ESCUELA SUPERIOR POLITECNICA DE CHIMBORAZO

FACULTAD DE INFORMATICA Y ELECTRONICA

ESCUELA DE INGENIERIA ELECTRONICA EN

TELECOMUNICACIONES Y REDES

"ANALISIS DE VULNERABILIDADES EN PROTOCOLOS UTILIZADOS EN CENTRALES VoIP CON IPv6 UTILIZANDO TRONCALES SIP"

TESIS DE GRADO

PREVIA A LA OBTENCION DEL TITULO DE

INGENIERO ELECTRONICO EN TELECOMUNICACIONES Y REDES

Presentado por:

JOSE SANTIAGO CACERES GUAYANLEMA

RIOBAMBA – ECUADOR

2014

Agradezco primeramente a Dios, por su amor y salvación que me brinda todos los días de mi vida.

A mi madre Blanca América quien supo ser mi madre y padre a la vez y guiarme a ser lo que soy, a mis hermanos Juan Fernando y María del Carmen por brindarme su apoyo, amor y quienes me alientan a seguir adelante.

A mis amigos y compañeros, quienes me brindan todo su apoyo.

A la Escuela Superior Politécnica de Chimborazo, por formarnos como profesionales competitivos, para servir a la sociedad de manera ética y profesional.

Esta tesis va dedicada a Dios, a mi familia y a todos aquellos quienes me brindaron su apoyo para culminar este paso importante en el transcurso de mi vida.

FIRMAS RESPONSABLES

	FIRMA	FECHA
ING. IVÁN MENES CAMEJO **DECANO FAC. INFORMATICA Y ELECTRÓNICA**	_____	_____
ING. WILSON BALDEON **DIRECTOR ESC. ING. ELECTRÓNICA EN TELECOMUNICACIONES Y REDES**	_____	_____
ING. LUIS MARCELO DONOSO **DIRECTOR DE TESIS**	_____	_____
ING. FRANKLIN MORENO **MIEMBRO DEL TRIBUNAL**	_____	_____
DIRECTOR CENTRO DOCUMENT.	_____	_____
NOTA DE TESIS	_____	

Yo, José Santiago Cáceres, declaro que soy el autor del trabajo de esta tesis “ANALISIS DE VULNERABILIDADES EN PROTOCOLOS UTILIZADOS EN CENTRALES VoIP CON IPv6 UTILIZANDO TRONCALES SIP” elaborado por mi persona bajo la dirección del Ing. Luis Marcelo Donoso Velasteguí, por tanto, asumo la responsabilidad de las ideas, doctrinas y resultados expuestas en esta Tesis, y el patrimonio intelectual de la Tesis de Grado pertenece a la Escuela Superior Politécnica de Chimborazo.

_____

José Santiago Cáceres Guayanlema

INDICE DE ABREVIATURAS

A

ACK: ACUSES DE MENSAJE RECIBIDO

ADSL: ASYMMETRIC DIGITAL SUBSCRIBER LINE – LÍNEA DE ABONADO DIGITAL ASIMÉTRICA

B

BBDD: DATA BASE - BASE DE DATOS

BW: BAND WITH - ANCHO DE BANDA.

C

CEH: CERTIFIED ETHICAL HACKER – HACKER ETICO CERTIFICADO

CLI: COMMAND LINE INTERFACE – INTERFAZ DE LÍNEA DE COMANDO

D

DNS: DOMAIN NAME SYSTEM – SISTEMA DE NOMBRE DE DOMINIO

DoS: DENIAL OF SERVICE – DENEGACION DE SERVICIO

G

GPL: GENERAL PUBLIC LICENSE – LICENCIA PUBLICA GENERAL

H

HTTP: HYPER TEXT TRANSFER PROTOCOL – PROTOCOLO DE TRANSFERENCIA HYPERTEXTO

HW: HARDWARE

I

IANA: INTERNET ASSIGNET NUMBERS AUTHORITY – AUTORIDAD DE NUMEROS ASIGNADOS A INTERNET

IETF: INTERNET ENGINEERING TASK FORCE – GRUPO DE TAREAS DE INGENIERIA INTERNET

INVITE: PETICION DEL CLIENTE PARA SESION DE LLAMADAS

IP: INTERNET PROTOCOL – PROTOCOLO DE INTERNET

ITU: INTERNATIONAL TELECOMMUNICATION UNION - UNION INTERNACIONAL DE TELECOMUNICACIONES

M

MAC: MEDIA ACCESS CONTROL ADDRESS – CONTROL DE ACCESO AL MEDIO

MD5: MESSAJE-DIGEST ALGORITHM 5

MITM: MAN IN THE MIDDLE – HOMBRE EN EL MEDIO

P

PC: COMPUTADOR PERSONAL

R

RFC: REQUEST FOR COMMENTS – SOLICITUD DE COMENTARIOS

RTP: REAL TIME PROTOCOL – PROTOCOLO DE TIEMPO REAL

S

SIP: SESSION INITIATION PROTOCOL – PROTOCOLO DE INICIO DE SESSION

SRTP: SECURE REAL TIME PROTOCOL – PROTOCOLO DE TIEMPO REAL SEGURO

SSL: SECURE SOCKETS LAYER – SEGURIDAD EN CAPA DE CONEXIÓN

SYN: ESTABLECIMIENTO CLIENTE SERVIDOR

SW: SOFTWARE

T

TCP: TRANSMISSION CONTROL PROTOCOL – PROTOCOLO DE CONTROL DE TRANSMISIONES

U

UAC: USER ACCOUNT CONTROL – AGENTE DE USUARIO DE CLIENTE

UAS: USER AGENT SERVER – AGENTE DE USUARIO DE SERVER

UDP: USER DATAGRAMA PROTOCOL – PROTOCOLO DE DATAGRAMA DE USUARIO

URL: UNIFORM RESOURCE LOCATOR - LOCALIZADOR UNIFORME DE RECURSOS

UTP: CABLE DE PAR TRENZADO

V

VLAN: VIRTUAL LAN – LAN VIRTUAL

INDICE GENERAL

INDICE DE FIGURAS

INDICE DE TABLAS

INTRODUCCION

Hoy en día, el internet es la herramienta más utilizada a nivel mundial y el aumento de aplicaciones a través de internet en el envío de voz video y datos han ayudado en el desarrollo de las telecomunicaciones.

La Voz sobre el protocolo de internet (VoIP) es muy evidente tal como Skype y una de las razones es aprovechar los recursos y disminución de costes a través de internet frente a la telefonía tradicional.

Sin embargo, estas redes se ven amenazadas frente a las vulnerabilidades en protocolos que un atacante pudiera escuchar, espiar los paquetes de voz que circulan a través de la red si no se toman las medidas necesarias para proteger estos protocolos.

En este proyecto se analizará las vulnerabilidades que se encuentran en la capa de seguridad en protocolos de VoIP como se describe en el libro “Seguridad VoIP: Ataques, amenazas y riegos” de Roberto Gutiérrez, utilizando como plataformas el software libre (GNU/LINUX) para el diseño topológico de pruebas de conectividad de centrales VoIP.

Una vez diseñado y convergido el ambiente de simulación, se realizará el estudio para las propuestas de seguridad a la capa de seguridad en protocolos, realizando ataques a la red VoIP con las herramientas del software Kali-Linux Backtrack y herramientas adicionales para posteriormente realizar el análisis de seguridad.

Este proyecto consta de cinco capítulos los cuales se detalla a continuación:

CAPÍTULO I: MARCO REFERENCIAL.- En este capítulo se expone el planteamiento del problema y justificación del proyecto; así también como los objetivos y el alcance que se plantea para desarrollar la investigación de este proyecto.

CAPITULO II: MARCO TEORICO.- En este capítulo se realiza la introducción de los temas generales necesarios relacionados a este proyecto y las características esenciales de los elementos para realizar su implementación y análisis de vulnerabilidades.

CAPITULO III: MARCO HIPOTETICO Y METODOLOGICO.- El principal objetivo de este capítulo es describir el proceso metodológico empleado, los procedimientos, métodos y técnicas que identifica resultados que ayuden a comprobar la hipótesis planteada a través de pruebas y resultados.

CAPITULO IV: ESCENARIOS Y PRUEBAS.- En este capítulo se describe el proceso de elaboración del escenario de pruebas para determinar las configuraciones de seguridad a implementar para evitar intercepciones de llamadas y proteger las comunicaciones encriptándolas.

CAPITULO V: ANALISIS Y RESULTADOS.- En este capítulo se muestran las pruebas de los ataques a la que fue sometida la central VoIP y sus resultados.

Finalmente se llega a describir las Conclusiones y Recomendaciones, se incluye las síntesis de los resultados obtenidos, presentados en los capítulos anteriores y sugerencias finales del proyecto.

CAPÍTULO I

MARCO REFERENCIAL

I.I PLANTEAMIENTO DEL PROBLEMA

La voz sobre IP (VoIP) es muy evidente actualmente y hace posible que la señal de voz viaje a través de internet empleando un protocolo IP; se conoce que el direccionamiento en IPv4 se ha agotado por lo que hay la necesidad de la implementación de las centrales VoIP con direccionamiento IPv6 entre las soluciones para el agotamiento de direcciones en IPv4.

Sin embargo, cuando se implementan centrales VoIP se da prioridad al funcionamiento del envío y recepción de voz y datos, calidad de servicio mas no en la seguridad; una central VoIP por defecto es vulnerable a secuestros de cuentas de usuarios y passwords, escuchas indebidas, vulnerabilidades que se encuentran en la capa de protocolos VoIP.

Un atacante puede crear métodos de penetración (Escaneo, obtención de acceso, manipulación de la central), si el sistema es vulnerable para sustraer información de las centrales VoIP que resulta perjudicial para la organización si la información es confidencial

Mediante este estudio se pretende proponer las medidas de seguridad necesarias para configurar en centrales VoIP con direccionamiento IPv6 utilizando troncales SIP, y de esta manera evitar que los ataques puedan penetrar al sistema, para ampliar el nivel de seguridad de dichas centrales.

I.II JUSTIFICACION

En estas redes de siguiente generación se requiere encontrar la tecnología que permita transmitir en una misma red la convergencia de voz y datos. Esto obliga a establecer un modelo que permita empaquetar la voz para que pueda ser transmitida junto con los datos, este propósito se logra con los protocolos de VoIP.

La mayor parte de las redes de transmisión de voz que existen en la actualidad serán reemplazadas por redes de conmutación de paquetes en un futuro. Esta transición supone no solo una reducción de los costos, si no que proporcionará también el desarrollo de una serie de servicios nuevos para voz y datos.

IPv6 ofrece una plataforma escalable y mejorada para la convergencia, además que incluye IPsec que permite autenticación y encriptación del propio protocolo base, de forma que todas las aplicaciones se pueden beneficiar de ello ofreciendo comunicaciones más seguras.

Por lo tanto es necesario probar la funcionalidad de las centrales VoIP y observar la eficiencia sobre el análisis de las vulnerabilidades en los protocolos de dichas centrales, con el fin de prevenir ataques a la organización y observar la eficiencia en la transmisión de paquetes de voz en tiempo real y evitar que las llamadas puedan ser escuchadas sin el permiso respectivo de los usuarios.

I.III OBJETIVOS

I.III.I OBJETIVO GENERAL

“Determinar las vulnerabilidades en protocolos utilizados en centrales de voz sobre IP (VoIP) con IPv6 utilizando troncales SIP, para de tal manera ofrecer medidas de seguridad a la red.”

I.III.II OBJETIVOS ESPECIFICOS

1 Estudiar los conceptos y características de VoIP, IPv6 y temas relacionados para una implementación técnica, para realización de pruebas.

2 Implementar un escenario topológico con equipos CISCO y centrales ASTERISK, y configurar los protocolos de VoIP con un esquema de direccionamiento Dual-Stack.

3 Analizar las vulnerabilidades de los protocolos a través de la utilización de las herramientas de Backtrack.

4 Configurar los tipos de seguridad para la prevención de vulnerabilidades en centrales de VoIP y dar posibles soluciones técnicas en software.

I.III ALCANCE DEL PROYECTO

En el presente trabajo se estudiaran las principales vulnerabilidades de la capa de seguridad de protocolos de VoIP en SIP ya que con este protocolo de señalización con frecuencia trabajan las centrales PBX Asterisk y que son víctimas de escuchas indebidas o ilegales.

Se realizará una descripción acerca de las vulnerabilidades en protocolos de la central VoIP en SIP y RTP en direccionamiento IPv6; y se analizara la seguridad mediante requerimientos tales como: Disponibilidad, Integridad y Confidencialidad.

Tales pruebas se efectuaran en un escenario propuesto físico, es decir, en un escenario sin seguridad y las mismas pruebas en un escenario con seguridad implementada.

Todo este estudio se llevará a cabo a través de investigaciones, consultas, pruebas y análisis de resultados con el fin de implementar una red VoIP segura mediante técnica de cifrado a protocolos.

CAPÍTULO II

MARCO TEORICO

II.I INTRODUCCION A VoIP Y ASTERISK

II.I.I VOZ SOBRE IP (VoIP)

Una definición general de VoIP es la posibilidad de transportar conversaciones telefónicas en paquetes IP[1].

La tecnología VoIP trata de transportar la voz, previamente procesada, encapsulándola en paquetes para poder ser transportadas sobre redes de datos sin necesidad de disponer de una infraestructura telefónica convencional. Con lo que se consigue desarrollar una única red homogénea en la que se envía todo tipo de información ya sea voz, video o datos[2].

2.1.1.1 ALTERNATIVAS TECNOLOGICAS DE VoIP

[1] http://comunidad.asterisk-es.org/introduccion_voip.pdf

[2] **Gutiérrez, R**., "Seguridad en VoIP, Ataques, amenazas y riesgos"., 1ª Ed., 2010

Las alternativas tecnológicas de VoIP se pueden dividir de una manera sencilla en dos grandes grupos: tecnologías cerradas propietarias y sistemas abiertos.

En el primer grupo de tecnologías nos encontramos con el conocido Skype o el ya legendario Cisco Skinny (SCCP)[3].

En el segundo grupo de tecnologías nos encontramos con los estándares abiertos basados en SIP, H.323 e IAX.

H.323 es un protocolo desarrollado por la UIT que cobró cierta fama porque era el más usado por los grandes operadores en sus redes troncales.

Últimamente hemos presenciado el nacimiento y el fuerte crecimiento de una nueva alternativa conocida como IAX.

IAX2 (por ser la versión 2) está fuertemente influido por el modelo comunitario de desarrollo abierto y tiene la ventaja de haber aprendido de los errores de sus predecesores.

IAX2 resuelve muchos de los problemas y limitaciones de H.323 y SIP. Aunque IAX2 no es un estándar en el sentido más oficial de la palabra (RFC), no sólo tiene el gran reconocimiento de la comunidad sino todos los prerrequisitos para convertirse en el remplazo (de facto) de SIP. [1]

II.I.I ASTERISK

Asterisk es una implementación libre de una centralita telefónica, el programa permite tanto que los teléfonos conectados a la centralita puedan hacer llamadas entre ellos como servir de pasarela a la red telefónica tradicional. El código del programa fue originalmente creado por Mark Spencer (Digium) basado en las ideas y el trabajo previo de Jim Dixon (proyecto de telefonía Zapata).

El programa, sus mejoras y correcciones, es el resultado del trabajo colectivo de la comunidad del software (programas) libre. Aunque Asterisk puede funcionar en muchos sistemas operativos, GNU/Linux es la plataforma más estable y en la que existe un mayor soporte[4].

---

[3] **Skinny** es un protocolo de control de terminales bajo el control y diseño de CISCO.

[4] http://wilzer-rocha-campos.blogspot.com/2008/11/implementacin-de-software-libre.html

2.2.2.1 ARQUITECTURA

Asterisk fue diseñado de manera modular, de manera que cada usuario pueda seleccionar qué partes de Asterisk o módulos desea utilizar. Esto hace de Asterisk una aplicación realmente escalable y extensible:

Escalable.- Es posible desactivar los módulos no utilizados para instalar Asterisk en dispositivos embebidos de pocos recursos.

Extensible.- Para programar un nuevo módulo de Asterisk no es necesario conocer todo el código de Asterisk.

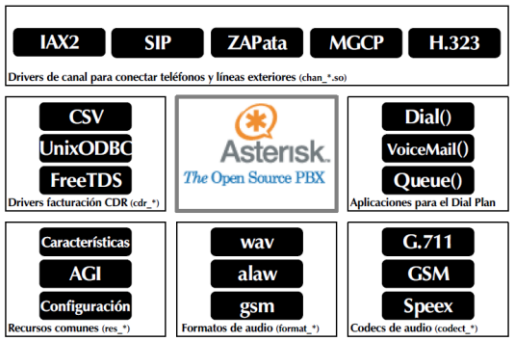


Figura II. I *Arquitectura de Asterisk*
Fuente *Gil, F., y Gómez, J., "VoIP y Asterisk redescubriendo la telefonía".*

- **Core.** Se trata del núcleo de Asterisk, que incluye las funciones más básicas y posibilita la carga de módulos.
- **Recursos.** Aportan funcionalidades adicionales al core, como la posibilidad de leer ficheros de configuración (res_config), música en espera, etc.
- **Canales.** Permiten a Asterisk manejar un dispositivo de una determinada tecnología. Por ejemplo, para manejar dispositivos SIP se utiliza el módulo chan_sip, para IAX2 chan iax y para canales analógicos/digitales chan_zap.
- **Aplicaciones y funciones.** Estos módulos conforman la "caja de herramientas" de Asterisk, ya que son los módulos que aportan las distintas herramientas para configurar el sistema Asterisk.

- **Códec's.** Para que Asterisk pueda codificar y decodificar la información de audio/vídeo que tiene que enviar y recibir dispone de distintos códec's.
- **Formatos.** Estos módulos posibilitan a Asterisk "entender" y manejar ficheros en distintos formatos, como mp3, alaw, ulaw, etc[5].

2.2.2.2 TRONCALES ASTERISK

Las troncales (Trunks) 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 o IP.

El tipo de troncal a utilizar dependerá de la manera que el proveedor nos brinde el servicio de telefonía. Tradicionalmente el servicio es entregado por medio de líneas de cobre o fibra óptica, últimamente se está utilizando mucho la red IP, vía Internet o enlaces dedicados de datos, con esta última opción no es necesario instalar ningún hardware de comunicación en el servidor Elastix, muy recomendado para servidores virtualizados.

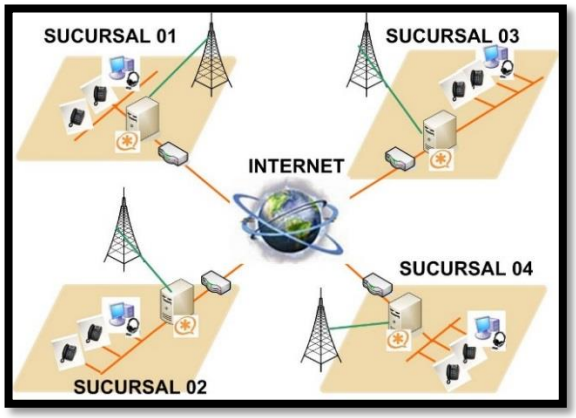


Figura II. II *Troncales para VoIP*
Fuente *http://elastixtech.com/troncales-y-rutas-en-elastix/*

Los tipos de troncales (Trunks) en el servidor Asterisk-Elastix pueden ser:

[5] **Gil, F., y Gómez, J**., "VoIP y Asterisk, Redescubriendo la telefonía"., 1ª Ed., 2008

Troncales SIP (SIP Trunk): es una conexión ofrecida por un Proveedor de Servicios de Telefonía por Internet (ITSP), conecta una PBX de la empresa a una infraestructura de sistema de telefonía existente (PSTN) a través de Internet utilizando el estándar de SIP VoIP.

Como una conexión lógica más que física, las líneas troncales SIP ofrecen el beneficio de no tener límite para el número de llamadas que pueden transferirse a una línea troncal única. Cada llamada consume una determinada cantidad de ancho de banda de la red, entonces el número de llamadas se encuentra limitado únicamente por la cantidad de ancho de banda que puede fluir entre la PBX IP y el equipo del ITSP.

A diferencia de la telefonía tradicional, donde los cables físicos una vez se distribuyeron desde el proveedor del servicio hacia la empresa, una línea troncal SIP les permite a las empresas reemplazar las líneas PSTN tradicionales fijas con conectividad PSTN mediante un proveedor de servicios de líneas troncales SIP en Internet .

Troncales IAX2 (IAX2 Trunk): El medio de transporte para la voz es la red IP, se utiliza para establecer enlaces entre 2 o más servidores Asterisk-Elastix, aún no se ha convertido en estándar, por esta razón son pocos los fabricantes de equipos que lo soportan, una de sus mayores ventajas es la utilización de un solo puerto (UDP 4569) para la comunicación, esto lo convierte en el método ideal para unir 2 o más Asterisk en redes con Firewall de por medio.

Troncales Análogas (Puertos FXO): Es la manera tradicional de recibir las líneas telefónicas, más allá de esto se recomienda utilizar E1. Por cada línea es necesario un puerto, es así por ejemplo si hay 4 líneas telefónicas es necesario utilizar un adaptador con 4 puertos FXO. Un método alterno al uso de los adaptadores FXO, es la utilización de adaptadores ATA con puertos FXO, estos permiten conectar las líneas telefónicas sin instalar ningún hardware en el servidor Elastix, la comunicación se hace vía el protocolo SIP[6].

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

II.II FUNCIONAMIENTO DEL PROTOCOLO SIP

SIP (Session Initiation Protocol) RFC 3261[7] es un protocolo simple de señalización y control utilizado para telefonía y videoconferencia sobre las redes IP, fue creado por el IETF y su estructura está basada en otros protocolos como STMP y HTTP con los que guarda cierta similitud. Su simplicidad, escalabilidad y facilidad para integrarse con otros protocolos y aplicaciones lo han convertido en un estándar de la telefonía IP.

SIP es un protocolo de señalización por lo que solo maneja el establecimiento, control y terminación de las sesiones de comunicación. Normalmente una vez se ha establecido la llamada se produce el intercambio de paquetes RTP que transportan realmente el contenido de la voz.

Encapsula también otros protocolos como SDP utilizado para la negociación de las capacidades de los participantes, tipo de codificación, etc. No hace falta señalar que SIP es un protocolo de aplicación y funcionará tanto sobre UDP como TCP. [2]

Agentes de Usuario (UA) y servidores.

Entre los User Agent (UA), a su vez, podemos encontrar los agentes de usuario clientes (UAC) que son los que inician las peticiones de llamada y los agentes de usuario servidor (UAS) que reciben las peticiones del UAC.

En la siguiente tabla se aprecia un resumen de los mensajes SIP:

Mensaje	Explicación
INVITE	Permite invitar un usuario o servicio para participar en una sesión o para modificar parámetros en una sesión ya existente
ACK	Confirma el establecimiento de una sesión.
OPTION	Solicita información sobre las capacidades de un servidor
BYE	Indica la terminación de una sesión
CANCEL	Cancela una petición pendiente de llamada.
REGISTER	Registrar al User Agent.

Tabla II. I *Mensajes SIP*
Fuente: *Gutierrez, R., "Seguridad en VoIP, Ataques, Amenazas y riesgos.*

Del mismo modo tenemos un listado de los códigos de respuesta a las peticiones SIP: [2]

[7] **RFC 3261** SIP – Session Initiation Protocol

Código	Significado
1xx	Mensajes provisionales
2xx	Respuestas de éxito
3xx	Respuestas de redirección
4xx	Respuestas de fallo de método
5xx	Respuestas de fallo de servidor
6xx	Respuestas de fallos globales

Tabla II. II *Respuestas a las peticiones SIP*
Fuente: *"VoIP y Asterisk: redescubriendo la telefonía" Julio Gómez.*

Una sesión de llamada SIP entre 2 teléfonos es establecida como sigue:

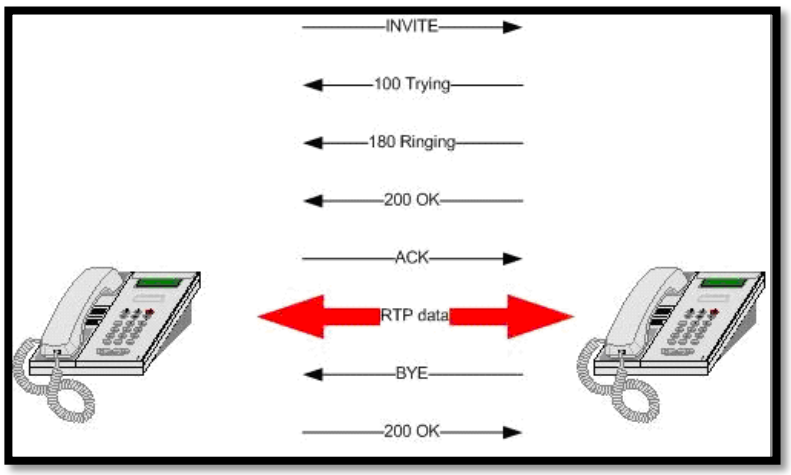


Figura II. III *Sesión de llamada en SIP*
Fuente *Anaya N., Fundamento de telefonía IP e Introduccion a Asterisk / Elastix.*

1. El teléfono llamante envía un "invite"

2. El teléfono al que se llama envía una respuesta informativa 100 – Tratando – retorna.

3. Cuando el teléfono al que se llama empieza a sonar una respuesta 180 – sonando – es retornada.

4. Cuando el receptor levanta el teléfono, el teléfono al que se llama envía una respuesta 200 – OK

5. El teléfono llamante responde con un ACK – confirmado

6. Ahora la conversación es transmitida como datos vía RTP

7. Cuando la persona a la que se llama cuelga, una solicitud BYE es enviada al teléfono llamante

8. El teléfono llamante responde con un 200 – OK.

II.II.I PROTOCOLO SDP

El protocolo SDP (Session Description Protocol) RFC 2327[8] se utiliza para describir sesiones multicast en tiempo real, siendo útil para invitaciones, anuncios, y cualquier otra forma de inicio de sesiones.

La propuesta original de SDP fue diseñada para anunciar información necesaria para los participantes y para aplicaciones de multicast MBONE (Multicast Backbone). Actualmente, su uso está extendido para el anuncio y la negociación de las capacidades de una sesión multimedia en Internet.

Puesto que SDP es un protocolo de descripción, los mensajes SDP se pueden transportar mediante distintos protocolos con SIP, SAP, RTSP, correo electrónico con aplicaciones MIME o protocolos como HTTP. Como el SIP, el SDP utiliza la codificación del texto.

II.II.II PROTOCOLO RTP

RTP (Real Time Protocol) RFC 3550[9] es el verdadero portador para el contenido de voz y vídeo que intercambian los participantes en una sesión establecida por SIP.

Las funciones básicas del protocolo incluyen:
Determinar la ubicación de los usuarios, aportando movilidad.
Establecer, modificar y terminar sesiones multi-partitas entre usuarios[10].

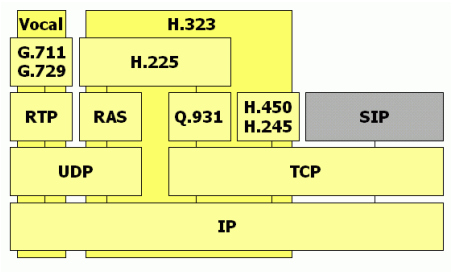


Figura II. IV *Funcionamiento de SIP*
Fuente *Anaya N., "Fundamentos de telefonía IP e introducción a Asterisk/Elastix"., *

[8] **RFC 2327** SDP – Session Description Protocol
[9] **RFC 3550** RTP – Real time Protocol
[10] **Anaya N.**, "Fundamentos de telefonía IP e introducción a Asterisk/Elastix"., 2013

II.III SEGURIDAD DE LAS REDES VoIP

A medida que crece su popularidad aumentan las preocupaciones por la seguridad de las comunicaciones y la telefonía IP. VoIP es una tecnología que ha de apoyarse necesariamente muchas otras capas y protocolos ya existentes de las redes de datos. Por eso en cierto modo la telefonía IP va a heredar ciertos problemas de las capas y protocolos ya existentes, siendo algunas de las amenazas más importantes de VoIP problemas clásicos de seguridad que afectan al mundo de las redes de datos. Existen varios ataques específicos de VoIP como se muestra a continuación.

Figura II. V *Capas de seguridad VoIP*
Fuente*: R, Gutiérrez., "Seguridad en VoIP: Ataques, amenazas y riesgos"*

En la siguiente tabla se detallan algunos de los puntos débiles y ataques que afectan a cada una de las capas. [2]

CAPA	ATAQUES Y VULNERABILIDADES
Políticas y Procedimientos	Contraseñas débiles. Ej: Contraseña del VoiceMail Mala política de privilegios Accesos permisivos a datos comprometidos.
Seguridad Física	Acceso físico a dispositivos sensibles. Reinicio de máquinas. Denegaciones de servicio.
Seguridad de Red	DDoS ICMP unreacheable SYN floods
Seguridad en los Servicios	SQL injections Denegación en DHCP DoS

Seguridad en el S.O.	Buffer overflows Gusanos y virus Malas configuraciones.
Seguridad en las Aplicaciones y protocolos de VoIP	Fraudes SPIT (SPAM) Vishing (Phising) Fuzzing Floods (INVITE,REGISTER,etc..) Secuestro de sesiones (Hijacking) Interceptación (Eavesdroping) Redirección de llamadas (CALL redirection) Reproducción de llamadas (CALL replay)

Tabla II. III *Vulnerabilidades y ataques a las capas de seguridad VoIP*
Fuente*: R, Gutiérrez., "Seguridad en VoIP: Ataques, amenazas y riesgos"*

II.IV INTRODUCCION A IPv6

IPv6 fue adoptado por Internet Engineering Task Force (IETF) en 1994. IPv6 también se conoce por "IP Next Generation" o "IPng", IPv6 es la nueva versión del Protocolo Internet, diseñado como el sucesor de IPv4.

El uso de IPv6 ha sido frenado temporalmente por el uso de técnicas de traducción de direcciones de red (NAT), que alivian parcialmente el problema de la falta de direcciones IP. El problema es que NAT hace difícil el uso de voz sobre IP (VOIP), los juegos multiusuario y las aplicaciones P2P. IPv6 ofrece un espacio de direcciones mucho más grande que IPv4, lo que garantiza que cada dispositivo electrónico funcione con IPv6 sin miedo a que este se llegase agotar.

IPv4 tiene un espacio de direcciones de 32 bits, es decir 2ˆ32 (4.294.967.296 Direcciones IP)

En cambio IPv6 nos ofrece un espacio de 128 bits, es decir 2ˆ128[11].

(340.282.366.920.938.463.463.374.607.431.768.211.456 Direcciones IP).

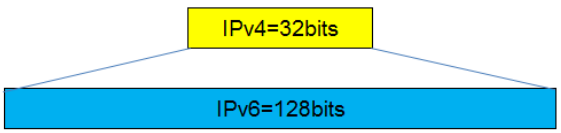


Figura II. VI *Bits IPv4 e IPv6*
Fuente *Edson, Hernández., "IPv6 La evolución"*

[11] **Edson, Hernández.,** "IPv6 La evolución"., 1ª Ed., 2013

II.IV.I DIRECCIONAMIENTO

En lugar de usar formato decimal con puntos como en IPv4, las direcciones IPv6 se escriben con números hexadecimales, con dos puntos entre cada conjunto de cuatro dígitos hexadecimales (que es de 16 bits), tal como se define en el **RFC 2373[12].**

El formato es x: x: x: x: x: x: x: x, donde x es un campo hexadecimal de 16-bit; cada "x" es por lo tanto cuatro dígitos hexadecimales.

Un ejemplo de una dirección IPv6 es:

2035:0021:2FC5:0000:0000:387C:0000:0001

Los dígitos hexadecimales A, B, C, D, E y F en las direcciones IPv6 no distinguen entre mayúsculas y minúsculas.

Afortunadamente se puede abreviar la escritura de las direcciones IPv6, haciéndolas menos complejas, facilitando el aprendizaje de estas. Las siguientes son formas de abreviar una dirección IPv6:

- **Omisión de ceros**

Podemos omitir todos los ceros que se encuentra a la izquierda en cada campo hexadecimal de 16bits. Ejemplo:

Antes: 2035:**000**1:2FC5:0000:0000:**0**87C:0000:**000**1
Después: 2035**:1:**2FC5:0000:0000**:87C:**0000**:1**

- **Agrupación de ceros continuos**

Se pueden utilizar un par de dos puntos seguidos (::), para agrupar un grupo de ceros continuos, no importa si estos estas en un solo campo o en dos. Ejemplo:

Antes: 2035:0001:2FC5:**0000:0000**:087C:0000:0001
Después: 2035:1:2FC5**::**87C:0000:1

Los dos puntos solo se pueden utilizar una sola vez en la dirección IPv6.[5]

- **Resumen de ceros**

[12]**RFC 2373** Formato de Direccionamiento IPv6

Para las situaciones en las que ya utilizamos la agrupación de los ceros continuos por medio de los dos puntos y todavía tenemos a parte otro bloque de ceros, estos podemos resumirlos en un solo cero. Ejemplo:

Antes: 2035:0001:2FC5:0000:0000:087C:**0000**:0001

Después: 2035:1:2FC5::87C**:0:**1

II.IV.II CLASIFICACION DE LAS DIRECCIONES IPv6

Una interfaz puede tener asignadas múltiples direcciones de diferentes tipos y para diferentes propósitos. Independientes de la representación y la división en subredes, las direcciones IPv6 se clasifican de la siguiente manera:

2.3.5.1 DIRECCIONES IPv6 UNICAST

Hay dos tipos de direcciones Unicast:

- ✓ **Unicast Link-local**

Son direcciones IPv6 que identifica la interfaz en un solo enlace. La dirección es única sólo en este enlace, y no es enrutable fuera del enlace. Los paquetes con un destino de enlace local deben permanecer en el enlace donde se generaron.

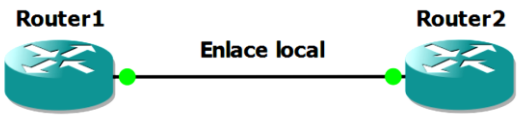


Figura II. VII *Direcciones Unicast Link-local*
Fuente: *"Conceptos básicos y evolución de IPv6" Edson Hernández*

En IPv6 las direcciones Unicast Link-local se crean dinámicamente utilizando el prefijo **FE80::/10** y un identificador de interfaz de 64 bits (La dirección MAC) en un proceso llamado autoconfiguración

A todas las direcciones IPv6 Unicas Link-Local se les asigna un prefijo /64. Por lo tanto la autoconfiguración se lleva acabo solo en los últimos 64 bits de la dirección.

La autoconfiguración consiste en asignarle una dirección IPv6 tomando como base su dirección MAC del host. Esta autoconfiguración llamada EUI-64 divide la dirección MAC mediante la inserción de **FF:FE,** número hexadecimal de 16 bits entre el OUI y el código del proveedor.

La dirección MAC consta de 12 dígitos hexadecimales, lo que corresponde a 48 bits, por lo tanto nos hace falta 16 bits para poder llevar la dirección de 64 bits, por este motivo se hace a la inserción de los números **FF:FE** entre el OUI y el código del proveedor.

- ✓ **Unicast Globales**

Las direcciones Unicast Globales se definen por un prefijo de enrutamiento de un ID de subred y un ID de interfaz. El espacio de direcciones IPv6 Unicast abarca toda la gama de direcciones IPv6, con la excepción de FF00 :: / 8 (1111 1111), que se utiliza para las direcciones de Multicast.

2.3.5.2 DIRECCIONES ANYCAST

Las direcciones Anycast están diseñados para proporcionar redundancia y balanceo de carga en situaciones en las que varios hosts o routers proporcionan el mismo servicio, Anycast no fue creado para IPv6, sino que fue definido en el RFC 1546 en 1993 como una especificación experimental para ser utilizado con IPv4. Los RFC asignan un prefijo especial para Anycast, el cual estaba destinado a ser utilizado para servicios tales como DNS y HTTP.

En la práctica Anycast no ha sido aplicado, para lo que fue diseñado a ser, a menudo un método llamado direcciones Unicast compartidas son elegidas, este método se lleva a cabo mediante la asignación de una dirección Unicast ordinaria a múltiples interfaces y la creación de varias entradas en la tabla de enrutamiento.

2.3.5.3 DIRECCIONES MULTICAST

Una dirección Multicast identifica a un grupo de interfaces, el tráfico enviado a una dirección Multicast viaja a un grupo específico de host al mismo tiempo. Una interfaz puede pertenecer a cualquier número de grupos de Multicast.

Multicast es muy importante para IPv6, ya que es en el centro de muchas de sus funciones, y es un reemplazo para las direcciones de Broadcast.

El rango de las direcciones IPv6 Multicast está reservado dentro de este intervalo FF00:: hasta FF0F::, los siguientes son algunos ejemplos de las direcciones asignadas por la IANA.

Dirección	Descripción
Interface-local scope	
FF01:0:0:0:0:0:0:1	All-nodes address
FF01:0:0:0:0:0:0:2	All-nodes address
Link-local scope	
FF02:0:0:0:0:0:0:1	All-nodes address
FF02:0:0:0:0:0:0:2	All-nodes address
FF02:0:0:0:0:0:0:3	Unassigned
FF02:0:0:0:0:0:0:4	DVMRP routers
FF02:0:0:0:0:0:0:5	OSPFIGP
FF02:0:0:0:0:0:0:6	OSPFIGP designated routers
FF02:0:0:0:0:0:0:7	ST routers
FF02:0:0:0:0:0:0:8	ST hosts
FF02:0:0:0:0:0:0:9	RIP routers
FF02:0:0:0:0:0:0:A	EIGRP routers
FF02:0:0:0:0:0:0:B	Mobile agents
FF02:0:0:0:0:0:0:C	All PIM routers
FF02:0:0:0:0:0:0:D	RSVP encapsulation
FF02:0:0:0:0:0:0:16	All MLDv2-capable routers
FF02:0:0:0:0:0:0:6ª	All snoopers
FF02:0:0:0:0:0:1:1	Link name
FF02:0:0:0:0:0:1:2	All DHCP agents
FF02:0:0:0:0:0:1:3	Link-local Multicast Name
FF02:0:0:0:0:0:1:4	DTCP Announcement
FF02:0:0:0:0:0:1:FFXX:XXXX	Solicited-node address
Site-local scope	
FF05:0:0:0:0:0:0:2	All-routers address
FF05:0:0:0:0:0:1:3	All DHCP servers
FF05:0:0:0:0:0:1:4	Deprecated
FF05:0:0:0:0:0:1:1000 to FF05:0:0:0:0:01:13FF	Service location (SLP) Version 2

Tabla II. IV *Rangos de direcciones Multicast*
Fuente: *"Conceptos básicos y evolución de IPv6" Edson Hernández*

II.IV.III VENTAJAS DE INTEGRAR IPV6 A VOIP

Con respecto a VoIP, las ventajas de IPv6 sobre el protocolo IPv4 que se puede destacar son:

- **Clasificación de tráfico:** La clasificación de tráfico que realiza IPv6 consiste en identificar las prioridades de los paquetes a ser enviados, este campo identifica dos prioridades distintas en cada paquete: La primera, los paquetes se clasifican como parte de un tráfico para el cual la fuente está ofreciendo control de congestión o no; y la segunda, a cada paquete se le asigna uno de los ocho niveles de prioridad relativa dentro de cada clasificación anterior.
- **Etiquetado de flujo (flow):** Es una secuencia de paquetes en este caso de voz que reciben un tratamiento específico no estándar por parte de los routers que intervienen en el tráfico de paquetes entre el origen y el destino, está determinado por la combinación de la dirección de fuente y una etiqueta de flujo, de este modo, todos los paquetes que formen parte del mismo flujo tienen asignada la misma etiqueta de flujo por parte de la fuente, lo cual permite una distribución de contenido multimedia de manera eficiente y óptima.
- **Fragmentación:** En IPv6 la fragmentación sólo puede hacerse en los nodos origen, y no a lo largo de los nodos de la red como lo hacía IPv4, gracias a que los paquetes no se fraccionan en la red éstos no se pierden evitando así que un nodo tenga que almacenar muchos fragmentos, y todos los demás problemas que trae la fragmentación en la red como son la sobrecarga de procesamiento en los equipos de red y la pérdida de fragmentos.

Luego de analizar los protocolos y observar las mejoras realizadas en el protocolo IPv6 se expresa en la siguiente tabla las diferencias más importantes:

	IPv6	IPv4
Direcciones	128 bits (16 bytes)	32 bits (4 bytes)
Arquitectura	Jerarquica	Plana

Configuracion	Automatica	Manual
Trafico	Multicast y anycast	Broadcast
Seguridad	Obligatoria (IPsec)	Opcional
Identificacion de carga para el control de QoS	Incluida en el encabezado	Sin identificacion QoS
Fragmentacion	Se realiza en el host de inicio	Es posible en los Routers y el host fuente
Opciones encabezado	Todos los datos opcionales se mueven a extensiones de encabezado IPv6	El encabezado incluye opciones
ARP (Address Resolution Protocol)	Se reemplaza por el protocolo Neighbor Solicitation (Solicitud de vecino)	Utiliza ARP para la resolucion de direcciones a nivel de enlace de datos

Tabla II. V *Diferencia entre IPv4 e IPv6 para VoIP*
Fuente: *"Implementación de VoIP sobre IPv6" Jefferson Jiménez*

La siguiente tabla ilustra el por qué la integración de IPv6 a VoIP es beneficiosa en relación a la actual implementación del servicio VoIP que trabaja sobre la actual versión de IP, IPv4.

Beneficios	IPv4	IPv6
Integridad de punto a punto de la señalización de VoIP	NO	SI
Seguridad (Escucha disimulada Hacking)	NO	SI
Escalabilidad		
Adaptabilidad	SI	SI
Fiabilidad	NO	SI
Alojamiento NAT (Network Address Translation)	SI	NO
Calidad de servicio QoS	NO	SI
Soporte a trafico multimedia en tiempo real	NO	SI
Movilidad	NO	SI
Configuración dinámica	NO	SI

Tabla II. VI *Ventajas de integración IPV6 a VoIP*
Fuente: *"Implementación de VoIP sobre IPv6" Jefferson Jiménez*

A continuación se realiza una comparación entre VoIP IPv4 y VoIP IPv6, utilizando la ponderación de las características más importantes que se deben cumplir para obtener una comunicación de calidad entre los usuarios de VoIP.

Ponderación de los aspectos a comparar:

3: Eficiente y óptimo

2: Poco eficiente.

1: No cumple.

Aspectos	VoIP IPv4	VoIP IPv6
Etiquetado de flujo	1	3
Seguridad de datos de punta a punta	1	3
Clasificación de trafico	2	3
Asignación de prioridades según el tipo de trafico	2	3
Velocidad de transmisión	2	3
Fragmentación	2	3
Control de retardo y latencia	2	3
Calidad de servicio en aplicaciones de tiempo real	2	3
Carga de procesamiento en los routers	2	3
Seguridad	2	3
QoS	1	3
TOTAL	**19**	**33**

Tabla II. VII *Comparación entre VoIPv4 y VoIPv6*
Fuente: *"Implementación de VoIP sobre IPv6" Jefferson Jiménez*

El cuadro anterior muestra las características principales que VoIP IPv6 tiene frente a VoIP IPv4 y justifica el porqué es mejor la implementación de VoIP sobre IPv6, expresando la tabla anterior en forma gráfica se obtiene[13]:

[13] **JIMENEZ, J.,** Implementación de VoIP sobre IPv6., TESIS., 2008

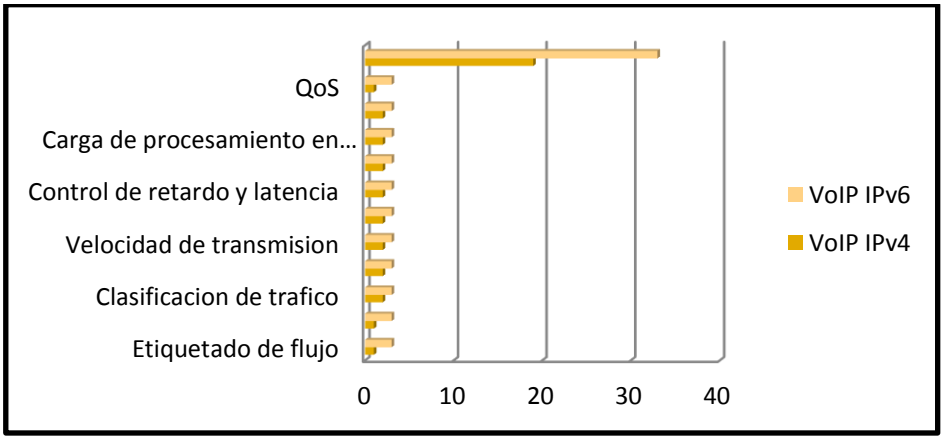


Figura II. VIII *VoIPv4 vs VoIPv6*
Fuente: *"Implementación de VoIP sobre IPv6" Jefferson Jiménez*

II.V HACKING ÉTICO VOIP

Las empresas que están migrando su telefonía tradicional a VoIP por las múltiples ventajas que ofrece no deberían ignorar los riesgos de seguridad que aparecen cuando convergen las redes de voz y datos. Los ataques que pueden sufrir los sistemas VoIP son múltiples: robo de servicio, interceptación de comunicaciones, denegación de comunicaciones telefónicas, etc. Al mismo tiempo, al modificar nuestras redes de datos para permitir el uso de VoIP puede estar abriendo inadvertidamente vías de ataque a los sistemas informáticos. A través del servicio de Hacking Ético VoIP es posible identificar los puntos débiles en su infraestructura de comunicaciones para minimizar estos riesgos.

Figura II. IX *Actividades de Hacking*
Fuente: *http://www.gitsinformatica.com/hackers.html*

II.V.I BENEFICIOS

• Conocimiento del grado de vulnerabilidad de los sistemas de información, que es imprescindible para aplicar las medidas correctoras.

• Reducción de aquellos riesgos que, en caso de materializarse las amenazas que les originan, pueden representar pérdidas ingentes de capital, bien por facturación fallida, por reposición de los daños causados, por pérdida de oportunidad de negocio, por reclamación de clientes, por sanciones legales etc.

• Ahorro de tiempo y dinero al afrontar y corregir situaciones nefastas antes de que ocurran y nos obliguen a resolverlas con prisas y a cualquier precio[14]

[14] **GRAVES, K.,** Certified Ethical Hacker, Review Guide., 1st ed., 2012

CAPÍTULO III

MARCO METODOLÓGICO E HIPOTÉTICO

INTRODUCCIÓN

El objetivo principal de este capítulo es el análisis del proceso metodológico, es decir, los procedimientos, métodos y técnicas que identifica resultados que ayuden a comprobar la hipótesis planteada a través de pruebas y mediciones.

Se emplea además el proceso Hipotético para realizar el análisis para la operacionalización de las variables a ser medidas, de esta manera facilitar el estudio del presente proyecto.

III.I DISEÑO DE LA INVESTIGACIÓN

Este proyecto se basa dentro de un estudio **Cuasi-Experimental,** en los cuales los elementos de estudio no están asignados al azar, sino que se los tendrá definidos antes de realizar dicho ambiente por el autor.

Además se manipula una variable independiente y la evaluación de su correspondiente efecto en la variable dependiente. Su validez se alcanzará a medida que se demuestre el acceso seguro en redes VoIP, escogiendo las herramientas adecuadas en función a las contramedidas frente al análisis de las vulnerabilidades de los protocolos de las centrales VoIP.

III.II TIPO DE INVESTIGACIÓN

En este proyecto se considera que el tipo de estudio que se va a realizar es una **investigación descriptiva**, ya que se utilizará el conocimiento para realizar un estudio para el análisis de

vulnerabilidades en centrales VoIP con IPv6 utilizando troncales SIP, permitiendo analizar las vulnerabilidades en capa de protocolos y aplicaciones VoIP para posteriormente ofrecer seguridad en las redes VoIP en IPv6, implementando un escenario de pruebas para su estudio.

Además, se usa la **investigación experimental** puesto que se realiza sus pasos como son la observación, análisis e interpretación de los resultados en cuanto al comportamiento de las variables de los criterios de seguridad de la información en la transmisión VoIP.

III.III MÉTODOS

Para este proyecto se utilizarán los siguientes métodos de investigación.

Método Científico: Servirá para recopilar toda la información necesaria para ser aplicada en el ambiente de pruebas, ya que las ideas, conceptos, y teorías expuestas en este proyecto de tesis son verificables como válidos.

Se ha realizado las siguientes consideraciones:

- Se plantea la investigación en base al problema de vulnerabilidad de los protocolos de centrales VoIP con IPv6 utilizando troncales SIP.

- Se proponen los objetivos de la investigación que permitirán resolver el problema de vulnerabilidades, para el acceso seguro en redes VoIP en IPv6.
- Se elabora un marco teórico que ayude a tener una idea general para la realización del proyecto de tesis.
- Se plantea una hipótesis, la cual es una posible respuesta al problema planteado y posee una íntima relación entre el problema y el objetivo.
- Se realiza la recolección de datos, y se observa el comportamiento del ambiente de pruebas en el acceso vulnerable y seguro.
- Se realiza la prueba de la hipótesis con los resultados obtenidos.
- Se determinan las conclusiones y recomendaciones con los resultados obtenidos de la investigación realizada.

III.IV TÉCNICAS

Se usará ciertas técnicas para la elaboración del proyecto, entre ellas están:

- Recopilación de información.
- Implementación del ambiente de simulación.
- Análisis.
- Pruebas.

III.V FUENTES DE INFORMACIÓN

La información necesaria para la elaboración del proyecto, se obtiene de los elementos como:

- E-books.

- Libros.
- RFC´s.
- Blogs informáticos.

III.VI RECURSOS

RECURSOS HUMANOS

Dentro de la parte humana intervienen:

- Tesista.
- El Asesor de tesis.
- Miembros del tribunal de tesis.

RECURSOS MATERIALES

- Hojas de Papel Bond
- CD's
- Flash Memory
- Bibliografía
- Internet

RECURSOS TÉCNICOS

✓ **Hardware**

NOMBRE	FUNCION	UTILIZACION
PC	Computador personal	Utilizados para ser el Servidor, clientes y el atacante.
ROUTER CISCO 3960	Conexión de redes LAN y WAN	Determinación de los nodos de las LAN y WAN

SWITCH CISCO CATALYS 2960	Conexión de dispositivos finales de la red y conexión con el ROUTER	Realiza conexión total entre dispositivos de la intranet
CABLES UTP Y SERIAL	Medios de transmisión de datos	Conexión de dispositivos de red

Tabla III. VIII *Hardware utilizado para el proyecto*
Fuente: *Autor de la tesis.*

✓ **Software**

NOMBRE	FUNCION	UTILIZACION
CentOS	Sistema Operativo	Sistema para la ejecución de Asterisk
Asterisk versión elastix	Centralita PBX para VoIP en IPv6	Servidor VoIP para registro de cuentas de usuario
Backtrak / Kali Linux	Software para Pentesting para VoIP	Herramientas necesarias para escaneo y penetración al sistema
VMWARE Workstation 9	Máquina virtual	Virtualización para CentOS y Backtrak
Linphone	Softphone	Cliente para sesiones SIP en IPv6

Tabla III. IX *Software utilizado en el proyecto*
Fuente: *Autor de la tesis.*

- **VALIDACION DE INSTRUMENTOS**

La aplicación de los recursos técnicos indicados en la tabla 3.2 dará la opción de realizar mediciones y comparaciones de aquellos factores de vulnerabilidades y seguridad que es objeto de estudio llegando a la evaluación de la hipótesis planteada.

A continuación se detalla las herramientas a utilizarse en el proyecto.

Asterisk, en su versión Elastix dará servicio de central PBX VoIP, montada en una plataforma de software libre Linux CentOS, la cual es una central de fácil manejo y de interface amigable de

configuración en creación de extensiones VoIP, su implementación no es costosa ya que Asterisk lo podemos descargar de internet desde su página oficial.

http://downloads.digium.com/

http://www.elastix.org/index.php/es/descargas.html

Backtrack y/o Kali Linux, basado en Debian será el software que utilice su herramientas para pentesting de Hacking y seguridad de la central Asterisk VoIP, es igualmente una distribución Linux el cual lo podemos descargar de internet en su página oficial, el cual también podemos incorporar herramientas q se necesiten para un Hacking ético del escenario planteado.

http://www.kali.org/downloads/

Linphone, es el softphone cliente que tiene soporte para IPv6 para el protocolo SIP, además es muy estable a configuraciones para SSL/TLS en SIP y SRTP, se lo puede descargar en internet desde su página oficial y que además tiene soporte para Windows, Linux, Mac, etc.

http://www.linphone.org/eng/download/packages/linphone.html

III.VII SISTEMA HIPOTETICO

III.VII.I HIPOTESIS

"El estudio del análisis de vulnerabilidades en protocolos utilizados en centrales VoIP con IPv6 utilizando troncales SIP, permitirá mejorar los niveles de seguridad en estas redes."

III.VII.II OPERACIONALIZACION CONCEPTUAL DE LAS VARIABLES

A continuación se considera las siguientes variables para el estudio del proyecto:

- ✓ **Variable Independiente**

La variable independiente es aquella que permite manipular características de otras variables que estarán en función de esta y que varían según su aplicación.

Para este caso se considera a la aplicación de propuestas de seguridad en centrales VoIP en IPv6.

- ✓ **Variable Dependiente**

Las vulnerabilidades en protocolos utilizados en centrales VoIP, es la variable dependiente, porque al momento de aplicar una propuesta de seguridad se debe medir si las vulnerabilidades se corrigen en la transmisión de VoIP.

En las siguientes tablas se presentan la operacionalización conceptual y metodológica de las variables, las mismas que se han identificado de acuerdo a la hipótesis:

- **Operacionalizacion conceptual de las variables**

VARIABLE	TIPO	CONCEPTO
V1. El análisis de vulnerabilidades en protocolos utilizados en centrales de VoIP con IPv6 utilizando troncales SIP	**DEPENDIENTE**	Son los puntos débiles de la central VoIP, que cuando resulta ser descubiertos por un atacante, resulta en una violación de la seguridad.
V2. Seguridad en redes VoIP	**INDEPENDIENTE**	Es cumplir ciertas normas y políticas de seguridad para reducir las vulnerabilidades de la red, tanto físicas como lógicas

Tabla III. X *Operación conceptual de las variables de la hipótesis.*
Fuente: *Autor de la tesis.*

III.VII.III OPERACIÓN METODOLOGICA DE LAS VARIABLES

VARIABLES	INDICADORES	TECNICAS	HERRAMIENTAS
DEPENDIENTE El análisis de vulnerabilidades en protocolos utilizados en centrales de VoIP con IPv6 utilizando troncales SIP	- Eavesdropping - SIP - RTP	- Recolección de Información. - Razonamiento - Test de penetración	- Kali Linux módulos SIP (Metasploit) - Wireshark
INDEPENDIENTE Seguridad en redes VoIP	- Disponibilidad - Confidencialidad - Integridad	- Análisis - Pruebas - Resultados	- SSL / TLS sobre SIP y RTP

Tabla III. XI *Operación Metodológica de las variables de la hipótesis.*
Fuente: *Autor de la tesis.*

CAPÍTULO IV

ESCENARIOS Y PRUEBAS

INTRODUCCIÓN

En este capítulo se diseña el ambiente de simulación apto para la realización de pruebas, indicando los recursos técnicos en Hardware y Software haciendo un análisis en las características de los equipos a usar en el proyecto.

A continuación se implementara el escenario topológico con los recursos técnicos indicados, se implementara los servidores sin ningún tipo de seguridad, sino solamente brindando el servicio de VoIP en el protocolo IPv6 con el objetivo de realizar capturas de los protocolos de dichas centrales tal como SIP y RTP.

Las capturas de los paquetes SIP y RTP se realiza a través mediante el ataque de sniffing mediante el uso de un sniffer para de tal manera decodificar los paquetes de voz.

Para proteger los protocolos de estas centrales VoIP se debe cifrar estos paquetes mediante técnicas de encriptación que vienen en texto plano evaluando a través de requerimientos de seguridad como son: Integridad, Confidencialidad y Disponibilidad.

IV.I RECURSOS TECNICOS

Son las herramientas necesarias para la implementación del ambiente de simulación tanto hardware como software, que sirven para pruebas y resultados mediante el análisis de vulnerabilidades en los protocolos de centrales VoIP.

A continuación se detallan las herramientas para la implementación del escenario de pruebas.

- **DIAGNÓSTICO DE HARDWARE A UTILIZAR**

EQUIPO	FINALIDAD	CARACTERISTICAS
Router CISCO 2811	Establecimiento y conexión de enlaces WAN y LAN	Entre las principales: -- Soporte para IPv6 unicast-routing -- Conexiones Inter-vlan -- Protocolos de enrutamiento en IPv6 -- VoIP con Call Manager Express -- Soporte VoIP en SIP SCCP, SKINNY -- IPsec, SSL, VPN -- Códigos de configuración de cifrado de datos -- Cumplimiento de normas: IEEE 803.11af
Switch CISCO Catalyst 2960	Conexión de Dispositivos finales y troncales	**-- Inteligencia:** asigna prioridad al tráfico de voz **-- Seguridad mejorada:** soporte para configuración de algoritmos de encriptación para cifrado de datos y seguridad de puertos mediante port-security. **-- Confiabilidad:** aprovecha los métodos basados en estándares o el apilamiento FlexStack para aumentar la confiabilidad y para una rápida recuperación tras problemas.
PC´s	Interacción entre usuario y sistema	-- Clientes Softphone Linphone en IPv6 -- Soporte de Simulación para servidores VoIP -- Soporte de Simulación para Kali-Linux Backtrack

Tabla IV. XII *Hardware para el ambiente de pruebas y características.*
Fuente *https://tools.cisco.com/search/results/es/la/get#q=router+2811 y elaboración propia*

El ambiente de simulación se lo realiza en la academia de redes CISCO ESPOCH, en el cual se utilizan los equipos descritos en la tabla anterior.

- **DIAGNOSTICO DE SOFTWARE**

HERRAMIENTA	FUNCION	CARACTERISTICAS
Elastix	Servidor VoIP	-- Centralita PBX open source GLP con soporte para IPv6 basado en Asterisk -- Soporte para Secure RTP -- RTP es utilizado para la transmisión de voz en tiempo real definidos por la IETF en los RFC 3550 y 3511. -- Entorno grafico http amigable al administrador de red en la creación de extensiones y troncales SIP -- SIP es el protocolo de señalización multimedia definida por la IETF en el RFC 3261.
Kali-Linux Backtrack	Auditor para VoIP	-- Licencia open source, utilizado para PENTEST y auditorias de seguridad -- Versión reciente de Backtrack basado en Debian -- Utilización de Wireshark como Sniffer para extraer paquetes de audio y analizador de protocolos -- Pruebas de penetración en SIP con IPv6 a través de exploits y payloads.
VMWare	Máquina Virtual	-- Virtualización para el servidor PBX y Kali-Linux Backtrack -- Implementación de tarjetas de red virtuales -- Soporte para redes LAN virtuales
Linphone	Softphone	-- Soporte para SIP en IPv6 -- Permite comunicación gratuita de voz -- Soporte de llamadas en espera -- Soporte para SRTP y SIPS

Tabla IV. XIII *Software para el ambiente de pruebas y características*
Fuente *Autor de la tesis.*

IV.II ESQUEMA TOPOLOGICO DEL ESCENARIO DE PRUEBAS.

Una vez analizadas las características de los equipos a utilizar en el proyecto, se plantea el siguiente esquema como prototipo de pruebas utilizando troncales SIP entre dos servidores VoIP como en el esquema de Juan Oliva en su publicación web titulada “Unión Elastix y Asterisk puro vía SIP Trunk”, así también como David López Bautista en su artículo científico titulado “Implementación de Protocolos de Señalización VoIP sobre un entorno de red IPv6”.

Con estos antecedentes se plantea el siguiente escenario de pruebas física.

Figura IV. X *Escenario físico de pruebas*
Fuente *Autor de la tesis.*

Una vez implementado se pone en marcha a la configuración de usuarios, extensiones y la troncal SIP por cada servidor, el tipo de direccionamiento en IPv6 está en forma global como se observó en el capítulo 3, sea de la forma 2001: db8::/64 y direccionamiento en IPv4 de clase C.

Cada servidor tiene un plan de marcado y tipos de direccionamientos diferentes, por lo cual se logran comunicarse a través de la Troncal SIP, finalmente el prototipo de pruebas lógica a plantearse seria:

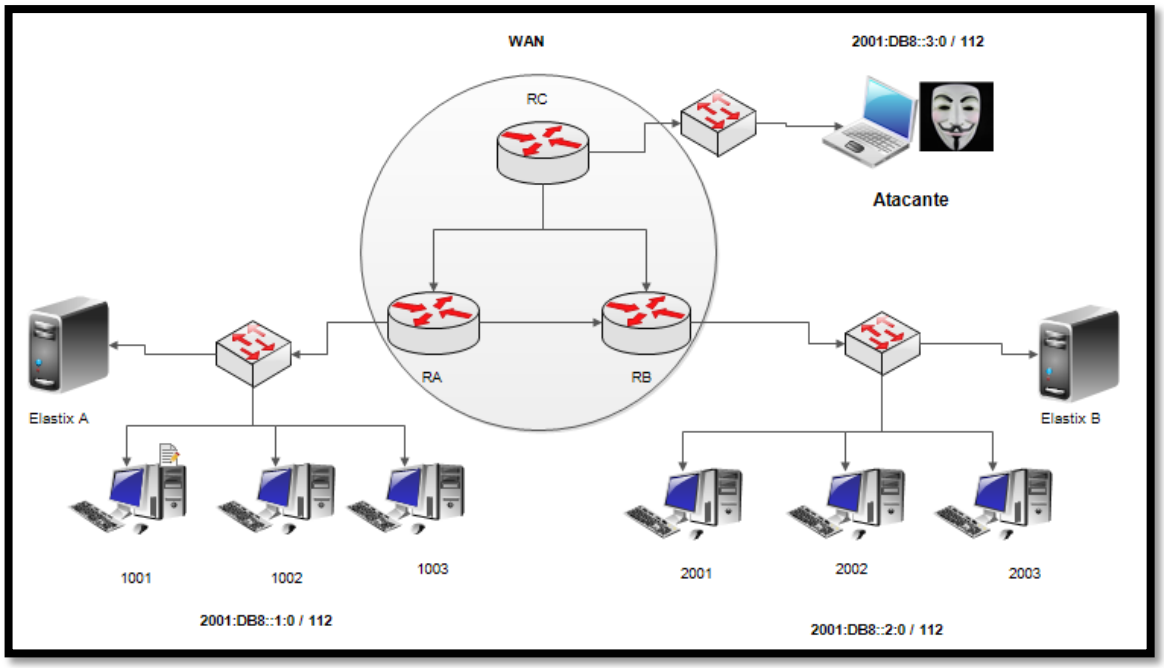


Figura IV. XI *Escenario lógico de pruebas*
Fuente *Autor de la tesis.*

En la figura se aprecia que en el router RA se encuentra la LAN de una empresa x, en el router RB se encuentra la LAN de la sucursal de la empresa x en otro punto geográfico, cada LAN posee un servidor VoIP.

Las extensiones 1xxx se comunican con las extensiones 2xxx a través de la troncal SIP configurada en ambos servidores con direccionamiento en IPv6.

En el router RC el atacante trata de vulnerar los protocolos de las centrales VoIP, es decir, trata de espiar, sustraer paquetes de voz entre transmisor y emisor en el protocolo IPv6.

El proyecto a plantearse requiere de dos escenarios.

El primer escenario será implementado sin ninguna medida de seguridad, es decir solo con las configuraciones por defecto por parte de la central PBX, únicamente asignando contraseñas a las extensiones de la central que serán usadas por los usuarios registrados en la central.

El segundo escenario se aplica las soluciones a los ataques, con el fin de verificar si se corrige o no, para lo cual se emplea el proceso de hacking ético el cual consta de lo siguiente:

1) PENTEST (Prueba de penetración)
2) Metodología de corrección de vulnerabilidades.
3) Análisis comparativo entre los dos escenarios.

A continuación se realiza un PENTEST (Prueba de penetración) para el análisis de vulnerabilidades en los protocolos de centrales VoIP, en el cual se realizaran llamadas para toma de datos para su respectiva interpretación de resultados.

IV.III IMPLEMENTACION DEL AMBIENTE DE SIMULACION

IV.III.I ESCENARIO 1: RED VoIP SIN SEGURIDAD (VULNERABLE)

El primer escenario es desarrollado mediante el esquema planteado en la figura 3.2, sin la implementación de medidas de seguridad para la transmisión de VoIP, ver ***Anexo 1***.

Se ejecutara la siguiente técnica de ataque para vulnerar los protocolos de centrales VoIP.

Eavesdropping.- es espiar los paquetes de voz en RTP que circula por la red mediante un sniffer o analizador de protocolos para su traducción de un archivo .cap de manera ilegal.

IV.III.II IMPLEMENTACIÓN DEL SERVIDOR VOIP.

- **Hardware utilizado.**
  - Intel Dual Core de 2.4 Ghz.
  - Memoria RAM de 4 Gb.
  - Disco duro de 750 Gb
  - Tarjeta de red 10/100 Mbps.
- **Software utilizado.**
  - VMware Workstation 9
  - Elastix-2.4.0-Stable-i386-bin

Elastix es un software aplicativo basado en Asterisk que integra varias funcionalidades, entre ellas la central PBX de código abierto, ofreciendo una interfaz gráfica, amigable y cómoda para la creación de extensiones por parte del administrador.

Elastix es un software completo ya que indica reportes de comportamiento de sí mismo, es decir que ofrece una interfaz gráfica indicando el consumo de recursos de sus herramientas.

- **Instalación de Elastix**

La imagen .iso de Elastix se puede descargar desde la Web en su página oficial http://www.elastix.org/index.php/es/descargas.html.

A continuación, en VMware se procede con la instalación de Elastix, teniendo en cuenta la configuración que se realizó con el siguiente Hardware virtual.

- Memoria RAM de 1 Gb
- Disco duro de 10 Gb

El tipo de procesador y tarjeta de red se configura de acuerdo al Hardware de la PC física.

A continuación se procede con la instalación.

Click en Enter para la instalación.

Figura IV. XII *Arrancando la instalación de Elastix*
Fuente: *Autor de la tesis.*

Elegir el idioma

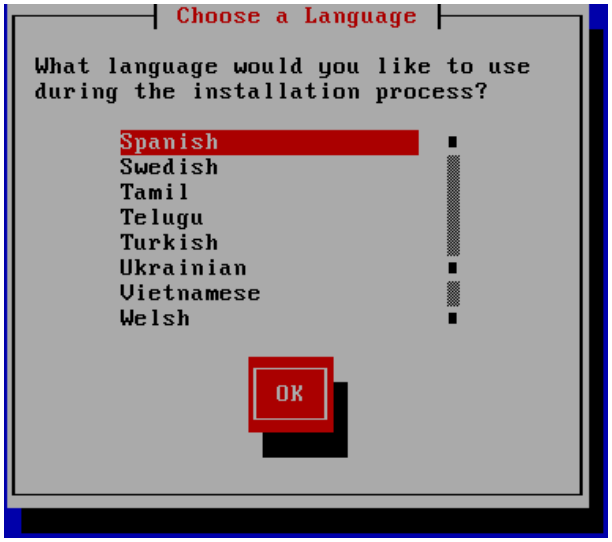


Figura IV. XIII *Elección del idioma de Elastix*
Fuente: *Autor de la tesis.*

Elegir el tipo de teclado.

Figura IV. XIV *Elección del tipo de teclado de Elastix*
Fuente: *Autor de la tesis.*

Elegir la zona horaria

Figura IV. XV *Elección de la zona horaria de Elastix*
Fuente: *Autor de la tesis.*

Introducir usuario y contraseña para el acceso al sistema.

- Username: root
- Password: tesis2013

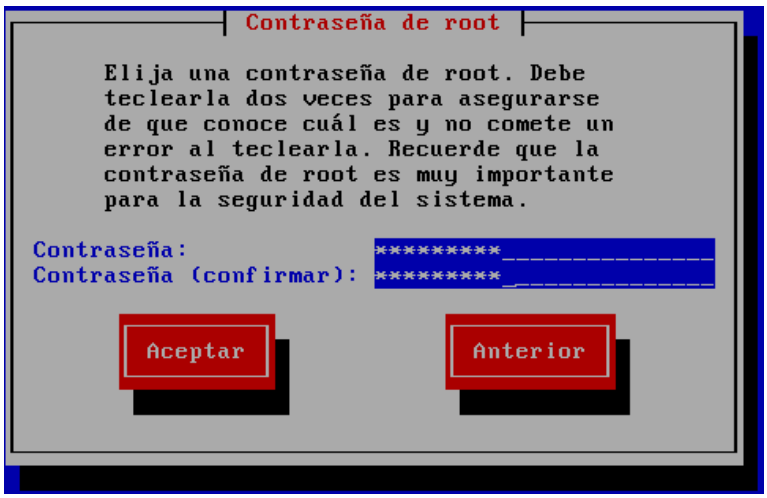


Figura IV. XVI *Asignación de usuario y contraseña en Elastix*
Fuente: *Autor de la tesis.*

A continuación se instalan las dependencias de Elastix

Figura IV. XVII *Instalación de dependencias en Elastix*
Fuente: *Autor de la tesis.*

Esperar a que termine de instalar los paquetes.

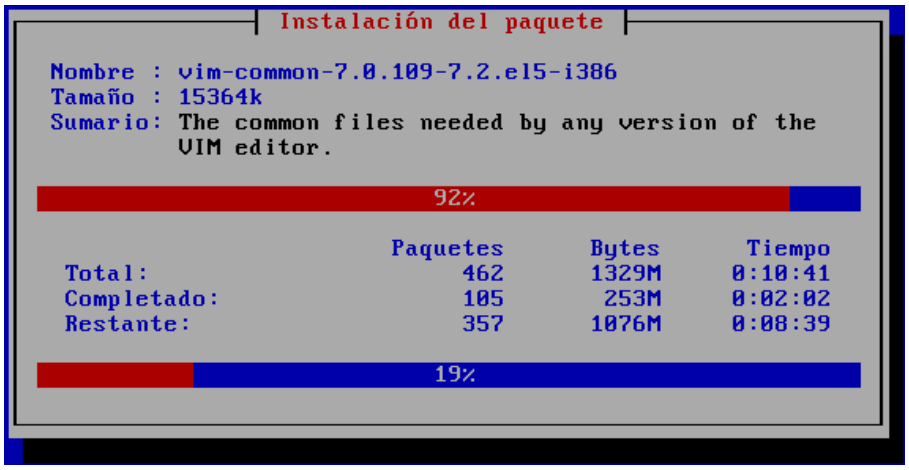


Figura IV. XVIII *Instalación de paquetes en Elastix*
Fuente: *Autor de la tesis.*

Luego de que se reinicie el sistema, ingresar el usuario y contraseña.

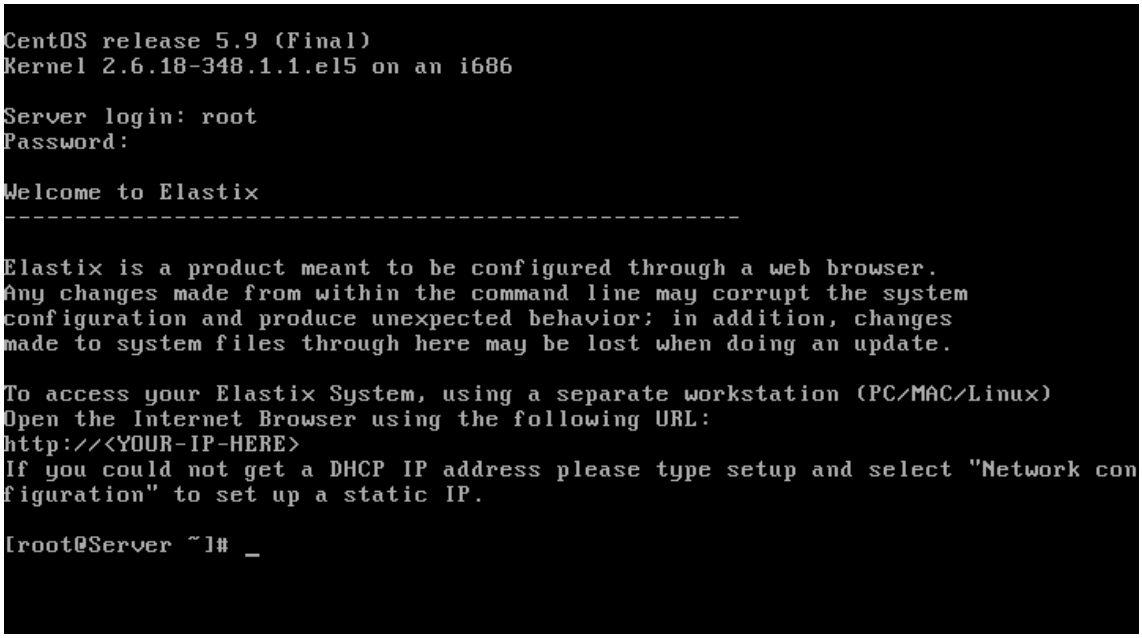


Figura IV. XIX *Inicio de sesión en Elastix*
Fuente: *Autor de la tesis.*

- **Habilitando el soporte IPv6 en Elastix**

Antes de empezar (En el Servidor)

Desactivar el firewall de Linux y la seguridad extendida

#chkconfig iptables off
#chkconfig ipv6tables off
#vi /etc/selinux/config
SELINUX=disabled # cambiar de enabled a disabled
#vi /etc/sysconfig/network
networking=yes
networking_ipv6=yes
vi /etc/sysconfignetwork-script/ifcfg-eth0
DEVICE=eth0
ONBOOT=yes
NM_CONTROLLED=no
BOOTPROTO=static
IPV6ADDR=2001:db8::1:100/112
IPV6INIT=yes
#vi sip.conf
udpbindaddr = ::
#vi manager.conf
[general]
Binaddr = ::
Finalmente reiniciar el servidor (reboot).

IV.III.III CREACIÓN DE EXTENSIONES PARA USUARIOS.

En el entorno de Elastix es sencillo hacer la creación de usuarios, para lo cual se sigue los siguientes pasos:

1. Abrir el navegador en el cliente e ingresamos la URL del Servidor Elastix, (Para el ejemplo es: http://[2001:db8::1:100]) hay que asegurarse que la dirección IP corresponda a la que asignaron durante la instalación.
2. Ingresar el usuario y contraseña a la interfaz web de elastix

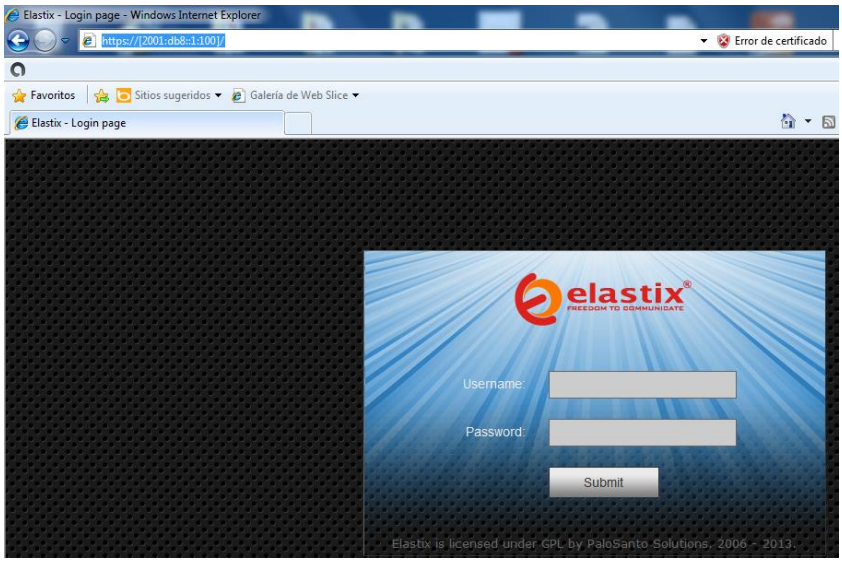


Figura IV. XX *Interfaz web de Elastix en IPv6*
Fuente: *Autor de la tesis.*

3. Dar click en PBX, a continuación dar click en Extensions y dar click en Generic SIP Device.
4. Se crea al usuario, por ejemplo: “santyEa” con la extensión “1001”

5. Asignar la clave para el cliente, ya sea un teléfono IP o un Softphone.

Aplicar los cambios y se crea esta información por defecto después de abrir la extensión.

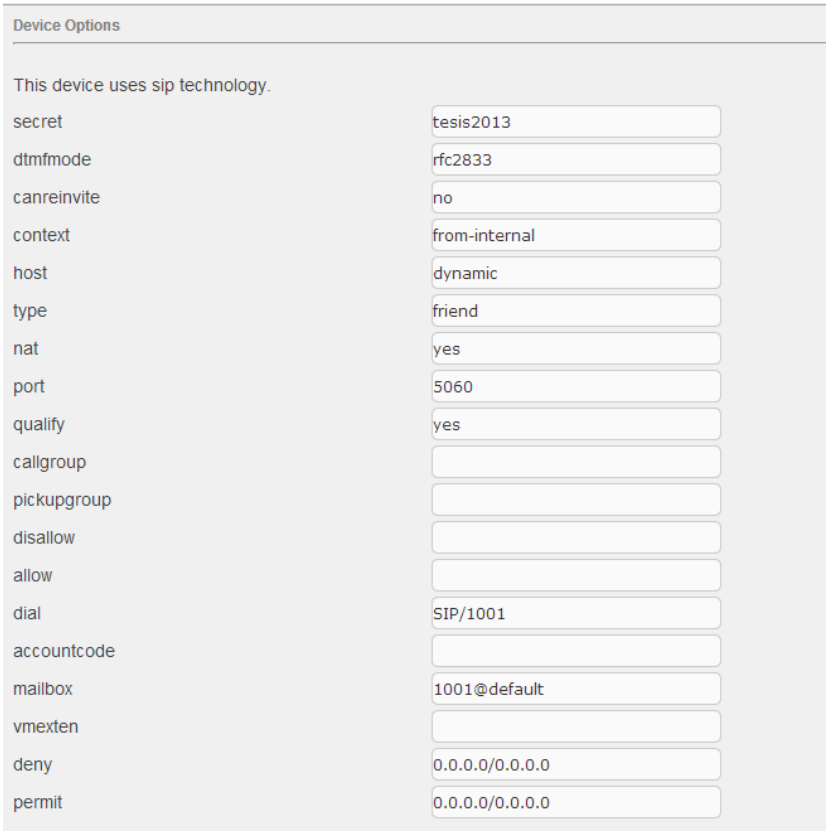
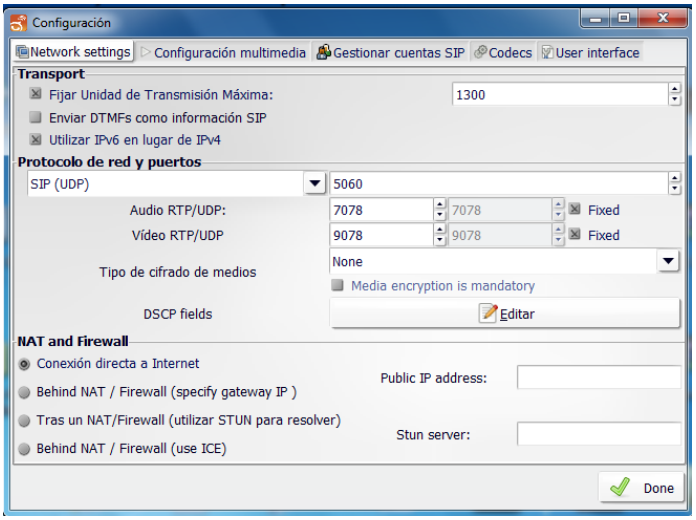


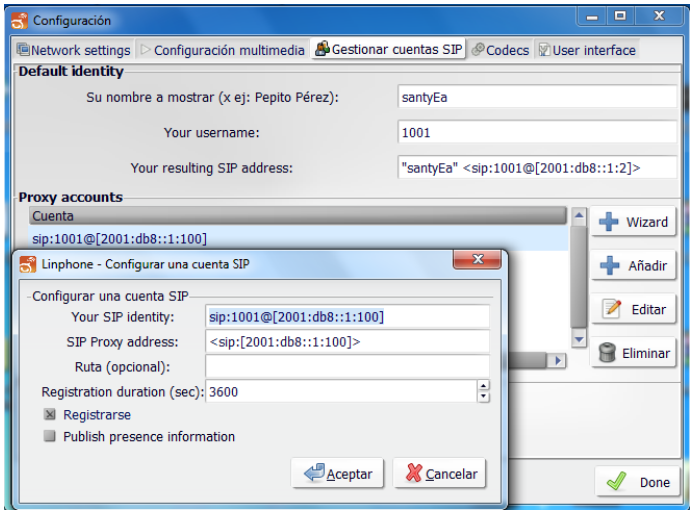
Figura IV. XXI *Creación de extensiones*
Fuente: *Autor de la tesis.*

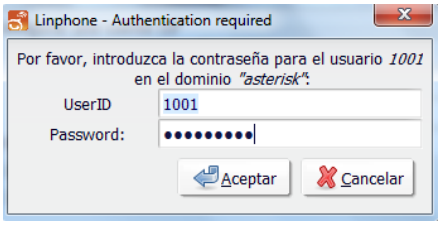
Estos son los pasos para la creación de extensiones de usuarios, lo mismo se hizo con las extensiones del Servidor Elastix B con sus extensiones correspondientes.

IV.III.IV CREACION DE CLIENTES SOFTPHONE

Se ejecuta Linphone, dar click en Opciones y luego dar click en preferencias, habilitar el soporte para ipv6, luego se da click en Gestionar cuentas SIP y se configura tal como se indica en las figuras.







Introducir la clave de la extensión y verificar su registro, debe ser “Successful”

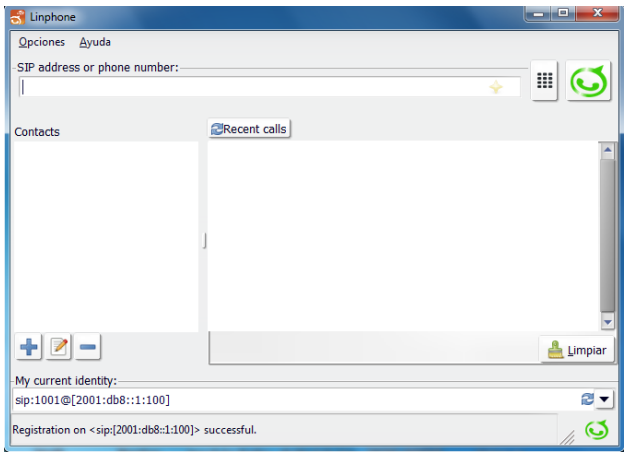


Figura IV. XXII *Configuración del softphone en IPv6*
Fuente: *Autor de la tesis.*

Ahora se verifica en el servidor PBX las cuentas registradas.

*server1*CLI> sip show peers*

Name/username	*Host*	*Dyn*	*Forcerport*	*ACL*	*Port*	*Status*
1001/1001	*2001:db8::1:2*	*D*	*N*	*A*	*5060*	*OK (2 ms)*
1002/1002	*172.30.60.101*	*D*	*N*	*A*	*5038*	*OK (25 ms)*

Como se puede observar, están registrados los clientes en IPv6 para la extensión santyEa “1001” y previamente configurado santyEa2 “1002” en IPv4 dando a notar que el servidor tiene un direccionamiento Dual-Stack para el protocolo SIP.

Para el Server2 (Elastix B) se tiene las siguientes cuentas registradas.

*Server2*CLI> sip show peers*

Name/username	*Host*	*Dyn*	*Forcerport*	*ACL*	*Port*	*Status*
2001/2001	*2001:db8::2:8*	*D*	*N*	*A*	*5060*	*OK (1 ms)*
2002/2002	*192.168.4.19*	*D*	*N*	*A*	*5060*	*OK (3 ms)*

De la misma manera se configura las cuentas en el servidor B, la extensión “santyEb” “2001” y previamente configurado santyEb2 “2002” en IPv4 dando a notar que el servidor tiene un direccionamiento Dual-Stack para el protocolo SIP.

IV.III.V CONFIGURACION DE LA TRONCAL SIP

En la pestaña “PBX”, dar click en “Troncales”, luego escoger la opción “Añadir Troncales SIP”, a continuación se asigna un nombre a la troncal. (Elastix A)

*Trunk Name: **ea2eb***

En “PEER Details” se configura los parámetros de la troncal local y remota.

PEER Details
Username=elastix1
Type=peer
Secret=troncal21

Qualify=yes
Nat=no
Host=2001:db8::2:100 *///IP del servidor B*
Fromuser=elastix1
Fromdomain=2001:db8::1:100 *///IP del servidor A*
Dynamic=no

USER Context elastix2
USER Details
Secret=troncal12
Type=user
Context=from-internal
Host=2001:db8::2:100

Ahora dar click en “Rutas Salientes”, se asigna el nombre del servidor remoto y su extensión.

Route Name: elastix2

Dial Patterns that will use this route
(prepend) + prefix | [2xxx / CallerId]

Guardar los cambios.

A continuación se hace lo siguiente en Elastix B

Trunk Name: eb2ea

Configuramos “PEER DETAILS”

PEER Details
Username=elastix2
Type=peer
Secret=troncal12
Qualify=yes
Nat=no
Host=2001:db8::1:100 *///IP del servidor A*
Fromuser=elastix2
Fromdomain=2001:db8::2:100 *///IP del servidor B*
Dynamic=no

USER Context elastix1
USER Details
Secret=troncal21
Type=user
Context=from-internal
Host=2001:db8::1:100

Guardar los cambios y se procede a configurar la “RUTA SALIENTE”

Route Name: elastix1

Dial Patterns that will use this route
(prepend) + prefix | [1xxx / CallerId]

Guardar los cambios.

Se verifica si la troncal está o no configurada a través de modo Web. (Elastix A)

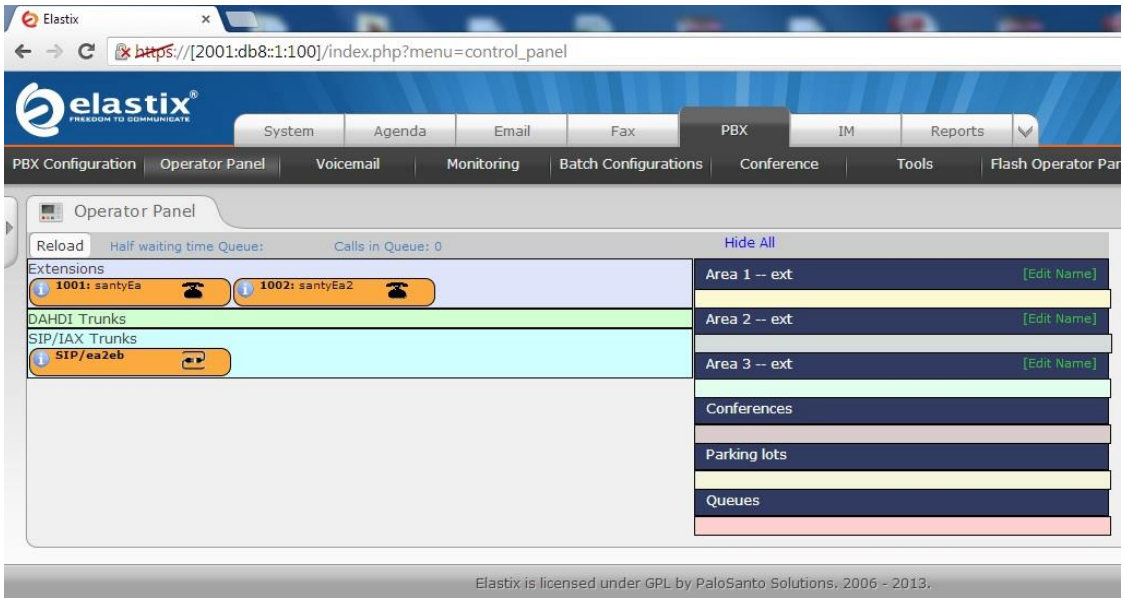


Figura IV. XXIII *Troncal SIP modo WEB Elastix A*
Fuente: *Autor de la tesis.*

La figura anterior nos indica que están configuradas las extensiones creadas y además está configurada la troncal SIP.

Verificar en el servidor la troncal SIP.

*server1*CLI> sip show peers*

Name/username	*Host*	*Dyn*	*Forcerport*	*ACL*	*Port*	*Status*
1001/1001	*2001:db8::1:2*	*D*	*N*	*A*	*5060*	*OK (2 ms)*
1002/1002	*172.30.60.101*	*D*	*N*	*A*	*5060*	*OK (25 ms)*
ea2eb/elastix1	*2001:db8::2:100*				*5060*	*OK (3 ms)*

3 sip peers [Monitored: 3 online, 0 offline Unmonitored: 0 online, 0 offline]

*server1*CLI>*

Como se observa, están configuradas las extensiones y la troncal SIP en IPv6 por el puerto 5060.

Ahora, se verifica si la troncal está o no configurada a través de modo Web. (Elastix B)

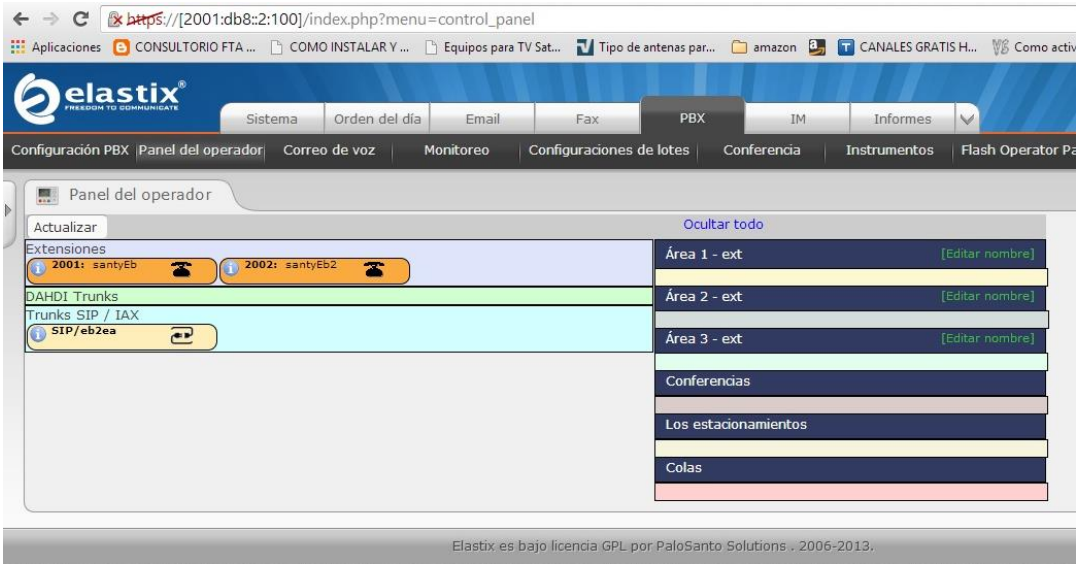


Figura IV. XXIV *Troncal SIP modo WEB Elastix B*
Fuente: *Autor de la tesis.*

Se verifica en el servidor la troncal SIP

*Server2*CLI> sip show peers*

Name/username	*Host*	*Dyn*	*Forcerport*	*ACL*	*Port*	*Status*
2001/2001	*2001:db8::1:8*	*D*	*N*	*A*	*5060*	*OK (1 ms)*
2002/2002	*192.168.4.19*	*D*	*N*	*A*	*5060*	*OK (3 ms)*
eb2ea/elastix2	*2001:db8::1:100*				*5060*	*OK (3 ms)*

3 sip peers [Monitored: 3 online, 0 offline Unmonitored: 0 online, 0 offline]

*server1*CLI>*

Como se observa, están configuradas las extensiones y la troncal SIP en IPv6 por el puerto 5060 en el servidor Elastix B.

- **ANALISIS DE HACKING Y SEGURIDAD VoIP**

Para el análisis de vulnerabilidades en protocolos utilizados en centrales VoIP, se ejecuta el ataque **"Eavesdropping"** el cual se encarga de observar los paquetes SIP y RTP que circulan en la red

en texto plano para decodificarles y de esa manera obtener la información realizada en aquella llamada telefónica de manera ilegal.

Para efectuar el ataque se utiliza la herramienta Wireshark (Ethereal anteriormente) la cual está incluida en la distribución Kali-linux Backtrack. Wireshark hace el papel de sniffer y analizador de protocolos para poder capturar los paquetes de llamadas de voz y poder escuchar la llamada.

Para contrarrestar este ataque se debe cifrar los protocolos utilizados en centrales VoIP: SIP y RTP mediante certificados de seguridad SSL /TLS, para de esta manera ya no estén estos protocolos en texto plano sino en texto cifrado.

Los requerimientos de seguridad se analizará a través de los tres pilares fundamentales como son: Integridad, Confidencialidad y Disponibilidad.

IV.IV PRUEBAS DE PENETRACION PENTEST

Para las pruebas de penetración y captura de los paquetes de los protocolos SIP y RTP se realiza lo siguiente:

- ✓ **Convergencia del escenario:** se realizan llamadas para probar si los servidores brindan su servicio con la calidad de voz buena además probar si la troncal SIP está configurada correctamente en IPv6.
- ✓ **Lanzamiento del ataque:** para poder capturar los paquetes de los protocolos se realiza un sniffing utilizando el analizador de protocolos Wireshark, herramienta que está disponible en Kali-Linux Backtrack.
- ✓ **Captura de paquetes:** utilizando Wireshark se utilizan filtros de captura de paquetes de señalización y audio, en este caso “SIP or RTP” donde únicamente se realizara capturas de dichos protocolos.

Una vez que se realiza un sniffing en la red y únicamente observando protocolos SIP y RTP se procede al análisis de las capturas realizadas entre extensiones de la central VoIP

Se realiza una llamada desde la extensión 1XXX hacia la extensión 2XXX, la utilización de la troncal SIP hace posible que se conecten extensiones diferentes.

El sniffer se encarga de presentar los protocolos que circular a través de la red, para nuestro interés se utiliza el filtro “SIP or RTP”.

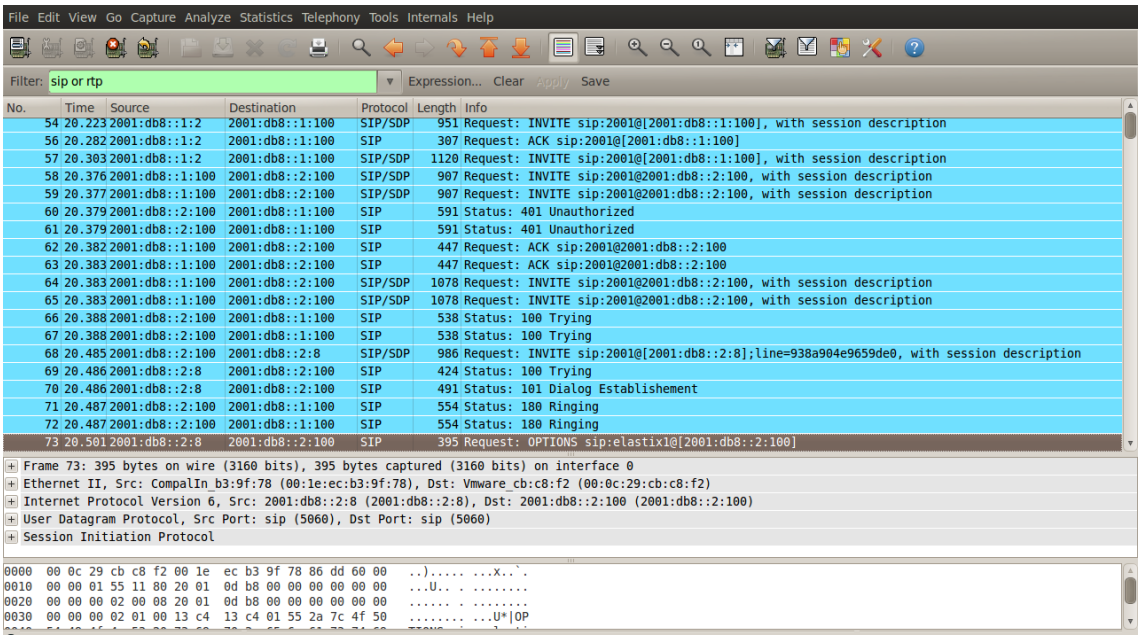


Figura IV. XXV *Captura de paquetes SIP*
Fuente: *Autor de la tesis.*

Realizando una llamada desde la extensión 1001@[2001:db8::1:2] del servidor Elastix A hacia la extensión 2001@[2001:db8::2:8] del servidor Elastix B podemos observar el tráfico que circula por la red desde Wireshark observando los paquetes del protocolo SIP en IPv6 como muestra la figura 4.16.

A continuación en la figura 4.17 se observa los paquetes de Audio RTP que circula por la red.

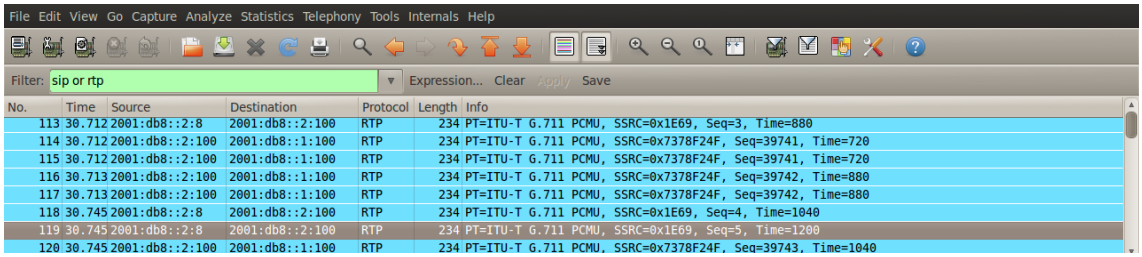


Figura IV. XXVI *Paquetes de Audio RTP*
Fuente: *Autor de la tesis.*

Dar click en la pestaña “Analyze”, escoger la opción “VoIP Calls”, dar cick en “Select All”, se observa las llamadas realizadas entre las extensiones donde ya se ha capturado paquetes RTP para su análisis y el contenido del mensaje como se muestra en la figura 4.18.

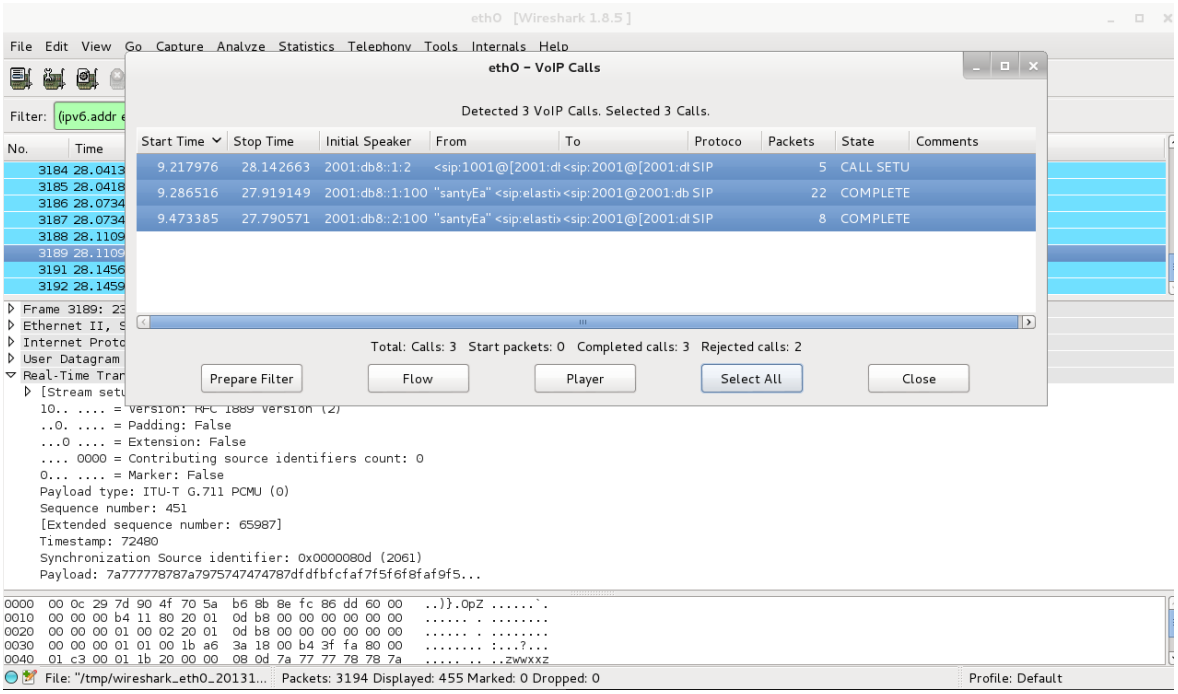


Figura IV. XXVII *Llamadas realizadas y captura de paquetes RTP*
Fuente: *Autor de la tesis.*

A continuación dar click en “Flow” y se indica las peticiones de SIP desde una terminal a otra, como se puede observar en la figura 4.19 se realiza la llamada entre las extensiones brindando un esquema básico y grafico del proceso de la llamada realizada desde que comenzó hasta cuando finalizo la llamada indicando códec’s y protocolos VoIP.

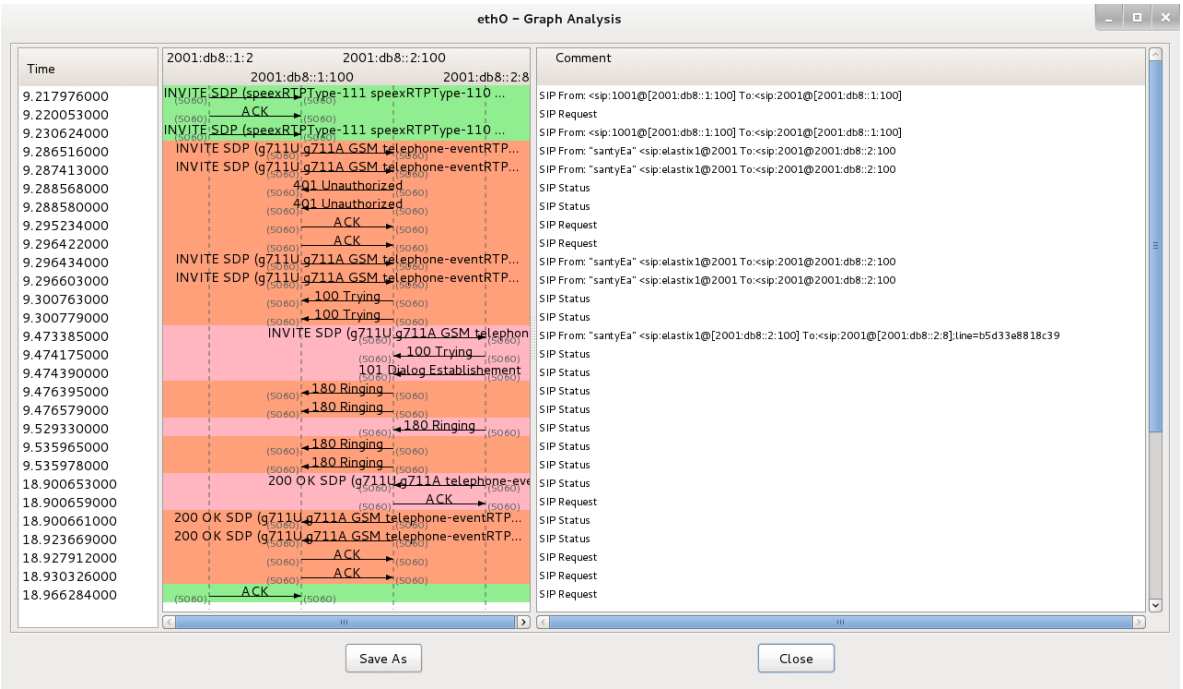


Figura IV. XXVIII *Diagrama del proceso de llamadas en SIP*
Fuente: *Autor de la tesis.*

Ahora dar click en “Player” y luego en “Decode”; se presenta el audio capturado entre las terminales de una extensión a otra, obteniendo de esta forma el mensaje en texto plano, el cual fue informado desde el transmisor al receptor.

Damos un click en “Play” y escuchamos el audio de la conversación.

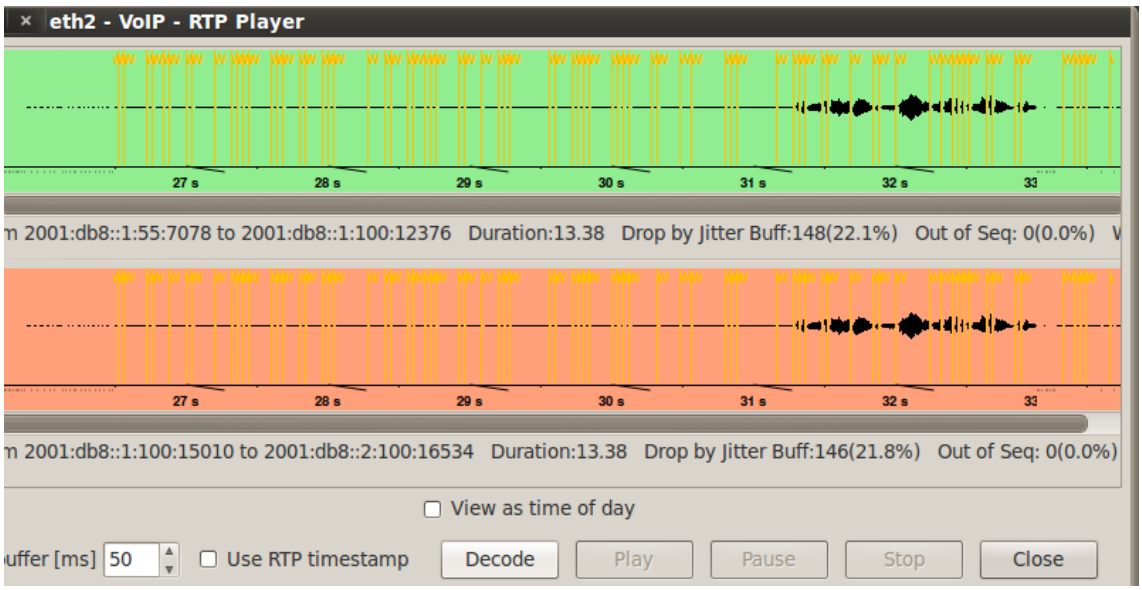


Figura IV. XXIX *Decodificación de la llamada*
Fuente: *Autor de la tesis.*

IV.V PROPUESTA DE SEGURIDAD ANTI-ATAQUE

IV.V.I ESCENARIO 2: RED VoIP CON PROPUESTA DE SEGURIDAD

Para brindar seguridad a los protocolos en centrales VoIP, se ha configurado certificados de seguridad tls y srtp para que de esta manera los paquetes sean cifrados y no estén en texto plano, con la finalidad de que no puedan ser escuchadas las conversaciones telefónicas, ***Anexo 2***.

Transport Layer Security (TLS) y secure Real Time Protocol (sRTP) son métodos de encriptación para cifrado de VoIP en SIP y RTP respectivamente y únicamente puede ser desencriptados por la parte del usuario final interesado, de esta manera se previene intercepciones de terceras personas.

Elastix cuenta con estos scripts de configuración por defecto y con soporte para IPv6, además viene compilados openssl y libSRTP para que únicamente puedan ser ejecutados obviamente teniendo conocimientos de como configurar.

Elastix es un sistema operativo basado en Linux CentOS, es una versión compilada de Asterisk y Free PBX el cual ya están generados los scripts para la configuración de TLS y sRTP y que son soportados por teléfonos físicos como en Softphones.

Para encriptar las llamadas y proteger los protocolos en centrales VoIP se realiza lo siguiente:

- ✓ **Modificar el fichero function.inc.php.**
- ✓ **Configurar encriptación entre servidores para asegurar la troncal SIP**
- ✓ **Configurar la encriptación para clientes locales.**

IV.V.II MODIFICACION SCRIPT FUNCTIONS.INC.PHP

Por defecto Elastix en su parte web, no presenta los campos (encription y transport) que son campos fundamentales para la encriptación en extensiones y en la troncal.

Sin embargo se puede modificar el contenido del script ***functions.inc.php*** para poder visualizar en la parte web de Elastix, asignando campos adicionales de programación para que acepte los parámetros de modificación y que no altere la funcionalidad de Elastix

Este script se encuentra en el siguiente path:

 # cat /var/www/html/admin/modules/core/

Las modificaciones se las hizo de la siguiente manera en ambos servidores:

```
if ( !is_array($sipfields) ) { // left for compatibilty....lord knows why !
        $sipfields = array(
            array($account,'accountcode',$db-
>escapeSimple((isset($_REQUEST['accountcode']))?$_REQUEST['accountcode']:''),$flag++),
            array($account,'secret',$db-
>escapeSimple((isset($_REQUEST['secret']))?$_REQUEST['secret']:''),$flag++),
            array($account,'canreinvite',$db-
>escapeSimple((isset($_REQUEST['canreinvite']))?$_REQUEST['canreinvite']:'no'),$flag++),
            array($account,'context',$db-
>escapeSimple((isset($_REQUEST['context']))?$_REQUEST['context']:'from-internal'),$flag++),
            array($account,'dtmfmode',$db-
>escapeSimple((isset($_REQUEST['dtmfmode']))?$_REQUEST['dtmfmode']:''),$flag++),
            array($account,'host',$db-
>escapeSimple((isset($_REQUEST['host']))?$_REQUEST['host']:'dynamic'),$flag++),
            array($account,'type',$db
            >escapeSimple((isset($_REQUEST['type']))?$_REQUEST['type']:'friend'),$flag++),3793
        array($account,'mailbox',$db->escapeSimple((isset($_REQUEST['mailbox'])) &&
        !empty($_REQUEST['mailbox']))?$_REQUEST['mailbox']:$account.'@device'),$fl ag++),
            array($account,'username',$db-
>escapeSimple((isset($_REQUEST['username']))?$_REQUEST['username']:$account),$flag++),
            array($account,'nat',$db-
>escapeSimple((isset($_REQUEST['nat']))?$_REQUEST['nat']:'yes'),$flag++),
```

```
            array($account,'port',$db-
>escapeSimple((isset($_REQUEST['port']))?$_REQUEST['port']:'5060'),$flag++),
                    array($account,'qualify',$db-
>escapeSimple((isset($_REQUEST['qualify']))?$_REQUEST['qualify']:'yes'),$flag++),
                    array($account,'callgroup',$db-
>escapeSimple((isset($_REQUEST['callgroup']))?$_REQUEST['callgroup']:''),$flag++),
                    array($account,'pickupgroup',$db-
>escapeSimple((isset($_REQUEST['pickupgroup']))?$_REQUEST['pickupgroup']:''),$flag++),
                    array($account,'deny',$db-
>escapeSimple((isset($_REQUEST['deny']))?$_REQUEST['deny']:''),$flag++),
                    array($account,'permit',$db-
>escapeSimple((isset($_REQUEST['permit']))?$_REQUEST['permit']:''),$flag++),
                    array($account,'disallow',$db-
>escapeSimple((isset($_REQUEST['disallow']))?$_REQUEST['disallow']:''),$flag++),
                    array($account,'allow',$db-
>escapeSimple((isset($_REQUEST['allow']))?$_REQUEST['allow']:''),$flag++),
                    array($account,'encryption',$db-
>escapeSimple((isset($_REQUEST['allow']))?$_REQUEST['allow']:''),$flag++),
                    array($account,'transport',$db-
>escapeSimple((isset($_REQUEST['allow']))?$_REQUEST['allow']:''),$flag++)
                     );
```

Para modificar los parámetros de configuración se realiza lo siguiente agregando los campos:

```
// sip
     $tmparr = array();5995
    $tmparr['secret'] = array('value' => '', 'level' => 0, 'jsvalidation' => '(isEmpty() &&
    !confirm('".$msgConfirmSecret."')) || (!isEmpty() && weakSecret())', 'failvalidationmsg' =>
    $msgInvalidSecret);
```

```
$tmparr['dtmfmode'] = array('value' => 'rfc2833', 'level' => 0, 'jsvalidation' => 'isEmpty()', 'failvalidationmsg'
=> $msgInvalidDTMFMODE );
$tmparr['canreinvite'] = array('value' => 'no', 'level' => 1);
$tmparr['context'] = array('value' => 'from-internal', 'level' => 1);
$tmparr['host'] = array('value' => 'dynamic', 'level' => 1);
$tmparr['type'] = array('value' => 'friend', 'level' => 1);
$tmparr['nat'] = array('value' => 'yes', 'level' => 1);
$tmparr['port'] = array('value' => '5060', 'level' => 1);
$tmparr['qualify'] = array('value' => 'yes', 'level' => 1);
$tmparr['callgroup'] = array('value' => '', 'level' => 1);
$tmparr['pickupgroup'] = array('value' => '', 'level' => 1);
$tmparr['disallow'] = array('value' => '', 'level' => 1);
$tmparr['allow'] = array('value' => '', 'level' => 1);
$tmparr['dial'] = array('value' => '', 'level' => 1);
$tmparr['accountcode'] = array('value' => '', 'level' => 1);
$tmparr['mailbox'] = array('value' => '', 'level' => 1);6011
$tmparr['vmexten'] = array('value' => '', 'level' => 1);
$tmparr['deny'] = array('value' => '0.0.0.0/0.0.0.0', 'level' => 1);6013
$tmparr['permit'] = array('value' => '0.0.0.0/0.0.0.0', 'level' => 1);
$tmparr['encryption'] = array('value' => 'no', 'level' => 1);
$tmparr['transport'] = array('value' => 'udp', 'level' => 1);
$currentcomponent->addgeneralarrayitem('devtechs', 'sip', $tmparr);
unset($tmparr);
```

Una vez realizado los cambios se reinicia el amportal.

```
#amportal stop
#amportal start
```

IV.V.III CREACION DE CERTIFICADOS DE SEGURIDAD TLS/SSL Y SRTP

Elastix cuenta con los scripts necesarios para compilar los certificados de seguridad haciendo una autenticación de quienes se afilian a estos certificados firmados y codificados según la configuración de Elastix para encriptación de SIP y RTP

CERTIFICADOS PARA EL SERVIDOR Y LA TRONCAL SIP

Primero debemos generar los certificados solo en uno de los servidores, en este caso se lo hará en el servidor Elastix1 de la figura 4.2.

Se crea la carpeta “claves” para guardar los certificados en el servidor, el path es el siguiente:

 # mkdir /etc/asterisk/claves

 # sh /usr/share/doc/asterisk-1.8.20.0/contrib/scripts/ast_tls_cert -C 2001:db8::1:100 -O "Tesis" -d /etc/asterisk/claves/ -o server1

Donde:

-C: es el nombre (DNS) o dirección IP de la organización Matriz.

-O: nombre del objetivo, similar al objetivo al redactar un correo en Outlook.

-o: nombre de salida hacia un directorio especificado.

Click en enter y se genera el certificado:

No config file specified, creating '/etc/asterisk/claves//tmp.cfg'

You can use this config file to create additional certs without

re-entering the information for the fields in the certificate

Creating CA key /etc/asterisk/claves//ca.key

Generating RSA private key, 4096 bit long modulus

.....

....++

.....++

e is 65537 (0x10001)

Enter pass phrase for /etc/asterisk/claves//ca.key:

Verifying - Enter pass phrase for /etc/asterisk/claves//ca.key:

Creating CA certificate /etc/asterisk/claves//ca.crt

Enter pass phrase for /etc/asterisk/claves//ca.key:

Creating certificate /etc/asterisk/claves//server1.key

Generating RSA private key, 1024 bit long modulus

.++++++

.....++++++

e is 65537 (0x10001)

Creating signing request /etc/asterisk/claves//server1.csr

Creating certificate /etc/asterisk/claves//server1.crt

Signature ok

subject=/CN=2001:db8::1:100/O=Tesis

Getting CA Private Key

Enter pass phrase for /etc/asterisk/claves//ca.key:

Combining key and crt into /etc/asterisk/claves//server1.pem

Ahora se crea otro para el servidor Elastix2 con la finalidad de encriptar la troncal SIP entre estos servidores.

 # sh /usr/share/doc/asterisk-1.8.20.0/contrib/scripts/ast_tls_cert -C 2001:db8::2:100 -O "Tesis" -d /etc/asterisk/claves/ -o server2

Click en enter:

No config file specified, creating '/etc/asterisk/claves//tmp.cfg'

You can use this config file to create additional certs without

re-entering the information for the fields in the certificate

Creating CA key /etc/asterisk/claves//ca.key

Generating RSA private key, 4096 bit long modulus

.....++

.....++

e is 65537 (0x10001)

Enter pass phrase for /etc/asterisk/claves//ca.key:

Verifying - Enter pass phrase for /etc/asterisk/claves//ca.key:

Creating CA certificate /etc/asterisk/claves//ca.crt

Enter pass phrase for /etc/asterisk/claves//ca.key:

Creating certificate /etc/asterisk/claves//server2.key

Generating RSA private key, 1024 bit long modulus

.....++++++

....++++++

e is 65537 (0x10001)

Creating signing request /etc/asterisk/claves//server2.csr

Creating certificate /etc/asterisk/claves//server2.crt

Signature ok

subject=/CN=2001:db8::2:100/O=Tesis

Getting CA Private Key

Enter pass phrase for /etc/asterisk/claves//ca.key:

Combining key and crt into /etc/asterisk/claves//server2.pem

Ahora se observa que se han creado algunos certificados en el path:

 # ll /etc/asterisk/claves

---------- 1 root root 151 abr 27 11:06 ca.cfg

---------- 1 root root 1740 abr 27 11:06 ca.crt

---------- 1 root root 3311 abr 27 11:06 ca.key

---------- 1 root root 1196 abr 25 23:05 server1.crt

---------- 1 root root 562 abr 25 23:05 server1.csr

---------- 1 root root 891 abr 25 23:05 server1.key

---------- 1 root root 2087 abr 25 23:05 server1.pem

---------- 1 root root 1196 abr 27 11:06 server2.crt

---------- 1 root root 562 abr 27 11:06 server2.csr

---------- 1 root root 887 abr 27 11:06 server2.key

---------- 1 root root 2083 abr 27 11:06 server2.pem

---------- 1 root root 114 abr 27 11:06 tmp.cfg

A continuación se envía por copia segura encriptada (SCP) hacia el servidor Elastix2 los siguientes ficheros:

[root@server1 ~]# scp /etc/asterisk/claves/server2.pem root@[2001:db8::2:100]:/etc/asterisk/claves/

The authenticity of host '2001:db8::2:100 (2001:db8::2:100)' can't be established.

RSA key fingerprint is c2:0d:f3:81:81:27:5a:5b:72:27:29:29:c5:39:d8:ea.

Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added '2001:db8::2:100' (RSA) to the list of known hosts.

root@2001:db8::2:100's password:

server2.pem 100% 2087 2.0KB/s 00:00

[root@server1 ~]# scp /etc/asterisk/claves/ca.crt root@[2001:db8::2:100]:/etc/asterisk/claves/

root@2001:db8::2:100's password:

ca.crt 100% 1740 1.7KB/s 00:00

[root@server1 ~]# scp /etc/asterisk/claves/ca.key root@[2001:db8::2:100]:/etc/asterisk/claves/

root@2001:db8::2:100's password:

ca.key 100% 1370 1.2KB/s 00:00

No olvidar cuando pida autenticación en password, escribir la clave de Elastix2, además de tener previamente creado el directorio “claves”.

A continuación se habilita el soporte para “tls y srtp” en el servidor Elastix.

Ingresar a la web de Elastix y escribir el usuario y contraseña:

https://2001:db8::1:100

A continuación se ingresa a la configuración en Free PBX no embebido.

Se iniciara una página web con la interfaz de Free PBX de Asterisk, en donde se habilita “tls y srtp”, de igual manera se tendrá que ingresar autenticándose con usuario y contraseña.

Presionar click en “Tools” y luego en “SIP settings”

A continuación se procede a habilitar tls y srtp de la siguiente manera:

Tlsenable=yes

Tlsbindaddr=[::]

Tlsdontverifyserver=yes

Tlscertfile=/etc/asterisk/claves/server1.pem

Tlscafile=/etc/asterisk/claves/ca.crt

Tlscipher=ALL

Srtpcapable=yes

Tcpenable=yes

Encryption=no

En el servidor Elastix2 se cambia a *Tlscertfile=/etc/asterisk/claves/server2.pem*

Se guardan los cambios y reiniciamos.

Ahora nuevamente abrir la página web de Elastix y modificar “Trunks/outgoing settings”

Se agrega lo siguiente en ambos servidores:

Encryption=yes

Transport=tls

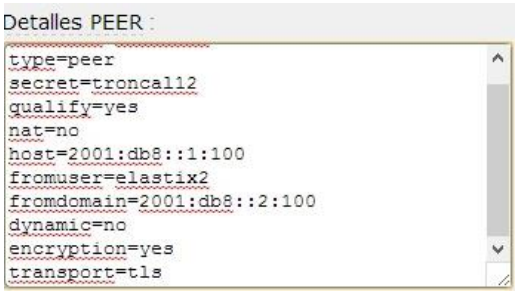


Figura IV. XXX *Configuración TLS y sRTP en la troncal SIP*
Fuente: *Autor de la tesis.*

Si se ha configurado correctamente en el servidor se mostrara:

*server1*CLI> sip show peers*

Name/username Host Dyn Forcerport ACL Port Status

ea2eb/elastix1 2001:db8::1:100 5061 OK (13 ms)

1 sip peers [Monitored: 1 online, 0 offline Unmonitored: 0 online, 0 offline]

En el servidor Elastix2 se mostrara:

*Server2*CLI> sip show peers*

Name/username Host Dyn Forcerport ACL Port Status

eb2ea/elastix2 2001:db8::2:100 5061 OK (11 ms)

1 sip peers [Monitored: 1 online, 0 offline Unmonitored: 0 online, 0 offline]

De esta manera se observa que la troncal SIP está siendo escuchada por el puerto 5061 y ya no por el puerto 5060, ya que el puerto 5061 es SIP seguro (SIPS) y el puerto 5060 es SIP en UDP.

IV.V.IV CERTIFICADOS PARA CLIENTES SOFTPHONE.

Para crear certificados para las extensiones locales se hace lo siguiente:

 # sh /usr/share/doc/asterisk-1.8.20.0/contrib/scripts/ast_tls_cert -m client -c /etc/asterisk/claves/ca.crt -k /etc/asterisk/claves/ca.key -C 1002.2001:db8::1:100 -O "Tesis" -d /etc/asterisk/claves/ -o 1002

Donde:

-m client: utilizado para crear certificados para extensiones locales.

-c: certificado de autenticación cliente-servidor.

-k: llaves de autenticación cliente-servidor.

-C: extensión a registrarse.

-O: nombre objetivo.

-d: directorio de almacenamiento de certificados.

-o: nombre de la extensión.

Click en enter para generar el certificado.

Se procede a la configuración del softphone.

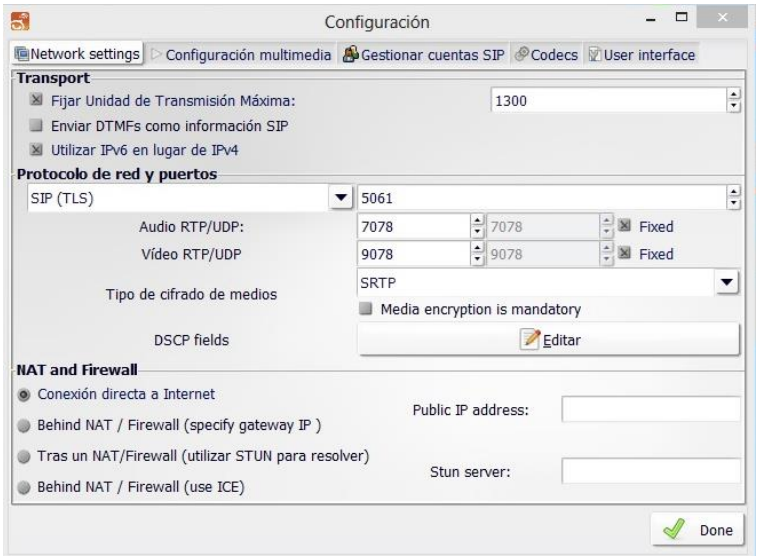


Figura IV. XXXI *Configuración de encriptación de llamadas en el softphone*
Fuente: *Autor de la tesis.*

Se observa lo siguiente en el servidor.

*server1*CLI> sip show peers*

Name/username	*Host*	*Dyn*	*Forcerport*	*ACL*	*Port*	*Status*
1001/73596184	*172.30.60.101*	*D*	*N*	*A*	*54917*	*OK (2 ms)*
1002/541275	*2001:db8::1:2*	*D*	*N*	*A*	*54963*	*OK (25 ms)*
ea2eb/elastix1	*2001:db8::2:100*				*5061*	*OK (3 ms)*

3 sip peers [Monitored: 3 online, 0 offline Unmonitored: 0 online, 0 offline]

*server1*CLI>*

Y en el servidor2

*server1*CLI> sip show peers*

Name/username	*Host*	*Dyn*	*Forcerport*	*ACL*	*Port*	*Status*
2001/58231	*192.168.4.19*	*D*	*N*	*A*	*58231*	*OK (1 ms)*

2002/2002 2001:db8::2:8 D N A 5061 OK (3 ms)

eb2ea/elastix2 2001:db8::1:100 5061 OK (3 ms)

3 sip peers [Monitored: 3 online, 0 offline Unmonitored: 0 online, 0 offline]

*server1*CLI>*

IV.VI COMPROBACION DE LA PROPUESTA DE SEGURIDAD

Se realiza una llamada de la extensión 1XXX hacia la extensión 2XXX cualquiera para verificar si los paquetes pueden ser capturados y escuchados.

Para ello utilizamos el analizador de protocolos Wireshark, el cual monitorea los paquetes que circula por la red, para nuestro caso se filtra los protocolos SIP y RTP.

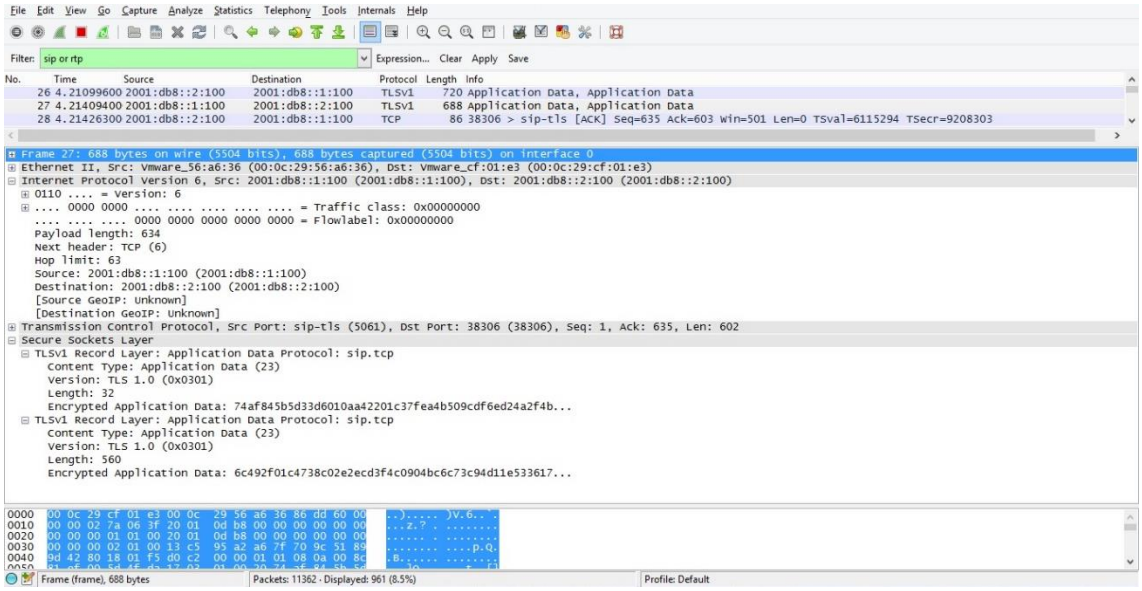


Figura IV. XXXII *Monitoreo de los protocolos SIP y RTP*
Fuente: *Autor de la tesis.*

Como se puede apreciar en la figura 4.23, el protocolo TLSv1 está configurado en las extensiones y en la troncal SIP, denotando que SIP está protegido por este protocolo ya que generalmente SIP funciona en UDP.

En los clientes se prueba que la información esta encriptada, ya que SIP está escuchando en el puerto 5061 por SIP seguro (SIPS), además se puede observar en la figura 4.24 que el audio está siendo cifrado a través del protocolo sRTP.

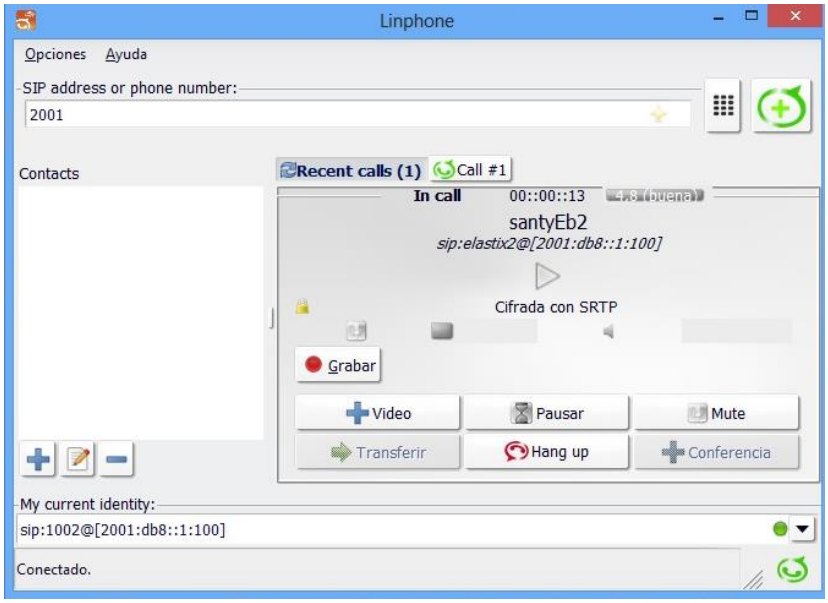


Figura IV. XXXIII *Cifrado en los softphones*
Fuente: *Autor de la tesis.*

A continuación se probara si está cifrado RTP en el analizador de protocolos Wireshark.

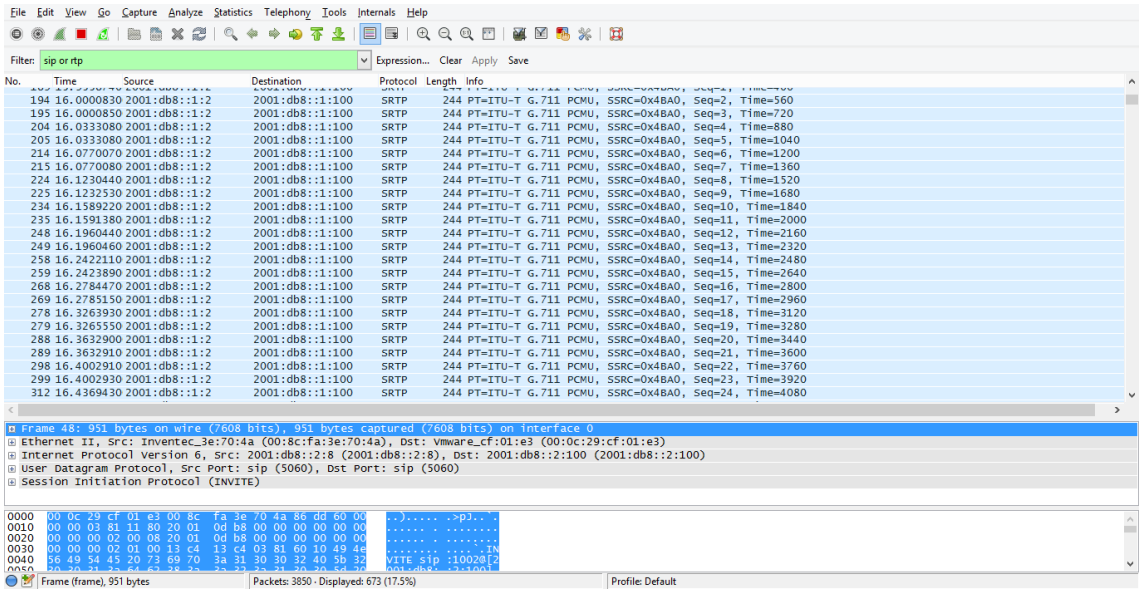


Figura IV. XXXIV *Paquetes cifrados sRTP*
Fuente: *Autor de la tesis.*

A continuación se observa en la figura que el audio está cifrado, por lo tanto no puede ser escuchado ya que está protegido a través del protocolo sRTP que únicamente puede ser decodificado por el softphone de la dirección de destino cuyo certificado de seguridad es asignado desde el servidor al cliente.

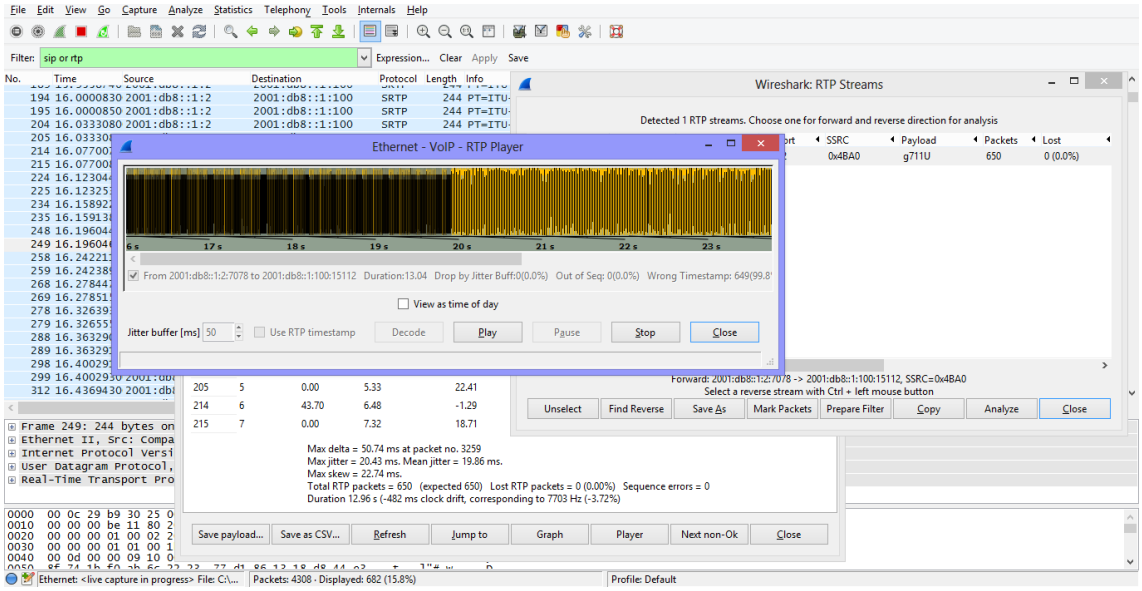


Figura IV. XXXV *Stream de audio de un paquete sRTP*
Fuente: *Autor de la tesis.*

CAPÍTULO V

ANÁLISIS Y RESULTADOS

V.I INTRODUCCIÓN

En este capítulo se realizará un análisis de seguridad en base a las vulnerabilidades en protocolos de centrales VoIP y los indicadores de los principios de seguridad (Confidencialidad, Integridad y Disponibilidad).

Cabe recalcar que en escenario 1 (vulnerable) los paquetes de audio RTP pueden ser extraídos por el atacante para realizar escuchas indebidas, mientras que en el escenario 2 (propuesta de seguridad) los paquetes de audio RTP son encriptados, por tanto no pueden ser escuchados; mientras que el protocolo de señalización SIP es protegido mediante TLS/SSL.

Se realizará una comparación de resultados entre los escenarios tanto vulnerable como el empleado las técnicas de seguridad, como los realizados en el capítulo anterior para de esta manera poder comprobar si la hipótesis planteada es verdadera realizando un análisis estadístico para su comprobación.

V.II ANALISIS DE SEGURIDAD ESCENARIO 1 (VULNERABLE)

Para el análisis de vulnerabilidades en protocolos utilizados en centrales VoIP se los puede analizar mediante requerimientos de seguridad, mediante los pilares fundamentales como son:

- **Disponibilidad:** garantiza el acceso a la información de comunicaciones en redes VoIP únicamente a aquellos autorizados en el momento que requieran del servicio.
- **Integridad:** garantiza que la información recibida por el receptor sea la misma que envió el transmisor, libre de modificaciones.
- **Confidencialidad:** garantiza que la conexión no pueda ser interceptada por terceros.

Mediante estos principios se evaluara si las redes VoIP son seguras mediante la utilización del protocolo IPv6 utilizando troncales SIP.

- **Muestreo de llamadas para la realización de pruebas.**

Para tomar una muestra de cuantas llamadas realizar, se utiliza la técnica de muestreo de población aleatoria infinita ya que podemos efectuar un sin número de llamadas en las centrales PBX, utilizando la siguiente formula:

$$n = \frac{Z_{\alpha}^{2} \cdot p \cdot q}{i^{2}}$$

Donde:

N: número de llamadas a realizar para las pruebas.

Z: factor probabilístico correspondiente a la distribución de Gauss.

P: probabilidad de éxito.

Q: probabilidad de fracaso.

I: nivel de error máximo para identificar la muestra.

A continuación se establece los valores a cada variable para determinar la muestra (N).

α : nivel de confianza al 10%

1 - α = 90% » » **Z** = 1,65
P + Q = 1 » » **P** = 0,5
Q = 1 – P » » **Q** = 1 – 0,5 = 0,5
I = 10% » » **I** = 0.1

$$N = \frac{Z^2 * P * Q}{I^2}$$

$$N = \frac{1{,}65^2 * 0{,}5 * 0{,}5}{0{,}1^2}$$

$$N = \frac{0{,}681}{0{,}01}$$

$N = 68$ llamadas a realizar como muestra para cada escenario.

Una vez realizadas todas las llamadas se observó que a través de Wireshark, todas las llamadas por paquetes RTP bajo señalización SIP fueron capturadas, de esta manera se establece el siguiente análisis:

Abreviaturas:

CF: Confidencialidad

IN: Integridad

DP: Disponibilidad

Nivel de seguridad:

1: Insuficiente

2: Aceptable

3: Excelente

	SIP			RTP		
Llamada No	**DP**	**IN**	**CF**	**DP**	**IN**	**CF**
1	1	1	1	1	1	1
2	1	1	1	1	1	1
3	1	1	2	1	1	1
4	1	1	1	1	1	1
5	1	1	1	1	2	2
6	1	1	1	1	1	1
7	1	1	1	1	1	1

8	1	1	1	1	1	1
9	1	1	1	1	1	1
10	1	2	1	1	1	1
11	1	1	1	1	1	1
12	1	1	1	1	1	1
13	1	1	1	1	1	1
14	1	1	1	1	1	1
15	1	1	1	1	1	1
16	1	1	1	1	1	1
17	1	1	1	2	2	2
18	1	1	1	1	1	1
19	1	1	1	1	1	1
20	1	1	1	1	1	1
21	1	1	1	1	1	1
22	1	1	1	1	1	1
23	2	1	1	1	1	1
24	1	1	1	1	1	1
25	1	1	1	1	1	1
26	1	1	1	1	1	1
27	1	1	1	1	1	1
28	1	1	1	1	1	1
29	1	1	1	1	1	1
30	1	1	1	1	1	1
31	1	1	1	1	1	1
32	1	1	1	2	1	2
33	1	2	2	1	1	1
34	1	1	1	1	1	1
35	1	1	1	1	1	1
36	1	1	1	1	1	1
37	1	1	1	1	1	1
38	1	1	1	1	1	1
39	1	1	1	1	1	1
40	1	1	1	1	1	1
41	1	1	1	1	1	1
42	1	1	1	1	1	1
43	1	1	1	1	1	1
44	1	1	1	1	1	1
45	1	1	1	1	1	1
46	2	1	2	1	1	1
47	1	1	1	1	1	1

48	1	1	1	1	1	1
49	1	1	1	1	2	2
50	1	1	1	1	1	1
51	1	1	1	1	1	1
52	1	1	1	1	1	1
53	1	1	1	1	1	1
54	1	1	1	2	1	1
55	1	1	1	1	1	1
56	1	1	1	1	1	1
57	1	1	1	1	1	1
58	1	1	1	1	1	1
59	1	1	1	1	1	1
60	1	1	1	1	2	1
61	1	1	1	1	1	1
62	1	1	1	1	1	1
63	1	1	1	1	1	1
64	1	1	1	1	1	1
65	1	1	1	1	1	1
66	1	1	1	1	1	1
67	2	2	2	1	1	1
68	1	1	1	1	1	2
Promedio	1	1	1	1	1	1

Tabla V. XIV *Datos tomados de cada llamada para el Escenario 1.*
Fuente: *Autor de la tesis.*

	CF	**IN**	**DP**	**Total**	**Promedio**	**Percent**
SIP	1	1	1	3	1	**33,33**
RTP	1	1	1	3	1	**33,33**
Total	2	2	2			
Percent	**33,33**	**33,33**	**33,33**			

Tabla V. XV *Nivel de seguridad del escenario 1*
Fuente: *Autor de la tesis.*

V.II.I ANALISIS DE SEGURIDAD EN PROTOCOLOS (V. DEPENDIENTE)

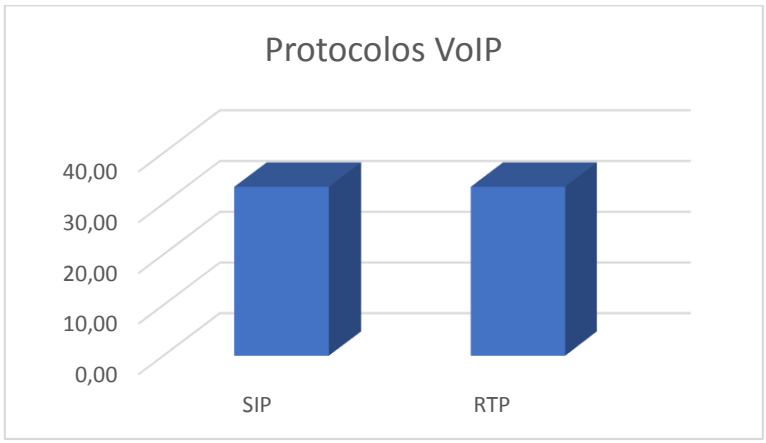


Figura V. XXXVI *Seguridad en la variable dependiente*
Fuente: *Autor de la tesis.*

INTERPRETACION: Como se puede observar en la figura V.XXXVI y el análisis de la tabla V.XV, tanto SIP como paquetes RTP fueron capturados a través de todas las llamadas realizadas, ya que el receptor y el transmisor no saben que su conversación está siendo interceptada, porque es un ataque discreto.

Se aprecia en la figura que un servidor Elastix ofrece un mínimo porcentaje de seguridad, pero brinda un buen servicio en comunicaciones VoIP.

V.II.II ANALISIS DE SEGURIDAD SEGÚN REQUERIMIENTOS (V. INDEPENDIENTE)

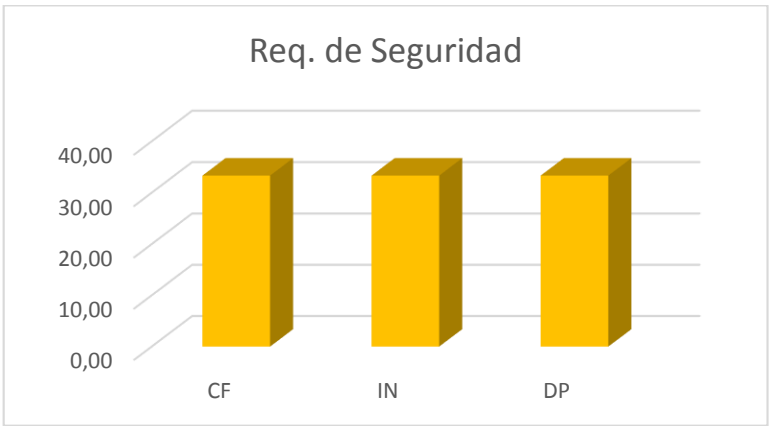


Figura V. XXXVII *Seguridad a la variable independiente*
Fuente: *Autor de la tesis.*

INTERPRETACION: Como se observa en la figura V.XXXVII, según los requerimientos de seguridad, los paquetes de señalización y audio pueden ser vistos a través de un sniffer disponible para el atacante, pueden ser sustraídos los paquetes para ser reproducidos y escuchados, afectando la integridad, disponibilidad y confidencialidad.

Elastix ofrece un porcentaje mínimo se seguridad si no se toman las prevenciones necesarias que este mismo servidor ofrece, para realizar configuraciones de seguridad.

V.III ANALISIS DE SEGURIDAD ESCENARIO 2 (PROP. DE SEGURIDAD)

De la misma manera, una vez realizadas todas las llamadas se observó que a través de Wireshark, todas las llamadas por paquetes RTP bajo señalización SIP no pudieron ser capturadas, de esta manera se establece el siguiente análisis:

Abreviaturas:

CF: Confidencialidad

IN: Integridad

DP: Disponibilidad

Nivel de seguridad:

1: Insuficiente

2: Aceptable

3: Excelente

	SIPS			SRTP		
Llamada No	DP	IN	CF	DP	IN	CF
1	3	3	2	3	3	3
2	3	2	2	3	3	3
3	3	3	2	3	3	3
4	2	3	1	3	3	3
5	1	3	3	3	3	2
6	2	3	1	3	2	3
7	2	3	2	3	3	2
8	2	3	2	3	3	3
9	2	3	3	3	3	3
10	2	3	2	2	3	3

11	2	3	3	3	3	3
12	2	3	2	3	3	3
13	2	3	2	3	3	3
14	2	1	2	3	3	3
15	2	2	1	3	3	3
16	1	3	3	3	3	3
17	2	3	2	3	2	3
18	2	3	2	3	3	3
19	2	3	2	3	2	3
20	2	3	1	3	3	3
21	2	3	2	3	3	3
22	3	3	3	3	3	3
23	2	2	3	3	3	3
24	2	3	2	3	3	3
25	2	3	2	3	3	3
26	2	3	3	3	3	3
27	2	3	3	3	3	3
28	2	3	2	3	3	3
29	2	3	2	3	3	3
30	2	3	1	3	3	3
31	2	3	3	3	3	3
32	2	3	3	3	3	3
33	2	2	2	3	3	3
34	2	2	2	3	3	3
35	2	2	2	3	3	3
36	2	2	2	3	3	3
37	2	1	2	3	3	3
38	2	3	2	3	3	3
39	2	3	2	3	3	3
40	2	3	1	3	3	3
41	2	3	1	3	3	3
42	2	3	3	3	3	3
43	2	3	2	3	3	3
44	2	3	2	3	3	3
45	2	3	3	3	3	3
46	2	3	2	3	3	3
47	3	3	2	3	3	3
48	1	3	2	3	3	3
49	2	3	2	3	3	2
50	2	3	2	3	3	3

51	2	3	1	3	3	3
52	2	3	2	3	3	3
53	2	3	3	3	3	3
54	2	3	3	2	3	3
55	2	3	2	3	3	3
56	2	3	2	3	3	3
57	2	3	2	3	3	3
58	2	3	2	3	3	3
59	2	3	2	3	3	3
60	2	3	2	2	2	3
61	2	3	2	3	3	3
62	2	3	2	3	3	3
63	2	3	3	3	3	3
64	2	3	2	3	3	3
65	2	3	2	3	3	3
66	3	3	2	2	3	3
67	2	2	2	3	3	3
68	1	3	3	3	3	3
Promedio	2,03	2,82	2,12	2,94	2,94	2,96
Redondeo	**2**	**3**	**2**	**3**	**3**	**3**

Tabla V. XVI *Datos tomados de cada llamada en el Escenario 2.*
Fuente: *Autor de la tesis.*

	CF	**IN**	**DP**	**Total**	**Promedio**	**Percent**
SIPS	2	3	2	7	2	77,78
SRTP	3	3	3	9	3	100
Total	5	6	5			
Percent	83,33	100	83,33			

Tabla V. XVII *Análisis de seguridad escenario 2*
Fuente: *Autor de la tesis.*

V.III.I ANALISIS DE SEGURIDAD EN PROTOCOLOS (V. DEPENDIENTE)

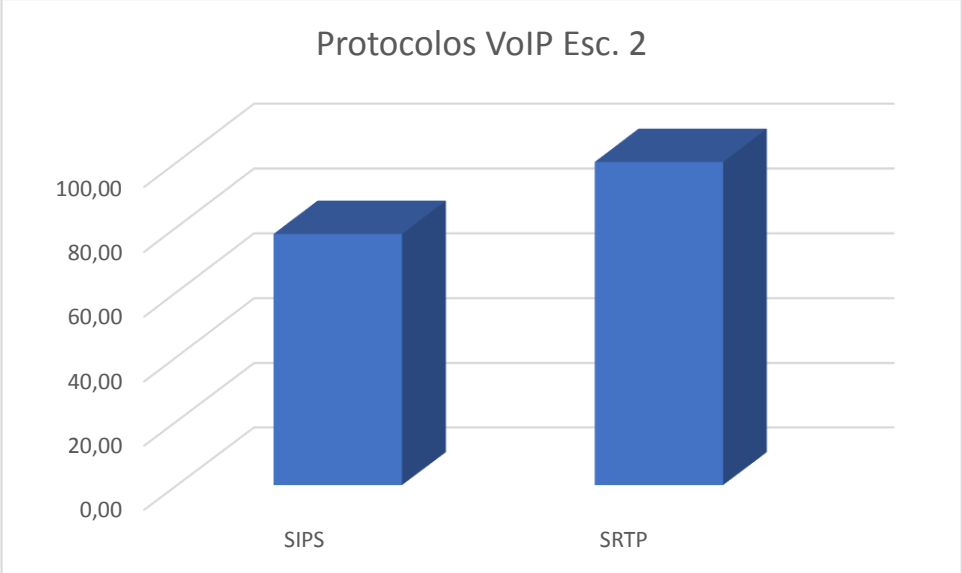


Figura V. XXXVIII *Seguridad en protocolos escenario 2*
Fuente: *Autor de la tesis.*

INTERPRETACION: Como se observa en la figura V.XXXVIII y el análisis de la tabla V.XVII, según el muestreo de llamadas realizadas, el nivel de seguridad ha aumentado debido a la configuración de TLS/SSL sobre SIP y encriptación de los paquetes RTP seguro (sRTP), de esta manera asegurando las conversaciones en VoIP en el protocolo IPv6 y asegurada también la troncal SIP permitiendo de esta manera que las comunicaciones no sean interceptadas.

De esta manera Elastix protege las conversaciones telefónicas bajo configuraciones de SIP seguro (SIPS) y audio y multimedia seguro (sRTP) en un buen porcentaje.

V.III.II ANALISIS DE SEGURIDAD EN REQUERIMIENTOS (V. INDEPENDIENTE)

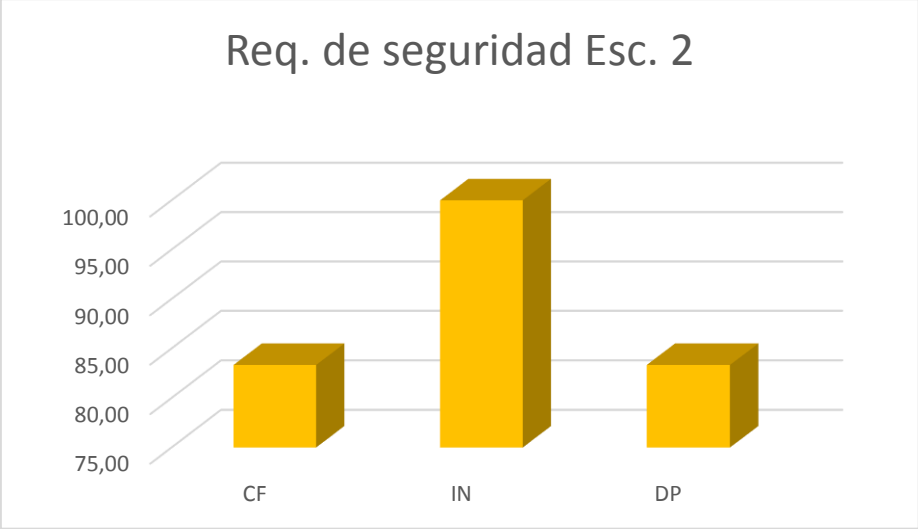


Figura V. XXXIX *Seguridad según requerimientos escenario 2*
Fuente: *Autor de la tesis.*

INTERPRETACION: Como se observa en la figura II.XXXIX, aumentan los porcentajes de los requerimientos de seguridad, los paquetes de audio y señalización no pueden ser vistos ni modificados y estarán disponibles sin que estos puedan ser capturados y descifrados.

De esta manera Elastix asegura sus comunicaciones con las debidas configuraciones en el mismo sobre herramientas de seguridad que este posee.

V.IV COMPARACION DE SEGURIDAD EN LOS ESCENARIOS 1 Y 2

A continuación se realiza un análisis entre los resultados del escenario vulnerable con los resultados del escenario con metodología de seguridad.

V.IV.I ANALISIS DE SEGURIDAD EN PROTOCOLOS (V. DEPENDIENTE)

	% Esc. 1	% Esc. 2	Diferencia
SIP	33,33	77,78	44,5
RTP	33,33	100	66,7

Tabla V. XVIII *Comparación de seguridad en protocolos entre escenarios*
Fuente: *Autor de la tesis.*

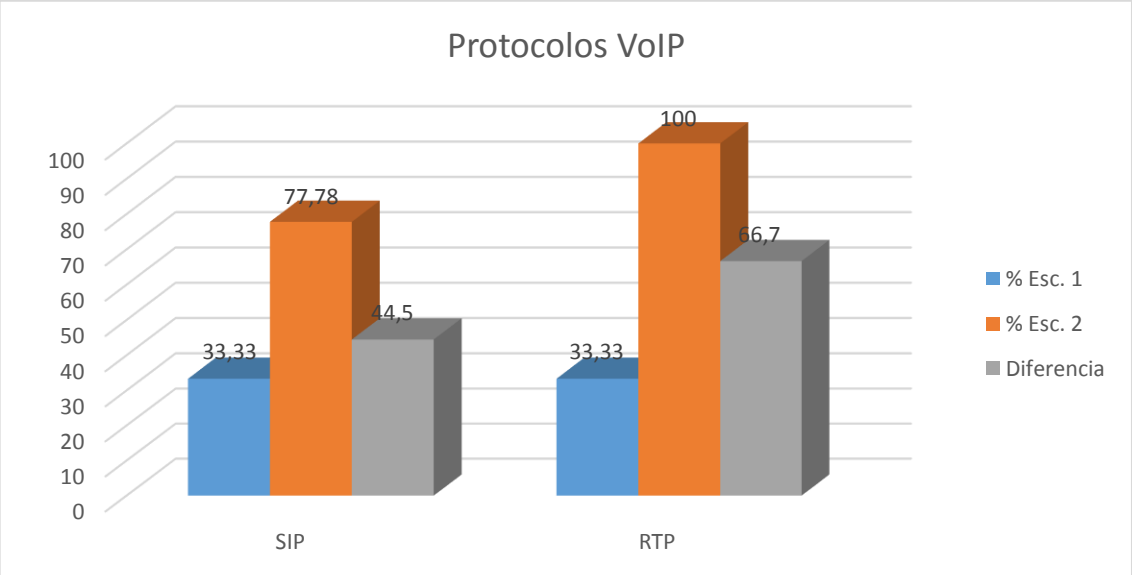


Figura V. XL *Comparación de seguridad de protocolos entre escenarios*
Fuente: *Autor de la tesis.*

INTERPRETACION: En la figura V.XL, se puede observar que a través de las propuestas de seguridad configuradas sobre el servidor, clientes y la troncal SIP en IPv6, la seguridad ha aumentado previniendo las capturas y escuchas de conversaciones en VoIP, por tanto la red VoIP en IPv6 está segura con la implementación de TLS/SSL y sRTP para cifrado de las comunicaciones en un alto porcentaje y evitando así, que la voz sea escuchada.

V.IV.II ANALISIS DE SEGURIDAD EN REQUERIMIENTOS (V. INDEPENDIENTE)

	CF	IN	DP
% Esc. 1	33,33	33,33	33,33
% Esc. 2	83,33	100	83,33
Diferencia	50	66,67	50

Tabla V. XIX *Comparación de requerimientos de seguridad entre escenarios*
Fuente: *Autor de la tesis.*

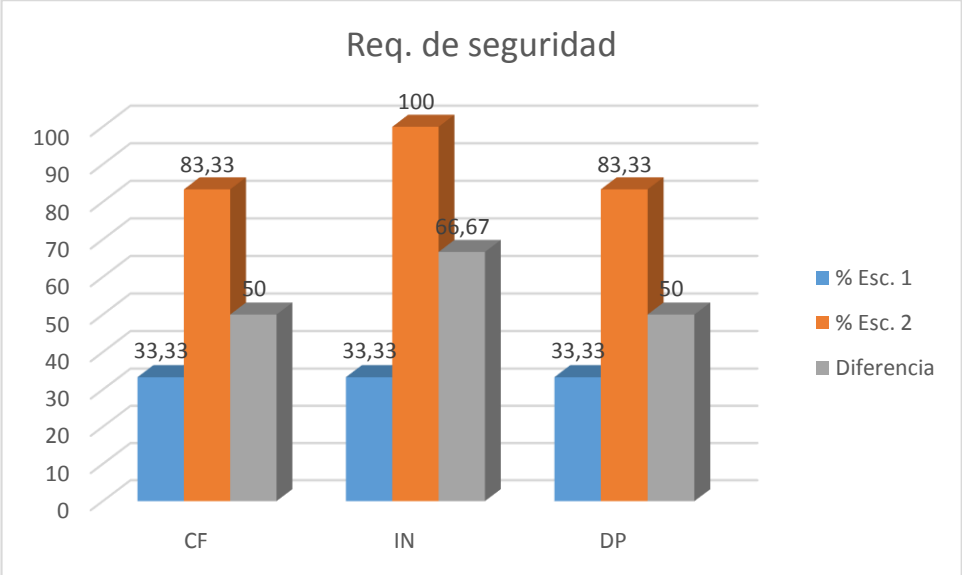


Figura V. XLI *Comparación de requerimientos de seguridad entre escenarios*
Fuente: *Autor de la tesis.*

INTERPRETACION: En la figura V.XLI se puede observar que los requerimientos de seguridad han aumentado debido a la encriptación de llamadas VoIP en IPv6, de esta manera los paquetes ya no están en texto plano sino en texto cifrado, asegurando que no puedan ser escuchados ni modificados y disponible en cualquier momento, ofreciendo un buen porcentaje de seguridad.

V.V MODELO ESTADISTICO DE LOS RESULTADOS.

Para el proyecto se emplea la distribución JI-CUADRADO en el campo de la estadística no paramétrica para el cálculo del análisis de resultados en la comprobación de la hipótesis, con media 0 y desviación típica 1; y así poder demostrar si la hipótesis planteada es verdadera en base en los resultados obtenidos en las tablas anteriores según el análisis de seguridad[15] en redes VoIP con IPv6.

Para el proyecto se emplea la distribución JI-CUADRADO con Corrección de Yates porque se tiene simplemente dos categorías: un escenario vulnerable (antes) y el escenario con propuestas de seguridad (después); para verificar el nivel de seguridad si ha mejorado en relación al primer escenario (vulnerable), en el cual se emplea la siguiente fórmula:

$$\chi^2 = \sum \frac{(|\text{observada} - \text{teorica}| - 0.5)^2}{\text{teorica}}$$

Donde "observada" son los eventos observados, "teorica" es el número teórico esperado de eventos, las pruebas son realizadas con (k - 1) grados de libertad, donde "k" es el número de categorías en donde se encuentran las observaciones.

V.VI COMPROBACION DE LA HIPOTESIS.

La hipótesis planteada en el proyecto es la siguiente:

"El estudio del análisis de las vulnerabilidades en protocolos utilizados en centrales de VoIP con IPv6 utilizando troncales SIP, permitirá mejorar los niveles de seguridad en estas redes"

[15] http://web.upcomillas.es/personal/peter/estadisticabasica/JiCuadrado.pdf

- **Planteamiento De Hipótesis Nula y de Investigación.**

✓ Para identificar la **hipótesis de investigación** se tiene la hipótesis planteada, se expresa como H_i.

H_i: "El estudio del análisis de las vulnerabilidades en protocolos utilizados en centrales de VoIP con IPv6 utilizando troncales SIP, permitirá mejorar los niveles de seguridad en estas redes".

✓ Para plantear la **hipótesis nula**, negamos la hipótesis de investigación que se refiere a la hipótesis planteada, se expresa como Ho.

Ho: "El estudio del análisis de las vulnerabilidades de los protocolos utilizados en centrales de VoIP con IPv6 utilizando troncales SIP, no permitirá mejorar los niveles de seguridad en estas redes".

Después de haber implementado las propuestas de seguridad en los equipos y observar la eficiencia de las propuestas empleadas para cada uno de ellos, se obtiene los siguientes resultados.

Nivel de seguridad	Escenario Vulnerable	Escenario con propuestas de seguridad	Resultado (RCo)
SIP	1	2	3
RTP	1	3	4
Resultado (RCe)	2	5	14

Tabla V. XX *Nivel de seguridad entre los escenarios 1 y 2*
Fuente: *Autor de la tesis.*

Estos datos se han obtenido en base a los promedios indicados en las tablas II.XV y II.XVII donde se establece el número 3 que es el valor máximo.

Procedemos a calcular X^2 con los siguientes parámetros:

✓ **Nivel de confianza** α = 0.05

✓ **Corrección de Yates X^2:** $\chi^2 = \sum \frac{(|\text{observada} - \text{teorica}| - 0.5)^2}{\text{teorica}}$

✓ **Grados de libertad (g):** g = (Filas – 1) (Columnas - 1); g = (2-1) (2-1); g = 1

En la siguiente tabla se indica las frecuencias observadas:

Nivel de seguridad	Escenario Vulnerable	Escenario con propuestas de seguridad
SIP	1	2
RTP	1	3

Tabla V. XXI *Frecuencias observadas*
Fuente: *Autor de la tesis.*

En la siguiente tabla se obtiene las frecuencias esperadas; se lo obtiene de la siguiente manera: **(RCe * Rco) / RT**; que se lo puede observar en la tabla 4.7 haciendo el análisis para cada celda.

Los resultados son los siguientes:

Nivel de seguridad	Escenario Vulnerable	Escenario con propuestas de seguridad
SIP	0,43	1,07
RTP	0,57	1,43

Tabla V. XXII *Frecuencias esperadas*
Fuente: *Autor de la tesis.*

A continuación se realiza el análisis de JI-CUADRADO con corrección de Yates.

	Frecuencia Observada (fo)	Frecuencia Esperada (fe)	(fo - fe - 0.5)^2	(fo - fe - 0.5)^2 / fe
Escenario vulnerable	1	0,43	0,32	0,76
	1	0,57	0,18	0,32
Escenario con prop. De seguridad	2	1,07	0,86	0,81
	3	1,43	2,46	1,72
			X^2 =	3,61

Tabla V. XXIII *Cálculo de ji-cuadrado*
Fuente: *Autor de la tesis.*

Luego del cálculo de JI-CUADRADO, se realiza el análisis si se valida o no la hipótesis planteada; si se observa la tabla de valores de ji-cuadrado, ver ***Anexo 4***, con un nivel de confianza de 0.05 y con un grado de libertad igual a 1 indica el valor del punto crítico igual a 3,841.

Luego se ha obtenido el valor de ji-cuadrado igual a 3.61.

Se concluye que este valor está dentro de la zona de aceptación por lo tanto la hipótesis de investigación es verdadera, donde indica que los niveles de seguridad han mejorado con las propuestas de seguridad implementadas en las centrales VoIP en IPv6.

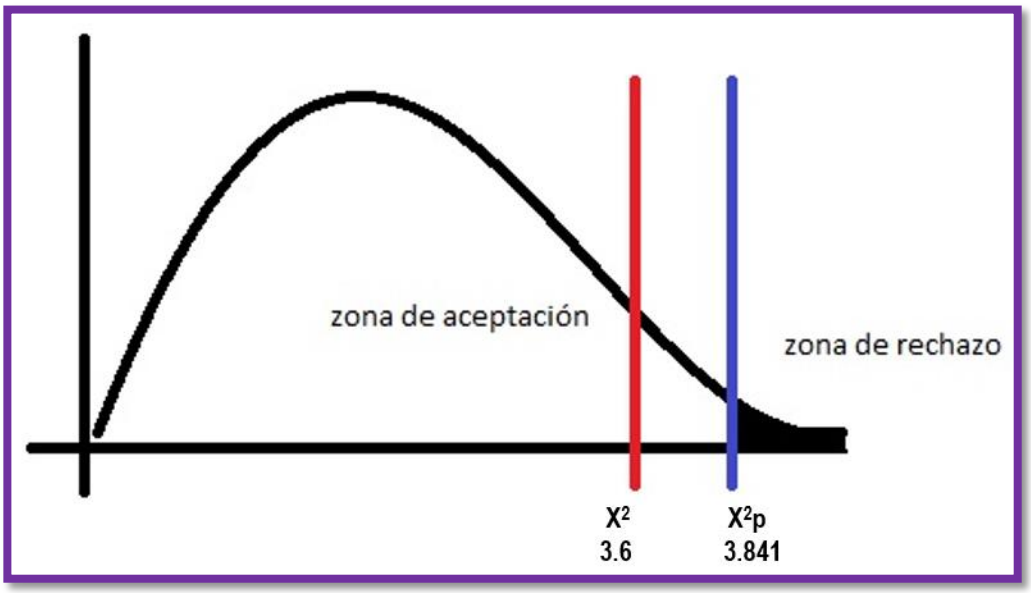


Figura V. XLII *Diagrama de ji-cuadrado*
Fuente: *Autor de la tesis.*

Por tanto se acepta la Hipótesis de investigación **(Hi)** y se rechaza la hipótesis nula **(Ho).**

CONCLUSIONES

- "Eavesdropping" es el ataque que afecta a los protocolos en centrales VoIP más discreto, ya que nadie sospecharía que su conversación telefónica en IP está siendo interceptada por terceros, a través de un sniffer se muestra los paquetes SIP y RTP que son visibles y pueden ser escuchados afectando los protocolos: 87% en SIP y 92% en RTP según la muestra de 68 llamadas empleadas.

- Con los requerimientos de seguridad citadas (Disponibilidad, Integridad, Confidencialidad), se observa que son afectados el: 88 %, 92% y 90% respectivamente.

- A través de la configuración de TLS/SSL se generan certificados de seguridad para el servidor VoIP, troncal SIP y extensiones clientes, de esta manera se previene que las llamadas puedan ser escuchadas asegurando SIP en el puerto 5061 (SIPS) y sRTP, mejorando la seguridad en dichos protocolos en: 91% y 95% respectivamente.

- Con las propuestas de seguridad citadas, se observa que la confidencialidad mejora en un 83%, disponibilidad en un 79% e Integridad en un 90%.

- Se ha elegido TLS/SSL porque en Elastix viene ya la herramienta únicamente para ser configurada, sin descartar otras como Open-VPN y otras, pero cabe recalcar que Open-VPN se basa en TLS/SSL para hacer su funcionalidad de encriptación.

RECOMENDACIONES

- El uso de software libre en la implementación de sistemas VoIP es altamente recomendable, ya que permite implementar múltiples servicios multimedia, además de que utiliza protocolos estandarizados por organismos reconocidos a nivel internacional, lo que permite la convivencia con la mayoría de las tecnologías propietarias.
- Habilitar el soporte para IPv6 en Elastix para que los softphones se puedan registrar, en las versiones anteriores a Elastix 2.4.0 se debe actualizar el sistema escribiendo en el prompt o terminal **#yum update && init 6.**
- Configurar los puertos del switch en modo shutdown y activarlos en caso de asignarlo a un usuario nuevo.
- Para asegurar aún más la red se recomienda el uso de Firewall en IPv6 para abrir solo los puertos necesarios que se requieran, y solamente para usuarios registrados, ***Anexo 3***.
- Se debe tener un conocimiento profundo de cómo trabaja VoIP sobre el protocolo IPv4 antes de implementarlo sobre IPv6, para de esta manera poder instalar la central telefónica y aprovechar al máximo los beneficios que trae la aplicación del nuevo protocolo en la transmisión de comunicaciones VoIP.
- Cambiar las contraseñas por defecto de Elastix con caracteres alfanuméricos y robustos; cambiar de usuario o sea no autenticarse como root sino hacer tareas de delegaciones de super usuario asignando permisos según políticas de seguridad.
- Ubicar el Hardware en sitios donde sean seguros obedeciendo políticas de seguridad para que no tengan acceso personas particulares sino personas debidamente autorizadas.

RESUMEN

El presente estudio trata de determinar las vulnerabilidades en protocolos de centrales VoIP en IPv6 utilizando trocales SIP, para proporcionar las medidas necesarias de seguridad para dichas centrales, realizada en la Academia CISCO ESPOCH.

El método científico envuelve la observación de información necesaria para ser aplicada en el ambiente de pruebas a ser implementado, luego la postulación de hipótesis y su comprobación mediante la experimentación, con la finalidad de incrementar el nivel de seguridad en centrales VoIP.

Los materiales para la implementación del escenario son los siguientes: Un router CISCO 2800, dos switch CISCO 2960 y 6 estaciones de trabajo donde dos estaciones son servidores VoIP.

Realizadas las pruebas de penetración a cada escenario, se muestra que el nivel de seguridad en el escenario con propuesta de seguridad ha mejorado respecto a los resultados del escenario vulnerable indicando que este es inseguro.

De acuerdo a los resultados obtenidos se concluye: el nivel de seguridad ha mejorado aplicando las propuestas de seguridad configuradas obteniendo los siguientes resultados: Eavesdropping 92% aumentando con relación al primer escenario con diferencia del 60%.

Una central VoIP brinda ahorros significativos en administración, mantenimiento, costos de llamadas, por tanto cualquier empresa debería contemplar la opción de actualizarse a una central VoIP en protocolo IPv6.

Se recomienda a técnicos tener un conocimiento profundo de cómo trabaja VoIP sobre el protocolo IPv4 antes de implementarlo sobre IPv6, para de esta manera poder instalar la central telefónica y aprovechar al máximo los beneficios que trae la aplicación del nuevo protocolo en la transmisión de comunicaciones VoIP.

SUMMARY

The present study determines the vulnerabilities in VoIP central protocols on IPv6 using SIP trunks, to provide the necessary safety precautions for those centrals, carried out in the CISCO ESPOCH academy.

The scientific method involves the observation of information necessary to apply in the test environment to be implemented, then the postulation and verification of the hypothesis through experimentation, with the purpose to increase the security level in VoIP centrals.

The materials for implementation of the scenario are the following: A CISCO 2800, two CISCO 2960 switches and six workstations where two stations are VoIP servers. Carried out the test of access of each scenario, showing the security level in the scenario with the proposal in security has improved against the results of the vulnerable scenario indicating its insecurity.

According to the results obtained it is concluded: The security level has improved applying the security proposals configured obtaining the following results: Eavesdropping 92% increase compared to the first scenario with 60% difference.

A VoIP central affords significant savings in administration, maintenance; call cost and thus any company should contemplate the option to update to a VoIP central over IPv6 protocols.

It is recommended to the technicians have in-depth knowledge about how VoIP Works over IPv4 protocol before to be implemented over IPv6, in order to install the telephone switchboard and take the most advantage the benefits the application brings from the new protocol in the VoIP communication transmissions.

GLOSARIO

VoIP.- "La Voz sobre protocolo de internet, puede ser empaquetada para ser enviada por conmutación de paquetes a diferencia de la telefonía tradicional que viaja por conmutación de circuitos, es una gran ventaja para alcanzar puntos geográficos distantes, además ofrece economía en los gastos ya que utiliza el internet".

PBX.- "Son centrales de servicio para VoIP, además ofrece otros servicios tales como: mensajería instantánea, videoconferencias, IVR, etc. Son muy útiles para ser implementados en organizaciones públicos y privados, tal como con licencia y open source. Ejemplo Asterisk".

IPv6.- "Protocolo de internet versión 6, es la nueva tecnología en protocolo para la solución de agotamiento de direcciones de su antecesor IPv4, a diferencia de su antecesor, posee 128 bits de direccionamiento contra 32 bits de IPv4, haciendo que este protocolo sea mucho más extenso para ser asignado a muchos dispositivos informáticos fijos y móviles.

Vulnerabilidad.- "Son susceptibles a amenazas, es decir que si no se toman medidas de seguridad, un atacante puede hacer uso de estas amenazar para atacar a un servicio y apoderarse de él resultando muy perjudicial en la confidencialidad e integridad de la información".

Troncales SIP.- "Son utilizadas para transmitir información en paquetes SIP desde un servidor PBX hacia otro, además pueden ser enviados hacia un proveedor de servicios VoIP para salir las llamadas hacia la telefonía tradicional".

Hacking Etico.- “Es un método para evaluar vulnerabilidades hacia nuestra propia organización, es decir que se emplea ataques para poder determinar las vulnerabilidades de la propia infraestructura, para corregirlas y hacer mucho más seguro ante ataques”.

Wireshark.- “Es un software para analizar protocolos que circulan en la red, es una herramienta muy útil para monitoreo de paquetes y para determinar si existen anomalías en la red, además generan reportes para fácil entendimiento del administrador”.

CAPITULO VI

BIBLIOGRAFÍA

1. **ANAYA, N.,** Fundamentos de Telefonía IP e Introducción a Asterisk / Elastix., 1a ed., Almería – España, Editorial Alianza., 2013., Pp. 25 – 27, 36.
E-BOOK www.elastixtech.com

2. **GIL, F. y GÓMEZ, J.,** VoIP y Asterisk, Redescubriendo la telefonía., 1a ed., Madrid – España., RA – MA Editorial., 2008., Pp. 62 – 64.

3. **GUTIERREZ, R.,** Seguridad en VoIP: Ataques, Amenazas y Riesgos., 1a ed., Valencia – España., Editorial Universal., 2012., Pp. 3, 6 -8, 10 - 11.

4. **GRAVES, K.,** Certified Ethical Hacker, Review Guide., 1st ed., Indianapolis – United States of America., Creative-commons Editorial., 2012., Pp.3-11.
E-BOOK www.solarware.ir/client/data/book/file7.pdf

5. **HERNANDEZ, E.,** IPv6 la evolución., 1a Ed., San Salvador - El Salvador., Editorial La Ceiba., 2013., Pp. 6 – 7, 14, 17 - 18, 20, 24 - 25.
E-BOOK www.isoc.org.ar/ediciones/ipv6ParaTodos.pdf

6. **LANDIVAR, E.,** Comunicaciones Unificadas con Elastix., 2a ed., Sunnyvale – Estados Unidos., Editorial Gutemberg., 2013., Pp. 17-24, 36-41, 73-75, 80-82.

7. **JIMENEZ, J.,** Implementación de VoIP sobre IPv6., Facultad de Sistemas y Computación., Escuela de Ciencias de la Computación., Universidad Técnica Particular de Loja., Loja – Ecuador., TESIS., Pp. 36, 54, 56-57.

8. ASTERISK: APLICACION PARA CONTROLAR Y GESTIONAR APLICACIONES
http://www.bilib.es/noticias/noticia/articulo/asterisk-aplicacion-para-controlar-y-gestionar-c/
2013 – 08 – 20

9. **FUNDAMENTOS DE VOIP CON TECNOLOGÍA CISCO**
http://cisconetworkingspain.blogspot.com
2013 – 09 – 07

10. INTRODUCCION A VOIP
http://comunidad.asterisk-es.org/introduccion_voip.pdf
07/04/2014 ; Pp 2,3

11. **TRONCALES Y RUTAS EN ELASTIX**
http://elastixtech.com/troncales-y-rutas-en-elastix/
2013 – 09 – 20

ANEXOS

ANEXO 1

CONFIGURACION DEL ESCENARIO 1

(VULNERABLE)

ROUTER A

```
enable
configuration terminal
!
hostname RA
!
ipv6 unicast-routing
!
interface FastEthernet0/0
 ip address 172.30.60.1 255.255.255.0
 ipv6 address 2001:DB8::1:1/112
 ipv6 eigrp 100
 ipv6 enable
 no shutdown
!
interface Serial0/2/0
 ip address 192.168.251.1 255.255.255.0
 ipv6 address 2001:DB8::11:1/112
 ipv6 eigrp 100
 ipv6 enable
 clock rate 64000
 no shutdown
!
interface Serial0/2/1
 ip address 192.168.250.1 255.255.255.0
 ipv6 address 2001:DB8::10:1/112
 ipv6 eigrp 100
 ipv6 enable
 clock rate 64000
 no shutdown
!
router rip
 network 172.30.0.0
```

```
 network 192.168.250.0
 network 192.168.251.0
 no auto-summary
!
ipv6 router eigrp 100
 router-id 1.1.1.1
 no shutdown
!
end
```

ROUTER B

```
enable
configure terminal
!
hostname RB
!
ipv6 unicast-routing
!
interface FastEthernet0/0
 ip address 192.168.4.1 255.255.255.0
 duplex auto
 speed auto
 ipv6 address 2001:DB8::2:1/112
 ipv6 eigrp 100
 ipv6 enable
 no shutdown
!
interface Serial0/1/0
 ip address 192.168.250.2 255.255.255.0
 ipv6 address 2001:DB8::10:2/112
 ipv6 eigrp 100
```

```
 ipv6 enable
 no shutdown
!
interface Serial0/1/1
 ip address 192.168.252.2 255.255.255.0
 ipv6 address 2001:DB8::12:2/112
 ipv6 eigrp 100
 ipv6 enable
 no shutdown
!
router rip
 network 192.168.4.0
 network 192.168.250.0
 network 192.168.252.0
 no auto-summary
!
ipv6 router eigrp 100
 router-id 2.2.2.2
 no shutdown
!
end
```

ROUTER C

```
enable
configure terminal
!
hostname RC
!
ipv6 unicast-routing
!
interface FastEthernet0/0
```

```
 ip address 192.168.5.1 255.255.255.0
 duplex auto
 speed auto
 ipv6 address 2001:DB8::3:1/112
 ipv6 eigrp 100
 ipv6 enable
 no shutdown
!
interface Serial0/3/0
 ip address 192.168.251.2 255.255.255.0
 ipv6 address 2001:DB8::11:2/112
 ipv6 eigrp 100
 ipv6 enable
 no shutdown
!
interface Serial0/3/1
 ip address 192.168.252.1 255.255.255.0
 ipv6 address 2001:DB8::12:1/112
 ipv6 eigrp 100
 ipv6 enable
 clock rate 64000
 no shutdown
!
router rip
 network 192.168.5.0
 network 192.168.251.0
 network 192.168.252.0
 no auto-summary
!
ipv6 router eigrp 100
 router-id 3.3.3.3
 no shutdown
!
End
```

ANEXO 2

CONFIGURACION ESCENARIO 2 (PROPUESTA DE SEGURIDAD)

ROUTER A

```
Building configuration...
Current configuration : 1123 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname RA
!
enable secret 5 $1$mERr$Z.LBo7o0/srb0pAWdrjIC.
enable password 7 0822455D0A165747435F
!
ipv6 unicast-routing
!
username tesis password 7 0822455D0A165747435F
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.2
 encapsulation dot1Q 2
 ip address 172.30.60.1 255.255.255.0
 ipv6 address 2001:DB8::1:1/112
 ipv6 eigrp 100
 ipv6 enable
!
interface FastEthernet0/0.99
 encapsulation dot1Q 99 native
 ip address 172.30.99.1 255.255.255.0
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/1.20
 encapsulation dot1Q 20
 ip address 192.168.4.1 255.255.255.0
 ipv6 address 2001:DB8::2:1/112
 ipv6 eigrp 100
 ipv6 enable
!
interface FastEthernet0/1.100
 encapsulation dot1Q 100 native
 ip address 192.168.100.1 255.255.255.0
!
interface Vlan1
 no ip address
 shutdown
!
line con 0
 login local
!
```

```
line aux 0
!
line vty 0 4
 login local
!
ipv6 router eigrp 100
 router-id 3.3.3.3
 no shutdown
!
end
```

SWITCH1

```
Switch#sh runn
Building configuration...
Current configuration : 1903 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Switch
!
enable secret 5 $1$mERr$Z.LBo7o0/srb0pAWdrjlC.
!
!
username tesis privilege 1 password 7 0822455D0A165747435F
!
interface FastEthernet0/1
 switchport access vlan 2
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0090.0C46.CA6E
!
interface FastEthernet0/2
 shutdown
!
interface FastEthernet0/9
 shutdown
!
interface FastEthernet0/10
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/11
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface GigabitEthernet1/2
 switchport trunk native vlan 99
 switchport mode trunk
```

```
!
interface Vlan99
 ip address 172.30.99.2 255.255.255.0
!
ip default-gateway 172.30.99.1
!
line con 0
 login local
!
line vty 0 4
 login
line vty 5 15
 login local
!
end
```

SWITCH2

```
Switch#sh runn
Building configuration...
Current configuration : 1838 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
interface FastEthernet0/1
 switchport access vlan 20
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0007.EC51.CD62
!
interface FastEthernet0/2
 shutdown
!
interface FastEthernet0/9
 shutdown
!
interface FastEthernet0/10
 switchport access vlan 20
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/11
 switchport access vlan 20
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
!
!
interface GigabitEthernet1/2
 switchport trunk native vlan 100
```

```
 switchport mode trunk
!
interface Vlan100
 ip address 192.168.100.2 255.255.255.0
!
ip default-gateway 192.168.100.1
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
End
```

ANEXO 3

CONFIGURACION DE IP6TABLES

FIREWALL IMPLEMENTADO EN IPV6 PARA DENEGAR PERMISO A INTRUSOS.

#nombre del archivo: voipip6tables

```
#!/bin/bash
echo –e "Aplicando configuraciones de forwarding"
echo "1" > /proc/sys/net/ipv6/conf/all/forwarding
echo "1" > /proc/sys/net/ipv6/conf/all/icmp_echo_ignore_broadcasts
echo "1" > /proc/sys/net/ipv6/conf/all/icmp_echo_ignore_all
echo "1" > /proc/sys/net/ipv6/conf/all/tcp_syncookies
echo "1" > /proc/sys/net/ipv6/conf/all/icmp_ignore_bogus_error_responses
echo "30" > /proc/sys/net/ipv6/conf/all/tcp_fin_timeout
echo
# Evitar ataques de footprinting...
echo "1" > /proc/sys/net/ipv6/conf/all/rp_filter
# Deshabilitar la redireccion del ping...
echo "0" > /proc/sys/net/ipv6/conf/all/accept_redirects
#Reglas por defecto
echo -e "Flushing de Reglas por Defecto"
echo
IP6TABLES -F
IP6TABLES -X
IP6TABLES -t nat -F
IP6TABLES -t mangle -F
IP6TABLES -t mangle -X
echo -e "Cargando Reglas Generales Para el FireWall"
# Bloqueo de Ataques Syn.
echo
IP6TABLES -N bad_tcp_packets
IP6TABLES -t filter -A bad_tcp_packets -p tcp ! --syn -m state --state NEW -j LOG -
-log-prefix
IP6TABLES -t filter -A bad_tcp_packets -p tcp ! --syn -m state --state NEW -j DROP
IP6TABLES -t filter -A INPUT -p tcp --dport 80 -j bad_tcp_packets
IP6TABLES -N PKT_FAKE
IP6TABLES -F PKT_FAKE
IP6TABLES -A PKT_FAKE -m state --state INVALID -j DROP
IP6TABLES -A PKT_FAKE -p tcp ! --syn -m state --state NEW -j DROP
IP6TABLES -A PKT_FAKE -f -j DROP
echo -e "Protegiendo de Anti-flooding o inundacion de tramas para DoS"
echo
IP6TABLES -N syn-flood
IP6TABLES -A INPUT -i eth0 -p tcp --syn -j syn-flood
IP6TABLES -A syn-flood -m limit --limit 1/s --limit-burst 4 -j RETURN
IP6TABLES -A syn-flood -j DROP
IP6TABLES -A FORWARD -p tcp --syn -m limit --limit 1/s -j ACCEPT
IP6TABLES -A FORWARD -p tcp --tcp-flags SYN,ACK,FIN,RST RST -m limit --limit
1/s -j ACCEPT
IP6TABLES -A FORWARD -p icmp --icmp-type echo-request -m limit --limit 1/s -j
ACCEPT
IP6TABLES -A FORWARD -p tcp ! --syn -m state --state NEW -j LOG --log-prefix
echo –e "evitar SYN consecutivos"
echo
IP6TABLES -A FORWARD -p tcp ! --syn -m state --state NEW -j DROP
echo -e "Cambiando FORWARD"
echo
IP6TABLES -A FORWARD -m limit --limit 3/minute --limit-burst 3 -j LOG --log-level
DEBUG --log-prefix
# Descartar paquetes invalidos.
```

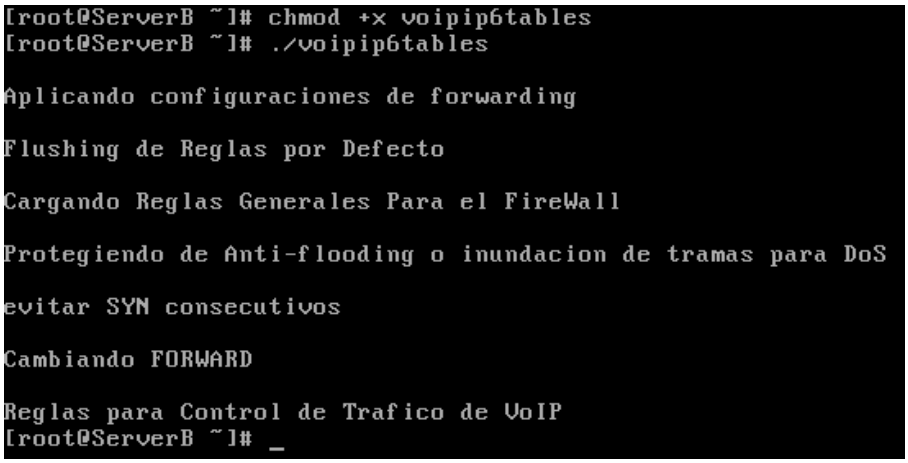
```
IP6TABLES -A FORWARD -m state --state INVALID -j DROP
echo -e “Reglas para Control de Trafico de VoIP”
echo
IP6TABLES -A INPUT -p udp -m state --state NEW -m udp --dport 1024:5059 -j
QUEUE
IP6TABLES -A INPUT -p udp -m state --state NEW -m udp --dport 5060:5070 -j
QUEUE
IP6TABLES -A INPUT -p udp -m state --state NEW -m udp --dport 5071:65535 -j
QUEUE
```

Asignamos permisos al script de configuración.

```
#chmod +x voipip6tables
```

Ejecutamos el script.

```
#./voipip6tables
```



ANEXO 4

TABLA JI-CUADRADO

GL/ P	Valores Críticos de la Distribución Ji Cuadrado (1 cola)														
	0,999	**0,995**	**0,99**	**0,975**	**0,95**	**0,90**	**0,75**	**0,50**	**0,25**	**0,10**	**0,05**	**0,025**	**0,01**	**0,005**	**0,001**
1	0,000	0,000	0,000	0,001	0,004	0,016	0,102	0,455	1,323	2,706	3,841	5,024	6,635	7,879	10,827
2	0,002	0,010	0,020	0,051	0,103	0,211	0,575	1,386	2,773	4,605	5,991	7,378	9,210	10,597	13,815
3	0,024	0,072	0,115	0,216	0,352	0,584	1,213	2,366	4,108	6,251	7,815	9,348	11,345	12,838	16,266
4	0,091	0,207	0,297	0,484	0,711	1,064	1,923	3,357	5,385	7,779	9,488	11,143	13,277	14,860	18,466
5	0,210	0,412	0,554	0,831	1,145	1,610	2,675	4,351	6,626	9,236	11,070	12,832	15,086	16,750	20,515
6	0,381	0,676	0,872	1,237	1,635	2,204	3,455	5,348	7,841	10,645	12,592	14,449	16,812	18,548	22,457
7	0,599	0,989	1,239	1,690	2,167	2,833	4,255	6,346	9,037	12,017	14,067	16,013	18,475	20,278	24,321
8	0,857	1,344	1,647	2,180	2,733	3,490	5,071	7,344	10,219	13,362	15,507	17,535	20,090	21,955	26,124
9	1,152	1,735	2,088	2,700	3,325	4,168	5,899	8,343	11,389	14,684	16,919	19,023	21,666	23,589	27,877
10	1,479	2,156	2,558	3,247	3,940	4,865	6,737	9,342	12,549	15,987	18,307	20,483	23,209	25,188	29,588
11	1,834	2,603	3,053	3,816	4,575	5,578	7,584	10,341	13,701	17,275	19,675	21,920	24,725	26,757	31,264
12	2,214	3,074	3,571	4,404	5,226	6,304	8,438	11,340	14,845	18,549	21,026	23,337	26,217	28,300	32,909
13	2,617	3,565	4,107	5,009	5,892	7,041	9,299	12,340	15,984	19,812	22,362	24,736	27,688	29,819	34,527
14	3,041	4,075	4,660	5,629	6,571	7,790	10,165	13,339	17,117	21,064	23,685	26,119	29,141	31,319	36,124
15	3,483	4,601	5,229	6,262	7,261	8,547	11,037	14,339	18,245	22,307	24,996	27,488	30,578	32,801	37,698
16	3,942	5,142	5,812	6,908	7,962	9,312	11,912	15,338	19,369	23,542	26,296	28,845	32,000	34,267	39,252
17	4,416	5,697	6,408	7,564	8,672	10,085	12,792	16,338	20,489	24,769	27,587	30,191	33,409	35,718	40,791
18	4,905	6,265	7,015	8,231	9,390	10,865	13,675	17,338	21,605	25,989	28,869	31,526	34,805	37,156	42,312
19	5,407	6,844	7,633	8,907	10,117	11,651	14,562	18,338	22,718	27,204	30,144	32,852	36,191	38,582	43,819
20	5,921	7,434	8,260	9,591	10,851	12,443	15,452	19,337	23,828	28,412	31,410	34,170	37,566	39,997	45,314

Celda tomada los grados de libertad (1) al 5% de nivel de confianza (0,05) para la demostración de la hipótesis planteada.