se requieran en el mismo deberán ser adquiridos por los propios medios de quienes presentan la propuesta.

Finalmente, damos vía libre para que realicen las prácticas que conllevan al levantamiento de la información necesaria.

Por lo anterior se da la aceptación de la solicitud presentada y deseándoles éxitos en el desarrollo óptimo del mismo.

Atentamente,

Oscar Castaño Tangarife.
Jefe Administrativo.
Creamigo Motul.
Cali – Valle.

Comercializadora de Importados Los Amigos S.A.
NIT. 800.187.910-2
Carrera 1A # 47 – 51
PBX: +57 (2) 410 00 10
info@creamigo.com
creamigo.com
Cali - Colombia

Anexo C. Acta de capacitación Telefonía IP Asterisk.

Santiago de Cali, 3 de Octubre de 2017.

Ing. Oscar Castaño Tangarife.
Jefe Administrativo.
Creamigo Motul S.A.
La ciudad

Asunto: Capacitación Sistema de Telefonía IP Asterisk.

A las 8:30 am del presente día se realiza la capacitación y explicación de los temas relacionados a la Telefonía IP Asterisk:

- Telefonía convencional Vs. IP Asterisk.
- ¿Qué es Asterisk?
- Recursos.
- Beneficios y desventajas.
- Costos de la telefonía IP vs Telefonía convencional.
- Configuración básica Softphone
- Configuración básica Teléfono IP.
- Seguridad.

En la presente capacitación se impartieron conceptos básicos en torno a la telefonía VoIP basada en Asterisk, el personal asistente demostró gran empatía y acogida a este producto, debido que han notado las múltiples ventajas y/o beneficios de tener este tipo de servicios a favor de la empresa CREAMIGO MOTUL.

Siendo las 10 am, se da por terminada la capacitación, agradeciendo al Ingeniero Jorge Iván Mosquera Palacios, en darnos a conocer de manera más detallada lo relacionado al producto Asterisk.

Anexo. Listado de personal asistente a la capacitación.

Atentamente,

JORGE IVÁN MOSQUERA PALACIOS.
Ing. Informático
Soporte Telemático Creamigo Motul.
Cali – Valle.

Contacto:
Cel. 312 750 24 67
Email: ivannetce@hotmail.com
Skype: iv3041

Fecha: 03 de Octubre de 2017
Hora:
Objetivo: Explicar la funcionalidad y aspectos relacionados con la Telefonía IP mediado por Asterisk.
Responsable: Jorge Iván Mosquera Palacios.

N°	NOMBRE COMPLETO	CARGO	FIRMA
1	Lina Figueroa Velásquez	Asistente Gerencia	
2	Elizabeth Grisales	Jefe de Contabilidad	
3	Oscar Castaño Tangarife	Jefe Administrativo	
4	Vanessa Usuga	Recepción	
5	Jhonatan Ospina	Jefe Servicio	
6	Cristian Ospina	Supervisor Técnico	
7	Angela María Imbachi	Aux. Contable	
8	Larry Fabian Bedoya	Pagador	
9	Lenher Belalcazar	Gerente Comercial	
10	Walter Romero	Jefe Producción	
11			
12			
13			
14			
15			
16			
17			
18			
19			

Anexo D. Divulgación del proyecto.

INFORME EJECUTIVO Y DESARROLLO TÉCNICO

NOMBRE DEL PROYECTO: MEDICIÓN DE LA SEGURIDAD DE LA TELEFONÍA IP ASTERISK EN CREAMIGO MOTUL BAJO TÉCNICAS DE PENTESTING.

FECHA: 11 de diciembre de 2017.

ELABORADO POR: Jorge Iván Mosquera Palacios.

Cesar Augusto Mejía Osorio.

Introducción:

Creamigo es una Sociedad Anónima cuya denominación social es COMERCIALIZADORA DE IMPORTADOS LOS AMIGOS S.A. Sigla CREAMIGO S.A, bajo NIT. 800187910 - 2, es una empresa Caleña con 22 Años de tradición y experiencia en el sector automotriz y de autopartes. Inició en 1993, importando repuestos para motores de Gasolina y Diésel.

Desde hace 10 años se solidifica en una alianza estratégica con MOTUL, empresa francesa global que fabrica, desarrolla y distribuye lubricantes para motores (motos, coches y otros vehículos) y para la industria de alto rendimiento desde hace 160 años.

Importando sus lubricantes a los departamentos colombianos del Valle, Cauca, Nariño, Huila, Cauca, Caldas, Risaralda, Quindío, Caquetá y Putumayo. [1]

En la actualidad, la empresa cuenta con un Servidor Gigabyte Thermaltake de 5ta Generación, el cual es el núcleo de las comunicaciones VozIP, este brinda los servicios de telefonía IP mediado por Asterisk sobre plataforma operativa Linux

[1] http://www.creamigo.com/creamigo-es

Centos 5.6, cuenta con un total de 33 usuarios tanto locales como remotos y 5 troncales digitales para el procesamiento de las llamadas a la red PSTN a distancia Local, Nacional, Celular e Internacional. En el mismo, opera la sede Principal ubicada en la ciudad de Santiago de Cali, como también de las sucursales ubicadas en la misma ciudad como también en Yumbo, Neiva y Pasto.

El planteamiento de la propuesta de Proyecto de Grado, surge de la necesidad de poner en práctica los conocimientos aprendidos hasta el momento relacionándolos con las experiencias vividas donde el propósito es solucionar y/o mitigar problemas del entorno en cuanto a aspectos de la seguridad informática se refiere.

El impulso a seleccionar el proyecto de grado como tipo aplicado, radica en la aplicación de conocimientos y prácticas que contribuyan en la solución de problemas focalizados en una organización; Creamigo Motul S.A. es la organización que dio viabilidad en la gestión y desarrollo de esta propuesta, permitiendo iniciar con un esquema de trabajo, la cual se focaliza en el sistema de telefonía IP - Asterisk, tema que es de gran interés por parte de los autores, el proceso del levantamiento de la información, identificación de problemas y demás aspectos que se relacionan directamente con el sistema en mención.

Finalmente en la estructuración de esta idea de proyecto se logra entender y comprender a partir de la problemática planteada el objetivo del mismo con el fin de satisfacer las dos partes, por un lado y principalmente la empresa previamente mencionada, puesto que se solventará en aspectos que a seguridad informática se refiere y están ligados al sistema de telefonía IP - Asterisk y por el otro lado los autores de la propuesta de proyecto puesto que podrán afianzar sus conocimientos en la aplicación de los mismos obtenidos en el desarrollo de la especialización.

Descripción del proyecto:

ANTECEDENTES

En el momento de la presente investigación CREAMIGO MOTUL S.A no cuenta con una estructura de seguridad informática que proteja ante fraudes o posibles ataques al servidor de telefonía IP Asterisk, hecho que es riesgoso a nivel de seguridad informática, debido que no cuenta con un sistema de seguridad a nivel lógico, que garantice la estabilidad e integridad del servicio de telefonía IP.

En la actualidad no es indiferente saber acerca de los múltiples riesgos que se corren con servicios telemáticos, y ante un servidor de Voz sobre IP no hay excepción, a mediados del año 2016 el servidor Asterisk de la empresa Creamigo Motul S.A. sufrió una falla de seguridad por mala configuración en el servicio de Apache, permitiendo el acceso de un individuo sin autorización alguna, secuestrando troncales y generando miles de llamadas a destinos internacionales, todo a causa de inseguridad o medidas de seguridad mal configuradas, por tal razón es de vital importancia contar con mecanismos y políticas que garanticen la integridad de Información de la organización. Por tales razones es primordial que la empresa Creamigo Motul S.A. permita evaluar la seguridad informática tanto en aspectos hardware como software del Servidor de Telefonía IP – Asterisk, mediante la práctica de Penetration Testing para determinar la efectividad de las medidas que posiblemente en la actualidad este tenga implementadas y de la misma manera identificar vulnerabilidades y/o fallos de seguridad que pongan en riesgo la información de la empresa, proceso que permitirá establecer nuevos métodos y políticas de seguridad a partir de los resultados obtenidos y contar con mecanismos de detección, identificación y defensa que permitan minimizar los riesgos ante posibles ataques o amenazas a los que se expone la empresa con su servidor de telefonía IP.

DESCRIPCIÓN DEL PROBLEMA

Formulación del problema:

¿Cuáles son las herramientas lógicas de seguridad informática garantes de la integridad de la información del servidor de telefonía IP-Asterisk de Creamigo Motul S.A. y de su protección ante posibles ataques informáticos?

OBJETIVOS

Objetivo general:

- Identificar los mecanismos apropiados de seguridad informática garantes de la integridad de la información y del servidor de telefonía IP-Asterisk de Creamigo Motul S.A. protegiéndolo ante posibles amenazas informáticas.

Objetivos específicos:

- Explicar la funcionalidad y aspectos relacionados con la Telefonía IP mediado por Asterisk.

- Examinar las posibles amenazas informáticas a las que está expuesto el servidor de telefonía IP Asterisk de la empresa Creamigo Motul S.A.

- Determinar las herramientas de Pentesting idóneas para minimizar los riesgos de seguridad a los que se expone el servidor de telefonía IP de la empresa Creamigo Motul S.A.

Logros alcanzados

Tabla 1. Logros alcanzados.

ACTIVIDAD	FASE 1 24 AGO 6 SEP		FASE 2 7 SEP 4 OCT		FASE 3 5 OCT 29 NOV		FASE 4 30 NOV 13 DIC	
	¿SE EJECUTO ACTIVIDAD?							
	SI	NO	SI	NO	SI	NO	SI	NO
Consolidación y presentación final de la propuesta de trabajo de Grado.	X							
Creación de imagen del Servidor de Telefonía IP Asterisk de la Empresa Creamigo Motul S.A.	X							
Explicar la funcionalidad y aspectos relacionados con la Telefonía IP mediado por Asterisk.			X					
Realizar capacitación acerca de la funcionalidad de Asterisk como sistema de telefonía IP al personal administrativo y usuarios del Sistema de Telefonía Asterisk de la empresa Creamigo Motul S.A.			X					
Implementación del banco de trabajo virtual para el desarrollo de las pruebas de Pentesting.			X		X			
Examinar las posibles amenazas informáticas a las que está expuesto el servidor de telefonía IP Asterisk de la empresa Creamigo Motul S.A.					X			
Realizar un informe detallado de las posibles fallas, vulnerabilidades y amenazas a las que se expone un servidor de telefonía IP basado en Asterisk.					X			
Determinar las herramientas de Pentesting idóneas para minimizar los riesgos de seguridad a los que se expone el servidor de telefonía IP de la empresa Creamigo Motul S.A.					X			
Pruebas de Pentesting para la identificación de vulnerabilidades y amenazas del Servidor de Telefonía IP Asterisk de la empresa Creamigo Motul S.A.					X			
Análisis de los resultados obtenidos posterior a los procesos de Pentesting realizados al Servidor de Telefonía IP Asterisk de la empresa Creamigo Motul S.A.							X	
Conclusiones y recomendaciones.							X	
Crear y presentar un informe técnico y gerencial al Jefe Administrativo de la empresa Creamigo Motul S.A. sobre todo el proceso realizado, los resultados obtenidos y las recomendaciones de seguridad propuestas para minimizar los riesgos encontrados en el Servidor de Telefonía IP Asterisk.							X	

Fuente: El Autor

Resumen técnico del desarrollo del proyecto

Para el desarrollo del Pentesting sobre el servidor Asterisk de la empresa Creamigo Motul S.A, se determinó por el equipo de estudiantes de especialización en seguridad informática, el uso de un ambiente controlado en el cual se pudiera desarrollar la actividad de búsqueda de vulnerabilidades, sin que el ambiente de producción se viera afectado.

Para dar inicio a esto, se solicitó una copia de la configuración del servidor Elastix de Creamigo Motul S.A, con esta copia procedimos restaurarla y realizar la instalación de todo el Elastix en un ambiente virtualizado, el cual emula el funcionamiento en su totalidad de cada una de las características del servidor real de PBX que ustedes poseen.

Luego de tener este ambiente de pruebas virtualizado en operación, procedimos a utilizar herramientas especializadas en seguridad informática, que realizaron escaneo en varios niveles, donde se revisa la integridad de cada uno de los sistemas y servicios que poseen instalados en el entorno del servidor Elastix.

Luego de terminar la parte de escaneo, se obtienen reportes que ayudan la identificación de vulnerabilidades, las cuales son medidas en escala baja, media y alta. La obtención de estas vulnerabilidades ayuda a entender el estado actual que poseen los servicios que ofrece Elastix y como estos pueden impactar de manera crítica la disponibilidad, integridad e inalterabilidad de los servicios que se ofrecen en esta suite de PBX la cual su núcleo es basado en tecnología Asterisk.

Por las anteriores razones, se recomienda que la empresa Creamigo Motul S.A, tome en consideración las recomendaciones técnicas que hemos realizado, debido que no acatarlas podría nuevamente verse inmersos en futuros ataques que comprometerían la operatividad y continuidad del negocio de la compañía.

Dificultades presentadas

Llevar a cabo con éxito los procesos de explotación de algunas de las vulnerabilidades encontradas.

Recomendaciones

- Mantener el Sistema Operativo actualizado, para ello establecer y/o implementar un proceso de mantenimiento lógico con el fin de identificar mejoras por parte del proveedor.

- Mantener actualizadas las aplicaciones o componentes de terceros que interactúan en la plataforma operativa.

- Configurar y revisar regularmente las políticas y/o reglas establecidas en el sistema firewall del sistema operativo.

- Cambiar todas las configuraciones que vengan por defecto o predeterminadas en un sistema operativo, como es el caso de los puertos de acceso, SSH, HTTP, SSL, entre otros como también contraseñas de usuario por default en el sistema.

- Deshabilitar los permisos y la activación de uso del usuario ROOT en un sistema operativo.

- ¡Lo que no se usa, se desecha! Eliminar o deshabilitar todo software, componente o aplicativo que se encuentre activo en el sistema pero que no cumple con ninguna función ni soluciona una necesidad.

- Habilitar controles de acceso y seguridad a servicios primordiales dentro del sistema operativo, como es el caso de habilitar un usuario Apache antes de acceder a la GUI de administración de Elastix.

- Revisar y definir los permisos de los usuarios creados en el sistema como también someter a los usuarios a realizar cambios de contraseñas de alta seguridad y de manera periódica.

- Revisar o definir las políticas de seguridad de la información de la empresa con el fin de garantizar la calidad y seguridad de la operatividad del servicio de telefonía IP mediado por Asterisk.

Conclusiones

Se logra satisfactoriamente realizar un proceso practico de Ethical Hacking o Pentesting con objetivos educativos y con la misión de identificar vulnerabilidades en el sistema de telefonía IP de la empresa Creamigo Motul S.A., sistema el cual opera bajo Asterisk; este proceso entrega resultados los cuales se abordaron y posteriormente se le dio tratamiento, concluyendo y recomendando una serie de pautas que de seguro permitirán que el sistema sea mucho más robusto ante las amenazas a las que se exponen actualmente.

La seguridad informática debe ser vista hoy por hoy como un tema de fuerza mayor, puesto que es este el componente que garantiza la disponibilidad, la integridad y confidencialidad de la información de una empresa u organización.

El contar con un sistema flexible como lo es Asterisk también requiere de llevar a cabo una serie de controles y procedimientos que ayudan a que este sistema sea más confiable y seguro, minimizando en un gran porcentaje riegos de ataques por parte de terceros o fallas operativas.

Revisar de manera completa el sistema con un chequeo regulado o periódico son buenas prácticas que permitirán identificar con facilidad el estado del sistema, razón el cual permitirá actuar en el momento preciso y evita vulnerabilidades.

Conocer la estructura del sistema de comunicaciones Asterisk permite identificar de qué manera opera el mismo, factor que evitará que se tenga en operatividad componentes innecesarios que pueden comprometer el sistema.

Responsables:

JORGE IVÁN MOSQUERA PALACIOS CESAR AUGUSTO MEJÍA OSORIO

Estudiantes Especialización en Seguridad Informática.
UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD