ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

ESCUELA DE INGENIERÍA ELECTRÓNICA EN TELECOMUNICACIONES Y REDES

"PROPUESTA DE SOLUCIONES A LAS VULNERABILIDADES DEL PROTOCOLO DE SEÑALIZACIÓN SIP EN VOZ SOBRE IP, CASO PRÁCTICO: RED IP-PBX."

Tesis de Grado

Previa a la obtención del título de

Ingeniero en Electrónica y Computación

Presentado por:

Magaly Carmen Arroba Huebla

Mónica Patricia Salazar Orozco

Riobamba – Ecuador

2011

Ing. Daniel Haro
Ing. Alberto Arellano

Por compartir sus conocimientos y en especial por su amistad, para ustedes nuestro respeto y admiración.

Agradezco infinitamente a Dios porque sin el nada seria posible, a las tres personas mas importantes de mi vida que siempre les llevo en mi corazón mi Mami Sra.Carmen Huebla A. por estar siempre a mi lado en los buenos y malos momentos, a mi hermano Alex Arroba H. por tu apoyo incondicional que Dios te bendiga y a mi Papi Antonio Arroba J. que por su sacrificio y esfuerzo me ayudado a llegar a esta etapa de mi vida, gracias a ustedes que fueron mi inspiración principal de lucha en mi vida .Los AMO

MAGALY A.

Agradezco en primer lugar a DIOS por darme la vida y las fuerzas que necesitaba en los momentos más difíciles. A mis padres Ing. Miguel Salazar Y. y Sra. Mónica Orozco M., por su amor, apoyo, y sacrificios, sin ustedes nada de esto hubiera sido posible. A mis hermanos Luis y Valeria, por su apoyo incondicional.

A todas aquellas personas que de una u otra manera han llegado a ser parte de mi vida durante el transcurso de estos últimos años.

MÓNICA S.

Nombre	Firma	Fecha
Ing. Iván Menes. **Decano Facultad de Informatica y Electrónica**	_____	_____
Ing. Pedro Infante. **Director Escuela de Ingeniería Electrónica en Telecomunicaciones Y Redes.**	_____	_____
Ing. Daniel Haro **Director de Tesis**	_____	_____
Ing. Alberto Arellano **Miembro de Tesis**	_____	_____
Tlgo. Carlos Rodríguez **Director Centro Documentación**	_____	_____

Nosotras, MAGALY CARMEN ARROBA HUEBLA Y MÓNICA PATRICIA SALAZAR OROZCO, somos las responsables de las ideas, doctrinas y resultados expuestos en esta: Tesis, y el patrimonio intelectual de la misma pertenecen a la Escuela Superior Politécnica de Chimborazo".

ÍNDICES

ÍNDICE DE ABREVIATURAS

3GPP	3rd Generation Partnership Program
ACR	Absolute Category Rating
ADSL	Asymmetric Digital Subscriber Line
DNS	Domain Name Server
DNS	Domain Name System
EDGE	Enhanced Data rates for GSM Evolution
EFR	Enhanced Full Rate
FXO	Foreign eXchange Office
FXS	Foreign eXchange Subscriber
GPRS	General Packet Radio Service
IANA	Internet Assigned Numbers Authority
IAX	Inter-Asterisk eXchange protocol
IE	Information Element
IP	Internet Protocol
MD5	Message-Digest Algorithm 5
MG	Media Gateway
MGC	Media Gateway Controller
MGCP	Media Gateway Control Protocol
MMS	Multimedia Messaging Service
OC	Oficina Central
PAS	Punto de Acceso al Servicio
PCM	Pulse CodeModulation
QoS	Quality of Service
RAS	Registration Admision and Status
RDSI	Red Digital de Servicios Integrados
RFC	Request For Comments
RTCP	Real Time Control Protocol
SCCP	Skinny Client Control Protocol
SDP	Session Description Protocol
SG	Signaling Gateway
SIP	Session Initiation Protocol
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing

ToS	Type of Service
UA	User Agents
UDP	User Datagram Protocol
UIT	Unión Internacional de Telecomunicaciones
UMTS	Universal MobileTelecommunications System
URI	Uniform Resource Identifier
URL	Uniform Resource Locater

ÍNDICE GENERAL

Pag

INDICE DE TABLAS

INDICE DE FIGURAS

Fig.V.8. Ubicación del Estadístico de Prueba en la Distribución Chi-cuadrada para la prueba de hipótesis.

Fig.V.9. Ubicación del Estadístico de Prueba en la Distribución Chi-cuadrada para la prueba de hipótesis.

INTRODUCCIÓN

En la actualidad la tecnología informática, ha alcanzado increíbles avances, permitiéndonos desde almacenar una pequeña carta en un dispositivo de almacenamiento hasta envió de datos, voz y video a través de medios alámbricos, inalámbricos y que por qué no decirlo comunicaciones satelitales, que permiten comunicar a individuos y/o instituciones ubicadas en cualquier parte del planeta y fuera de este.

Es así, como hoy en día algunos servicios como la telefonía convencional (por conmutación de circuitos), han pasado a otro entorno, nos referimos a la telefonía IP (por conmutación de paquetes), que aprovechando la tecnología sobre IP, implementa la comunicación de voz sobre el Protocolo de Internet (VoIP). Gracias a esta novedosa tecnología, se pueden brindar servicios de comunicación de voz entre redes de datos (LAN, WAN, Internet), que se encuentren en lugares geográficamente distantes. Así como también implementarlo en telefonía fija en hogares y empresas.

La tecnología Voz sobre el Protocolo de Internet VoIP, junto con nuevas aplicaciones Web, son para muchos la tecnología del futuro en las comunicaciones.

De igual forma y en paralelo a estos avances, se han desarrollado herramientas de software, que permiten implementar servicios de telefonía a través de una PBX virtual basada en IP, mediante el empleo de protocolos como H.323, SIP, IAX, entre otros. Es así como hoy en día encontramos Software como Asterisk, Elastix, Trixbox, 3CXPHONE con soporte para VoIP.

Sin embargo a pesar de aportar significativamente al desarrollo de las comunicaciones reduciendo gastos y aumentando el rendimiento, durante estos últimos años, han aparecido vulnerabilidades específicas que afectan a algunos servicios IP, como mensajería instantánea y VoIP, que fundamentalmente aprovechan las debilidades de los protocolos estándares como SIP, H.323, RTP entre otros, es así que siendo la Telefonía sobre IP un método de comunicación masiva y de gran avance en la actualidad es importante realizar un estudio y análisis de esta tecnología que es una infraestructura la cual podría llegar a sustituir a las PBX tradicionales.

Para esto se implementara un servicio de Voz sobre IP VoIP sobre la plataforma de código abierto Elastix.

Esto se lograra utilizando solamente herramientas con licenciamiento GPL de Software libre, donde el sistema Operativo será una versión de Linux llamada Centos sobre el cual se montara una IP PBX basado en el Software Elastix, que es una PBX con soporte para VoIP que se puede administrar vía Web.

Por todos los motivos descritos anteriormente este documento fue desarrollado para implementar la tecnología VoIP con Elastix y de esta forma realizar un estudio de la seguridad de este tipo de comunicación, basándonos exclusivamente en el protocolo SIP. Para cumplir los objetivos del trabajo se desarrollan cinco capítulos organizados de la siguiente forma: El Capítulo I está centrado en los conceptos básicos y veremos una explicación de la tecnología de voz sobre una red IP, mostrando los protocolos de red necesarios, los aspectos que afectan la calidad de voz, parámetros relacionados con la calidad de voz en redes de paquetes. En el Capítulo II se profundizará en el protocolo de señalización SIP lo quenos llevará a conocer el funcionamiento del mismo. El Capítulo III daremos a conocer los Problemas frecuentes en VoIP Ataques, Amenazas y Riesgos a los que puede estar expuesto el protocolo SIP, además de las herramientas utilizadas para analizar dichos problemas. En el Capítulo IV donde encontraremos detalles de la implementación tanto en máquina servidor como en clientes, pruebas de transmisión, de análisis de vulnerabilidades y por último en el Capítulo V veremos un Análisis de Resultados.

CAPÍTULO I
CONCEPTOS BÁSICOS

1.1. Protocolo TCP/IP

1.1.1 Introducción

Las siglas TCP/IP se refieren a un conjunto de protocolos para comunicaciones de datos. Este conjunto toma su nombre de dos de sus protocolos más importantes, el protocolo TCP (Transmission Control Protocol) y el protocolo IP (Internet Protocol).

La evolución del protocolo TCP/IP siempre ha estado muy ligada a la de Internet.

En estas circunstancias se desarrolla el primer conjunto básico de protocolos TCP/IP. Posteriormente, y ya entrados en la década de los ochenta, todos los equipos militares conectados a la red adoptan el protocolo TCP/IP yse comienza a implementar también en los sistemas Unix. Poco a poco ARPAnet deja de tener un uso exclusivamente militar, y se permite que centros de investigación, universidades y empresas se conecten a esta red.

Se habla cada vez con más fuerza de Internet y en 1990 ARPAnet deja de existir oficialmente.

En los años sucesivos y hasta nuestros días las redes troncales y los nodos de interconexión han aumentado de forma imparable. La red Internet parece expandirse sin límite, aunque manteniendo siempre una constante; el protocolo TCP/IP.

En efecto, el gran crecimiento de Internet ha logrado que el protocolo TCP/IP sea el estándar en todo tipo de aplicaciones telemáticas, incluidas las redes locales y corporativas. Y es precisamente en este ámbito, conocido como Intranet, donde TCP/IP adquiere cada día un mayor protagonismo.

1.1.2. Arquitectura del protocolo TCP/IP

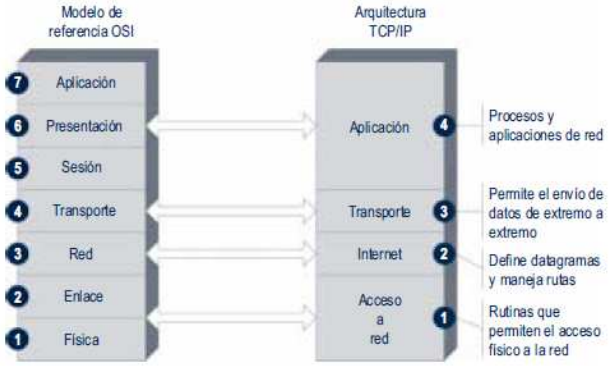


Fig. I.1. Correspondencia del modelo OSI con TCP/IP.

El protocolo TCP/IP fue creado antes que el modelo decapas OSI, así que los niveles del protocolo TCP/IP no coinciden exactamente con los siete que establece el OSI.
Existen descripciones del protocolo TCP/IP que definen de tres a cinco niveles. La Figura I.1 representa un modelo de cuatro capas TCP/IP y su correspondencia con el modelo de referencia OSI.

Los datos que son enviados a la red recorren la pila del protocolo TCP/IP desde la capa más alta de aplicación hasta la más baja de acceso a red. Cuando son recibidos, recorren la pila de protocolo en el sentido contrario.
Durante estos recorridos, cada capa añade o sustrae cierta información de control a los datos para garantizar su correcta transmisión.

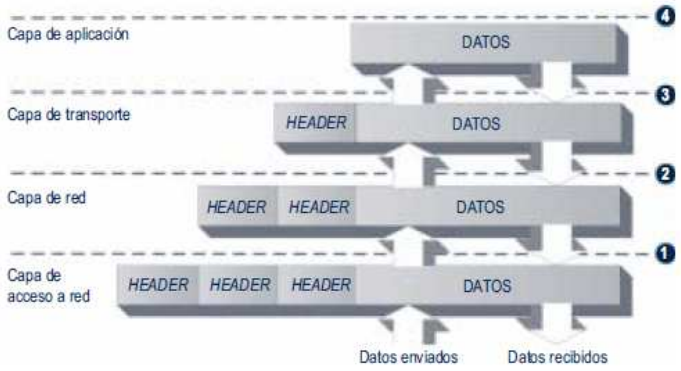


Fig. I.2. Encapsulado de datos por los niveles TCP/IP.

Como esta información de control se sitúa antes de los datos que se transmiten, se llama cabecera (header). Enla Figura I.2 se puede ver cómo cada capa añade una cabecera a los datos que se envían a la red. Este procesose conoce como encapsulado. Si en vez de transmitir datos se trata de recibirlos, el proceso sucede

al revés. Cada capa elimina su cabecera correspondiente hasta que quedan sólo los datos.
En teoría cada capa maneja una estructura de datos propia, independiente de las demás, aunque en la práctica estas estructuras de datos se diseñan para que sean compatibles con las de las capas adyacentes. Se mejora así la eficiencia global en la transmisión de datos.

1.2. Sistemas Analógicos.

La Red Telefónica Básica (RTB1) fue creada para transmitir la voz humana. Tanto por la naturaleza de la información a transmitir, como por la tecnología disponible en la época en que fue creada, es de tipo analógico.
Cada línea RTB tiene asignada una numeración específica (su número telefónico) y está físicamente construida por dos hilos metálicos (conocidos como par de cobre), que se extienden desde la central telefónica hasta la instalación del abonado (se conoce también como bucle de abonado). Cada central atiende las líneas de abonado de un área geográfica determinada. A su vez, las centrales telefónicas están unidas entre sí por sistemas más complejos y basados en tecnología digital. Esta unión de centrales constituye el sistema telefónico nacional que a su vez está enlazado con los restantes del mundo.
En los años 60 las centrales telefónicas, mayoritariamente analógicas, fueron transformando su tecnología a digital. Ello solventó diversos problemas, como los relacionados con la degradación de la señal de voz y la imposibilidad de manejar gran cantidad de llamadas. Del mismo modo, la intención fue también digitalizar el bucle local pero por motivos meramente económicos el bucle local continuó siendo analógico.
Finalmente, la medida que se adoptó fue la de digitalizar la comunicación entre las centralitas telefónicas, manteniendo el bucle local analógico, y obteniéndose así los beneficios de la telefonía digital a un precio razonable. Esta medida dio lugar a lo que se conoce como RD “Red Digital Integrada”.

Como hemos visto, se disponga por tanto de tecnología RDSI o analógica se requiere de un enlace desde nuestro hogar hasta la central telefónica asignada a nuestra zona. Es por ello que es de gran importancia conocer los dos tipos de conexiones telefónicas analógicas existentes, conocidas como FXS y FXO, es decir, los nombres de los puertos o interfaces usados por las líneas telefónicas y los dispositivos analógicos.

1.2.1. FXS

Fig. I.3. Roseta telefónica o PTR

La interfaz Foreign eXchange Subscriber o FXS es el puerto por el cual el abonado accede a la línea telefónica, ya sea de la compañía telefónica o de la central de la empresa. Enotras palabras, la interfaz FXS provee el servicio al usuario final (teléfonos, módems o faxes).
Los puertos FXS son, por lo tanto, los encargados de:

- Proporcionar tono de marcado.
- Suministrar tensión (y corriente) al dispositivo final.

Para entender mejor el concepto, piense en el caso de un hogar tradicional. La interfaz FXS es el punto donde se conectan los teléfonos del hogar que quieren hacer uso de la línea.
La interfaz FXS sería entonces la roseta de telefonía del hogar.

1.2.3. FXO

Fig. I.4. Dispositivo FXO

La interfaz Foreign eXchange Office o FXO es el puerto por el cual se recibe a la línea telefónica. Los puertos FXO cumplen la funcionalidad de enviar una indicación de colgado o descolgado conocida como cierre de bucle.
Un ejemplo de interfaz FXO es la conexión telefónica que tienen los teléfonos analógicos, fax, etc. Es por ello que a los teléfonos analógicos se les denomina "dispositivos FXO".

A modo de resumen se quiere destacar que dos puertos se pueden conectar entre sí con la condición de ser de distinto tipo, es decir, FXO y FXS son siempre pareja (similar a un enchufe macho/hembra).

En la figura I.5, se muestra el escenario de un hogar tradicional. Como podemos apreciar siempre se conectan entre sí interfaces de distintos tipos, es decir, FXS con FXO o viceversa. El teléfono posee una interfaz FXO como se muestra en la imagen, el cual esconectado a la roseta de la compañía telefónica (FXS).

Fig.I.5. FXS /FXO sin centralita

1.3. Sistemas Digitales

1.3.1. RDSI

Los trabajos de desarrollo de la Red Digital de Servicios Integrados (RDSI o ISDN, siglas en inglés de Integrated Services Digital Network) comenzaron en la década de los 80, pero ésta no sería comercializada hasta principios de los años 90. Se esperaba que la RDSI pudiera revolucionar la industria de las comunicaciones telefónicas como hoy día se espera que lo pueda hacer la VoIP. Sin embargo, y aunque las compañías telefónicas pusieron mucho empeño en extenderlo al mayor número de lugares posibles, muchos consideran la RDSI un fracaso debido a que todo lo que prometía no se pudo llevar a cabo.

La RDSI permite que en una línea coexistan múltiples canales, pudiendo contener cada uno de ellos datos (canales B) o señalización (canales D). Pero además, la RDSI no se limita sólo a la transmisión de voz.

Tal y como se muestra en la figura I.6, la línea RDSI básica, también conocida como BRI (Basic Rate Interface), tiene tres canales (dos canales B y un canal D), de forma que pueden realizarse dos llamadas telefónicas de forma simultánea en una única BRI.

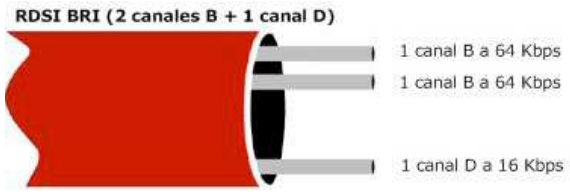


Fig. I.6. Arquitectura de un cable RDSI BRI

A diferencia de la versión BRI de RDSI, la PRI (PrimaryRate Interface) posee dos versiones, una de 31 (30 canales B y 1 canal D) y otra de 24 canales (23 canales B y 1 canal D), por lo tanto, con ésta pueden realizarse 30 ó 23 llamadas telefónicas al mismo tiempo, respectivamente.

1.3.2. E1/T1

Un T1 es un acceso digital que dispone de 24 canales, pudiéndose realizar en cada uno de ellos (menos uno) una llamada.

Mientras que el T1 es muy común en Estados Unidos y Japón, en Europa se emplea con mayor frecuencia el E1. A diferencia del T1, esta línea dispone de 32 canales en vez de 24.

Tanto los T1s como los E1s tienen que señalizar las llamadas de alguna manera. Esto se consigue mediante lo que se conoce como Señalización por Robo de Bit (Robbed Bit Signaling), es decir, que cada cierto tiempo se usa un bit de cada canal para así señalizar y enviar información a través de la línea (T1s), o mediante multiplexación del bit en un canal común, algo que se emplea sobre todo en Europa (E1s).

1.4. Centralitas Tradicionales PBX.

1.4.1. Introducción.

Una centralita privada o PBX5 es un dispositivo de telefonía que actúa como conmutador de llamadas en una red telefónica o de conmutación de circuitos.

La centralita es un dispositivo de telefonía que se suele utilizar en la mayoría de las medianas y grandes empresas, no así en los hogares, donde los terminales existentes son pocos y las exigencias no son importantes. Permite a los usuarios o abonados compartir un determinado número de líneas externas (analógicas o digitales) para hacer llamadas telefónicas entrantes o salientes, así como establecer comunicaciones internas entre todos los dispositivos que dependen de la PBX.

Las llamadas realizadas a números de teléfono externos, mediante una PBX, se suelen realizar anteponiendo un dígito (habitualmente el 0) al número externo en algunos sistemas, de forma que la PBX selecciona automáticamente una línea troncal saliente.

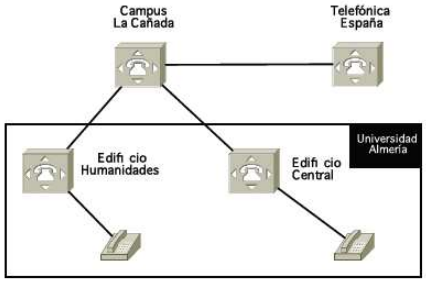


Fig.I.9. Esquemas de interconexión de centralitas

1.4.2. Sistemas Comerciales

Actualmente existe una gran diversidad de modelos de centralitas, centralitas con mayor o menor número de extensiones para pequeñas o grandes empresas, de más o menos prestaciones, con mayor o menor funcionalidad, totalmente analógicas, híbridas o completamente IP.

Fig. I.10. Centralitas tradicionales

Las centralitas híbridas combinan las prestaciones de una central telefónica con la tecnología IP. A nivel empresarial esta integración con la tecnología IP ofrece grandes ventajas, los recursos humanos de la empresa pueden estar dispersos geográficamente manteniendo los recursos telefónicos centralizados, además de que aquellas empresas quede sean utilizar su cableado de red para conectar teléfonos en lugares donde no siempre hay conectado un terminal telefónico, o bien trasladarse de un punto a otro de la red junto con suterminal telefónico (con todas sus prestaciones asociadas), sin tener que volver a configurar el terminal, resulta muy práctico.

En la figura I.11, puede ver una centralita modelo "Panasonic TDA15". Otros fabricantes que se dedican a la comercialización son Alcatel, Ericsson, Avaya, Siemens, etc.

Las prestaciones entre uno y otro fabricante son muy similares.

Fig.I.11. Centralita híbrida (Panasonic TDA15)

1.5. Voice Over Internet

1.5.1. ¿Qué es la Voz sobre IP?

Desde hace unos años el avance tecnológico ha permitido la aparición de redes substitutas a la PSTN, aunque sin reemplazarla. La tecnología más ampliamente aceptada es la de telefonía celular, que a pesar de su gran penetración, no ha logrado destronar a la telefonía fija, en gran parte debido a los costos de las comunicaciones y la escasa cobertura en muchas regiones. Pero con el pasar de los años, la velocidad de acceso a la red de redes ha ido creciendo, y lo que al principio no parecía más que una promesa o una curiosidad, al fin se está masificando: nos referimos al uso de un ordenador convencional, conectado a Internet, para comunicarnos con otro en las mismas condiciones o incluso con un teléfono de la red PSTN o móvil.

La integración de la voz y los datos en una misma red es una idea antigua, desde hace tiempo han surgido soluciones desde distintos fabricantes que, mediante el uso de multiplexores, permiten utilizar las redes de datos para la transmisión del tráfico de voz, dado que una vez que es convenientemente codificada, un paquete de voz es indistinguible del paquete de datos, y por lo tanto puede ser transportado a través de una red que estaría normalmente reservada para transmisión de datos. La aparición del VoIP junto con el abaratamiento de los DSP’s (procesador digital de señal), los cuales son claves en la compresión y descompresión de la voz, son los elementos clave de estas tecnologías.

Esto quiere decir, que IP es una serie de normas que permiten a un paquete de datos transmitirse de un ordenador a otro.

Los datos dentro de una red basada en IP son enviados en bloques, que reciben el nombre de "paquetes" o "datagramas.

El Protocolo de Internet (IP) provee un servicio de datagramas no fiable, conocido también como "mejor esfuerzo" (besteffort), que hará lo mejor posible a su alcance en el momento de enviar los paquetes, pero en realidad garantizando poco. En sí, IP no provee ningún mecanismo para determinar si un paquete alcanza o no su destino y únicamente proporciona seguridad (mediante algoritmos de checksums o sumas de comprobación) de sus cabeceras y no de los datos transmitidos. Por ejemplo, al no garantizar nada sobre la recepción del paquete, éste podría llegar dañado, en otro orden con respecto a otros paquetes, duplicado o simplemente no llegar. Si se necesita fiabilidad, esta es proporcionada por los protocolos de la capa de transporte, como TCP.

Una de las características de IP es que sus datagramas tienen un tamaño fijo. Estos fragmentos podrán ir cada uno por un camino diferente dependiendo de cómo estén de congestionadas las rutas en cada momento.

La telefonía IP viene a unir dos mundos que estaban separados: la transmisión de voz y la de datos. Efectivamente, el truco es encapsular la voz, previamente convertida a datos para utilizar toda la infraestructura existente dedicada al transporte de datos. Es importante recalcar que la voz una vez digitalizada y codificada es indistinguible de un paquete cualquiera de datos.

Lo revolucionario tras la idea de VoIP es el no utilizar circuitos físicos para las conversaciones, sino que se envían múltiples conversaciones a través de un mismo canal, de manera que se hace un uso mucho más eficiente de los recursos. Los algoritmos empleados son capaces, por ejemplo, de aprovechar los tiempos de silencio dentro de una conversación para transmitir datos correspondientes a otras.

Los elementos necesarios para que se puedan realizar llamadas vocales a través de una red IP dependen básicamente de qué terminal se utiliza en ambos extremos de la conversación. Estos pueden dividirse en dos grandes grupos, terminales IP o terminales no IP. Entre los primeros está el teléfono IP, un ordenador multimedia, un fax IP; entre los segundos tenemos al teléfono o fax convencional.

La VoIP consiste en transmitir voz sobre protocolo IP.

Por tanto transmitir voz sobre protocolo IP es toda una empresa con muchos problemastécnicos que resolver. Por suerte la tecnología ha evolucionado y la pericia de algunosingenieros talentosos ha resultado en que podamos abstraernos en gran medida deaquellos problemas inherentes a las redes IP que perjudican la calidad de voz.

1.5.2. Protocolos VoIp

Hay muchos protocolos involucrados en la transmisión de voz sobre IP. Ya de por síhay protocolos de red involucrados como el propio protocolo IP y otros protocolos detransporte como TCP o UDP.
Para simplificar las cosas podríamos clasificar a los protocolos utilizados en la VoIP entres grupos.

1.5.3. Protocolos de señalización

Los protocolos de señalización en VoIP cumplen funciones similares a sus homólogosen la telefonía tradicional, es decir tareas de establecimiento de sesión, control delprogreso de la llamada, entre otras. Se encuentran en la capa 5 del modelo OSI, es decir en la capa de Sesión.
Existen algunos protocolos de señalización, que han sido desarrollados por diferentesfabricantes u organismos como la ITU o el IETF, y que se encuentran soportados porAsterisk. Algunos son:

- SIP
- IAX
- H.323
- MGCP
- SCCP

Entre estos los más populares en el ámbito de Asterisk son SIP e IAX.

1.5.3.1 Protocolo SIP (Session Initiation Protocol).

El protocolo SIP, protocolo de inicio de sesión, permite establecer el procedimiento inicial de conexión para que dos UAs se conecten. UserAgents (UAs) se llaman así a los terminales SIP que pueden ser Teléfonos SIP, Softphone, Gateways FXS/IP, Routers SIP, Teléfonos USB, etc. Este protocolo es abierto, no está amarrado a ningún proveedor de hardware ni de software por lo que hoy en día en el mercado existen diversos fabricantes que están produciendo estos productos a precios realmente muy bajos. Este protocolo no solo se usa para establecer llamadas telefónicas si no también se utiliza para CHAT y Video.

Procedimiento de llamada

Usuario 1 quiere comunicarse con Usuario 2, Usuario 1 le pregunta al servidor SIP sobre la IP del Usuario 2, el servidor SIP procesa los datos de inicialización y establece la llamada telefónica entre los dos usuarios. Usuario 1 transmite y recibe directamente la voz con el Usuario 2, el servidor SIP no interviene en esto, Servidor SIP supervisa la señalización de los dos usuarios mientras dura la comunicación.

SIP es un protocolo basado en texto (de acuerdo con RFC-2279 para la codificación del set de caracteres) y el mensaje basado en http (RFC-2068 para la semántica y sintaxis). La dirección usada en SIP se basa en un localizador URL (UniformResourceLocater) con un formato del tipo sip:monica@192.190.132.31 (o mediante el dominio Domain: teleinfo.com.ec). De esta forma SIP integra su servicio a la Internet. En este modelo se requiere el auxilio de un server de resolución de dominio DNS (DomainName Server).

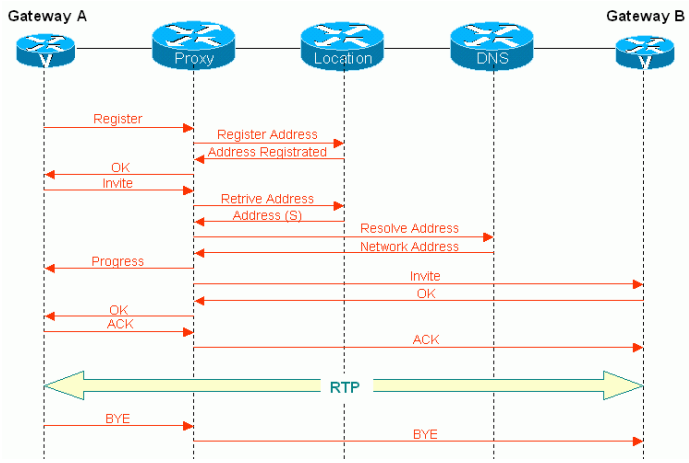


Fig.I.12. Intercambio de mensajes para establecer una comunicación con protocolo SIP.

El protocolo SIP incorpora también funciones de seguridad y autentificación, así como la descripción del medio mediante el protocolo SDP.

Las fases de comunicación soportadas en una conexión unicast mediante el protocolo SIP, son las siguientes:

- **User location:** En esta fase se determina el sistema terminal para la comunicación.
- **User capabilities:** Permite determinar los parámetros del medio a ser usados.

- **User availability:** Para determinar la disponibilidad del llamado para la comunicación.
- **Call setup ("ringing"):** Para el establecimiento de la llamada entre ambos extremos.
- **Call handling:** Incluye la transferencia y terminación de la llamada.

1.5.3.2 Protocolo IAX (Inter-AsteriskeXchangeprotocol)

IAX (Inter - AsteriskeXchangeprotocol) es un protocolo propietario, desarrollado por Mark Spencer (creador de Asterisk), Brian Capouch, Ed Guy y Frank Miller. La versión más reciente es la 2 y por ello lo encontramos más comúnmente como IAX2. Aunque surgió como un proyecto privado, desde febrero del 2010 figura ya dentro de los RFCs bajo el número 5456 con el carácter de informativo y en el mismo documento se aclara que tal publicación, se hace a discreción del editor y que de ninguna manera IAX2 es candidato a convertirse en estándar de la IETF.

Descripción y características generales del protocolo IAX2

IAX2 es un protocolo de la capa de aplicación definido para crear, modificar y terminar sesiones multimedia sobre redes IP. IAX2 fue desarrollado para el desarrollo Open SourceAsterisk y está orientado hacia el control de llamadas VoIP, sin embargo, también puede ser usado para controlar flujo de video y otros medios.

A diferencia de otros protocolos como SIP y H.323, IAX2 es un protocolo "todo en uno", ya que combina los servicios de señalización y transporte de medios en el mismo protocolo. Además de lo anterior, IAX2 utiliza un único socket UDP, evitando así la problemática que implican atravesar dispositivos como NATs y firewalls. IAX2 es un protocolo binario, lo cual reduce de forma significativa el overhead y el uso de ancho de banda. Por último, IAX2 permite la adición de nuevos tipos de carga útil (medios) para soportar nuevos servicios.

Elementos del protocolo IAX2

El protocolo IAX2 es un protocolo peer2peer orientado al control de llamadas VoIP. Algunos de los elementos que conforman este protocolo son:

- **Peer**: Es cualquier dispositivo o host que implemente el protocolo IAX2 para comunicarse.

- **Frame:** Es la unidad elemental de comunicación entre dos Peers IAX2. Todos los mensajes del protocolo son enviados en forma de Frames.
- **Elemento de Información (IE)**: Es una unidad discreta de datos que se añade a un frame IAX2 y que contiene datos específicos a una llamada o usuario.
- **UniformResourceIdentifier (URI) de IAX**: Al igual que SIP, IAX utiliza el mecanismo de URI, en su caso en particular, IAX sigue la siguiente sintaxis:

```
iax:[username@]host[:port][/number[?context]]

iax: - Literalmente IAX
username - Cadena usada para propósitos de identificación.
host - Dominio del recurso. Puede ser el FQDN, una dirección IPv4 o
[IPv6] encerrada entre corchetes.
port - Puerto UDP para IAX
number - El número del peer al que se desea contactar.
context - El subconjunto de recursos al cual pertenece el usuario
llamado dentro del host solicitado.

  Ejemplos:

iax:voip.unam.mx/israel
iax:ucol.mx:4569/yocelin
iax:ejemplo.com:4570/israel?gtvoip
  iax:192.0.2.4:4569/israel?gtvoip
iax:[2001:db8::1]:4569/israel?gtvoip
iax:ejemplo.com/12022561414
iax:gio@voip.unam.mx/12022561414
```

Frames y mensajes

El elemento sobre el cual se basa el protocolo IAX es el frame. Éste constituye la unidad elemental para cualquier comunicación. Hay diferentes tipos de frames, el "full frame" transporta datos de señales y control, mientras que los "mini frames" transportan los flujos de medios. De manera opcional, dentro de los full frames, se puede transportar lo que se denomina "information element, (IE)". Los IEs se

utilizan para describir diferentes tipos de usuarios o datos específicos dentro de una llamada. Otro tipo de frames son los "meta frames", que se utilizan para realizar troncales o para la transmisión de flujo de video.

Dentro del lenguaje del IAX, existen dos tipos de mensajes, los confiables o garantizados, y los no garantizados. En la primera categoría caen los "full frames" mientras que en la segunda los "mini frames". De acuerdo con la funcionalidad del mensaje (frame), se puede clasificar a los mismos de la siguiente forma:

- Registro (OPCIONAL)
- Gestión de enlace de llamada
- Optimización de ruta de llamada (OPCIONAL)
- Mid-Call
- Terminación de llamada
- Monitoreo de la Red
- Marcación de dígitos (OPCIONAL)
- Misceláneos
- Mensajes de Medios

IAX proporciona control y transmisión de voz sobre redes IP. El IAX puede ser usado con cualquier tipo de medio como voz y vídeo, pero fue pensado principalmente para llamadas de voz. Los objetivos del proyecto do IAX derivarán de la experiencia con los protocolos de voz sobre ip como el SIP (Sesión Initiated Protocol) y el MGCP (Media Gateway Control Protocol) para control y el RTP para el flujo-multimedia (streaming media) y son:

- Minimizar el uso de banda ancha para el tráfico de ambos, media y control con énfasis específica en llamadas de voz individuales.

- Proveer transparencia a NAT (Network Address Translation).

- Tener la posibilidad de transmitir informaciones sobre el plan de discado.

- Soportar la implantación eficiente de recursos de paging e intercomunicación.

Teoría de Operación

IAX es un protocolo de media y señalización "peer-to-peer". Eso significa que los dispositivos mantienen conexiones asociadas con las operaciones de protocolo. Con respecto a los componentes de señalización de IAX, este tiene más parecido con el SIP que con el MGCP, que es un protocolo de control de tipo maestro-esclavo.

Como el IAX usa el mismo protocolo para señalización y media en un mismo puerto UDP, este no sufre de los problemas de atravesar dispositivos que realizan NAT (Network AddressTranslation), como, por ejemplo, ruteadores ADSL (Característica fundamental para operadoras de telefonía IP). El IAX usa el puerto UDP 4569 para comunicar todos los paquetes.

El protocolo IAX emplea un proceso similar de registro y autenticación al que usa SIP.

Uso de banda ancha

El uso de banda ancha en voz sobre IP es modificado por una serie de factores. Desde el CODEC, hasta cuestiones como compresión de encabezados.

El IAX permite el uso del modo Trunked. En este caso, cuando más de una llamada es hecha, el overhead de los encabezados IP es disminuido, encaminando múltiples paquetes de voz de diferentes llamadas en un único paquete. Con esto la necesidad de banda ancha es reducida.

1.5.3.3. Protocolo H.323

La UIT definió el estándar que proporciona a los fabricantes las normas a seguir para la voz sobre IP. En este estándar se definen 3 elementos básicos:

- **Terminales**: son los sustitutos de los terminales clásicos. Pueden ser hardware o software. Voz, datos y video y por separado.
- **Gateways**: son los que se utilizan para intercomunicar las redes de datos con las de telefonía de conmutación de paquetes, siendo su actuación transparente para los usuarios.
- **Gatekeepers**: este es opcional para este protocolo pero si está presente. Los terminales y gateways deben hacer uso de su servicio. Los obligatorios son:

1. La traducción de alias o números de teléfono en direcciones IP.

2. La administración de ancho de banda y control del tráfico generado por las diferentes comunicaciones, limitando el número máximo de comunicaciones simultáneas**.**
3. Enrutamiento teniendo la capacidad para elegir el gatewaymás adecuado al que redireccionar la llamada.
4. Control de admisión en la red utilizando para ello mensajes del protocolo **RAS ARQ, ACF y ARJ.**

El **H323** define un estándar que a su vez se apoya en una serie de protocolos para su implementación según los distintos aspectos de la comunicación que cubren:

1. **Direccionamiento: RAS** protocolo de comunicaciones que a traces de mensajes permite a un gatekeeper desempeñar sus funciones, y DNS servicio de resolución de nombres en direcciones IP del que ya hablamos en otras ocasiones.
2. **Señalización: Q.931** la señalización inicial de llamada. H225 control de llamada señalización registro y admisión y paquetización del stream o flujo de voz, H245 protocolo de control para especificar mensajes de apertura y cierre de canales para streams de voz.
3. **Compresión de voz:** requeridos G711 y G723. Opcionales G.728, G729 y G.722.
4. **Transmisión de voz: UDP**, la transmisión se realiza sobre paquetes UDP, RPT maneja los aspectos relativos a la temporarización marcando los paquetes UDP con la información necesaria para la correcta entrega de los mismos en recepción.
5. **Control de la transmisión:** RTCP se utiliza principalmente para detectar situaciones de congestión de la red y tomar en su caso acciones correctoras.

1.5.3.4. Protocolo MGCP (Media Gateway Control Protocol)

El protocolo del control de entrada de medios (MGCP) especifica la comunicación entre los elementos del control de la llamada y las entradas de la telefonía. Es un protocolo basado en texto. Las entradas de los medios son las entradas de la telefonía que convierten señales con conmutador de circuito de la voz a los paquetes de los datos para las redes. El Internet Engineering Task Force (IETF) creó MGCP para tratar algunos de los defectos percibidos de H.323.

El propósito principal de MGCP es poner el control de la inteligencia que señala de llamada y de proceso en agentes de la llamada o reguladores de la entrada de los medios.
Este protocolo interno se desarrolló principalmente para atender las demandas de las redes de telefonía IP con base en portaaviones. MGCP es un protocolo complementario para H.323 y SIP, que fue diseñado como un protocolo interno entre el controlador y el Media Gateway. En MGCP, un MGC principalmente se ocupa de todas las operaciones de procesamiento de llamadas mediante la vinculación con la red IP a través de constantes comunicaciones con un dispositivo de señalización IP, por ejemplo, un servidor SIP o un Gatekeeper H.323.

MGCP está compuesto por un agente de llamadas, un MG (media gateway) que realiza la conversión de las señales de los medios de comunicación entre circuitos y paquetes, y una SG (Signaling Gateway) cuando se conecta a la PSTN (PublicSwitchedTelephone Network). MGCP es ampliamente utilizado entre los elementos de una puerta de enlace multimedia descompuesto.

1.5.3.5. Protocolo SCCP (SkinnyClient Control Protocol)

La capa Parte de Control de la Conexión de Señalización o PCCS (SCCP –Signalling Connection Control Part), se incluye por encima de la Parte de Transferencia de Mensajes (PTM o MTP) de la pila N7 para proporcionar funciones adicionales de servicios de transferencia de información a nivel de red

Este servicio de transferencia de información no está relacionado con la señalización (establecimiento, mantenimiento o liberación) de un circuito de conversación, si - no que es utilizado para acceder a bases de datos que permitan conocer cómo debe evolucionar una llamada básica o un servicio suplementario en un entorno de red. De alguna forma complementa a la MTP para ofrecer servicios puros de capa de Red de OSI.

1.5.4. Protocolos de transporte de voz

La proliferación de equipos, sumada a la disponibilidad de hardware de audio/video económicos y la posibilidad de contar con velocidades de conexión cada vez más rápidas, ha aumentado el interés en el uso de Internet para enviar audio y video, tipos de datos que tradicionalmente se reservaban para redes especializadas.

Durante los últimos años, las audioconferencias y las videoconferencias se han convertido en una práctica común. Sin embargo, la misma naturaleza de Internet indica que esta red no está preparada para la transmisión de datos en tiempo real y, por consiguiente, la calidad del audio transmitido por Internet generalmente tiene una calidad mediocre. Esta teoría específicamente trata el análisis y la solución de estos problemas para permitirle a una audioconferencia o aplicación de teléfono por Internet que cambie su funcionamiento para mantener una calidad auditiva aceptable, incluso en los casos en los que la red esté algo congestionada.
No se debe confundir aquí con protocolos de transporte de bajo nivel como TCP y UDP.
Nos referimos aquí al protocolo que transporta la voz propiamente dicha o lo quecomúnmente se denomina carga útil. Este protocolo se llama RTP (Real-time TransportProtocol).
Este protocolo entra a funcionar una vez que el protocolo de señalización ha establecidola llamada entre los participantes.

1.5.4.1. RTP (Protocolo en Tiempo Real)

El objetivo de RTP es brindar un medio uniforme de transmisión sobre IP de datos que estén sujetos a las limitaciones de tiempo real (audio, video, etc.). La función principal de RTP es implementar los números de secuencia de paquetes IP para rearmar la información de voz o de video, incluso cuando la red subyacente cambie el orden de los paquetes.

De manera más general, RTP permite:

- Identificar el tipo de información transmitida;
- Agregarle marcadores temporales y números de secuencia a la información transmitida;
- Controlar la llegada de los paquetes a destino.

Además, los paquetes de difusión múltiple pueden utilizar RTP para enrutar conversaciones a múltiples destinatarios RTCP. El protocolo RTCP se basa en transmisiones periódicas de paquetes de control que realizan todos los participantes de la sesión.

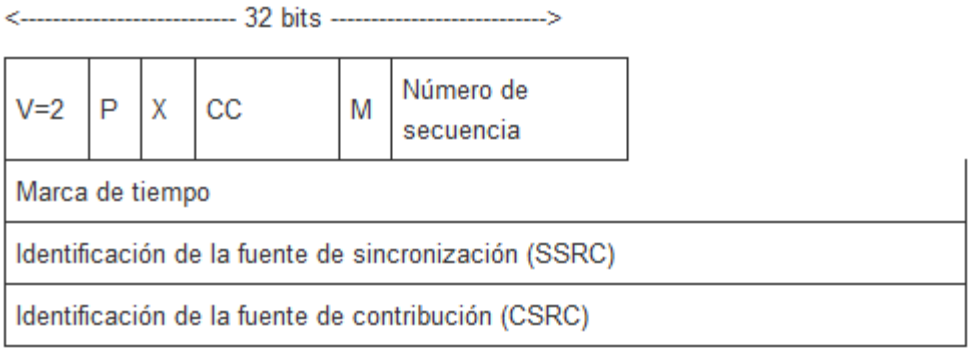
Es un protocolo de control para el flujo RTP, que permite transmitir información básica sobre los participantes de la sesión y la calidad de servicio.

Uso previsto de RTP y RTCP

RTP permite la administración de flujos multimedia (voz, video) sobre IP. RTP funciona sobre el protocolo UDP. El encabezado RTP lleva información de sincronización y numeración. La codificación de datos dependerá del tipo de compresión. Sin embargo, la adaptación de un método de compresión a RTP se describe en un documento RFC (petición de comentarios) específico. Se utiliza un canal RTP por tipo de flujo: uno para audio, uno para video. El campo xxx se utiliza para la sincronización. RTP ofrece un servicio extremo a extremo. Agrega un encabezado que brinda información de tiempo, necesaria para la sincronización de flujo en tiempo real de sonido y video. RTP y RTCP permiten, respectivamente, transportar y controlar bloques de datos que cuentan con propiedades de tiempo real. Los protocolos RTP y RTCP se encuentran en un nivel de aplicación y utilizan los protocolos de transporte subyacentes TCP o UDP. Pero el uso de RTP/RTCP generalmente se lleva a cabo por encima de UDP.

Formato de los encabezados y su contenido

El encabezado RTP lleva la siguiente información:



A continuación se indican los significados de los diferentes campos de encabezados:

- **Campo de versión V:** 2 bits de longitud. Indica la versión del protocolo (V=2).
- **Campo de relleno P:** 1 bit. Si P es igual a 1, el paquete contiene bytes adicionales para rellenar y finalizar el último paquete.

- **Campo de extensión X:** 1 bit. Si X = 1, el encabezado está seguido de un paquete de extensión.
- **Campo de conteo CRSC CC:**4 bits. Contiene el número de CRSC que le sigue al encabezado.
- **Campo de marcador M:** 1 bit. Un perfil de aplicación define su interpretación.
- **Campo de tipo de carga útil PT:** 7 bits. Este campo identifica el tipo de carga útil (audio, video, imagen, texto, html, etc.).
- **Campo Número de secuencia:** 16 bits. Su valor inicial es aleatorio y aumenta de a 1 por cada paquete enviado. Puede utilizarse para detectar paquetes perdidos.
- **Campo Marca de tiempo:** 32 bits. Refleja el instante de muestreo del primer byte del paquete RTP. Este instante debe obtenerse a partir de un reloj que aumenta de manera monótona y lineal para permitir la sincronización y el cálculo de la variación de retardo en el destino.
- **Campo SSRC:** 32 bits. Identifica de manera única la fuente. La aplicación elige su valor de manera aleatoria. SSRC identifica la fuente de sincronización (simplemente llamada "la fuente"). **Campo CSRC:** 32 bits. Identifica las fuentes contribuyentes.

Encabezados RTCP

El objetivo de RTCP es brindar diferentes tipos de información y una devolución con respecto a la calidad de recepción.

¿Cómo se utiliza RTCP con respecto a RTP?

RTCP es un protocolo de control asociado con RTP, que mide los desempeños pero no ofrece garantías. Para esto, se debe utilizar un protocolo de reserva como RSVP o asegurarse de que los enlaces de comunicación utilizados sean de proporción correcta en relación con el uso que se hace de ellos.

¿Sobre qué protocolos funcionan RTP y RTCP?

RTP/RTCP se encuentra sobre el transporte UDP/TCP, pero prácticamente sobre UDP.

RTP es un protocolo de sesión, pero se encuentra en la aplicación. Es el desarrollador que lo tiene que integrar.

¿Cómo se transporta el tipo de flujo?

RTP no tiene nada que ver con el tipo de flujo. Se encuentra sobre UDP, que está sobre IP. El tipo de flujo teóricamente se utiliza en IP.
RTP lleva un número de secuencia, una marca de tiempo y un identificador único de la fuente (SSRC).

1.5.4.2 Protocolos de plataforma IP

En esta categoría agruparemos a los protocolos básicos en redes IP y que forman la basesobre la cual se añaden los protocolos de voz anteriores. En estos protocolos podríamosmencionar a Ethernet, IP, TCP y UDP.

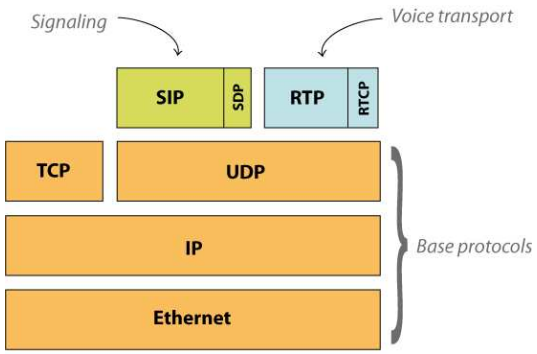


Fig. I.13. Protocolos involucrados en una llamada SIP.

En la Figura 14, podemos observar un hecho curioso y es que pese a que SIPsoporta tanto UDP como TCP sólo lo vemos posado sobre UDP. No se trata de un errorsino más bien que en Asterisk la implementación de SIP solo está disponible para UDP.

Protocolo IP
El protocolo IP sin duda es uno de los más populares jamás implementados, principalmente por el auge del Internet: La gran red de redes, que utiliza este protocolopara su enrutamiento

¿Qué es el Protocolo IP?

El protocolo IP (Internet Protocol) es un protocolo que trabaja a nivel de red donde lainformación se envía en paquetes llamados paquetes IP. Este protocolo ofrece unservicio "sin garantías" también llamado del "mejor esfuerzo". Es decir que nadagarantiza que los paquetes lleguen a destino, sin embargo se hará lo posible por hacerlosllegar.

Paquete IP

Como habíamos dicho antes el protocolo IP es un protocolo que divide la informaciónen paquetes que envía a su destino y la ventaja de tener la información paquetizada esque estos paquetes pueden tomar diferentes caminos para llegar a destino. Es decir quehay redundancia de caminos y es menos probable que todos los paquetes se pierdan.

1.5.5. Protocolos de Transporte

1.5.5.1. Protocolo TCP

Como ya habíamos dicho el protocolo IP no garantiza que los datos lleguen a destino, solo hace su mejor esfuerzo para que lleguen.
Por lo tanto era necesario un protocolo que se encargue de controlar la transmisión dedatos y por esta razón se diseñó lo que se llama Transmission Control Protocol osimplemente protocolo TCP. TCP es un protocolo de transporte que se transmite sobre IP.
TCP ayuda controlando que los datos transmitidos se encuentren libre de errores y seanrecibidos por las aplicaciones en el mismo orden en que fueron enviados. Si se pierdendatos en el camino introduce mecanismos para que estos datos sean reenviados.
Es por esto que TCP es un buen protocolopara control de sesiones pero no tan bueno para transmisión de datos en tiempo real. Sin embargo TCP juega un rolmuy importante en muchos protocolos relacionados con un servidor Elastix.

TCP es quien introduce el concepto de "puerto" que no es otra cosa que una abstracciónpara poder relacionar los flujos de datos con servicios de red específicos (o protocolosde más alto nivel). Por ejemplo, el puerto 80 se asocia con el servicio de Web o elprotocolo HTTP; el puerto 25 se asocia con el servicio de correo electrónico o protocoloSMTP.

1.5.5.2. Protocolo UDP

UDP (UserDatagramProtocol) es otro protocolo de transporte. Se diferencia con TCPen que a este protocolo no le importa si los datos llegan con errores o no y tampoco leimporta si llegan en secuencia.

Un protocolo de transporte no necesariamente tiene que garantizar que lainformación llegue a destino o llegue en secuencia. Esta es solo una característica extra.
Es más o menos análogo a un servicio de transporte de mercancía. Imaginémonos unaflota de motocicletas que ofrece el servicio de transporte en una ciudad e imaginémonos que le encomendamos a dicha flota la tarea de transportar un gran cargamento de archivos de una oficina u otra. La compañía se encargará de dividir nuestro cargamentode archivos y distribuirlo en cantidades o paquetes que puedan ser transportados en susvehículos. Hará lo necesario para que nuestro cargamento llegue a destino. Esto es enesencia el servicio de transporte. Sin embargo podemos escoger dos clases de servicio: una que garantiza que la mercancía llegue segura y otra que no. Estos dos tipos deservicio son análogos a los dos tipos de protocolos de transporte que estamosdescribiendo en este apartado UDP y TCP.

En fin, UDP divide la información en paquetes, también llamadosdatagramas, para ser transportados dentro de los paquetes IP a su destino.
Al no ser necesario incluir mucha información de control, el protocolo UDP reduce lacantidad de información extra en los paquetes por lo que es un protocolo más rápido que TCP y adecuado para transmisión de información que debe ser transmitida en tiemporeal como la voz.
Es por esta razón que la voz en aplicaciones de VoIP es transmitida sobre esteprotocolo.

1.5.6. Codificación de la voz

Ya tenemos claro que para transportar la voz se utilizan algunos protocolos como SIP, IAX y otros como RTP o RTCP. Pero la voz es una onda analógica que necesitatransformarse a digital en algún formato antes de ser transmitida.
Lógicamente podríamos tratar de transmitirla tal cual resulta de la conversión analógica-digital(ADC) pero resulta que nos encontramos en una red de paquetes así quedebemos paquetizar esta información. Además si la transmitimos tal cual

resulta de laconversión ADC desperdiciaríamos recursos de la red por lo que hace falta encontrar unformato óptimo.
Esa búsqueda de un formato óptimo generó algunas alternativas de formatos detransmisión llamadas codecs.

1.5.6.1. Codecs

La palabra codec proviene de abreviar las palabras COdificación y DECodficación. Sufunción principal es la de adaptar la información digital de la voz para obtener algún beneficio. Este beneficio en muchos casos es la compresión de la voz de tal manera quepodamos utilizar menos ancho de banda del necesario.
Algunos codecs, soportados por Asterisk y comúnmente usados en comunicaciones deVoIP, son G.711, G.729, GSM, iLBC, entre otros.
Explicaremos brevemente tres de ellos.

G.711
G.711 es uno de los codecs más usados de todos los tiempos y proviene de un estándar ITU-T que fue liberado en 1972. Viene en dos versiones u-law y a-law. Laprimera versión se utiliza en los Estados Unidos y la segunda se utiliza en Europa.
Una de sus características es la calidad de voz debido a que casi no la comprime. Utiliza 64kbit/s, es decir un muestreo de 8 bits a 8kHz. Es el códec recomendado para redes LAN pero hay que pensarlo dos veces antes de utilizarlo en enlaces remotos debido alalto consumo de ancho de banda.

El soporte para este códec ya viene habilitado en Elastix.

G.729
También se trata de una recomendación ITU cuyas implementaciones ha sido históricamente licenciadas.
La ventaja en la utilización de G.729 radica principalmente en su alta compresión y porende bajo consumo de ancho de banda lo que lo hace atractivo para comunicaciones porInternet. Pese a su alta compresión no deteriora la calidad de voz significativamente ypor esta razón ha sido ampliamente usado a través de los años por muchos fabricantes de productos de VoIP.
G.729 utiliza 8kbit/s por cada canal. Si comparamos este valor con el de G.711notaremos que consume 8 veces menos ancho de banda, lo cual a simple

vista es unahorro de recursos significativo. Existen variaciones de G.729 que utilizan 6.4kbit/s y 11.8kbit/s.
Para habilitar canales G.729 en Elastix hay que comprar una licencia por cada canal.

GSM

Muchas personas suelen preguntar si el codec GSM tiene algo que ver con el estándarde comunicaciones celulares y la respuesta es que sí.
El estándar que define la tecnología celular GSM (Global Systemfor Mobile communications) incluye este codec.
La ventaja de este códec también es su compresión. Acerca de la calidad de voz.
GSM comprime aproximadamente a 13kbit/s y ya viene habilitado en Elastix.

1.5.7. Sobrecarga de protocolos

Como ya vimos, para transportar la voz de un lugar a otro, en una red de paquetes, necesitamos la ayuda de algunos protocolos; pero ya nos habremos dado cuenta de queestos protocolos transmiten data adicional que ocupa ancho de banda extra a la vozpropiamente dicha. Algunos de ellos son Ethernet, IP, UDP, RTP.
En resumen esto hace que el ancho de banda real para transmitir voz sea mayor al delcódec.

Comparativa de codecs

A continuación una tabla que muestra el overhead para algunos de los codecs máspopulares soportados por Asterisk.

Codec	Ancho de banda códec	Ancho de banda real Ethernet	Porcentaje de overhead
G.711	64 Kbps	95.2 Kbps	48.75%
iLBC	15.2 Kbps	46.4 Kbps	205.26%
G.729A	8 Kbps	39.2 Kbps	390%

1.5.8. Calidad de Voz

1.5.8.1. Síntomas que afectan la calidad de voz

Enumerar los problemas que afectan la calidad de voz es difícil pues a lo largo de los años se han encontrado con muchos, algunos muy parecidos a otros lo cual hace difícilcategorizarlos y cuyas causas son muy variadas. Sin embargo, a continuación se enumera los más comunes explicando sus causas y posibles soluciones.

1.5.8.1.1 Eco

El eco se produce por un fenómeno técnico que es la conversión de 2 a 4 hilos de los sistemas telefónicos o por un retorno de la señal que se escucha por los altavoces y se cuela de nuevo por el micrófono. El eco también se suele conocer como reverberación. El eco se define como una reflexión retardada de la señal acústica original.

El eco es especialmente molesto cuanto mayor es el retardo y cuanto mayor es su intensidad con lo cual se convierte en un problema en VoIP puesto que los retardos suelen ser mayores que en la red de telefonía tradicional.

Valores Recomendados

El oído humano es capaz de detectar el eco cuando su retardo con la señal original es igual o superior a 10 ms. Pero otro factor importante es la intensidad del eco ya que normalmente la señal de vuelta tiene menor potencia que la original. Es tolerable que llegue a 65 ms y una atenuación de 25 a 30 dB.

Posibles Soluciones

En este caso hay dos posibles soluciones para evitar este efecto tan molesto.

- **Supresores de eco.-** Consiste en evitar que la señal emitida sea devuelta convirtiendo por momentos la línea full-duplex en una líneahalf-duplex de tal manera que si se detecta comunicación en un sentido se impide la comunicación en sentido contrario.
- **Canceladores de eco.-** Es el sistema por el cual el dispositivo emisor guarda la información que envía en memoria y es capaz de detectar en la señal de vuelta la misma información (tal vez atenuada y con ruido).

El problema se agrava cuando la impedancia de la línea telefónica varía mucho. Muchade la tarjetería telefónica disponible para Asterisk no dispone de un buen mecanismodinámico de ajuste de la impedancia de la línea con la impedancia de la tarjeta. Por estarazón una parte de la onda se refleja.
Sin embargo, existe una forma de acoplar estas impedancias lo mejor posible. Esto sepuede realizar con la utilería llamada fxotune disponible en Elastix.
Lamentablemente esta utilería se debe ejecutar manualmente y con el servicio Asteriskapagado. Para líneas con problemas se recomienda ejecutarlo en horas no laborables unavez por semana. El comando es el siguiente.

```
fxotune -i 5
```

Lo que hace el comando fxotune es hacer prueba y error enviando una señal pura porla línea y escuchando el retorno. Esto lo hace muchas veces para cada línea hastaencontrar el mejor valor de ganancia, el cual escribe en un archivo ubicado en:

/etc/fxotune.conf

Al finalizar su ejecución podemos encender Asterisk de nuevo pero antes hay queejecutar el siguiente comando para decirle a Zaptel que cargue los valores nuevos deganancia.

```
fxotune -s
```

Esto lo debemos ejecutar siempre antes de arrancar Asterisk por lo que se recomiendamejor incluirlo al final del script de arranque de Zaptel ubicado en la ruta:

/etc/init.d/zaptel para no tener que hacerlo manualmente cada vez.
Es muy importante hacer notar que si se utiliza el fxotune para tratar deacoplar las líneas no se deben configurar las variables txgain o rxgain en elzapata.conf ya que sobrescribirán el trabajo del fxotune.

Otra causa del eco es el eco acústico provocado cuando la señal de sonido seretroalimenta desde el micrófono al audífono. Esto es más notable cuando hablamos poraltavoz. Por supuesto el diseño del teléfono tiene mucho que ver aquí y hay modelosque introducen menos eco acústico que otros.

fxotune -i 5
fxotune -s

1.5.8.1.2 Bajo nivel o volumen

Muchas redes telefónicas de baja calidad atenúan la señal de manera significativahaciendo que oigamos un volumen muy bajo. Esto obviamente afecta la calidad de voz,haciendo que la conversación muchas veces sea inentendible o haciendo que no sepuedan detectar los dígitos DTMFs.
Tanto el volumen de recepción como el de transmisión pueden ser amplificadosmediante parámetros en el archivo zapata.conf.

1.5.8.1.3 Retardo

El retardo no es otra cosa que la demora de la voz en llegar a destino. Usualmente elretardo es menor a un segundo y si es menor a 200 ms pasa casi desapercibido.
Retardos mayores a 500 ms provocan que la conversación se pise, es decir que losinterlocutores se interrumpan y la conversación se traslape.
Cuando existe retardo es casi imposible eliminarlo a nivel del servidor pues en la granmayoría de los casos el retardo es un síntoma de problemas inherentes a la red decomunicaciones. Con esto se quiere decir que si se quiere eliminar el retardo habrá queanalizar si se puede cambiar o mejorar algo en la red de comunicaciones. S hablamos deuna red de paquetes, puede ser que uno de los equipos (por ejemplo un ruteador) estésaturado en su capacidad.

1.5.8.1.4 Distorsión de la voz

En esta categoría recaen diferentes problemas. Sin embargo uno común es el de losusuarios que reportan algo como “se escucha robotizado”.
Cuando se escucha robotizado usualmente se trata de usuarios que utilizan un códec ahorrador de ancho de banda como por ejemplo gsm. Estos codecs realizan un muybuen trabajo comprimiendo la voz lo máximo posible pero el costo es la

pérdida deinformación en el proceso de codificación. Si a esto se le agregan problemas con elancho de banda el problema empeora.
La solución en este caso en particular es cambiar de codec pero hay que tener presenteque eso podría disparar otro problema peor si es que se usa un codecmás consumidorde ancho de banda y el enlace se satura.

1.5.8.1.5 Comunicación entrecortada

Un problema muy molestoso por cierto que normalmente está relacionado con lapérdida de paquetes. A su vez la pérdida de paquetes puede ser causada por diferentesproblemas en la red, siendo el más común el de redes con una latencia elevada o anchode banda limitado. La comunicación entrecortada también puede ser ocasionada por unelevado jitter en la red

En todo caso lo normal es buscar la causa en la red y no en el servidor.
Por lo general si la latencia de la red es siempre de menos de150 ms y el canal de comunicaciones no se encuentra saturado podemos estar tranquilosde que los problemas de comunicación entrecortada no nos quitarán el sueño.

1.5.8.2 PARÁMETROS RELACIONADOS CON LA CALIDAD DE VOZ.

1.5.8.2.1 Retardo de red

Hay que distinguir aquí que no estamos hablando de retardo de voz sino el retardo delos paquetes de red en las redes de paquetes.
Una manera sencilla de calcular el retardo de la red es utilizar alcomando ping. El comando ping nos presenta al final un pequeño resumen estadísticode los paquetes enviados. El resumen luce como el siguiente.

```
--- ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5004ms
rtt min/avg/max/mdev = 73.055/74.181/74.852/0.710 ms
```

Aquí podemos ver algunos parámetros como el retardo mínimo, máximo, promedio ydesviación.

1.5.8.2.2 Pérdidas de paquetes

Las pérdidas son ocasionadas por paquetes que no llegaron a su destino. Pueden habermuchas razones para esto como equipos defectuosos o saturados, pérdidas en el mediode transmisión (cables mal ponchados, ruido ambiente elevado), etc.
En el reporte del comando ping examinado hace poco vemos que también se nos reportaporcentualmente las pérdidas de paquetes. Lo deseable es que no existan pérdidas depaquetes en lo absoluto. Si existen, hay que averiguar el por qué.
Inclusive pérdidas de menos del 1% pueden afectar a las conversaciones de voz sobreIP. Más aún si usamos codecs con gran compresión.

1.5.8.2.3. Jitter

El jitter es un parámetro muy importante cuando se habla de calidad de voz en redes depaquetes. El jitter se define como la variabilidad del retardo y normalmente está en elorden de los milisegundos.
Este parámetro es necesario para analizar la calidad de voz pues conocer que tenemosun promedio de retardo bajo no es suficiente para garantizar una buena calidad. ¿Por qué?
Porque si tenemos un promedio de retardo aceptable pero en cambio es muy variableesto significa que existe más probabilidad que los paquetes lleguen en desorden o conretardos excesivos y debemos recordar que debido a que estamos hablando decomunicaciones en tiempo real no se pueden esperar a que lleguen todos los paquetes, habrá que descartar los que se demoren más de lo necesario. Por tanto, si tenemos unjitter elevado es más probable que se descarten paquetes y por lo tanto oigamos unaconversación entrecortada.

1.5.8.3. Cómo medir la calidad de voz

Medir la calidad de voz siempre ha sido un rompecabezas para los ingenieros y sucomplejidad radica en que la calidad de voz es en parte un parámetro subjetivo de lapersona que escucha. Hay personas que justifican inconscientemente cierta falta de calidad de voz en pro de lasventajas o conveniencias personales percibidas y un ejemplo de esto es que las personasno se quejan mucho de la calidad de voz en teléfonos celulares (al menos de primerageneración) en pro de la ventaja de la movilidad. Sin embargo, si la misma calidad laescucharan en una línea fija es probable que llamen a la compañía telefónica a quejarse porque su línea suena raro

o con mala calidad. Dicho de otra manera inconscientemente estamos justificando esa falta de calidad y haciéndola "justificable".

1.5.8.4. Canceladores de eco

Cómo funciona un Canceladorde eco?

Es muy importante saber cómo funcionan los canceladores de eco para entender cómo sacarles el máximo provecho y quién sabe, para tener las bases para diseñar el nuestro propio o modificar alguno existente.

Un cancelador de eco parte de un principio lógico muy sencillo. Si se refleja una partede la señal de ida en la de regreso, entonces para eliminar el eco debería bastar conrestar la señal de ida (en cierta proporción) a la señal de regreso.
Debido a que el eco es una señal reflejada que se encuentra atenuada, la clave está en estimar adecuadamente dicha atenuación. Por ejemplo, supongamos que la señal de ecoes un 20% de la señal original. Entonces si podemos predecir que debemos restar a la señal de regreso un 20% de la señal de ida, habremos eliminado el eco completamente.

Esta "predicción" del factor de atenuación es una parte clave de todo algoritmo de cancelación de eco y recibe el nombre de algoritmo adaptativo o filtro adaptativo (adaptivefilter) ya que debe adaptar el valor constantemente para obtener los mejoresresultados.
En la siguiente figura supondremos que la atenuación de la señal reflejada está denotada por la letra ɑ.. La señal recibida es Rx, la señal transmitida es Tx y la señal transmitida con el componente de eco es Txe.

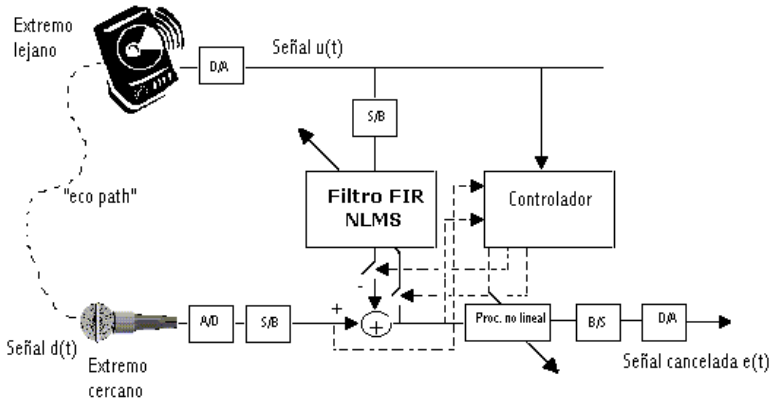


Fig. I.14. Diagrama básico del funcionamiento de un cancelador de eco

Sin embargo, no todo es tan sencillo como se explica aquí. El eco no es solo una señalreflejada atenuada sino que también puede estar desplazada en el tiempo con ciertoretardo. Ese retardo también hay que predecirlo para poder restar la indeseable señal deeco. Predecir el retardo no es una tarea sencilla y por lo general los canceladores de ecotienen limitantes. Si el retardo es muy grande dejan de funcionar ya que es mucho trabajo revisar la señal en busca de retardo por grandes lapsos de tiempo.

CAPÍTULO II
PROTOCOLO DE SEÑALIZACIÓN SIP

2.1 Protocolo Sip

SIP (Session Initiation Protocol) es un protocolo de señalización para conferencia, telefonía, presencia, notificación de eventos y mensajería instantánea a través de Internet. Fue desarrollado incialmente en el grupo de trabajo IETF MMUSIC (Multiparty Multimedia Session Control) y, a partir de Septiembre de 1999, pasó al grupo de trabajo IETF SIP.

2.2 Historia del Protocolo Sip

El 22 de febrero de 1996 Mark Handley y Eve Schooler presentaron al IETF un borrador del Session Invitation Protocol conocido ahora como SIPv1. El mismo estaba basado en trabajos anteriores de Thierry Turletti (INRIA Videoconferencing System o IVS) y de Eve Schooler (Multimedia Conference Control o MMCC). Su principal fortaleza, heredada por la versión actual de SIP, era el concepto de registración, por el cual un usuario informaba a la red dónde (en qué host de Internet) podía recibir invitaciones a conferencias. Esta característica permitía la nomadicidad del usuario.

Ese mismo día el Dr. Henning Schulzrinne presentó un borrador del Simple Conference Invitation Protocol (SCIP), que estaba basado en el HTTP (Hypertext Transport Protocol). Usaba TCP (Transmission Control Protocol) como protocolo de transporte. Como identificadores de los usuarios utilizaba direcciones de correo electrónico para permitir el uso de una misma dirección para recibir correos electrónicos e invitaciones a conferencias multimedia. No utilizaba al SDP para la descripción de los contenidos sino que creaba un mecanismo propio.

El IETF decidió combinar ambos en un único protocolo denominado Session Initiation Protocol, (es decir cambiando el significado de la inicial I en el acrónimo "SIP") y su número de versión fue el dos, dando origen al SIPv2. En diciembre de 1996 los tres autores (Schulzrinne, Handley y Schooler), presentaron el borrador del SIPv2. El mismo luego de ser discutido en el grupo de trabajo MMUSIC

(Multiparty Multimedia Session Control) del IETF alcanzó el grado de "proposed standard" en la [RFC 2543] publicada en Febrero de 1999. En septiembre de 1999 se creó el grupo de trabajo SIP en el IETF que continuó con el desarrollo del protocolo y en Junio de 2002 se publicó la [RFC 3261] que reemplazó a la anterior introduciendo modificaciones propuestas durante el trabajo del grupo SIP. Los autores de esta última RFC, hoy vigente son: Jonnathan Rosenberg, Henning Schulzrinne, Gonzalo Camarillo, Allan Johnston, Jon Peterson, Robert Sparks, Mark Handley y Eve Schooler.

2.3. Arquitectura Sip

El estándar define varios componentes SIP y hay varias formas de implementarlos en un sistema de control de llamadas.

- servidores *User Agent,*
- *Proxies*
- *Registrars,*
- *Redirect*
- *Location.*

A menudo, estos elementos son entidades lógicas que se ubican todas juntas para conseguir una mayor velocidad de procesamiento que dependerá a su vez de una buena configuración.
Normalmente los UA son una aplicación en el ordenador del usuario, aunque a veces los UA también pueden ser teléfonos móviles, PSTN gateways, una PDA, etc.

2.4. Diseño del protocolo

El protocolo SIP fue diseñado por el IETF con el concepto de "caja de herramientas", es decir, el protocolo SIP se vale de las funciones aportadas por otros protocolos, las que da por hechas y no vuelve a desarrollarlas . Debido a este concepto SIP funciona en colaboración con otros muchos protocolos. El protocolo SIP se concentra en el establecimiento, modificación y terminación de las sesiones, se complementa, entre otros, con el SDP, que describe el contenido multimedia de la sesión, por ejemplo qué direcciones IP, puertos y códecs se usarán durante la comunicación. También se complementa con el RTP (Real-time Transport Protocol). RTP es el verdadero portador para el contenido de voz y video que intercambian los participantes en una sesión establecida por SIP.

Otro concepto importante en su diseño es el de extensibilidad. Esto significa que las funciones básicas del protocolo, definidas en la RFC 3261, pueden ser extendidas mediante otras RFC (Requests for Comments) dotando al protocolo de funciones más potentes.
Las funciones básicas del protocolo incluyen:

- Determinar la ubicación de los usuarios, proveyendo nomadicidad.
- Establecer, modificar y terminar sesiones multipartitas entre usuarios.

El protocolo SIP adopta el modelo cliente-servidor y es transaccional. El cliente realiza peticiones (requests) que el servidor atiende y genera una o más respuestas (dependiendo de la naturaleza, Método, de la petición). Por ejemplo para iniciar una sesión el cliente realiza una petición con el método INVITE en donde indica con qué usuario (o recurso) quiere establecer la sesión. El servidor responde ya sea rechazando o aceptado esa petición en una serie de respuestas.
Las respuestas llevan un código de estado que brindan información acerca de si las peticiones fueron resueltas con éxito o si se produjo un error. La petición incial y todas sus respuestas constituyen una transacción.

Los servidores, por defecto, utilizan el puerto 5060 en TCP (Transmission Control Protocol) y UDP (User Datagram Protocol) para recibir las peticiones de los clientes SIP.
Como una de las principales aplicaciones del protocolo SIP es la telefonía, un objetivo de SIP fue aportar un conjunto de las funciones de procesamiento de llamadas y capacidades presentes en la red pública conmutada de telefonía. Así, implementó funciones típicas de dicha red, como son: llamar a un número, provocar que un teléfono suene al ser llamado, escuchar la señal de tono o de ocupado. La implementación y terminología en SIP son diferentes.
SIP también implementa muchas de las más avanzadas características del procesamiento de llamadas de SS7, aunque los dos protocolos son muy diferentes. SS7 es altamente centralizado, caracterizado por una compleja arquitectura central de red y unos terminales tontos (los tradicionales teléfonos de auricular). SIP es un protocolo peer to pee (también llamado p2p). Como tal requiere un núcleo de red sencillo (y altamente escalable) con inteligencia distribuida en los extremos de la red, incluida en los terminales (ya sea mediante hardware o software). Muchas características de SIP son implementadas en los terminales en oposición a las tradicionales características de SS7, que son implementadas en la red.

Aunque existen muchos otros protocolos de señalización para VoIP, SIP se caracteriza porque sus promotores tienen sus raíces en la comunidad IP y no en la industria de las telecomunicaciones. SIP ha sido estandarizado y dirigido principalmente por el IETF mientras que el protocolo de VoIP H.323 ha sido tradicionalmente más asociado con la Unión Internacional de Telecomunicaciones. Sin embargo, las dos organizaciones han promocionado ambos protocolos del mismo modo.

SIP es similar a HTTP y comparte con él algunos de sus principios de diseño: es legible por humanos y sigue una estructura de petición-respuesta. Los promotores de SIP afirman que es más simple que H.323. Sin embargo, aunque originalmente SIP tenía como objetivo la simplicidad, en su estado actual se ha vuelto tan complejo como H.323. SIPcomparte muchos códigos de estado de HTTP, como el familiar '404 no encontrado' (404 not found). SIP y H.323 no se limitan a comunicaciones de voz y pueden mediar en cualquier tipo de sesión comunicativa desde voz hasta vídeo o futuras aplicaciones todavía sin realizar.

2.5. Funcionamiento del protocolo

El protocolo SIP permite el establecimiento de sesiones multimedia entre dos o más usuarios. Para hacerlo se vale del intercambio de mensajes entre las partes que quieren comunicarse.

El Protocolo SIP es de forma nativa "peer to peer": Dos Agentes de usuario pueden establecer una sesión entresí:

Dos canales:

Señalización (UDP 5060)

Streaming RTP (UDP) y control (RTCP Protocolo de control en tiempo real)

Agentes de Usuario

Los usuarios, que pueden ser seres humanos o aplicaciones de software,[4] utilizan para establecer sesiones lo que el protocolo SIP denomina "Agentes de usuario". Estos no son más que los puntos extremos del protocolo, es decir son los que

emiten y consumen los mensajes del protocolo SIP. Un videoteléfono, un teléfono, un cliente de software (softphone) y cualquier otro dispositivo similar es para el protocolo SIP un agente de usuario. El protocolo SIP no se
ocupa de la interfaz de estos dispositivos con el usuario final, sólo se interesa en los mensajes que estos generan y cómo se comportan al recibir determinados mensajes.
Los agentes de usuario se comportan como clientes (UAC: User Agent Clients) y como servidores (UAS: User Agent Servers). Son UAC cuando realizan una petición y son UAS cuando la reciben. Por esto los agentes de usuario deben implementar un UAC y un UAS.
Además de los agentes de usuario existen otras entidades que intervienen en el protocolo, estos son los Servidores de Registro o Registrar, los Proxy y los Redirectores. A continuación se describe su finalidad.

2.6. Formato de los Mensajes

Los mensajes que se intercambian en el protocolo SIP pueden ser peticiones o respuestas.
Las peticiones tienen una línea de petición, una serie de encabezados y un cuerpo.
Las respuestas tienen una línea de respuesta, una serie de encabezados y un cuerpo.
En la línea de petición se indica el propósito de la petición y el destinatario de la petición.
Las peticiones tienen distintas funciones. El propósito de una petición está determinado por lo que sedenomina el Método (Method) de dicha petición, que no es más que un identificador del propósito de la petición. En la [RFC 3261] se definen los métodos básicos del protocolo. Existen otros métodos definidos en extensiones al protocolo SIP.
En la línea de respuesta se indica el código de estado de la respuesta que es un número indica el resultado del procesamiento de la petición.
Los encabezados de peticiones y respuestas se utilizan para diversas funciones del protocolo relacionadas con el encaminamiento de los mensajes, autenticación de los usuarios, entre otras. La extensibilidad del protocolo permite crear nuevos encabezados para los mensajes agregando de esta manera funcionalidad.
El cuerpo de los mensajes es opcional y se utiliza entre otras cosas para transportar las descripciones de las sesiones que se quieren establecer, utilizando la sintaxis del protocolo SDP.

Flujo de establecimiento de una sesión

El flujo habitual del establecimiento de una sesión mediante el protocolo SIP es el siguiente, en este ejemplo todos los servidores actúan como proxy:
Un usuario ingresa la dirección lógica de la persona con la que quiere comunicarse, puede indicar al terminal también las características de las sesión que quiere establecer (voz, voz y video, etc.), o estas pueden estar implícitas por el tipo de terminal del que se trate. El agente de usuario SIP que reside en el terminal, actuando como UAC envía la petición (en este caso con el método INVITE) al servidor que tiene configurado. Este servidor se vale del sistema DNS para determinar la dirección del servidor SIP del dominio del destinatario. El dominio lo conoce pues es parte de la dirección lógica del destinatario. Una vez obtenida la dirección del servidor del dominio destino, encamina hacia allí la petición. El servidor del dominio destino establece que la petición es para un usuario de su dominio y entonces se vale de la información de registración de dicho usuario para establecer su ubicación física. Si la encuentra, entonces encamina la petición hacia dicha dirección. El agente de usuario destino si se encuentra desocupado comenzará a alertar al usuario destino y envía una respuesta hacia el usuario originante con un código de estado que indica esta situación (180 en este caso). La respuesta sigue el camino inverso hacia el originante. Cuando el usuario destino finalmente acepta la invitación, se genera una respuesta con un código de estado (el 200) que indica que la petición fue aceptada. La recepción de la respuesta final es confirmada por el UAC originante mediante una petición con el método ACK (de Acknowledgement), esta petición no genera respuestas y completa la transacción de establecimiento de la sesión.
Normalmente la petición con el método INVITE lleva un cuerpo donde viaja una descripción de la sesión que quiere establecer, esta descripción es realizada con el protocolo SDP.[6] En ella se indica el tipo de contenido a intercambiar (voz, video, etc.) y sus caractarísticas (códecs, direcciones, puertos donde se espera recibirlos, velocidades de transmisión, etc.). Esto se conoce como "oferta de sesión SDP". La respuesta a esta oferta viaja, en este caso, en el cuerpo de la respuesta defnitiva a la petición con el método INVITE. La misma contiene la descripción de la sesión desde el punto de vista del destinatario. Si las descripciones fueran incompatibles,[7] la sesión debe terminarse (mediante una petición con el método BYE).

Al terminar la sesión, lo que puede hacer cualquiera de las partes, el agente de usuario de la parte que terminó la sesión, actuando como UAC, envía hacia la otra una petición con el método BYE. Cuando lo recibe el UAS genera la respuesta con el código de estado correspondiente.
Si bien se describió el caso de una sesión bipartita, el protocolo permite el establecimiento de sesiones multipartitas.
También permite que un usuario esté registrado en diferentes ubicaciones pudiendo realizar la búsqueda en paralelo o secuencial entre todas ellas.

2.7. Funciones Sip

El protocolo Sip actua de forma transparente, permitiendo el mapeo de nombres y la redirección de servicios ofreciendo asi la implementación de la IN (Red Intelignete) de la PSTN. Para conseguir los servicios de la IN el protocolo Sip dispone de distintas funciones. A continuación se enumeran las mas importantes:

- Localizacion del del usuario.
- Disponibilidad del usuario: determinación de la voluntad del receptor de la llamada de participar en las comunicaciones.
- Capacidad del usuario: Determinación del medio y de sus parámetros.
- Gestión de la sesión: transferencia, terminación de sesiones, modificación de los parámetros de la sesión desde el propio *User Agent*.

En definitiva, el protocolo SIP permite la interacción entre dispositivos, cosa que se consigue con distintos tipos de mensajes propios del protocolo que abarca dicha sección. Dichos mensajes proporcionan capacidades para registrar y/o invitar un usuario a una sesión, negociar los parámetros de una sesión, establecer una comunicación entre dos o más dispositivos y, por último, finalizar sesiones.

2.8 Elementos de una Red SIP Práctica

Los terminales físicos, dispositivos con el aspecto y forma de teléfonos tradicionales, pero que usan SIP y RTP para la comunicación, están disponibles comercialmente gracias a muchos fabricantes. Algunos de ellos usan numeración electrónica (ENUM) o DUNDi para traducir los números existentes de teléfono a direcciones SIP usando DNS (Domain Name Server), así llaman a otros usuarios SIP saltándose la red telefónica, con lo que un proveedor de servicio normalmente

actúa de pasarela hacia la red pública conmutada de telefonía para los números de teléfono tradicionales (cobrándo por ello).

Hoy en día, ya son habituales los terminales con soporte SIP por software. Microsoft Windows Messenger usa SIP y en Junio de 2003 Apple Computer anunció y publicó en fase beta su iChat, una nueva versión compatible con el AOL Instant Messenger que soporta charlas de audio y vídeo a través de SIP.

SIP también requiere proxy y elementos de registro para dar un servicio práctico. Aunque dos terminales SIP puedan comunicarse sin intervención de infraestructuras SIP (razón por la que el protocolo se define como punto-a-punto), este enfoque es impracticable para un servicio público. Hay varias implementaciones de softswitch (de Nortell, Sonus, Alcatel-Lucent y muchas más) que pueden actuar como proxy y elementos de registro. Otras empresas, como Ubiquity Software y Dynamicsoft tienen productos cuya implementación está basada en estándares, construidos sobre la especificación Java JAIN.

De los RFCs:

"SIP hace uso de elementos llamados servidores proxy para ayudar a enrutar las peticiones hacia la localización actual del usuario, autenticar y autorizar usuarios para darles servicio, posibilitar la implementación de políticas de enrutamiento de llamadas, y aportar capacidades añadidas al usuario." "SIP también aporta funciones de registro que permiten al usuario informar de su localización actual a los servidores proxy." "Es un concepto importante que la distinción entre los tipos de servidores SIP es lógica y no física."

2.9. Mensajes SIP

Son en texto plano y emplean el formato de mensaje genérico establecido en la RFC 2822, es decir:

- Una línea de inicio
- Campos de cabecera (header)
- Una línea vacía (indica el final de campo de cabeceras)
- Uncuerpo de mensajes opcionales

Linea de inicio
Cabeceras
Linea en blanco
Cuerpo del mensaje

Tabla. II.1. Mensajes SIP

Línea de inicio de un mensaje SIP

Peticiones SIP: tienen una Request-Line (línea de solicitud), cuyo formato es el siguiente:

Método	SP	Request-url	SP	Versión del protocolo	CRLF

Tabla. II.2 Peticiones SIP

Método corresponde a la acción que desea realizar. Se definen 6 métodos:

- REGISTER: petición de registro.
- INVITE: para iniciar una sesión.
- ACK: confirma la recepción de un INVITE.
- CANCEL: cancela una solicitud pendiente.
- BYE: termina una sesión o llamada.
- OPTIONS: consulta sobre las capacidadesy compatibilidades del receptor.

Request-URI corresponde a un SIP o SIPS URI que indica el usuario o servicio al cual va dirigida la petición.

Respuestas SIP: tienen una Status-Line (línea de estado), cuyo formato es el siguiente:

Versión del protocolo	SP	Status Code	SP	Reason-Phrase	CRLF

Tabla. II.3 Respuestas SIP

Status-Code es un entero de 3 dígitosque se genera como el resultado de una petición. El primer dígito define la clase dela respuesta. Se definen los siguientes:

- 1xx: provisional, solicitud recibida.
- 2xx: solicitud aceptada exitosamente.
- 3xx: solicitud fue redireccionada.
- 4xx: solicitud viene errada del cliente.
- 5xx: error del servidor.
- 6xx: fallo general.

Reason-Phrase representa una descripción corta y textual del Status-Code.

Cabeceras de los mensajes SIP

Los campos de cabecera especifican cosas como llamada, emisor dela llamada, la trayectoria del mensaje, tipo y largo del cuerpo del mensaje entre otras características.

* El número total de cabeceras definidas en el protocolo SIP son 46,aunque en la definición inicial de SIP eran solo 37.

* Los distintos tipos de cabeceras SIP se pueden dividir en cuatro tipos:

- Cabeceras generales: aplicadas tanto a los mensajes de peticiones como alos de respuesta.
- cabeceras de entidad: definen información sobre el cuerpo del mensaje. Sielcuerpo no está presente, sobre los recursos identificados por la petición.
- cabeceras de solicitud: actúan como modificadores de solicitud. Permitenque el cliente pase información adicional sobre la solicitud o sobre símismo.
- cabeceras de respuesta: permiten al servidor agregar información adicional sobre la respuesta cuando no hay lugar en la línea de inicio (Status-Line).

Cabeceras de los mensajes SIP

En la tabla se muestran los cuatros grupos de cabeceras y los campos que las componen.

Cabeceras Generales	Cabeceras de Entidad	Cabeceras de Solicitud	Cabeceras de Respuesta
Call-ID	Allow	Accept	Proxy-Authenticate
Contact	Content-Encoding	Accept-Encoding	Server
CSeq	Content-Length	Accept-Languaje	Unsupported
Date	Content-Type	Accept-Contact	Warning
Encryption	Content-Disposition	Authorization	WWW-Athenticate
From	Expires	Hide	RSeq
Organization	MIME-Version	In-Reply-To	
Retry-After		Max-Forwards	
Subject		Priority	
Timestamp		Proxy-Authorization	
To		Proxy-Require	
User Agent		Record-Route	
Via		Reject-Contact	
		Request-Disposition	
		Require	
		Response-Key	
		Route	

Tabla. II.4 Cabeceras de Mensajes SIP

Para un servicio detelefonía IP básica, los elementos de la red debeser capaces de generarlas cabeceras:

- Call-ID
- Cseq
- From
- To
- Via
- Content-Length
- Content-Type
- Expires
- Require
- Max-Forwards

Ejemplo de paquetes SIP

Ejemplo de un paquete de petición SIP.

REGISTER sip:192.168.28.124:5060 SIP/2.0	Línea de Inicio
From: <sip:201@192.168.28.210> To: <sip:201@192.168.28.124> Call-ID: d0b54a5788484465af65835507b2e47f@192.168.28.210 CSeq: 1 REGISTER Via: SIP/2.0/UDP 192.168.28.210:1855 Max-Forwards: 2 Contact: <sip:201@192.168.28.210:1855;transport=udp> Content-Length: 0	Cabeceras
	Línea en Blanco
	Cuerpo del mensaje

Tabla. II.5 Ejemplo de un Paquete de Peticion SIP

Ejemplo de un paquete de respuesta SIP.

SIP/2.0 200 OK	Línea de Inicio
From: <sip:201@192.168.28.124> To: <sip:201@192.168.28.210> Call-ID: d0b54a5788484465af65835507b2e47f@192.168.28.210 CSeq: 1 REGISTER Via: SIP/2.0/UDP 192.168.28.210:1855 User-Agent: Asterisk PBX Allow: INVITE,ACK,CANCEL,OPTIONS,BYE,REFER,SUBSCRIBE,NOTIFY Max-Forwards: 70 Expires: 120 Contact: <sip:201@192.168.28.210:1855;transport=udp>;expires=120 Date: Wed, 18 Oct 2006 20:24:17 GMT Content-Length: 0	Cabeceras
	Línea en Blanco
	Cuerpo del mensaje

Tabla. II.6 Ejemplo de un Paquete de Respuesta SIP

Cuerpo del mensaje SIP

El cuerpo es opcional, sin embargo muchas veces esutilizado para describir lassesiones multimedias.

- Se utiliza el protocolo SDP (Session DescriptionProtocol) para describir sesionesen tiempo real, cuyo propósito principal es conducir información acerca de losmedia streams en las sesiones multimedias.
- Al igual que los mensajes SIP, corresponden a campos de texto que se incluyen a los demás protocolos, loscuales con abreviados en una sola letra.

2.10 Ventajas del Protocolo Sip

A continuación se presentan las principales ventajas del protocolo SIP.

- Simplicidad: Basado en texto para una implementación y depuración simples, utilización de primitivas (métodos y respuestas al estilo HTTP) para establecimiento de sesiones.
- Simplicidad de las 'URIs' de usuario, basadas en DNS.
- Escalabilidad y flexibilidad, funcionalidades proxy, redirección, localización/registro pueden residir en un único servidor o en varios distribuidos.
- No es necesario un control centralizado, el funcionamiento "peer to peer" es totalmente posible.

2.11. Desventajas del Protocolo Sip

A continuación se presentan las principales desventajas del protocolo SIP.

- Problemas de Red: La utilización de un canal "peer to peer" para la transmisión de la voz plantea numerosos problemas a nivel de red con nat routers, firewalls, etc.

Operabilidad con PSTN: H.323 ofrece mayores ventajas.

2.12. Beneficios del protocolo Sip frente a otros protocolos

En la actualidad, los protocolos más usados en ToIP son tres: SIP, H.323 y IAX2.

H.323 es un estándar de la ITU que provee especificaciones para ordenadores, sistemas y servicios multimedia por redes que no proveen QoS (calidad de servicio). Como principales características de H.323 tenemos:

- Implementa QoS de forma interna.
- Control de conferencias

IAX2 (Inter Asterisk eXchange) es un protocolo creado y estandarizado por Asterisk. Unas de sus principales características son: *Media* y *señalización* viajan en el mismo flujo de datos.

- *Trunking*
- *Cifrado de datos*

Una de las ventajas de este protocolo es que al enviar el "streaming" y la señalización por el mismo flujo de datos, se evitan problemas derivados del NAT. Así pues, no es necesario abrir rangos de puertos para el tráfico RTP. Por último, IAX2 nos permite hacer *trunking* de forma que podemos enviar varias conversaciones por el mismo flujo, lo cual supone un importante ahorro de ancho de banda.

Finalmente, veamos qué hace de **SIP** un protocolo cada día más sólido. Aspectos importantes referentes a dicho protocolo se enumeran como sigue:

- El control de llamadas es *stateless* o sin estado, y proporciona escalabilidad entre los dispositivos telefónicos y los servidores.
- SIP necesita menos ciclos de CPU para generar mensajes de señalización de forma que un servidor podrá manejar más transacciones.
- Una llamada SIP es independiente de la existencia de una conexión en la capa de transporte.
- SIP soporta autentificación de llamante y llamado mediante mecanismos HTTP.
- Autenticación, criptográfica y encriptación son soportados salto a salto por SSL/TSL pero SIP puede usar cualquier capa de transporte o cualquier mecanismo de seguridad de HTTP, como SSH o S-HTTP.
- Un proxy SIP puede controlar la señalización de la llamada y puede bifurcar a cualquier número de dispositivos simultáneamente.

En definitiva, vemos que SIP es un protocolo con una gran escalabilidad, modular y muy apto para convertirse en el futuro inmediato de la ToIP.

CAPÍTULO III
PROBLEMAS EN REDES VOIP, ATAQUES AMENAZAS Y RIESGOS

3. 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 esoen 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 deseguridad que afectan al mundo de las redes de datos. Por supuesto, existen también multitud de ataques específicos de VoIP como veremos más adelante.

Fig.III.1. Seguridad de las Redes Voip

Como vemos la seguridad de VoIP se construye sobre muchas otras capas tradicionales deseguridad de la información.

En la siguiente Tabla.III.1 se detallan algunos de los puntos débiles y ataques que afectan a cada una de las capas. Aunque posteriormente se analizaran muchos de ellos en profundidad algunos ataques que pueden afectar directamente o

indirectamente a la telefonía VoIP no serán explicados al ser problemas comunes a cualquier otra red de datos o al alejarse demasiado de la temática del documento.

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. Ej: Acceso físico al un gatekeeper. Reinicio de máquinas. Denegaciones de servicio.
Seguridad de Red	DDoS ICMP unreacheable SYN floods Gran variedad de 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. III.1. Ataques y Vulnerabilidades

Se pude apreciar algunos de estos ataques tendrán como objetivo el robo de información confidencial y algunos otros degradar la calidad de servicio o anularla por completo (DoS).

Para el atacante puede ser interesante no solo el contenido de una conversación (que puede llegar a ser altamente confidencial) sino también la información y los datos de la propia llamada, que utilizados de forma maliciosa permitirán al atacante realizar registros de las llamadas entrantes o salientes, configurar y redirigir llamadas, grabar datos, utilizar información para bombardear con SPAM, interceptar y secuestrar llamadas, reproducir conversaciones, llevar a cabo robo de identidad e incluso realizar llamadas gratuitas a casicualquier lugar del mundo. Los dispositivos de la red, los servidores, sus sistemas operativos, los protocolos con los que

trabajan y prácticamente todo elemento que integrela infraestructura VoIP podrá ser susceptible de sufrir un ataque.

3.1 Clasificación de los Ataques

Durante los siguientes apartados se va a intentar detallar cuáles son las amenazas mássignificativas que afectan a la telefonía sobre redes IP. Como ya se ha comentado lamayoría los riesgos son inherentes de las capas sobre las que se apoya la tecnología VoIP por lo que muchos de los ataques se basarán en técnicas bien conocidas. Se mostraran, también, ciertas vulnerabilidades que afecta específicamente a las redes VoIP y a susprotocolos.
Las amenazas de las redes de telefonía IP las podemos clasificar en las siguientes categorías:

- Accesos desautorizados y fraudes.
- Ataques de denegación de servicio
- Ataques a los dispositivos
- Vulnerabilidades de la red subyacente.
- Enumeración y descubrimiento.
- Ataques a nivel de aplicación.

3.1.1 Accesos desautorizados y Fraudes

Los sistemas VoIP incluyen múltiples sistemas para el control de la llamada, administración, facturación y otras funciones telefónicas. Cada unos de estos sistemas debe contener datos que, si son comprometidos, pueden ser utilizados para realizar fraudes. El costo de usar fraudulentamente esos datos VoIP a nivel empresarial pueden ser devastadores. El acceso a los datos telefónicos (de facturación, registros, datos de cuentas, etc) pueden ser usados con fines fraudulentos.
Una de las más importantes amenazas de las redes VoIP, son los fraudes consecuencia de un acceso desautorizado a una red legal VoIP (por ejemplo haber obtenido anteriormente obtener datos de cuentas). Una vez se ha obtenido el acceso, usuario desautorizados realizan llamadas de larga distancia, en muchos casos incluso internacionales.
Principalmente ocurren en entornos empresariales. El control y el registro estricto de las llamadas puede paliar el problema A modo de curiosidad cabe señalar que

las técnicas utilizadas por estos individuos son descendientes de las que utilizaban los famosos "*phreakers*" en las antiguas líneas telefónicas

3.1.2 Explotando la red subyacente

Paradójicamente una de las principales debilidades de la tecnología VoIP es apoyarse sobreuna red potencialmente insegura como son las redes IP. Gran cantidad de ataques hacia lasinfraestructuras IP van a afectar irremediablemente a la telefonía Ataques de denegación de servicio, inundación de paquetes o cualquier otro tipo de ataque que intente limitar ladisponibilidad de la red suponen un gran problema para la telefonía IP tal y como hemosvisto anteriormente. Además VoIP será vulnerable a ataques a bajo nivel como el secuestrode sesiones, interceptación, fragmentación IP, paquetes IP malformados y spoofing.

Uno de los mayores problemas sea quizás la interceptación o **eavesdropping**, Traducido literalmente como "escuchar secretamente", es el término con el que se conoce a la capturade información (cifrada o no) por parte de un intruso al que no iba dirigida dicha información. En términos de telefonía IP, estamos hablando de la interceptación de lasconversaciones VoIP por parte de individuos que no participan en la conversación.

El **eavesdropping** en VoIP presenta pequeñas diferencias frente la interceptación de datosen las redes tradicionales. En VoIP vamos a diferenciar básicamente dos partes dentro de lacomunicación: **la señalización y el flujo de datos**. Los cuales utilizarán protocolosdiferentes. En la señalización nos centraremos durante todo el documento en el protocoloSIP mientras que en el flujo de datos normalmente se utilizará el protocolo RTP sobreUDP.

El impacto de esta técnica es más que evidente, interceptando comunicaciones es posible obtener toda clase información sensible y altamente confidencial. Y aunque en principio se trata de un técnica puramente pasiva, razón por la cual hace difícil su detección, es posible intervenir también de forma activa en la comunicación insertando nuevos datos (que en elcaso de VoIP se trataría de audio) redireccionar o impedir que los datos lleguen a sudestino.

Las formas de conseguir interceptar una comunicación pueden llegar a ser tan triviales como esnifar el tráfico de la red si los datos no van cifrados. Existen excelentes snifferscomo **ethereal/wireshark** que permitirán capturar todo el tráfico de tu segmento de lared. Por el contrario, lo normal es que nos encontramos dentro de redes conmutadas por loque para esnifar el tráfico que no vaya dirigido a nuestro equipo serán necesarias otrastécnicas más elaboradas como realizar un

"**Main in the Midle**" utilizando **Envenenamiento ARP**. Entre las herramientas que podremos utilizar se encuentra elconocido programa **ettercap, Cain & Abel,** la suite de herramientas para Linux **Dsniff** y**vomit** (Voice over misconfigured Internet telephones) por citar algunos ejemplos.
Hay que señalar también la creciente utilización de **redes inalámbricas** supone en muchos casos un vía más a explotar por parte del intruso. Redes Wifi mal configuradas junto con una infraestructura de red insegura puede facilitar el trabajo del intruso a la horade acceder a la red VoIP para lanzar sus ataques

3.1.3 Ataques de denegación de servicio

Los ataques de denegación de servicio son intentos malintencionados de degradarseriamente el rendimiento de la red o un sistema incluso llegando al punto de impedir lautilización del mismo por parte de usuarios legítimos. Algunas técnicas se basan en el envío de paquetes especialmente construidos para explotar alguna vulnerabilidad en elsoftware o en el hardware del sistema, saturación de los flujos de datos y de la red o sobrecarga de procesos en los dispositivos.
Llegan a ser especialmente dañinos los llamados DDoS o ataques de denegacióndistribuidos. Son ataques DoS simples pero realizados desde múltiples computadores de forma coordinada. Las redes y sistemas VoIP son especialmente vulnerables a los DDoSpor diversas razones:
La primera y quizás más importante es la dependencia y la necesidad de garantías enla calidad de servicio, que hacen que las redes IP donde se mantengan llamadas telefónicas tengan una tolerancia mucho menor a problemas de rendimiento.
Otra razón es que en una red VoIP existen multitud de dispositivos con funciones muy específicos por lo que ataques contra casi cualquier dispositivo de la red pueden afectar seriamente los servicios de telefonía IP. Muchos de estos dispositivos son muy susceptibles de no manejar, priorizar o enrrutar el tráfico de forma fiable si presentan unconsumo de CPU alto. Por lo que muchos de los ataques de DoS se centran en atacar los dispositivos de red y/o inundar la red de tráfico inútil para degradar su funcionamiento yque los paquetes pertenecientes a comunicaciones telefónicas se pierdan o retrasen.
La relación de VoIP y los ataques distribuidos de DoS viene reflejada en el siguiente párrafo:
Las aplicaciones y los dispositivos de telefonía IP suelen trabajan sobre ciertos puertosespecíficos, bombardear dichos puertos con tráfico innecesario pero aparentemente "real" puede causar una denegación de servicio y que usuarios

legítimos no puedan hacer uso delsistema. Modificaciones y ataques al servidor DNS pueden afectar de manera directa alservicio de voz. El robo o suplantación de identidad (del destinatario de la llamada o dealgún otro dispositivo VoIP) generalmente deriva en una denegación de servicio. El acceso SNMP a los dispositivos, además de ofrecer una gran cantidad de información permite potencialmente al atacante afectar al servicio de Voz sobre IP. En redes VoIP basadas en elprotocolo SIP, es posible enviar mensajes CANCEL, GOODBYE o ICMP PortUnreacheable, con el objetivo de desconectar ciertos usuarios de sus respectivas llamadas oevitar que se produzcan no permitiendo la correcta configuración inicial de la llamada (señalización).
Hay que destacar también que algunas situaciones VoIP será vulnerable a ataques de fragmentación IP o envío de resets TCP, que conllevarán la prematura finalización de la llamada.

3.1.4 Ataques a los dispositivos

Muchos de los ataques realizador hoy en día por hackers y crackers hacia las redes de datos tienen como objetivo principal el hardware y el software de los dispositivos. Por lo tanto, en redes VoIP, los gateways, call managers, Proxy servers sin olvidar los teléfonos IP serán potencialmente objetivos a explotar por parte de un intruso.
Hay que tener en cuenta que los dispositivos VoIP son tan vulnerables como lo es el sistema operativo o el firmware que ejecutan. Son muy frecuentes los ataques de *fuzzing* conpaquetes malformados que provocan cuelgues o reboots en los dispositivos cuando procesan dicho paquete. Otros ataques de denegación de servicio llamados "*flooders*" tienencomo objetivo los servicios y puertos abiertos de los dispositivos VoIP.
Otro aspecto que hace muchas veces de los dispositivos un punto débil dentro de la red son configuraciones incorrectas. A menudo los dispositivos VoIP trabajan con sus configuraciones por defecto y presentan gran variedad de puertos abiertos. Los serviciospor defecto corren en dichos puertos y pueden ser vulnerables a ataques de DoS, desbordamientos de buffer o cualquier otro ataque que pueden resultar en el compromiso del dispositivo VoIP.
El intruso a la hora de penetrar en la red tendrá en cuenta estos aspectos e intentará explotarlos. Buscará puertos por defecto y servicios innecesarios, comprobará passwords comunes o los que usa por defecto el dispositivo, etc. En el

apartado de Descubrimiento de objetivos se explicaran más detalladamente las técnicas utilizadas en este aspecto.

3.2. Descubriendo Objetivos

Una vez que el hacker ha seleccionado una red como su próximo objetivo, sus primeros pasos consistirán en obtener la mayor información posible de su victima. Cuando el intrusotenga información suficiente evaluará sus siguientes pasos eligiendo el método de ataque más adecuado para alcanzar su objetivo. Normalmente el método de obtención de información se realiza con técnicas de menos a más nivel de intrusión. De este modo en las primeras etapas el atacante realizará un **footprinting** u obtención de toda la información pública posible del objetivo. Más adelante una de las acciones más comunes consiste enobtener la mayor información posible de las máquinas y servicios conectados en la redatacada. Después de tener un listado de servicios y direcciones IP consistente, tratará debuscar agujeros de seguridad, vulnerabilidades y obtener la mayor información sensible deesos servicios (enumeración) para poder explotarlos y conseguir una vía de entrada.
Un ejemplo de ataque de enumeración, podría ser utilizar la fuerza bruta contra servidoresVoIP para obtener una lista de extensiones telefónicas válidas. Información que seria extremadamente útil para lanzar otros ataques como inundaciones INVITE o secuestro deregistro.
Durante este apartado se explicaran algunas técnicas de enumeración y descubrimiento deobjetos así como la obtención de información sensible que atacante podría utilizar a sufavor.

3.2.1. Footprinting.

Se conoce como footprinting el proceso de acumulación de información de un entorno dered especifico, usualmente con el propósito de buscar formas de introducirse en el entorno.
La herramienta básica para esta etapa del reconocimiento será el todo poderoso Google. Lasbúsquedas se centrarán entorno a la web de la empresa y en su dominio. Se intentarán encontrar perfiles o direcciones de contacto, correos y teléfonos. Estos datos ofreceráninformación al hacker para poder realizar ataques de suplantación de identidad y/oingeniería social. El contacto del servicio técnico también puede resultar útil para extraer algún tipo de información. Otro tipo de

información interesante pueden ser las ofertas detrabajo o los perfiles de personal que busca la empresa. Pueden dar información acerca dela estructura de la organización y de la tecnología que emplea

3.2.2. Escaneando

A partir de la dirección de red de la víctima, se pretende obtener un listado de direccionesIP y servicios activos en la red. La mejor forma es escaneando la red con las herramientasadecuadas. Quizás el mejor escáner de puertos existente hoy por hoy sea **NMAP**(http://insecure.org/namp) que ofrece muchas más posibilidades que un simple escáner depuertos.
Entre todas las funcionalidades de nmap existe una que destacaremos especialmente. Y esla identificación del sistema operativo de la máquina escaneada a partir de información queobtiene nmap, como los puertos abiertos que presenta, tipos de servicios, y huellasidentificativas de la pila TCP/IP.
En el caso concreto que nos ocupa, nmap tiene la mejor base de datos de huellas paraidentificar dispositivos VoIP.

3.2.3. Enumeración

La enumeración es una técnica que tiene por objetivo obtener información sensible que elintruso podría utilizar para basar sus ataques posteriores.
La primera información a obtener es el tipo de servicio que está corriendo en un determinado puerto, esta identificación ya la realiza correctamente herramientas como **nmap**, pero se podrían hacer manualmente conectado al puerto .En el siguiente ejemploconectamos a un servidor SIP utilizando la herramienta **netcat** bien conocida como lanavaja suiza:

Al conectar al puerto especificado manualmente se envía una petición OPTIONS genérica al servidor, para poder estudiar su respuesta. En ella podemos observar que nos muestra información clara sobre el tipo de dispositivo que se trata.
Algunas otras herramientas a automatizan este proceso son:

- **Smap:** Permite identificar dispositivos SIP.
- **Sivus:** Un escáner de vulnerabilidades para SIP. Permite entre otra cosa generarpeticiones SIP.
- **Nessus:** Uno de los mejores escáneres de vulnerabilidades. Permite

además identificar los servicios y sistemas.

- **VoIPAudit:** Otro escáner VoIP y de vulnerabilidades.

Para poder realizar la mayoría de ataques, el intruso deberá conocer nombres de usuario y extensiones telefónicas correctas. Existen diversos métodos para recabar ese tipo deinformación:

Una de las técnicas es utilizando las operaciones de registros de usuario. Cuando un usuario pretende registrarse envía una petición REGISTER al servidor de registro y este le responde con un **200 OK** si todo va bien o con un mensaje 4xx si ha habido algún error,el usuario no existe o no tiene los credenciales de autenticación adecuados. Dependiendo del software las respuesta del servidor de registro contra una petición de REGISTER de un usuario existe y no existente puede ser diferente en el sentido de que, si un usuario existepuede que conteste con un mensaje 401 ya que le falte autenticarse pero si el usuario noexiste responderá directamente con un mensaje **403 Forbidden**. Esta diferencia en larespuesta puede ser utilizada para enumerar y obtener un listado de usuarios válidos de lared VoIP.

Un método similar al anterior consiste en utilizar mensajes INVITE para enumerarposibles usuarios de la red. Algunos servidores responderán con un mensaje 401 cuando seintenta llamar a un usuario inexistente. El gran problema de este método es que cuando se acierte y se encuentre un usuario correcto, se estará realizando una llamada y el teléfono delusuario en cuestión sonará y quedará registrada la llamada.

Quizás el método más silencioso para enumerar usuarios es el que utiliza peticiones OPTION. Las peticiones OPTION se utilizan para determinar por ejemplo que codecs soporta un determinado UA. El servidor contestará con un **200 OK** si el usuario existe y un **404 Not Found** si no reconoce el usuario.

Algunas de las herramientas que automatizan todo este proceso, utilizando diccionarios o fuerza bruta con mensajes REGISTER, INVITE o OPTION son: Sipsaky Sipscan.

Dentro de la plataforma VoIP coexisten gran cantidad de servicios que se podrían aprovechar para obtener información. Algunos de ellos son el DHCP y DNS pero se estudiarán algunas técnicas contra el servicio TFTP y el protocolo SNMP.

La mayoría de dispositivos telefónicos utilizan el protocolo TFTP para manejar sus ficheros de configuración. Normalmente cada vez que un dispositivo VoIP se conecta intenta obtener su configuración del servidor TFTP. El problema es que el servicio TFTP es un servicio altamente inseguro problema que se agrava con el hecho de que en laconfiguración de los dispositivos se podrá encontrar todo tipo de

información valiosa: extensiones, usuarios, passwords, estructura de la red, servidores, etc. Por lo que losservidores TFTP de configuración se convierten en un objetivo claro para comprometer lared VoIP.

La premisa en TFTP es que si se puede averiguar el nombre del fichero de configuración,lo puedes descargar. Muchos dispositivos utilizan nombre por defecto públicamente conocidos, por lo tanto si se identifica el dispositivo puede resultar trivial obtener su configuración del servidor TFTP. Por ejemplo, los dispositivos CISCO el nombre delarchivo de configuración mantienen relación con su dirección MAC.

Evidentemente el primer paso debería ser localizar el servidor TFTP en la red. Podemos utilizar un escáner como nmap buscando direcciones con el puerto 69 UDP abierto.

Una vez localizado el servidor TFTP, el intruso intentará descargare los ficheros de configuración y como ya ha quedado demostrado la única dificultad que se le presenta esadivinar el nombre de los ficheros. Existen herramientas como tftpbrute (que utilizan listados de palabras y diccionarios para atacar el servidor TFTP y descargarse ficheros de configuración. También es posible realizar todo el trabajo manualmente, ya que existen diversas listas que relacionan modelo/fabricante con el nombre por defecto de su archivo de configuración.

El protocolo SNM P(Simple Network Management Protocol) que se presenta activo enmuchos de los dispositivos VoIP, es otro de los protocolos vulnerables de los que se puedeobtener gran cantidad de información.

Los pasos serían los siguientes:

1) Buscar dispositivos con soporte SNMP. Usualmente tendrán el puerto 162 UDP.
Se pueden utilizar herramientas como NMAP o Solar Windos SNMP Sweep.

2) Si no se conoce el OID del dispositivo utilizar la Solar Wind MIB para encontrarlo.

3) Con la herramienta snmpwalk y el OID del dispositivo es posible listar la mayoría de aspectos de su configuración.

3.3. Explotando el nivel de Aplicación

El nivel de aplicación de la red IP es quizás uno de los más vulnerables, debido en parte aque VoIP engloba gran cantidad de protocolos y estándares añadiendo cada uno ellos su propio riesgo de segundad. Un ejemplo claro de ellos es el protocolo SIP, muy discutido desde el punto de vista de la seguridad. Entre los ataques específicos contra el nivel deaplicación de VoIP encontramos ataques de secuestro de sesión, desconexiones ilegales, inundación de peticiones, generación de

paquetes malformados, falsificación de llamadas y algunos otros que se explicaran a continuación utilizando el protocolo SIP como base.

3.3.1. Autenticación en VoIP

En toda comunicación, servicio o transmisión de dato existe la necesidad de demostrar que los clientes son quien dicen ser. En VoIP la autenticación requiere que los dosdispositivos que se van a comunicar se autentiquen uno al otro antes de que se produzca cualquier intercambio de información. Esta autenticación mutua está basada en algún tipode secreto compartido que es conocido a priori por los dos.

3.3.1.1. Autenticación del protocolo SIP

El protocolo SIP utiliza la autenticación digest para comprobar la identidad de sus clientes.
La autenticación digest fue originalmente diseñada para el protocolo HTTP, y se trata deun mecanismo bastante simple, basado en hashes que evita que se envíe la contraseña delos usuarios en texto claro.
Cuando el servidor quiere autenticar un usuario genera un desafío digest que envía al usuario.

3.3.1.2. Crackeo de contraseñas SIP

Una vez entendido el proceso de autenticación se van a mostrar los métodos y las herramientas para romper esa autenticación y crackear los hashes digest con el fin deobtener el password de un usuario y poder utilizar la identidad de la víctima de forma maliciosa.
Entre las herramientas encontramos SIPCrack, que como su nombre indica, crackea las contraseñas del protocolo SIP en Linux. Contiene dos programas sipdump para esnifar los hashes de la autenticación y sipcrack para crackear los logins capturados.
En caso de encontrarnos una vez más en redes conmutadas puede que sea necesario el uso de herramientas como ettercap para realizar la técnica de man in the middle y poder esnifar el tráfico necesario.
Como es normal, el éxito de este ataque dependerá de lo bueno y preciso que sea el diccionario que utilicemos.

Otra herramienta que sin duda merece la pena comentar para el crackeo de contraseñas es Cain. Una vez más permite realizar todo el proceso de captura de tráfico, envenenamiento ARP, decodificación de protocolos y crackeo de hash por diccionario y fuerza bruta.

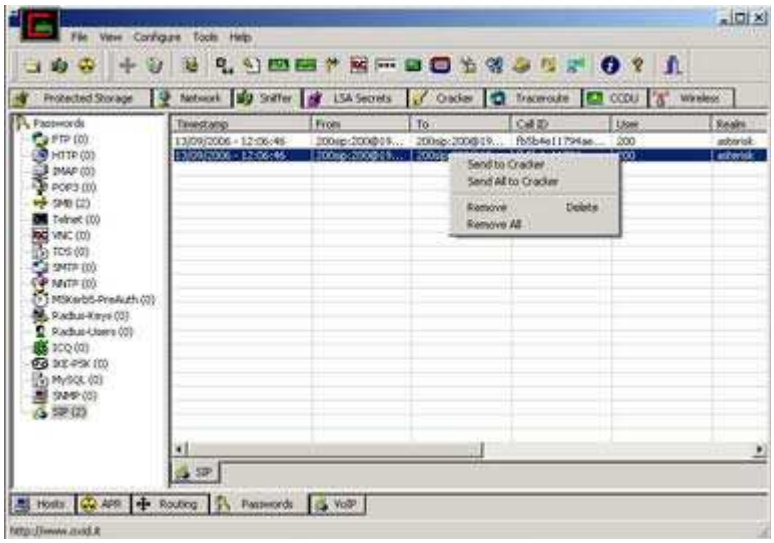


Fig.III.3. Caín y Abel, herramienta de crackeo de contraseñas

3.3.2. Manipulación de la Señalización

A continuación se detallan algunos de los ataques que se pueden conseguir capturando y manipulando los mensajes de señalización previos al establecimiento de la llamada.

3.3.2.1 Suplantación de identidad en el registro

El registro de usuarios es la primera comunicación que se estable en el entorno VoIP entreel usuario y el servidor de registro. Necesariamente esta comunicación debe de realizarse de forma segura, ya que en caso contrario no hay garantías de que el usuario registrado sea quien dice ser durante todo el resto de la sesión. A través de los mensajes REGISTER, los agentes de usuario SIP informan al servidor de su localización actual de manera que el servidor sepa dónde tiene que enviar peticiones posteriores. Si un servidor no autentica las peticiones REQUEST cualquiera puede registrar cualquier contacto para cualquier usuario, y por lo tanto secuestrar su identidad y sus llamadas.

Cuando un Proxy recibe la petición para procesar la llamada (INVITE), el servidor realiza una búsqueda para identificar donde puede ser encontrado el destinatario .

En la figura podemos observar un mensaje de respuestas del servidor de registro a una petición de búsqueda de un Proxy Server.

El mensaje REGISTER contiene el campo en la cabecera **Contact***:* que indica la dirección IP del hardware o software VoIP del usuario destino

Para generar la petición se ha utilizado la herramienta SiVus:

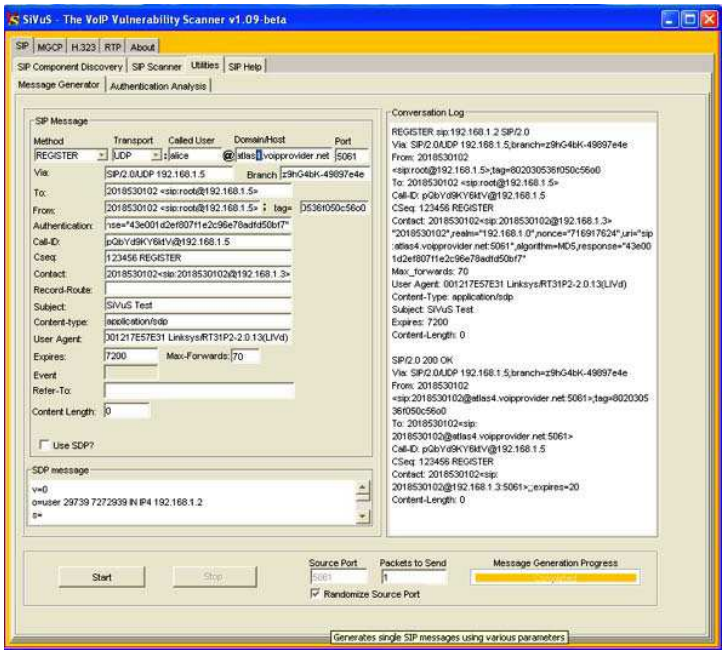


Fig.III.4. Sivus escanner de vulnerabilidades

El ataque funciona de la siguiente manera:

1. Deshabilitando el registro legítimo del usuario.

2. Enviando el mensaje REGISTER con la IP del atacante.

3. En el servidor de registro queda registrado con la dirección IP del hacker.

4. Cuando recibe la llamada, el servidor Proxy consulta la dirección del destinatario, pero obtendrá la dirección IP del atacante.

5. El ataque ha tendido éxito. El intruso ha suplantado la identidad y mientras mantenga el registro todas las llamadas llegara a su teléfono IP.

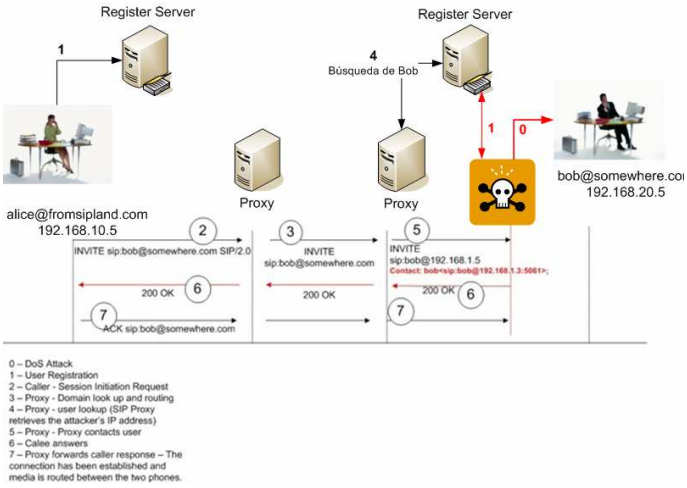


Fig.III.5. Ataque envió de mensaje register

Este ataque es posible llevarlo a cabo por el hecho de que lo mensajes de señalización se envían en texto plano, lo que permite al intruso capturarlos, modificarlo y retransmitirlo como él quiera.

Es posible que el servidor requiera autenticación, aspecto que no plantea ninguna problema si previamente el intruso a esnifado y crackeado la contraseña del usuario tal y como se explicaba en el apartado de Autenticación SIP.

A partir de la técnica de secuestro de registro se puede realizar alguna variante del ataque.

En el caso anterior evitábamos que el destinatario legítimo recibiera la llamada, pero en algunos casos se puede conseguir realizar un ataque de Main in the middle a nivel de red.

De esta forma el destinatario legítimo recibirá la llamada y el atacante actuara a modo de servidor Proxy. Se trataría entonces de un ejemplo claro de eavesdroping.

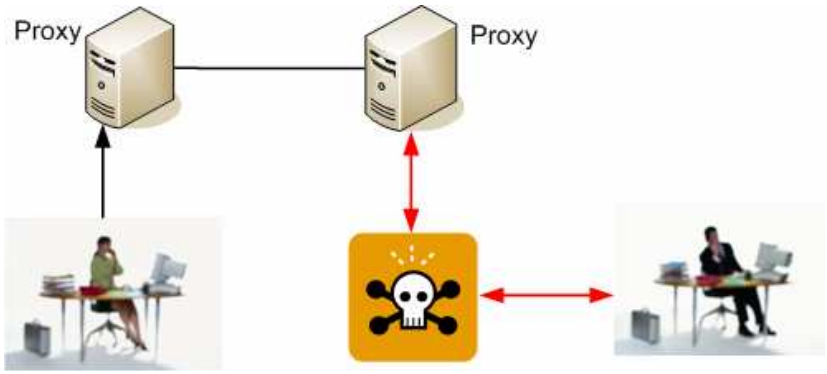


Fig.III.7. Ejemplo de eavesdroping

Además de la potente herramienta SiVus existen un conjunto de tres herramientas para manipular los aspectos del registro de usuarios en SIP:

3.3.2.2. Desregistrar Usuarios

El desregistro de usuarios legítimos es una necesidad para conseguir suplantar su identidad como hemos visto en el ejemplo anterior. Básicamente el intruso podrá conseguirlo de las siguientes formas:

- Realizando un ataque de DoS al usuario.
- Generando una condición de carrera en la que el atacante envía repetidamente peticiones REGISTER en un corto espacio de tiempo con el objetivo de superponerse a la petición de registro legítima del usuario.
- Desregistrando el usuario con mensajes REGISTER.

El intruso puede ser capaz de desregistrar fácilmente un usuario, enviando al servidor de registro una petición REGISTER (simulando ser la victima) con el siguiente campo "Contact: *" y valor del atributo "Expires" a cero. Esta petición eliminará cualquier otro registro de la dirección del usuario (especificada en el campo "To" de la cabecera).

El atacante deberá realizar este envío periódicamente para evitar el re-registro del usuario legítimo o en su defecto provocarle una ataque DoS para evitar que vuelva a registrarse al menos por el tiempo que necesite para realizar el secuestro de la llamada.

3.3.2.3 Desconexión de Usuarios

El hecho de que muchos de los protocolos se utilizan sin encriptación alguna y de que los mensajes no se autentican de forma adecuada, es trivial para un intruso desconectar a los usuarios de sus llamadas enviando mensajes BYE con la identidad falsificada simulando ser el usuario del otro lado de la línea.

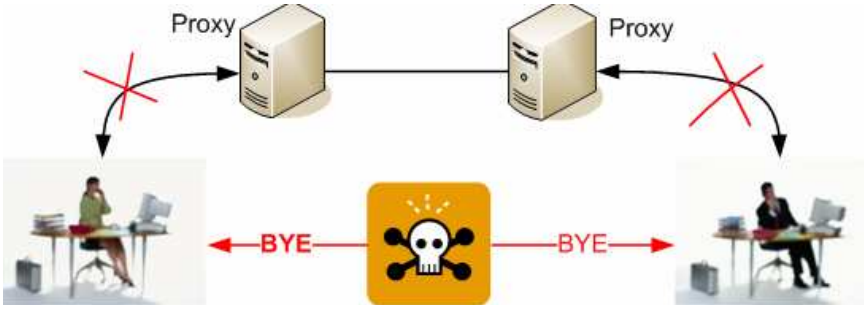


Fig.III.8. Ejemplo desconexión de usuario

Se puede realizar un ataque similar utilizando mensajes CANCEL, pero solo afectan cuando se está estableciendo la llamada, es decir, antes de que el destinatario descuelgue el teléfono.

3.3.2.4 Redirección de llamadas

La redirección de llamadas suele ser otro de los ataques comunes en las redes VoIP.

Existen diferentes métodos que van desde comprometer los servidores o el call manager de la red para que redirijan las llamadas donde el intruso quiera, hasta las técnicas ya mostradas de suplantación de identidad en el registro, man in the middle, etc.

Otra posibilidad es utilizar una herramienta como RedirectPoison que escucha la señalización SIP hasta encontrar una petición INVITE y responder rápidamente con un mensaje SIP de redirección, causando que el sistema envié un nuevo INVITE a la localización especificado por el atacante.

Otro modo de redirección el flujo de datos se consigue con las herramientas: sipredirectrtp y rtpproxy. Se basan en utilizar mensajes la cabecera SDP para cambiar la ruta de los paquete RTP y dirigirlas a un rtproxy que a su vez serán reenviados donde el intruso quiera.

3.3.3. Manipulación de la transmisión

3.3.3.1. Eavesdropping.

La técnica de la interceptación de la comunicación o eavesdropping ya ha sido explicada por lo que en este caso veremos un ejemplo práctico de cómo capturar la señalización y el flujo de una llamada para después poder reproducir el contenido

de la misma.

Lo pasos para capturar y decodificar los paquetes de voz interceptados son realmente sencillos. En el primer ejemplo utilizaremos un sniffer como ethereal.

• Capturar y decodificar los paquetes RTP. Esnifar el tráfico de la comunicación con el ethereal, este sniffer permite además interpretar los paquetes UDP indicándole que son del protocolo RTP.

• Seleccionar la opción "Analizar Sesión". Permite seleccionar un flujo de datos y analizarlo ya no como paquetes individuales sino común flujo continuo de datos.

• Salvar a un fichero de audio, para reproducirlo posteriormente. Ethereal permite analizar los datos RTP y salvarlos como un fichero de audio.

Se puede automatizar aún más el proceso si se utiliza la fabulosa herramienta Cain. Que además de ser un buen sniffer puede realizar infinidad de funciones y ataques.

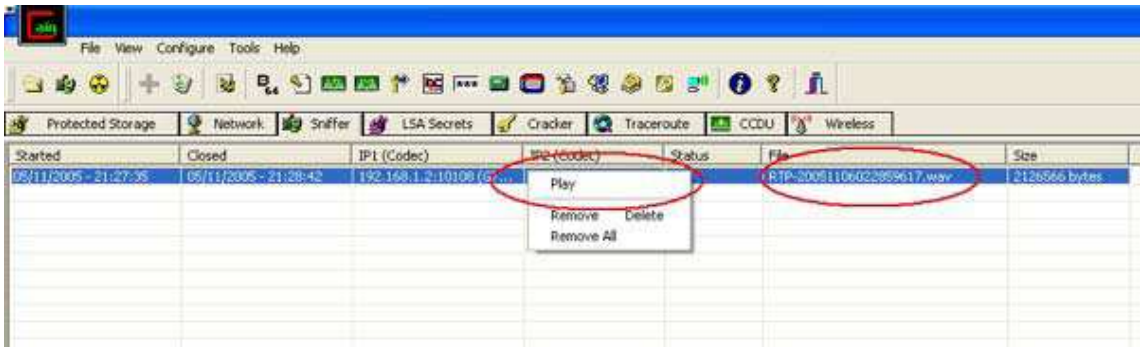


Fig.III.9. Esnifando la comunicación VoIP

3.3.3.2 Inserción de Audio

En las llamadas VoIP la transmisión del flujo de datos se realiza por razones de sencillez y eficiencia sobre el protocolo UDP. Desgraciadamente UDP es un protocolo que no da garantías en la entrega de sus mensajes y no mantiene ningún tipo de información de estado o conexión. Por lo que a priori la inserción de paquetes UDP extraños dentro de un flujo legítimo puede llegar a ser trivial.

Encapsulado en UDP se encuentra el protocolo RTP que transporta verdaderamente los datos de voz. RTP tampoco lleva un control exhaustivo sobre el flujo de datos relegando las funciones de recuento de paquetes y calidad de servicio al protocolo RTCP (Real Time Control Protocol). El único método que tiene RTP para controlar tramas perdidas y reordenar las que le llega es el campo número de secuencia de la cabecera.

Es evidente que la forma de manejar estas situaciones dependerá mucho del dispositivo o de la implementación del software pero en cualquiera de los dos casos

el atacante podría realizar ataques de inserción de paquetes dentro de un flujo RTP consiguiendo insertar de forma exitosa audio en una conversación telefónica. Incluso se ha comprobado que contra algunos dispositivos es suficiente bombardear con paquetes UDP para que estos se inserten en la conversación.
Algunas herramientas con las que poder realizar este tipo de ataque son:

- **RTP InsertSound:** Es capaz de insertar un archivo wav en una conversación activa que este esnifando.
- **RTP MixSound:** Muy parecida a la anterior pero mezcla el sonido insertado con el real de la conversación.

3.3.4. Fuzzing

Los ataques de fuzzing o también conocidos como testeo funcional del protocolo, es una de los mejores métodos para encontrar errores y agujeros de seguridad. Consiste en crear paquetes o peticiones especialmente malformadas para ir más allá de las especificaciones del protocolo. El objetivo es comprobar como manejan los dispositivos, las aplicaciones o el propio sistema operativo que implementa el protocolo, estas situaciones anómalas que desgraciadamente no se han tenido en cuenta en la implementación y casi siempre terminan en un error, denegación de servicio o en alguna vulnerabilidad más grave.
Gracias a la técnica de fuzzing se han llegado a encontrar gran cantidad de ataques de DoS y buffer overflows en los productos que implementan los protocolos SIP y H.323

3.3.4.1. Ingeniería social

3.3.4.1.1. SPIT: Spam over Internet Telephony

El SPAM es uno de los problemas más graves en las comunicaciones hoy en día, y la telefonía IP tampoco se escapa. Recibe el nombre de SPIT (Spam over InternetTelephony).
Se prevé que esta tendencia de realizar llamadas y llenar los voicemail de los usuarios con mensajes pregrabados crecerá durante los próximos años a medida que se generalice el uso de telefonía por IP.

3.3.4.1.2. Vishing: Voip Phishing

Al igual que ocurría con el SPAM las amenazas de phishing suponen un gran problema para el correo electrónico. Las denuncias por robo de información confidencial de forma fraudulenta están a la orden del día y exactamente las mismas técnicas son aplicables a la plataforma VoIP. Gracias a la telefonía IP un intruso puede realizar llamadas desde cualquier lugar del mundo al teléfono IP un empleado de la empresa y con técnicas de ingeniería social y mostrando la identidad falsa o suplantando otra conocida por la víctima, obtener información confidencial, datos personales, números de cuenta o cualquier otro tipo de información. Las opciones son prácticamente ilimitadas y al igual que el SPIT es posible que el número de incidentes de este tipo se disparen en los próximos años.

3.4. Asegurando la red Voip

Durante todo el trabajo mi intención ha sido dar a conocer la mayoría de problemas de seguridad que pueden llegar a sufrir las redes de telefonía IP y explicar las técnicas y los ataques que el intruso utilizaría para atacar entornos VoIP reales. Para redactar una guía de creación de infraestructuras VoIP seguras sería necesario un nuevo trabajo mucho más extenso que el actual, por lo que me limitaré he señalar qué controles de seguridad deben ser imprescindibles en el entorno VoIP y explicar las medidas necesarias para paliar la mayoría de riesgos y ataques comentados en apartados anteriores.

La primera regla de oro: **Mantener los sistemas actualizados y parcheados**. Es totalmente imprescindible, y ya no solo en infraestructura VoIP, que el administrador de lared esté al corriente de los nuevos parches y actualizaciones y los aplique en sus sistemas.

Es esencial que VoIP se asiente sobre una infraestructura de red segura, protegidas por cortafuegos bien administrador. Es muy recomendable la existencia en la red de sistemas deantivirusactualizados que la protejan de ataques de virus, gusanos y troyanos. La detección de muchos ataques se puede realizar instalando sistemas de detección de intrusos (IDS) o de prevención (IPS) en los lugares estratégicos de la red. Serán capaces de detectar y prevenir ataques contra los protocolos (fuzzing), ataques contra servicios (exploits y vulnerabilidades), escaneos y ciertos tipos de ataques DoS. Es evidente que el IDS/IPSrequerirá una configuración adecuada adaptada a la red en que funcione para conseguir su fiabilidad se al adecuada.

Es conveniente modificar los protocolos y configurar dispositivos para que utilicen autenticación en todos los mensajes que se intercambia. Además de la

autenticaciónya explicada anteriormente, existen otros dos aspectos esenciales de la seguridad en VoIP. Son laautorizacióny el cifrado. Los dispositivos deben de tener limitado los grupos de elementos o direcciones IP de los que pueden recibir tráfico. Realizando, de este modo, una correcta configuración es posible limitar muchos de los ataques de denegación de servicio.

El cifradoes quizás una de las principales y más necesarias medidas que se deben adoptaren una infraestructura VoIP. El uso de TLS/SSL para establecer canales de comunicación seguros resolverá la mayoría de problemas de eavesdroping, manipulación y reproducción de los mensajes que se intercambian.

Las comunicaciones de los datos pueden ser seguras incorporando algún tipo de cifrado. Los teléfonos VoIP pueden cifrar el audio con el protocolo SRTP. Secure RTP es una réplica del RTP pero ofrece confidencialidad, autenticación de mensajes y protección evitando los ataques de interceptación e inserción de audio entre toros. SRTP es ideal para proveer telefonía IP porque usando con una compresión de las cabeceras no afecta prácticamente a las Qos.

Es evidente que el canal de señalización también debe de ir completamente cifrado.

Utilizar VLAN’s para priorizar y proteger el tráfico VoIP separándolo en canales lógico de las redes de datos.

Intentar proteger y limitar el acceso a la red VoIP en la medida de lo posible, sobre todo desde el exterior.

Limitar los volúmenes de datos y ráfagas de paquetes en puntos estratégicos de la red para evitar gran cantidad de ataques DoS.

Y finalmente algunos consejos para protegerse de ataques de enumeración:

• Corregir los protocolos que contestan diferente modo si el usuario existe o no.

• Configurar correctamente los servicios para que no muestren más información dela necesaria.

• No usar nombres por defecto par archivos de configuración

• No usar TFTP, FTP aunque tampoco sea seguro. LA mejor solución es usar un canal cifrado.

• Desactivar puertos de administración http y snmp.

• Cambiar el password por defecto de todos los lugares

CAPÍTULO IV
IMPLEMENTACIÓN, PRUEBAS Y RESULTADOS

4.1 IMPLEMENTACIÓN DEL PROTOTIPO DE RED VOIP

Para poder cumplir con los objetivos planteados es necesario implementar un Prototipo de red VoIp (Anexo I) el cual será utilizado para el análisis y la realización de pruebas que nos ayudara a determinar las falencias del mismo.

4.1.1 Instalación del Servidor VoIP

Hardware Utilizado:

- Intel Pentium IV de 1.7 GHz.
- Memoria RAM de 520 MB
- Disco Duro de 40 GB
- Tarjeta de Red 10/100 Mbps

Como el servidor va a estar conectado a la PSTN de CNT, para la demostración del prototipo se necesitó una tarjeta que incluya módulos FXO que se inserte en la ranura PCI de la estación y que permita interactuar al servidor con la infraestructura telefónica analógica.

Para esto se empleó una tarjeta OpenVox A400P01 (ver Anexo I) con solo un módulo FXO habilitado, conectado a una ranura PCI en la tarjeta madre de la estación.
Asimismo se empleó un switch el cual se encargó de regular el tráfico generado por las estaciones clientes.

Software Utilizado:

- Elastix, versión 2.0 – IPBX

Elastix es un software aplicativo que integra las mejores herramientas disponibles para PBXs basados en Asterisk en una interfaz simple y fácil de usar. Además añade su propio conjunto de utilidades y permite la creación de módulos de terceros para hacer de este el mejor paquete de software disponible para la telefonía de código abierto.

Las características proveídas por Elastix son muchas y variadas. Elastix integra varios paquetes de software, cada uno incluye su propio conjunto de características. Además Elastix añade nuevas interfaces para el control y reportes de sí mismo, lo que lo hace un paquete completo.

Es por esto que se implementó la central telefónica en esta plataforma debido a que brinda todas las facilidades para poder crear con un ambiente amigable para el usuario.

Instalación de Hardware

El proceso de instalación de hardware no es otro más que el típico relacionado con agregar dispositivos PCI a la tarjeta madre de una estación de trabajo (tarjetaOpenVox A400P01) o conectar dispositivos de telecomunicaciones a través de un cable telefónico y un cable de red CAT5.

Eso a breves rasgos es lo que involucra la interconexión de los dispositivos que permitirán a los clientes interactuar con el servidor Elastixy viceversa.

- La tarjeta OpenVox A400P01 se conecta a una ranura PCI de la tarjeta madre de la PC, como una tarjeta de red común o una tarjeta de sonido.
- En el puerto FXO de la tarjeta se conecta a la línea telefónica (PSTN).
- El servidor está conectado a un switchque se encarga de la conmutación de los paquetes.
- Finalmente se conectaron varias computadoras portátiles y PCs con sistemas operativos Windows para que funcionen dentro del entorno de VoIPcomo clientes a través de softphones.

Pasos para la Instalación de Elastix

Insertamos el CD de instalación de Elastix 2.0 al momento de encender la máquina y aparecerá una pantalla como la que se muestra a continuación:

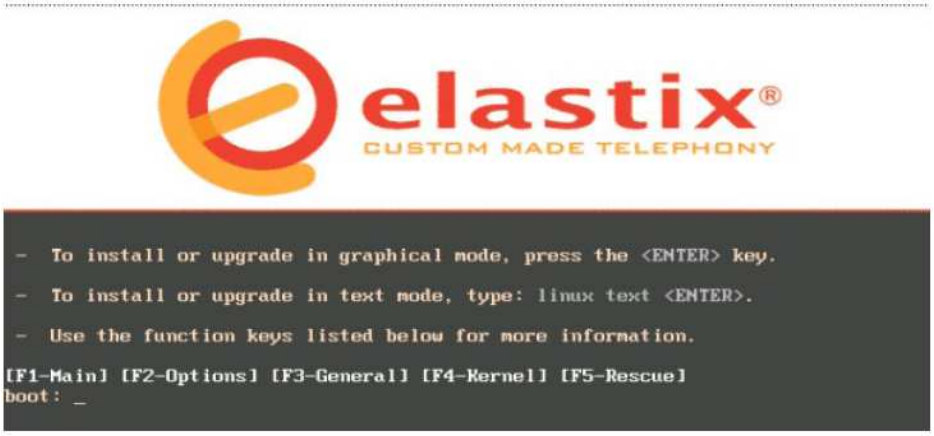


Fig.IV.1. Pantalla inicial de instalación.

Una vez hecho esto nos presentará una pantalla en la que debemos escoger el tipo de teclado, en nuestro caso el teclado de idioma español "es":

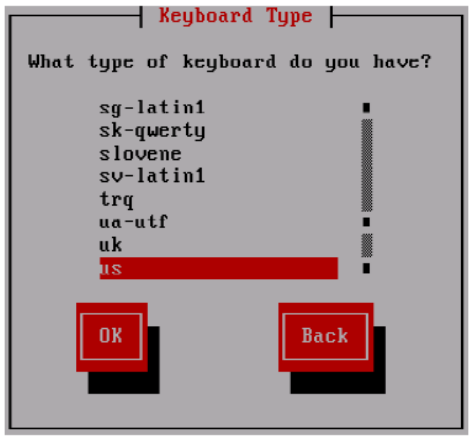


Fig.IV.2. Escoger tipo de teclado.

Después seleccionamos la hora zona horaria de nuestra región es decir América/Guayaquil:

Fig.IV.3. Escoger la zona horaria.

Nos pedirá que digitemos la contraseña que usaremos como el usuario administrador de Elastix, en nuestro caso.

- username: root
- password: administrador

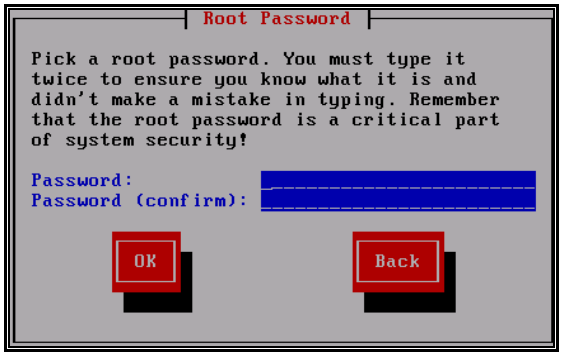


Fig.IV.4. Digitar clave de usuario administrador

A continuación buscará las dependencias necesarias para la instalación:

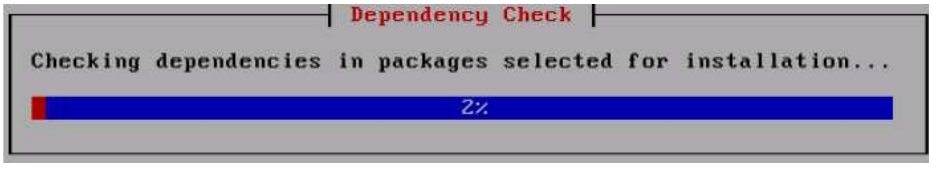


Fig.IV.5. Chequeo de dependencias para instalación

Luego se procede con la instalación, el sistema instala los paquetes automáticamente lo cual toma unos minutos:

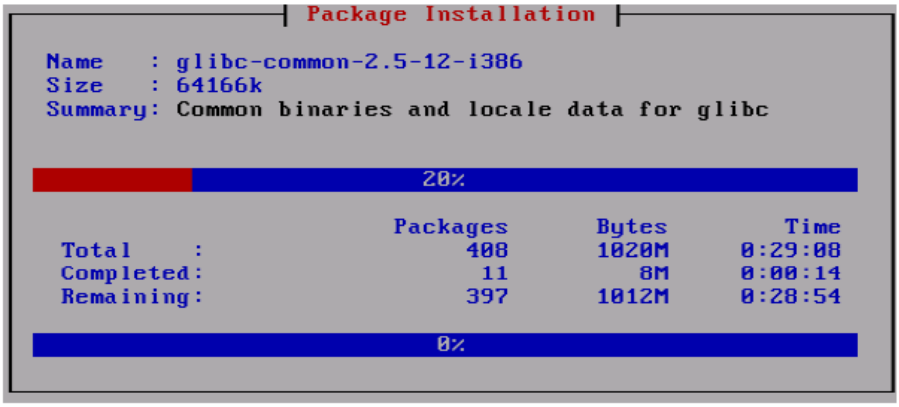


Fig.IV.6. Instalación en curso

Una vez que se realice la instalación completa, procedemos a reiniciar el sistema. Luego de reiniciar el sistema podremos escoger entre las opciones de boot la distro de Elastix.

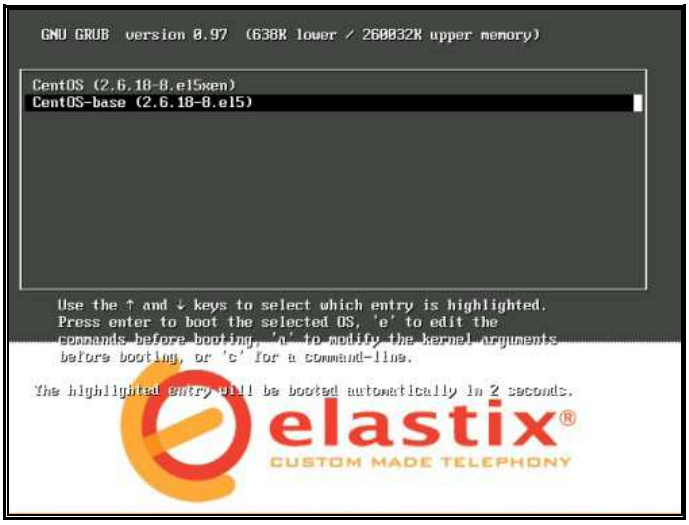


Fig.IV.7. Inicio de Elastix

Una vez seleccionada la opción de arranque, ingresamos como usuario root y la contraseña digitada al momento de la instalación.

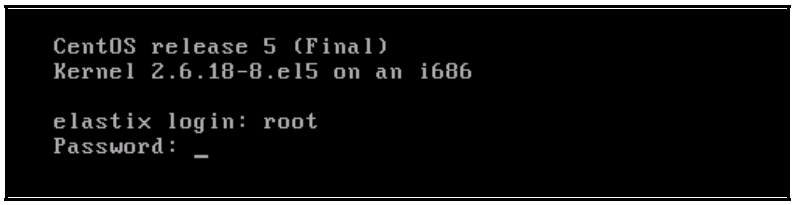


Fig.IV.8. Inicio de sesión como root

4.1.2 Configuración del Servidor VoIP

- **Configuración de extensiones.**

Lo primero que debemos hacer es ingresar a la interfaz gráfica de Elastix y los dirigimos al menú "PBX", por defecto se accede a la sección "Configuración PBX", en esta sección escogemos del panel izquierdo la opción "Extensiones". Ahora podremos crear una nueva extensión.

Escogemos el dispositivo de entre las opciones disponibles, en nuestro caso SIP.

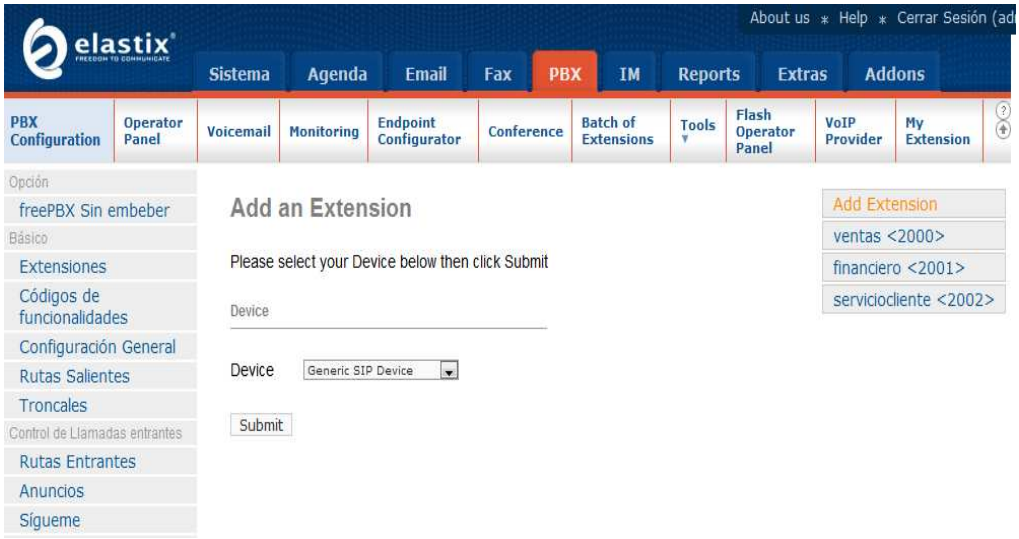


Fig. IV.9. Crear extensión SIP.

- **Configuración de troncal.**

Una troncal es aquella que permite llevar una llamada a cualquier proveedor de servicio de voz o a cualquier dispositivo que reciba su intento de llamada y la gestione a otro destino. Alguno de los tipos de troncales son:

- ZAP
- IAX2
- SIP
- Custom

En nuestro caso necesitamos configurar una troncal ZAP ya que son las asociadas a hardware de telefonía instalado en la máquina y usa el módulo chan_zap.so. Los archivos asociados a este tipo de troncales son el /etc/zaptel.conf y /etc/asterisk/zapata.conf.

Las troncales Zap son creadas mediante un número asociado a la posición del canal en el hardware, el nuestro caso solo se posee un canal.
Para esto accedemos al menú "PBX" y en el panel de la izquierda seleccionamos la opción "Troncales".

En la pantalla podemos apreciar que por defecto ya hay un tronco "ZAP/g0" creado en nuestra PBX Elastix. Por lo que al contar únicamente con un solo módulo FXO no es necesario configurar otra troncal, y utilizamos la que viene ya por defecto, debido a que éste abarca toda la configuración de los mismos.

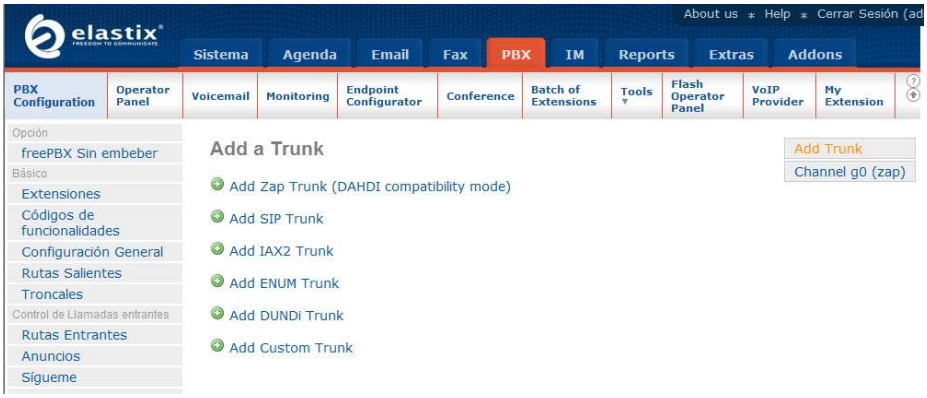


Fig. IV.10. Creación de troncal ZAP.

- **Configuración de rutas entrantes.**

Lo primero que hay que tomar en cuenta es dónde se quisiera recibir las llamadas, para esto se ha configurado una IVR denominada "Menú Principal" (Anexo III.), y las llamadas se recibirán por la troncal ZAP(DAHDI).
Para configurar una ruta entrante vamos al menú "PBX" en el panel izquierdo seleccionamos "Rutas Entrantes", le damos un nombre descriptivo y en la sección "Set Destination" escogemos el destino en este caso la IVR.

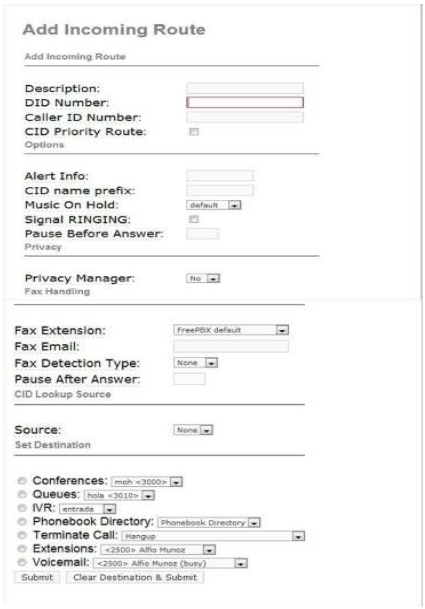


Fig. IV.11. Creación de Rutas Entrantes.

- **Configuración de rutas salientes.**

Lo primero que hacemos es ir al menú "PBX" en el panel de la izquierda seleccionamos "Rutas Salientes" y le damos click, ahí aparecerá un menú donde en "Route Name" pondremos un nombre descriptivo, en nuestro caso "saliente".

Es importante colocar un plan de marcado adecuado, en nuestro caso lo hemos seleccionado de tal manera que solo se puedan realizar llamadas locales.

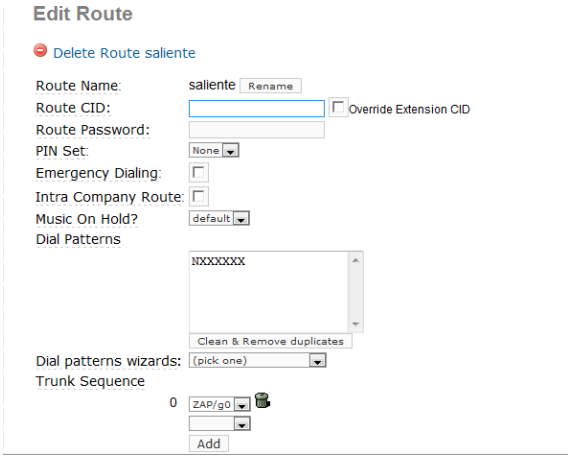


Fig. IV.12. Creación de Ruta Saliente.

4.1.3. Configuración de las maquinas clientes.

- **Hardware Utilizado**
  - Intel Pentium IV de 1.7 GHz.

- Memoria RAM de 520 MB
- Disco Duro de 12 GB

- **Software Utilizado**
  - X-Lite

- **Pasos para instalación de X-Lite**

  ✓ Inicio de instalación de X-Lite.

Fig. IV.13. Inicio de instalación X-Lite

  ✓ Detalle de la licencia del software.

Fig. IV.14. Información de licencia

  ✓ Ubicación en disco duro donde se va instalar el software.

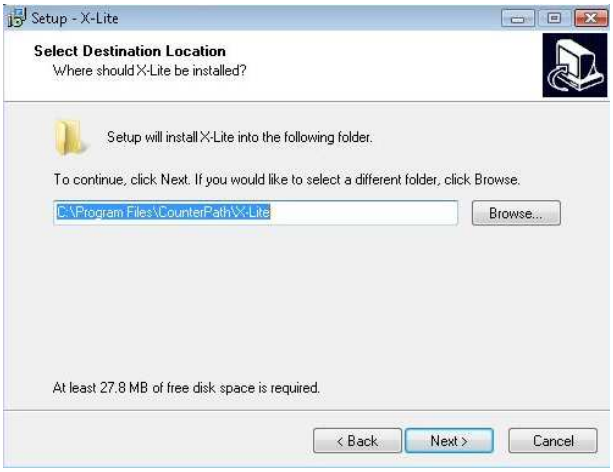


Fig. IV.15. Ubicación de destino

- ✓ Selección de tareas adicionales de instalación.

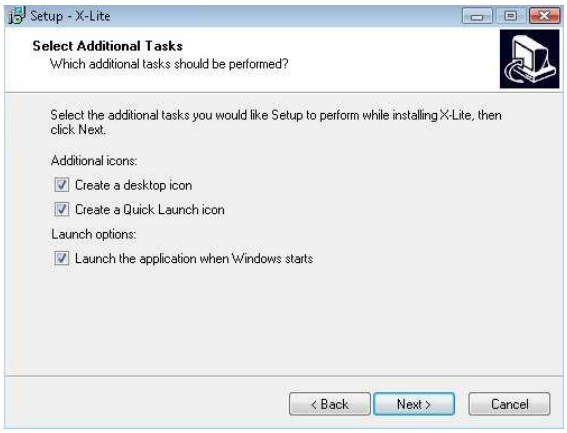


Fig. IV.16. Selección de tareas adicionales de instalación.

- ✓ Completando la instalación y finalizar.

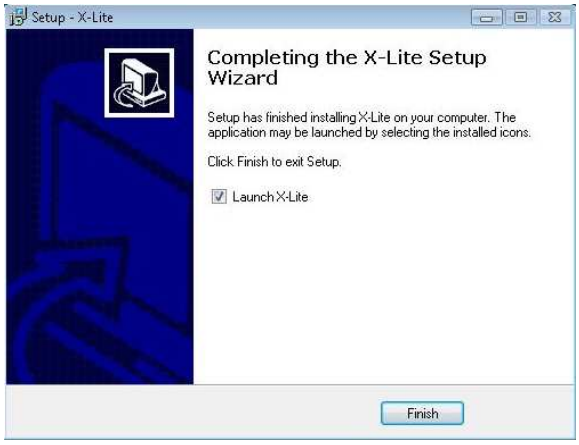


Fig. IV.17. Instalación finalizada.

Pasos para configuración de Softphone (X-Lite)

- Inicio del software X-Lite.

Fig. IV.18. Inicio de X-Lite

- Con un clic derecho seleccionamos la opción SIP Account Settings.

Fig. IV.19. Configuración de la cuenta SIP.

- Seleccionamos la opción Add para añadir la cuenta SIP.

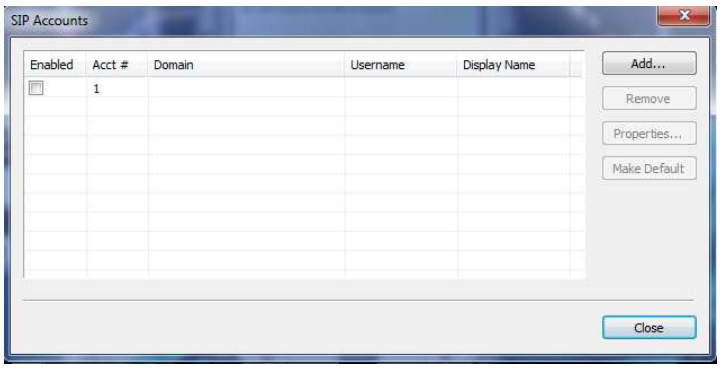


Fig.IV.20. Añadir nueva cuenta.

- Ingresamos toda la información correspondiente a la cuenta.

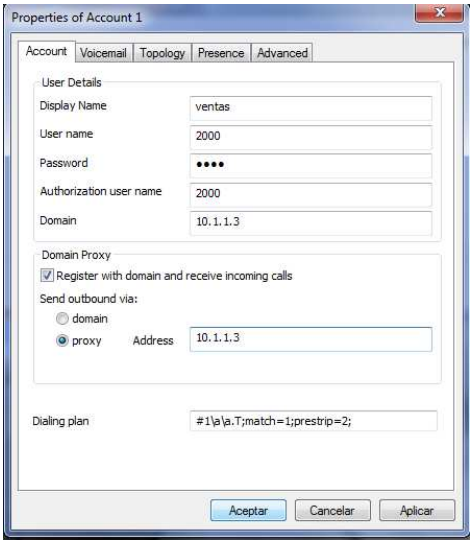


Fig.IV.21. Ingreso de datos de la cuenta.

4.2. PRUEBAS DEL PROTOTIPO

4.2.1 Definición del ambiente de pruebas de voz

En esta sección se define el esquema de pruebas del prototipo. Para ello se dispuso de un servidor de pruebas de voz sobre IP, con las características mencionadas anteriormente.

Se simuló una LAN formada por dispositivos que fueron conectados a un s*witch* y, a través de éste a un servidor de acceso a la PSTN. Estos dispositivos representaron a los usuarios internos de telefoníaIP del servidor *Elastix, alguno de ellos* fueron computadores con *softwaretelefónico* (Softphone) y otro fue un teléfono IP.

El softphoneque se utilizó para nuestras pruebas fue *Xlite 3.0,* que previamente hemos instalado.

Las direcciones IP que se asignaron fueron desde la 10.0.0.1 a la 10.0.0.20 con una máscara de 24 bits, y la puerta de enlace predeterminada es 10.0.0.1/24.

Departamento	Dirección IP	Extensión
Ventas	10.1.1.5	2000
Financiero	10.1.1.6	2001
Servicio al cliente	10.1.1.7	2002
Gerencia	10.1.1.8	2003

Tabla IV.1. Direccionamiento por departamentos.

La dirección IP para acceder a la Interfaz gráfica de Elastix es la 10.1.1.3. Esta conexión especial permitió que los usuarios internos se conecten al servidor *Elastix* a través de la LAN de la que forman parte.

Las pruebas consistieron básicamente en comprobar el funcionamiento de todas las aplicaciones cuya configuración se propuso con anterioridad, en base al siguiente proceso:

- Registro de clientes en el servidor.
- Establecimiento de llamadas internas.
- Establecimiento de llamadas hacia la PSTN.
- Ingreso de llamadas desde la PSTN.
- Aplicaciones de voz adicionales.

4.2.2. Pruebas de la central IPBX completa

Establecimiento de llamadas

El objetivo básico de un sistema de voz es permitir a los usuarios de este sistema comunicarse entre sí y con otros sistemas de voz. El servidor de telefonía dentro del escenario que se plantea, permite comunicar a los clientes directos de la central IP, en este caso las áreas de Ventas, Financiero y servicio al cliente, Gerencia.

Las pruebas que verifican este funcionamiento son:

1. Establecimiento de llamada de financiero a ventas durante 3 minutos

2. Establecimiento de llamada financiero a servicio al cliente durante 2 minutos

3. Establecimiento de llamada de Ventas a servicio al cliente durante 2 minuto

4. Establecimiento de llamada de Gerencia a servicio al cliente durante 1 minuto

5. Establecimiento de llamada desde y hacia la PSTN.

***Resultados*.-** Las llamadas individuales son exitosas, se establecen normalmente pues quienes las reciben están registrados en el servidor de Voz y contestan cuando empieza el timbrado de sus terminales (softphones).

Por otro lado, al disponer de una tarjeta con un módulo analógico FXO en el servidor, éste debe ser capaz de funcionar como Gateway y permitir la salida de llamadas desde el interior de la red LAN hacia la PSTN, así como el ingreso de

comunicaciones desde la red telefónica pública al interior de la LAN a través de la misma interfaz.

En este sentido, las pruebas que se realizan son las siguientes:

• Se realiza una llamada desde todos los departamentos hacia un número local(el escenario dispone de una línea telefónica, y está conectada al servidor).

• Se realiza una llamada desde un número telefónico dentro de la ciudad (atravésde la línea telefónica de pruebas) a la *troncal* (línea telefónica a la que está conectado el servidor de telefonía) y se digita un patrón de dígitos para comunicarse con cada uno de los departamentos de los que está formado el escenario.

Resultados.- Las dos pruebas se ejecutan de manera satisfactoria, las llamadas desde la LAN hacia la PSTN se enlutaron adecuada y transparentemente, permitiendo que se establezca la comunicación. Del mismo modo, las llamadas hacia la *troncal* son atendidas por el mecanismo de IVR que guía a los llamantes para alcanzar cada uno de los departamentos a través del marcado de su número de extensión.

• Para comprobar el funcionamiento del servicio de IVR (respuesta de voz interactiva), se realizó una llamada desde una línea convencional hacia la *troncal* conectada al servidor Elastix.

***Resultados*.-** La llamada es contestada automáticamente y una grabación de voz indica las extensiones a marcarse para alcanzar a los departamentos de las opciones que presenta.

Casos Especiales

• Para verificar el funcionamiento de la central en algunos casos especiales, serializa una llamada interna o desde la PSTN y se digitan patrones que no existen dentro del dial plan.

• Asimismo, en una llamada que ingresa a través de la troncal analógica se espera sin realizar ninguna acción luego del mensaje de voz del IVR (sin digitar ningún patrón o extensión).

• Por último se mantiene establecida una llamada realizada desde la LAN interna de forma prolongada.

Resultados.- Al generar estos pequeños escenarios especiales pero que pueden suceder, se tiene que cuando un usuario (interno o externo) digita un patrón que no corresponde a ninguna extensión creada dentro del plan de marcado, un mensaje de voz indica el error y el IVR vuelve a detallar las indicaciones de direccionamiento. Asimismo, si al recibir las instrucciones, el llamante no digita ningún patrón, la llamada se transfiere automáticamente (luego de pocos segundos) a la operadora.

4.2.4 PRUEBAS DE SEGURIDAD Y VULNERABILIDADES.

Para la realización de pruebas fue necesaria la utilización de varias herramientas cuyo propósito era encontrar las vulnerabilidades que existen en la red, enfocándonos en 3 de éstas como son: la captura y decodificación de los paquetes de voz, Flooding enviando una tormenta de paquetes RTP al destino escogido, por último el decifrado de contraseñas de los dispositivos de la red VoIP.

A continuación se describe las características de las herramientas utilizadas.

Herramienta	Descripción
Wireshark	• Disponible para UNIX, LINUX, Windows y Mac OS. • Captura los paquetes directamente desde una interfaz de red. • Permite obtener detalladamente la información del protocolo utilizado en el paquete capturado. • Cuenta con la capacidad de importar/exportar los paquetes capturados desde/hacia otros programas. • Filtra los paquetes que cumplan con un criterio definido previamente.

	• Realiza la búsqueda de los paquetes que cumplan con un criterio definido previamente. • Permite obtener estadísticas. • Sus funciones gráficas son muy poderosas ya que identifica mediante el uso de colores los paquetes que cumplen con los filtros establecidos.
Cain & Abel	Cain and Abel es una herramienta diseñada para administradores de redes, aunque también es usada en muchas ocasiones también por hackers. Con esta herramienta se puede comprobar el nivel de seguridad de una red, ya sea una red local doméstica o profesional. El programa permite recuperar contraseñas de una amplia variedad de protocolos, entre los protocolos soportados están el: FTP, SMTP, POP3, HTTP, MySQL, ICQ, Telnet, SIP y otros, además de poder recuperar también las claves ocultas debajo de la línea de asteriscos en Windows. El programa incluye otras utilidades destinadas a la administración y control de redes que permiten determinar la seguridad de una red. Entre otras cosas este programa permite descubrir las claves que circulan por una red, ya sean claves que viajan en texto plano (sin ningún tipo de codificación), o bien protegidas mediante algún sistema de encriptación. Al permitir capturar las claves (incluidas las claves de acceso de una red WiFi) permite que

	posteriormente estas puedan ser descubiertas al aplicarse Ataques por Fuerza Bruta (Brute Force Attack) o a través de Ataques de Diccionario (Dictionary Attack) o por Ataques de Cryptoanálisis (Cryptanalysis Attack). Es posible además conocer el password de una red WiFi que esté al alcance de nuestra antena, por eso recomendamos que estos password se modifiquen cada cierto tiempo. Este software hará saltar las alertas por troyanos de los antivirus, pero en este caso se trata de un falso positivo.
Inviteflood	Inundación de peticiones invite que satura el servidor provocando el mal funcionamiento del mismo impidiendo la realización de llamadas.

Tabla IV 3. Descripción de Scanners de Vulnerabilidades

4.2.4.1 Captura conversaciones VoIP, Extracción de Audio.

Es posible, tratándose de instalaciones VoIP no seguras, la captura de paquetes VoIP (emisión de voz en paquetesIP) y la extracción de conversaciones contenidas en este tipo de conexiones.

En este apartado vamos a usar una captura .pcap conteniendo una conversación usando el protocolo SIP (Session Initiation Protocol), un protocolo de señalización, similar a HTML y SMTP, encargado de la localización usuarios, parámetros, modificaciones e iniciar o finalizar una sesión. Los datos de audio serán transportados mediante el protocolo de transporte RTP (Real Time Transport Protocol) usando UDP**.** SIP encapsula otro protocolo: SDP, que es el encargado de la negociación de las capacidades de los participantes, tipo de codificación usada y otros aspectos.

Usaremos Wireshark para analizar la captura .pcap e ilustrar todos los aspectos comentados de SIP**,** SDPyRTP**,** además de la extracción del audio de las conversaciones.

Analizando los paquetes.

Realizaremos una llamada entre usuarios agentes y mediante el Software capturamos los paquetes que posteriormente serán analizados.

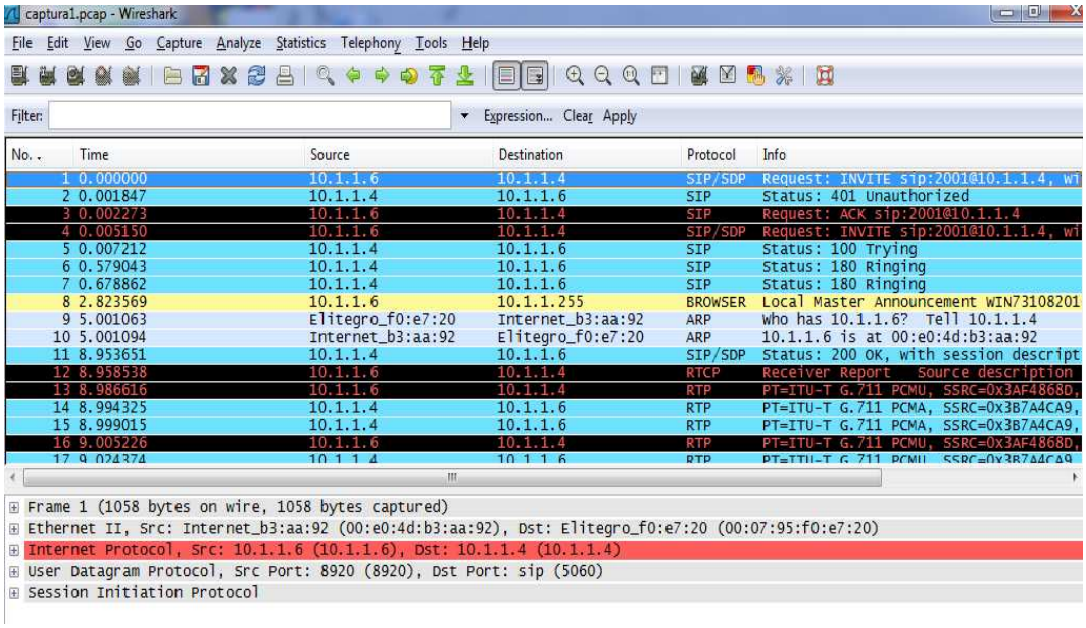


Fig. IV.22. Captura de paquetes de tráfico de voz.

El paquete número uno corresponde a un mensaje SIP de tipo Request**,** concretamente INVITE que se refiere al establecimiento de llamada o sesión**.**

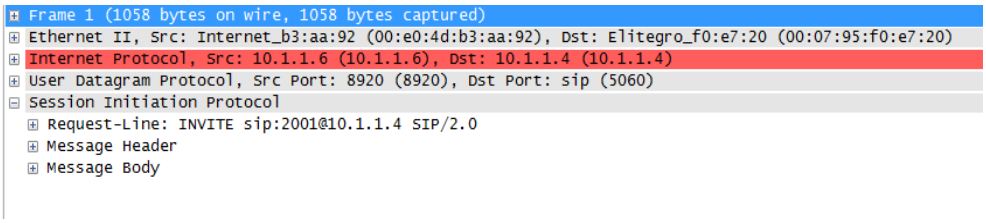


Fig.IV.23. Establecimiento de llamada o sesión.

El Request-Line **o t**ipo de mensaje**.** Tipo de mensaje INVITE**,** mensaje SIP dirigido a 2001@10.1.1.4 Vemos también la versión SIP que es SIP/2.0**.** El puerto de destinoes 5060.

Ahora tenemos elMessage Header o cabecera que contiene**:**

Fig.IV.24. Cabecera SIP Message Header.

Message Bodyocuerpo del mensaje contiene el Session Description Protocol SDP con los siguientes campos**:**

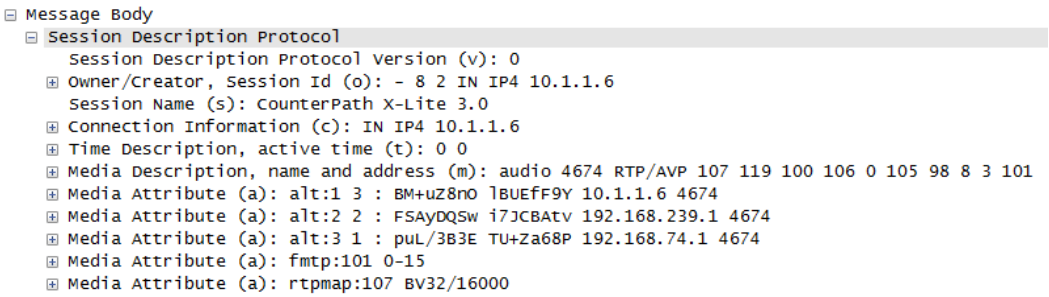


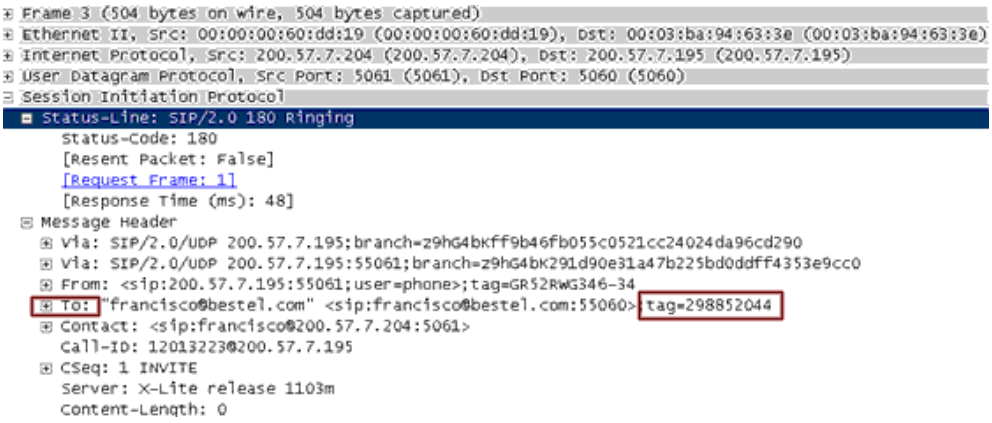
Fig.IV.25. Cabecera SIP Message Body.

Mensaje de respuesta de información de estado**.** Se informa, tal como dice su código 100, de que se está tratando la información**:**

Se observa el Status-Code**:** 100

En el Message Header tenemos la misma información que el Message Header del paquete número 1**.**

Tenemos un mensaje también de mensaje de respuesta de información de estado**.** Se informa que el INVITE fue recibido por la otra parte. Digamos que se está Rinnging (llamando) y se espera a que atienda la llamada:

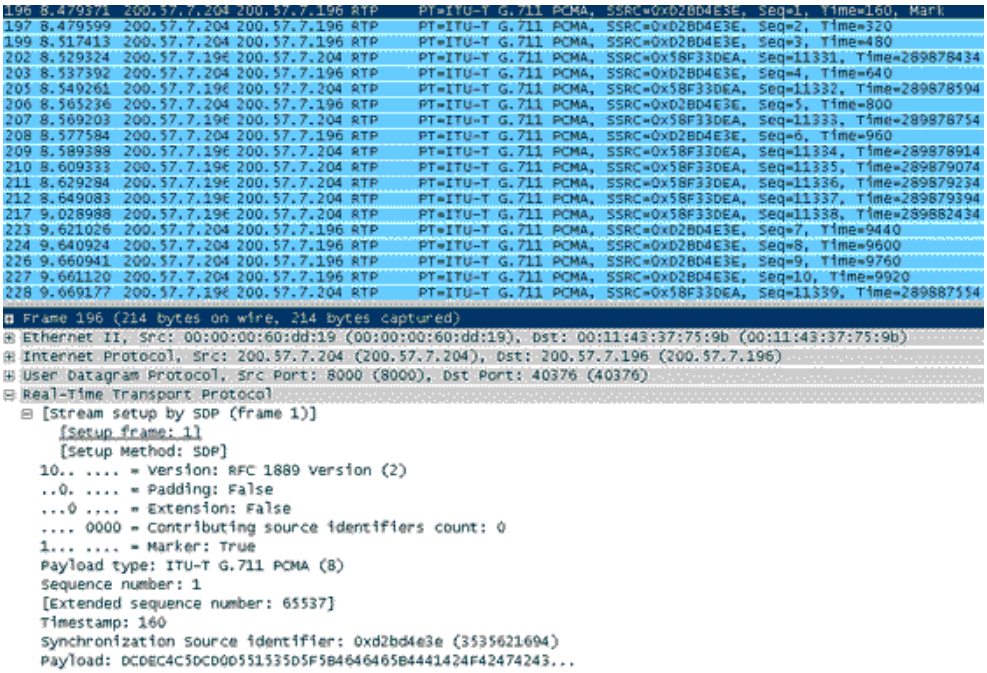


Ahora vamos a ver como con Wireshark podemos extraer la información de audio y otros datos de la captura**.**

Extracción del audio con Wireshark.

Si establecemos como filtro el protocolo RTP**,** veremos solo los paquetes correspondientes a dicho protocolo. Ya hemos visto más arriba para que sirve.

Observamos uno de estos paquetes



Vemos en el campo Payload Type **o** tipo de cargaque se trata de de ITU-T G.711 PCMA (8), es decir usa el códec audio G.711, estandarizado por ITU (International Telecom. Union). Frecuencia de muestreo 8KHz y usa para comprimir/descomprimir PCMA.

Nos situamos sobre este paquete y en el menú **Telephony > VoIP Calls**, nos aparece una ventana:

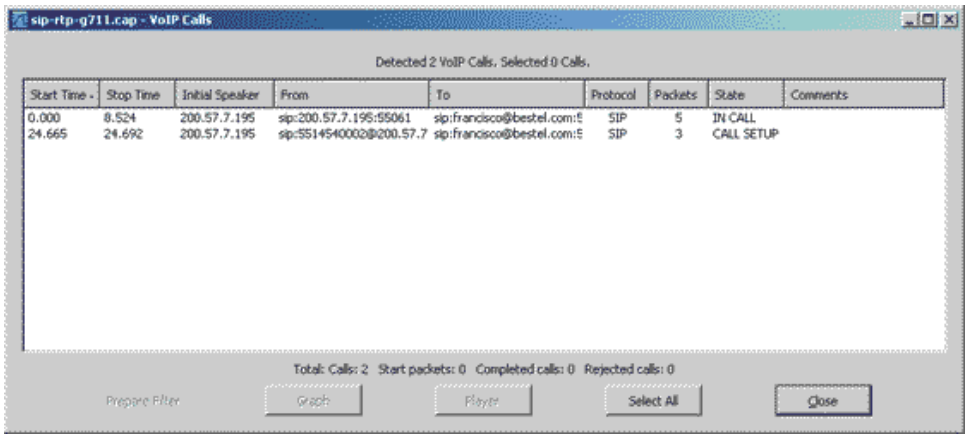


Fig. IV.26. Captura de llamadas.

Se trata de una lista de las llamadas incluidas en la captura. Tenemos una serie de columnas con información de cada llamada

Pulsamos Graph:

Aquí, tenemos un análisis gráfico de la conversación mantenida entre quien realiza la petición INVITE y las dos respuestas correspondientes.

Cerramos la ventana de análisis gráfico y sobre la ventana VoIP Calls, pulsamos el botón Player. Sobre la ventana que nos aparece pulsamos Decode y obtenemos:

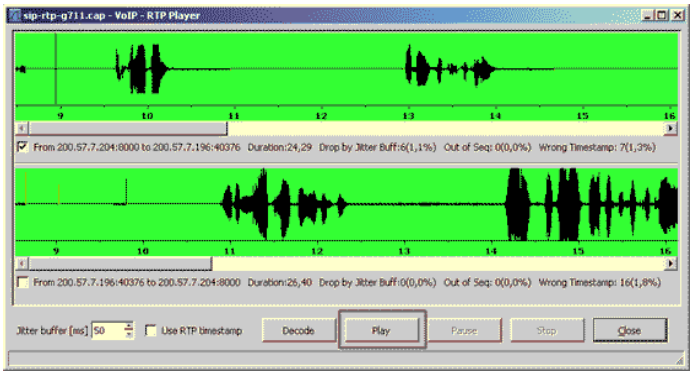


Fig. IV. 27. Reproducción de llamadas

Tenemosdos pistas de audios que corresponden a cada uno de los usuariosinvolucrados en la conversación**.** Si marcamos una pista uno y pulsamos Play oiremos el audio de la conversación. Pulsando ambas pistas escucharemos toda la conversación.

Resultado

Con esto demostramos que la conversación pudo ser fácilmente capturada y es así como usuarios no autorizados pueden tener acceso a ella para beneficio personal y así perjudicar a terceros.

4.2.4.2 Crackeo de contraseñas SIP

Para la realización de esta prueba existe un gran variedad de herramientas como ya se menciono en el capitulo anterior pero nosotros utilizamos el programa conocido Cain&Abel**.**

Cain & Abel

Cain & Abel es una herramienta de recuperación de todo tipo de contraseñas para sistemas Microsoft, las últimas versiones soportan cracking de contraseñas de SIP**.**

Capturar en un entorno conmutado

Para capturar tráfico en una red con switches, además de esnifar necesitamos activar el ataque Man in the middle, necesario para interceptar el tráfico del registro SIP entre el cliente y el servidor SIP. En caso de estar en un entorno con hubs o con wireless no es necesario y podemos saltarnos este paso.

Para llevar a cabo el ARP spoofing vamos a utilizar el propio Cain & Abel. En primer lugar activamos el botón de Start/Stop Sniffer de la parte superior. Nos situamos

sobre la pestaña superior Sniffer y la pestaña inferior Hosts para elegir la lista de hosts de la red cuyo tráfico queremos esnifar. Con el botón de + escaneamos la lista de hosts de nuestra red.

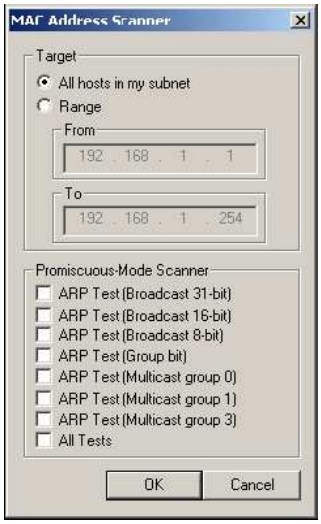


Fig.IV.28. Entorno conmutado cain&abel

Escaneo de hosts

Una vez que aparecen todos los hosts de la red, seleccionando cada uno y con el botón derecho, Remove, eliminamos los que no necesitamos. Los dos hosts que aparecen en la lista son el servidor SIP (Asterisk) y el cliente.

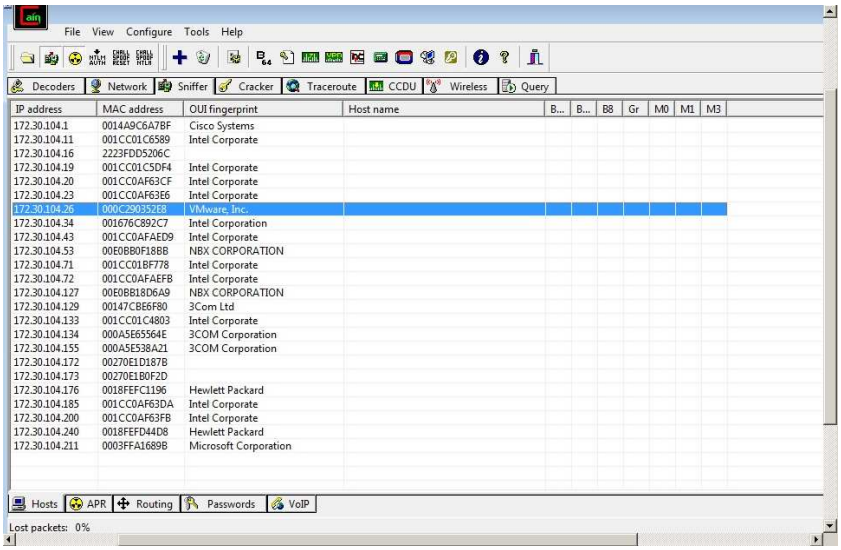


Fig.IV.29. Host escaneados

Lista de hosts

Sobre la pestaña ARP de la parte inferior pinchamos sobre el botón de +, Add to

list.

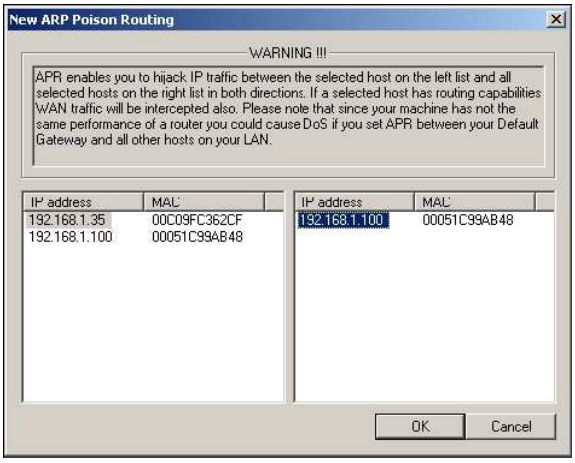


Fig.IV.30.Añadir Host a la lista Cain&Abel

Captura de logins SIP

Antes de comenzar debe estar la opción Start/Stop sniffer activada. Si es la primera vez que lo hacemos aparecerá la siguiente pantalla de configuración en la que deberemos seleccionar la interfaz de red por la cual deberá capturar.

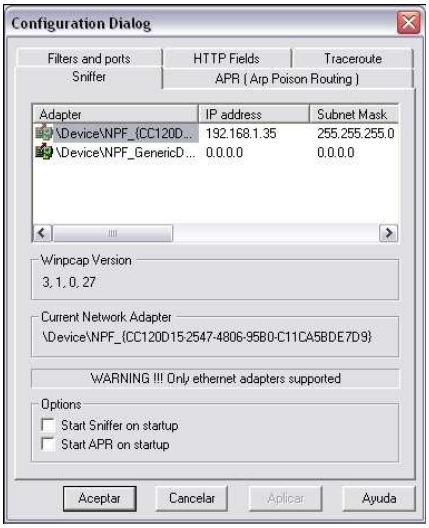


Fig.IV.31. Configuracion de Snniffer Cain&Abel

Configuración del sniffer

Para cambiar esta configuración más adelante deberemos ir al menú Configure. Nos situamos sobre la pestaña Sniffer de la parte superior, y en la parte inferior sobre Passwords. Si seleccionamos SIP de la lista de protocolos de la izquierda, entre paréntesis aparece el número de logins que ha capturado.

Crackeando contraseñas

Una vez que hemos capturado el hash, con el botón derecho sobre cada captura la enviamos al cracker para poder romperla.

Una vez que hemos capturado el hash, con el botón derecho sobre cada captura la enviamos al cracker para poder romperla.

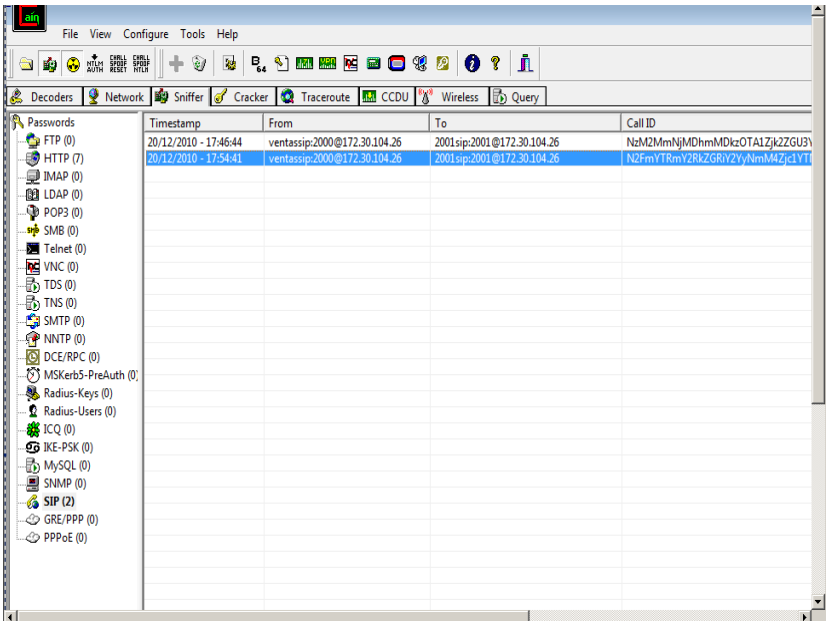


Fig.IV.32. Crackeando contraseñas Cain&Abel

Enviando hash al cracker

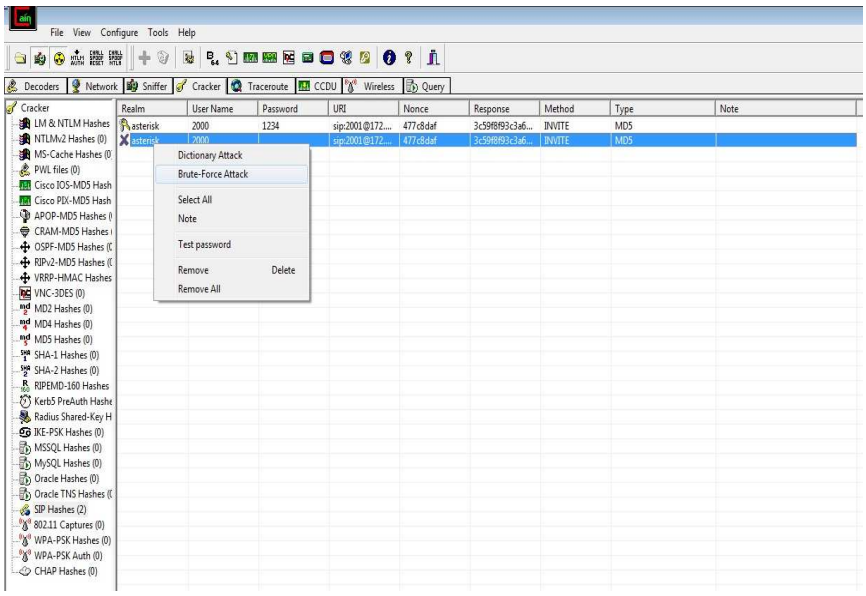


Fig.IV.33. Enviando hash al cracker Cain&Abel

Cracker de contraseñas SIP

Nos situamos en la pestaña Cracker. Podemos probar dos tipos de ataques contra el hash, ataque por diccionario o por fuerza bruta.

Ataque por diccionario

Si seleccionamos Dictionary Attack llegamos a la siguiente pantalla. Deberemos añadir un diccionario o diccionarios a la lista. En la ruta de instalación del Cain&Abel C:\Archivos de programa\Cain\Wordlists\Wordlist.txt tenemos un fichero que contiene XXX palabras comunes en inglés y castellano.

Además podemos seleccionar una serie de opciones para que pruebe distintas combinaciones de cada posible contraseña del diccionario, como por ejemplo que pruebe la palabra al revés, de mayúsculas a minúsculas y viceversa, etc.

Comenzamos el ataque seleccionando Start y esperamos a que termine de procesar el diccionario o diccionarios. En cada momento podremos ver en qué posición del diccionario y qué palabra se está probando.

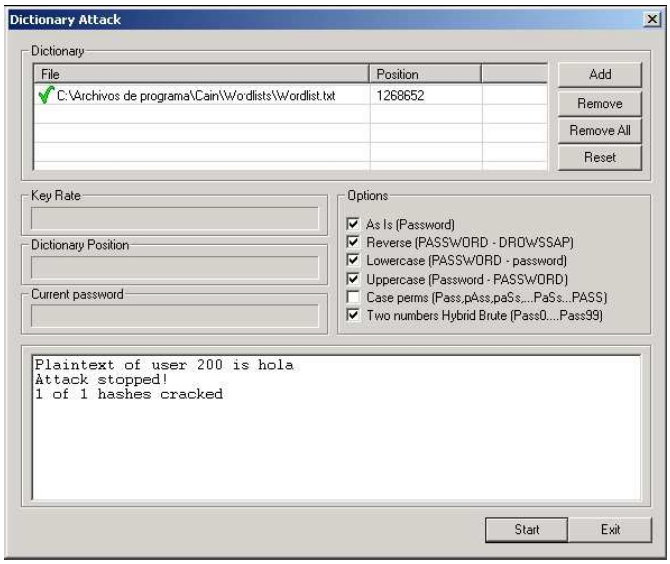


Fig.IV.34. Ataque por diccionario Cain&Abel

Ataque por fuerza bruta

Para comenzar, seleccionamos la opción Brute-Force Attack. Si sabemos la longitud mínima y/o máxima de la contraseña podemos especificarlo en Password length, sino dejamos los valores por defecto. Si pinchamos en la lista desplegable Predefined de Charset podremos elegir el rango de caracteres a partir del cual se probarán contraseñas: caracteres numéricos, alfanuméricos, especiales, etc.

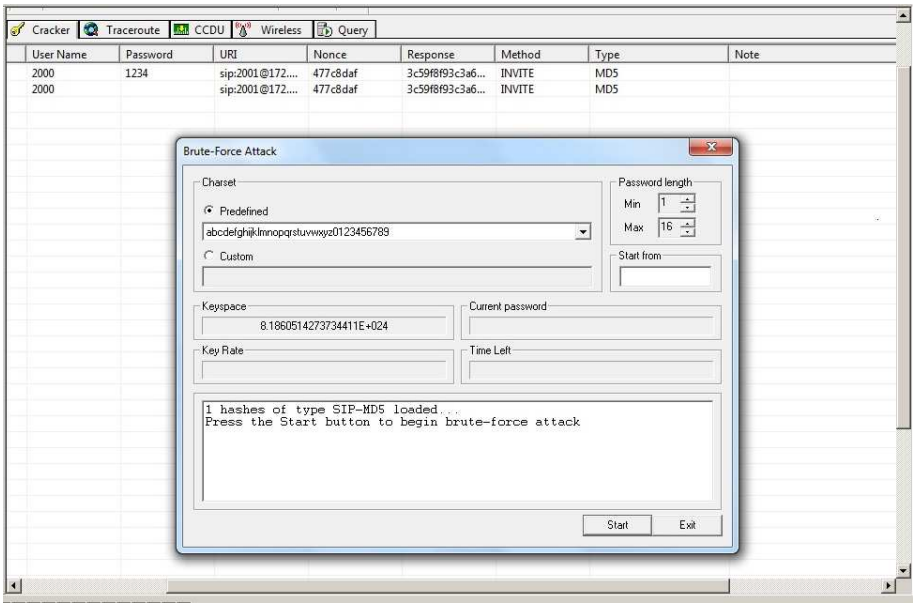


Fig.IV.35. Ataque por fuerza brutaCain&Abel

Una vez crackeadas todas las contraseñas aparecerán en texto claro.

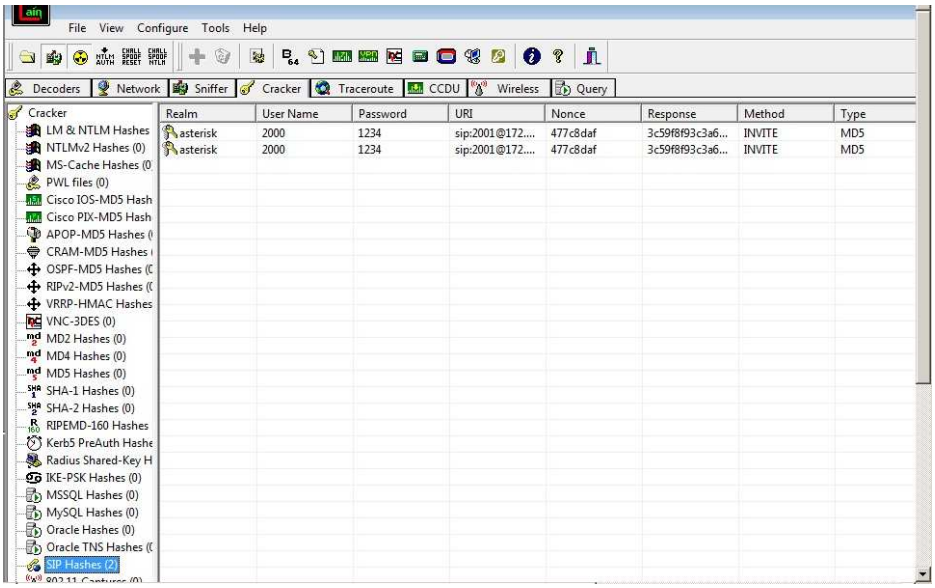


Fig.IV.36. Lista de contraseñas crackeadas Cain&Abel

El proceso realizado anteriormente se lo realizo para un entorno extensión a extensión el mismo proceso se lo realizo para un entorno extensión-PSTN y PSTN-extension

RESULTADOS

Captura de paquetes de la red para tratar de descifrar posibles contraseñas.

Es capaz de enumerar todas las contraseñas guardadas en la RAM del sistema, desde cuentas de usuario y contraseñas de administrador hasta contraseñas de messenger y redes sociales.
Muestra las contraseñas ocultas bajo los asteriscos y más.
Decifrado de contraseñas utilizadas para la utenticacion entre servidor y usuarios agentes o usuarios finales (softphone).
Se logra Descifrar contraseñas mediante ataques de fuerza bruta.

4.2.4.3 Denegación de Servicio, Ataques SIP inviteflood

MENSAJE INVITE

Cuando un usuario cliente desea iniciar una sesión (por ejemplo, audio, vídeo, o un juego), formula una petición INVITE. La petición INVITE pide establecer una sesión a un servidor. Esta petición puede ser forwardeada por los SIP Proxyes, llegando eventualmente a unos o más SIP UAS que puedan potencialmente aceptar la invitación. Estos UASs necesitarán con frecuencia preguntar al usuario si acepta la invitación. Luego, estos UASs pueden aceptar la invitación (la sesión debe ser establecida) enviando una respuesta 2xx.
Si la invitación no se acepta, se envía una respuesta 3xx, un 4xx, un 5xx o 6xx, dependiendo de la razón del rechazamiento. Antes de enviar una respuesta final, el UAS puede también enviar respuestas provisorias (1xx) para avisar al UAC del progreso de contacto con al usuario llamado.
Esto realmente puede resultar peligroso ya que el atacante conociendo el modo de funcionamiento puede realizar ataques de inundación para que colapse el servidor y pueda denegar cualquier servicio.

INSTALACIÓN DE LA HERRAMIENTA

En realidad este no es un concepto nuevo, siempre ha existido y mas por la deficiencia del protocolo sip que por el tipo de plataforma. El método consiste en explotar una vulnerabilidad del protocolo SIP, haciendo un envio masivo de peticiones INVITE de esta forma:

La Herramienta utilizada para la realización del ataque es ***"INVITEFLOOD"***, la cual se encarga de enviar una tormenta de Peticiones Invite al servidor que especifiquemos.

Para la instalación de la herramienta se utilizó una máquina virtual bajo Centos la cual fue agregada a la red para realizar el ataque.

Para la instalación se siguieron los siguientes pasos:

- Obtener el paquete desde la red del sitio:

wget http://www.hackingvoip.com/tools/inviteflood.tar.gz.

- Luego descomprimimos el archivo:

```
tar xvfz inviteflood.tar.gz
```

- En el archivo de lectura de esta herramienta nos detalla que esta necesita de otras librerías que deben ser obtenidas compiladas y ejecutadas, estas herramientas son libnet-devel y hack_library.
- Procedemos a descargarlo o actualizarlo de los repositorios de Linux (asterisk) :

```
yum -y install libnet-devel
wget http://www.hackingexposedvoip.com/tools/hack_library.tar.gz
tar -xzvf hack_library.tar.gz
```

- Para el funcionamiento de hack_library es necesario de la librería g711conversions la cual descargamos compilamos y ejecutamos :

```
wget
http://www.hackingexposedvoip.com/tools/g711conversions.tar.gz
tar -xzvf g711conversions.tar.gz
cd g711conversions
make
make install
```

- Este archivo ejecutado copiamos a /root/inviteflood

```
cp g711conversions.* /root/inviteflood
cd ..
```

- Nos ubicamos en el directorio inviteflood

```
cd inviteflood
```

- Instalamos la herramienta para que pueda ser utilizada

```
more inviteflood.c
```

```
more inviteflood.h
make
make install
```

- **Realización del Ataque.**

Enviar paquetes al Servidor Elastix para proceder a la denegación de servicio, nos ubicamos en el directorio inviteflood y ejecutamos el siguiente comando:

./inviteflood eth0 2000 10.1.1.10 10.1.1.4 1000000 -a hacker -D 2000 -v

Interfase de envío: eth0
Extension enviada: 2000
IP origen: 10.1.1.10
IP destino: 10.1.1.5
Cantidad de paquetes enviados: 1000000
User Alias: hacker
- D: puerto de destino
-v: Nivel de verbosidad

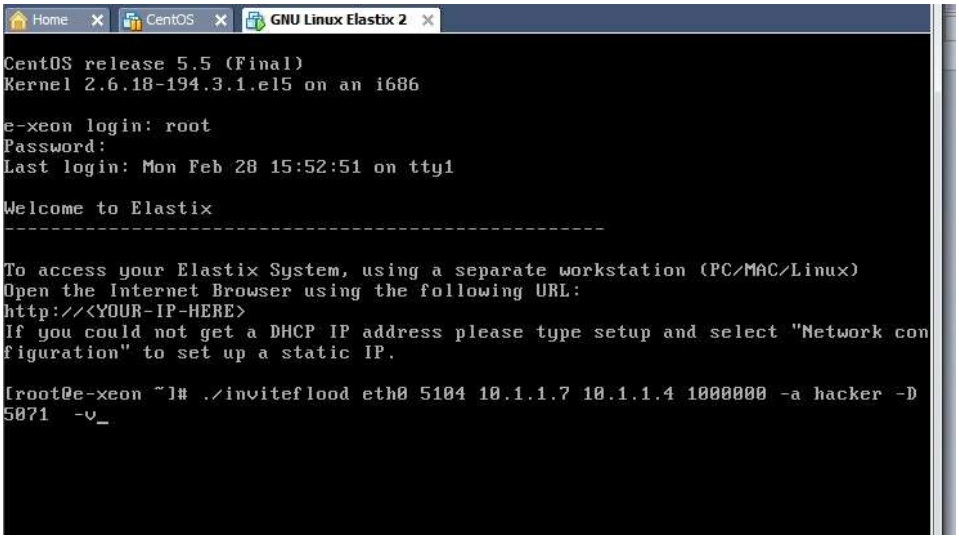
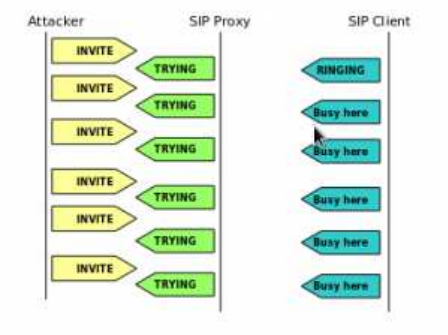


Fig.IV.37. Ejecución del ataque inviteflood.

De todos los nodos existentes en la red VoIP se decidió realizar el ataque hacia la dirección 10.1.1.5 que corresponde a la extensión ***"Ventas"***

Hacia Asterisk. El comportamiento sería de esta forma:



Esto causa una denegación de servicio hacia los sip client validos, lo cual es sumamente peligroso.

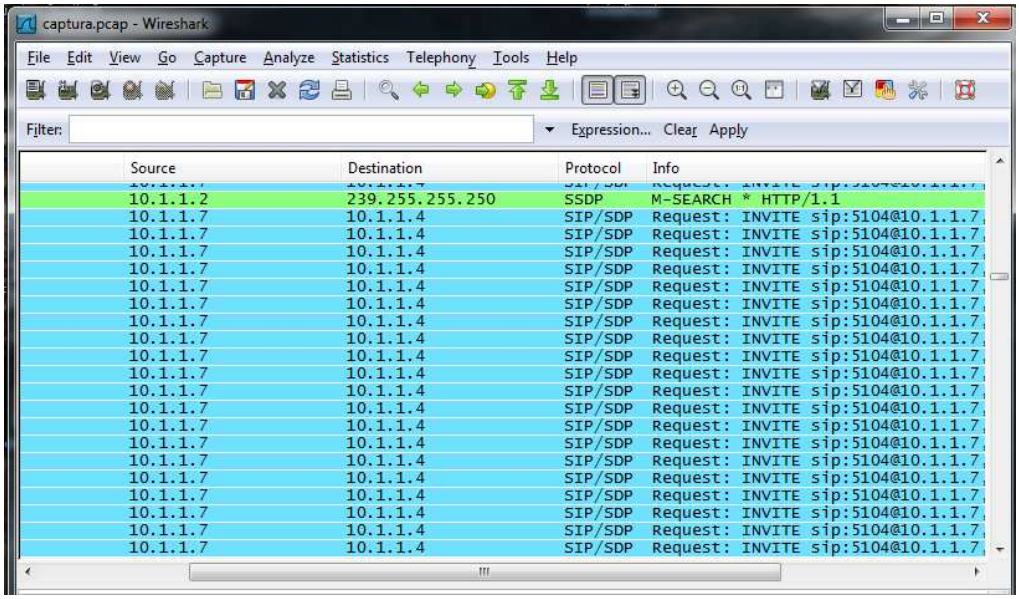


Fig.IV.38 Captura con Wireshark de paquetes INVITE hacia el servidor

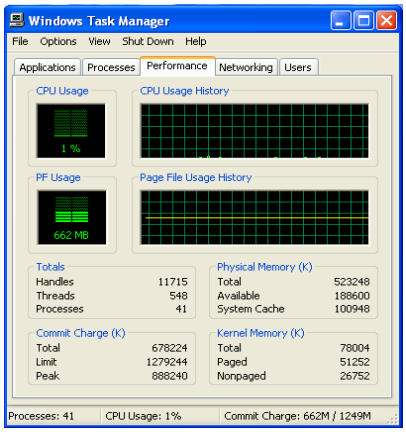
Se obtuvo los siguientes resultados:

Nº de Paquetes	Resultado
100	**Uso de CPU:** 11.17%, **Uso de la Memoria:** 29.88%. Aún es posible realizar llamadas entre las extensiones internas y hacia la PSTN.
1000	**Uso de CPU:** 12%, **Uso de la**

	Memoria: 29.90%. Aún es posible realizar llamadas entre las extensiones internas y hacia la PSTN.
10000	**Uso de CPU:** 42%, **Uso de la Memoria:** 29.92%. Aún es posible realizar llamadas entre las extensiones internas y hacia la PSTN.
100000	**Uso de CPU:** 45%, **Uso de la Memoria:** 39.50%. Aún es posible realizar llamadas entre las extensiones internas y hacia la PSTN.
1000000	**Uso de CPU:** 96%, **Uso de la Memoria:** 40.3%. En éste punto durante el ataque existe tono de marcado pero cualquier intentopara iniciar una conexión falla.

Tabla.III.4. Resultado de Mensajes Inviteflood en Servidor

Para que dicho ataque tenga efecto fue necesario esperar aproximadamente 60 minutos ya que se esta haciendo la petición enviando 1000000 paquetes. Luego de transcurrido este tiempo el sistema sufre un colapso.



4.3 PROPUESTAS DE SEGURIDAD

De acuerdo al análisis anterior nos pudimos dar cuenta que SIP es sensible a diversos tipos de ataques, pero si uno de estos ataques tiene éxito puede dejar no operativa las redes de voz de una empresa.
La flexibilidad y apertura de SIP ha hecho que sea un aspecto clave de la Voz sobre IP (VoIP), pero también hace que estas redes sean vulnerables a ataques que pueden provocar que no esté operativo el servicio durante días.

SIP está sujeto a ataques como de Denegación de Servicio (DoS), Interceptación de llamadas, Decifrado de contraseñas, entre otras, pero cuando uno de estos tiene éxito en SIP seguramente tiene un mayor impacto en las redes afectadas.
Por último, el análisis pretende ofrecer una serie de cuestiones importantes a tener en cuenta a la hora de abordar la seguridad de un entorno VoIP.

4.3.1 PROBLEMA: ESCUCHAS ILEGALES/CRACKEO DE CONTRASEÑAS.

Ya que son bien conocidas las vulnerabilidades de las redes IP sobre las que se envía los paquetes de voz, hemos planteado algunos requerimientos de seguridad a la hora de implementar VoIP, entre las cuales podemos anotar:

1. Protección de la privacidad de la conversación de la llamada.
2. Protección de los servidores de la red y los terminales contra amenazas bien conocidas tales como "negación del servicio" y "ataque del hombre en medio".

Aunque no puede haber un sistema completamente seguro, sí hay que tomar ciertas medidas para que las vulnerabilidades sean mínimas.
Primero hemos planteado la implementación de una VPN la cual permitirá encriptar todo el tráfico transmitido en la red, impidiendo de ésta manera descifrar contraseñas, además de que se evitará reproducir una conversación entre cualquier punto de la red, como lo pudimos demostrar anteriormente mediante la utilización de ciertos sniffers.

Autenticación en SIP

Debido a que el protocolo SIP utiliza la autenticación digest para la autenticación de los clientes. La autenticación digest es un mecanismo simple de autenticación desarrollada originalmente para HTTP. El mecanismo de autenticación es muy

simple, está basado en hashes criptográficos que evitan que se envíe la contraseña de los usuarios en texto claro.
La autenticación digest verifica que las dos partes que se comunican conocen un secreto compartido, que es la contraseña. Cuando un servidor quiere autenticar a un usuario, genera un desafío digest y se lo manda al usuario.

MEDIDA CONTRARRESTARIA.

OpenVPN es una solución de conectividad basada en softwareVPN Virtual Private Network (red virtual privada), OpenVPN ofrece conectividad punto-a-punto con validación jerárquica de usuarios y host conectados remotamente
Las VPN's se usan generalmente para:

- Conexión entre diversos puntos de una organización a través de Internet.
- Conexiones de trabajadores domésticos o de campo con IP's dinámicas.
- Soluciones extranet para clientes u organizaciones asociadas con los cuales se necesita intercambiar cierta información en forma privada pero no se les debe dar acceso al resto de la red interna.
- Además brinda una excelente fiabilidad en la comunicación de usuarios móviles así como también al unir dos puntos distantes como agencias de una empresa dentro de una sola red unificado.

También es posible establecer túneles en la capa de aplicación y de hecho son ampliamente utilizados hoy en día siendo algunas aproximaciones soluciones como SSL6 y TLS7. El usuario accede a la VPN de la organización a través de un browser iniciando la conexión en un sitio web seguro (HTTPS-Secured website).
Además, existen otros productos como SSL-Explorer y otros que ofrecen una combinación de gran flexibilidad, seguridad fuerte y facilidad de configuración. La seguridad es lograda mediante cifrado del tráfico usando mecanismos SSL/TLS, los cuales han probado ser muy seguros y están siendo constantemente sometidos a mejoras y pruebas.

¿Qué es OpenVPN?

OpenVPN es una excelente nueva solución para VPN que implementa conexiones de capa 2 o 3, usa los estándares de la industria SSL/TLS para cifrar y combina todos las características mencionadas anteriormente en las otras soluciones VPN. Su

principal desventaja por el momento es que hay muy pocos fabricantes de hardware que lo integren en sus soluciones. De todos modos no hay que preocuparse siempre que contemos con un Linux en el cual podremos implementarlo sin ningún problema mediante software.

Seguridad en VPN

Para cifrar datos se usan Passwords o claves de cifrado.
OpenVPN tiene dos modos considerados seguros, uno basado en claves estáticas pre-compartidas y otro en SSL/TLS usando certificados y claves RSA.
Cuando ambos lados usan la misma clave para cifrar y descifrar los datos, estamos usando el mecanismo conocido como "clave simétrica" y dicha clave debe ser instalada en todas las máquinas que tomarán parte en la conexión VPN.
Si bien SSL/TLS + claves RSA es por lejos la opción más segura, las claves estáticas cuentan con la ventaja de la simplicidad.

Las VPNs proveen seguridad a través de tres factores: privacidad, integridad yautenticidad. Para garantizar una transmisión segura de la información a través deredes compartidas. Además VPN utiliza las siguientes tecnologías:

- **Encriptación,** provee privacidad y seguridad de la información por medio dela aleatorización y desaleatorización de los datos. La seguridad de losdatos se logra usando varios esquemas de encriptación.
- **IPSec,** este tipo de encriptación protege la identidad y dirección IP de lafuente y de el destinatario y permite la transmisión de los datos a través deredes que no tienen habilitado IPSec.
- **Protocolos de tunneling,** el denominado tunneling es el proceso deencapsular un tipo de paquete dentro de otro tipo de paquete de tal formaque los datos puedan ser transportados por caminos que de otra forma nose podrían utilizar. Para crear un túnel, la fuente encapsula la informaciónen paquetes IP para transmitirlos a través del Internet.
- **Autorización,** a diferencia de la autenticación que se usa para permitir odenegar el acceso, la autorización se refiere a las características yprivilegios que tienen permitidos los usuarios. Una vez que los procesos deautenticación y autorización se han completado, se establece el túnel VPNy el usuario puede enviar datos a través del túnel.El nivel de seguridad que se tenga depende del protocolo seleccionado, delmétodo de encriptación

y del método de autenticación. La implementación deIPSec en BCM usa los protocolos ESP (Encapsulating Security Payload) y AH(Authentication Header). ESP provee confidencialidad de los datagramas IPmediante la encriptación de la porción de información o payload. AH por otro ladoprovee integridad y autenticación de la fuente pero no encriptación de lainformación.

IMPLEMENTACIÓN DE OPENVPN

Este método se usará como contramedida de protección ante los ataques analizados a lo largo de este proyecto, ya que el uso de VPNspermitirá al sistema VoIP usar aplicaciones y enviar datos a través de este de forma segura.

De acuerdo a lo dicho anteriormente a continuación se procede a realizar los pasos para crear tuneles con lo cual se demuestra que al realizar este proceso esta en marcha el uso de la encriptación necesaria que se requiere para dar seguridad a los datos.
Para la implemetación de la VPN se realizó el siguiente proceso:

- Instalamos el paquete de Openvpn disponible que en nuestro caso fue el openvpn-2.1.4.

```
yum install openvpn
cd /etc/openvpn/
cp -R /usr/share/doc/openvpn-2.1.4/easy-rsa/ /etc/openvpn
```

- Damos los permisos necesarios para hacer a los archivos ejecutables y a continuación utilizando el editor de texto editamos el archivo /etc/openvpn/easy-rsa/2.0/vars en las últimas líneas, creando de esta forma nuestro certificado.

```
------------
# These are the default values for fields
# which will be placed in the certificate.
# Don't leave any of these fields blank.
export KEY_COUNTRY="EC"
export KEY_PROVINCE="CH"
export KEY_CITY="Riobamba"
export KEY_ORG="OpenVPN Solution Ecuador"
export KEY_EMAIL="webmaster@opensolution.org.ec"
```

- Se requiere ejecutar del siguiente modo el fichero **/etc/openvpn/vars** a fin de que carguen las variables de entorno que se acaban de configurar.

```
./etc/openvpn/easy-rsa/2.0/vars
```

- A continuación creamos el certificado del servidor:

```
[root@localhost 2.0]# . /etc/openvpn/easy-rsa/2.0/build-ca
Generating a 1024 bit RSA private key
.....................................................................
.....................................................++++++
.........................++++++
writing new private key to 'ca.key'
-----
Country Name (2 letter code) [EC]:
State or Province Name (full name) [CH]:
Locality Name (eg, city) [Riobamba]:
Organization Name (eg, company) [OpenVPN Solution Ecuador]:
Organizational Unit Name (eg, section) []:Systems
Common Name (eg, your name or your server's hostname) [OpenVPN
Solution Ecuador CA]:elastix.opensolution.org.ec
Name []:Magaly
Email Address [webmaster@opensolution.org.ec]:

Certificate is to be certified until Mar 10 19:23:24 2021 GMT (3650
days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

- Se crea el fichero dh1024.pem, el cual contendrá los parámetros del protocolo **D**iffie-**H**ellman, de 1024 bits:

```
[root@localhost 2.0]# . /etc/openvpn/easy-rsa/2.0/build-dh
Generating DH parameters, 1024 bit long safe prime, generator 2
This is going to take a long time
.....................................................+.........+....
.............................................+.......................
............+..........................................................
......+......+.....................................+..........
.....................................................+.............
.........................+...................+..................+.......
...........+......+.....................................................
.....................................................................
.....................................................................+....
.....................................................+..+.....+...
.....................................................................
.....................................................................+..
............+...++*++*++*
```

- Generamos la firma digital utilizando el siguiente mandato:

```
/etc/openvpn/easy-rsa/2.0/build-key-server server
Generating a 1024 bit RSA private key
.++++++
...........++++++
writing new private key to 'server.key'
-----
Country Name (2 letter code) [EC]:
State or Province Name (full name) [CH]:
Locality Name (eg, city) [Riobamba]:
Organization Name (eg, company) [OpenVPN Solution Ecuador]:
Organizational Unit Name (eg, section) []:Systems
Common Name (eg, your name or your server's hostname)
[server]:elastix.opensolutions.org.ec
Name []:Magaly
Email Address [webmaster@opensolution.org.ec]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:administrador
An optional company name []:Open Solution Ecuador
Using configuration from /etc/openvpn/easy-rsa/2.0/openssl.cnf
Check that the request matches the signature
-------
Certificate is to be certified until Mar 10 19:23:24 2021 GMT (3650
days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

- Creamos el certificado del cliente:

```
[root@localhost 2.0]# . /etc/openvpn/easy-rsa/2.0/build-key client1
Generating a 1024 bit RSA private key
.....++++++
.................................................++++++
writing new private key to 'client1.key'
-----
Country Name (2 letter code) [EC]:
State or Province Name (full name) [CH]:
Locality Name (eg, city) [Riobamba]:
Organization Name (eg, company) [OpenVPN Solution Ecuador]:
Organizational Unit Name (eg, section) []:Systems
Common Name (eg, your name or your server's hostname)
[server]:elastix.opensolutions.org.ec
Name []:Magaly
Email Address [webmaster@opensolution.org.ec]:

-----
```

```
You are about to be asked to enter information that will be
incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or
a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [EC]:
State or Province Name (full name) [CH]:
Locality Name (eg, city) [Riobamba]:
Organization Name (eg, company) [OpenVPN Solution Ecuador]:
Organizational Unit Name (eg, section) []:Systems
Common Name (eg, your name or your server's hostname)
[client1]:elastix.opensolutions.org.ec
Name []:Magaly
Email Address [webmaster@opensolution.org.ec]:

Certificate is to be certified until Mar 10 19:26:58 2021 GMT (3650
days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

- Cramos la llave ta.key necesaria para generar la clave secreta en el servidor, este archivo se transferirá a cada cliente también.

```
openvpn --genkey --secret ta.key
```

- Copiamos los archivos generados a los directorios correspondientes.

```
cp ca.crt ca.key ta.key dh1024.pem server.crt server.key /etc/openvpn
cp /usr/share/doc/openvpn-2.1.4/sample-config-files/server.conf
/etc/openvpn
cp /usr/share/doc/openvpn-2.1.4/sample-config-files/client.conf ~/
```

- Editamos el archivo server.conf para permitir que los certificados sean utilizados por varios clientes.

```
vi /etc/openvpn/server.conf
...
duplicate-cn
...
;tls-auth ta.key 0 # This file is secret
tls-auth ta.key 0
...
;push "dhcp-option DNS 208.67.220.220"
```

```
push "dhcp-option DNS 10.8.0.1"
```

- Editamos el archivo client.conf para asignar la dirección IP de nuestro servidor Elastix que es la 10.1.1.4 y el puerto 1194 utilizado para la comunicación OPENVPN.

```
Vi client.conf
...
remote 10.1.1.4 1194
;remote my-server-2 1194
...
ca ca.crt
cert client1.crt
key client1.key
```

- Editamos el archivo sysctl.conf para realizar el enrutamiento de las direcciones y guardamos los cambios.

```
vi /etc/sysctl.conf
...
# Controls IP packet forwarding
net.ipv4.ip_forward = 1
...
[root@localhost ~]# echo 1 > /proc/sys/net/ipv4/ip_forward
```

- Creamos las reglas de iptables para que el servidor acepte el tráfico OPENVPN

```
/etc/rc.d/firewall/firewall.ipt

iptables -A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A FORWARD -s 10.8.0.0/24 -j ACCEPT
iptables -A FORWARD -j REJECT
iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -o eth0 -j MASQUERADE
```

- Para iniciar el servicio de openvpn ejecutamos el comando.

```
service openvpn start
```

- Para realizar un seguimiento de las conexiones hacia el servidor ejecutamos el siguiente comando:

tail -f /var/log/messeges

- Una vez configurado el servidor OPENVPN, empezamos con la instalación del cliente Windows.

  Para esto descargamos de la página http://www.openvpn.net el cliente OpenVPN-2.1.4 como se muestra:

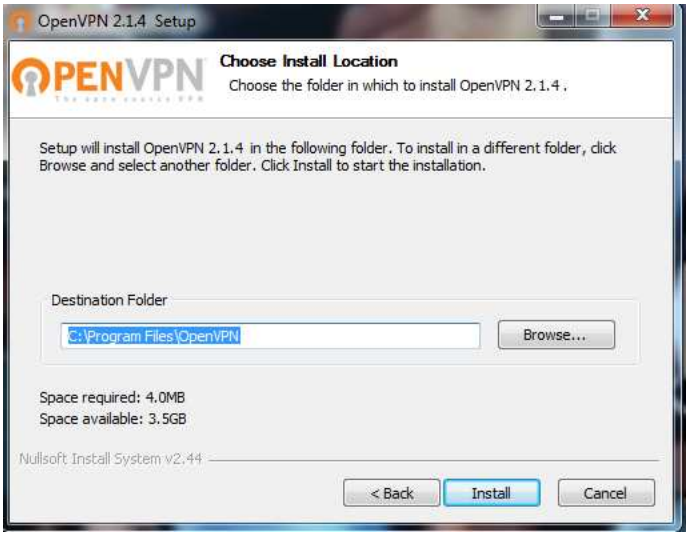


Fig. IV.39. Instalación de cliente OPENVPN en Windows

- Una vez instalado, copiamos los archivos configurados en el servidor como son: ca, ca.key, client1, client.csr, cliente.key, dh1024.pem, index, index.text.attr, ta.key, y los guardamos en la dirección C:\Archivos de programa\OpenVPN\config, de Windows.

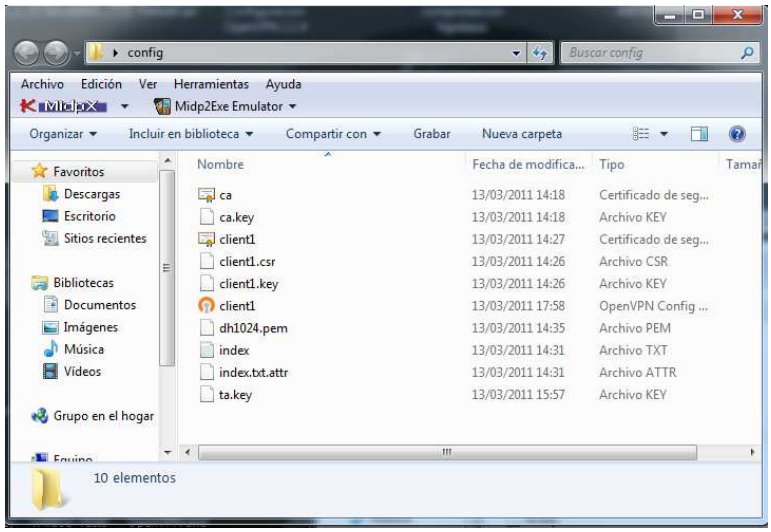


Fig. IV.40. Contenido de certificado OPENVPN en Windows

- Le damos permiso al programa para que se ejecute como administrador, vamos *Inicio* y en icono de OpenVPN GUI le damos clic en Propiedades/Compatibilidad y marcamos la opción de ejecutar este programa como administrador.

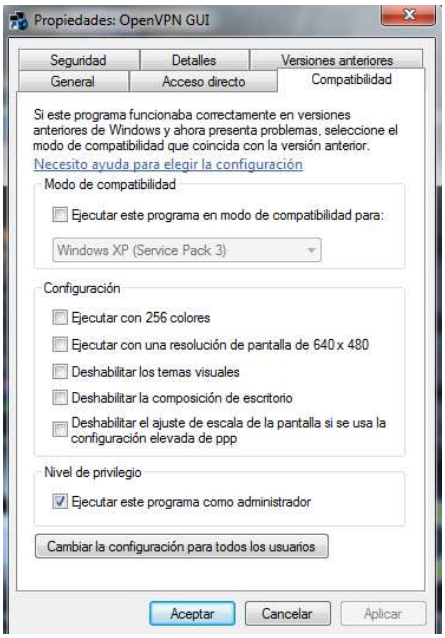


Fig. IV.41. Ejecución de OPENVPN en Windows como administrador

- Para conectarnos con el servidor OpenVPN damos clic derecho en el ícono y escogemos la opción Connect, de esta forma nos comunicaremos hacia el servidor Elastix por medio del túnel.

Fig. IV.42. Conexión de cliente OPENVPN en Windows

Al hacer clic en la opción Connect, aparece una ventana de notificación que muestra los procesos de verificación e intento de conexión al servidor VPN, con la última línea que indica "Initialization sequence completed".

Con esto, tal como se observa en la Fig.IV.53, el icono de notificación del cliente OpenVPN se muestra de color verde y muestra un valor aleatorio IP correspondiente a la red VPN.

Fig.IV.43 Mensaje de notificación al conectarse al servidor VPN

Esta IP puede ser vista también en el Command device de Windows con el comando ipconfig.

- Por último configuramos el sotfphone para que se conecte con la IP LAN del servidor y ya podemos conectarmos a la vpn en el servidor de Elastix.

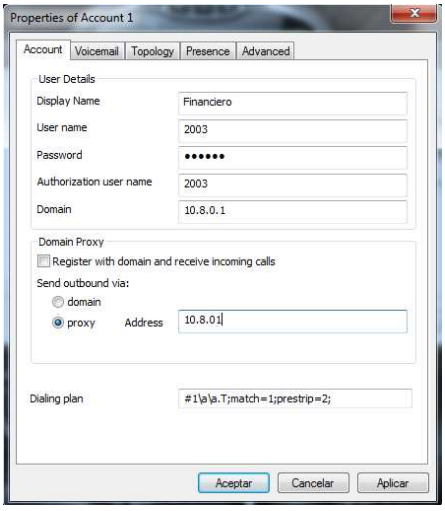


Fig.IV.44. Configuración de softphone Xlite con IP de Servidor OpenVPN.

- La configuración final del cliente OpenVPN Windows es la siguiente:

```
client
dev tun
proto udp
remote 10.1.1.4 1194
resolv-retry infinite
nobind
persist-key
persist-tun

# SSL/TLS parms.
ca ca.crt
```

```
cert client1.crt
key client1.key
ns-cert-type server
dh dh1024.pem
tls-auth ta.key 1
#cipher DES-CFB

# Set log file verbosity.
verb 3
mute 20
keepalive 10 120
comp-lzo

float
route 10.8.0.0 255.255.255.0
```

4.3.3.1 RESULTADO

Cada cliente al estar conectado mediante el túnel VPN se crea una red virtual y se asigna un nuevo segmento de red proporcionada por el servidor principal en este caso la 10.8.0.0/255.255.255.0.

El servidor VPN hace de pasarela para que todos los clientes puedan estar comunicados a través del túnel OpenVPN, por lo que todo el tráfico intercambiado entre éstos viajará encriptado haciendo que no sea posible la extracción de audio, si existe la captura de cualquier información de la red ésta estará cifradaproporcionando una conexión segura entre las máquinas impidiendo a cualquier atacante tener información que le resulte beneficiosa sobre nuestra red.

Observamos que al momento de configurar el tunel el protocolo por defecto que se configura para seguridad de la información es el protocolo TLS el cual es importante para que los datos tengan una mayor protección ante cualquier interceptación de un atacante.

Creando túneles entre el servidor y cada uno de los usuarios de la PBX, una máquina intrusa al tratar de capturar paquetes que no le corresponden lo hará por la interfaz que la une a la red VoIP, no logrando interceptar paquetes de la red, ya que estos pasaran a través de los túneles VPN.Todos los datos que se transmiten entre clientes y servidor estarán totalmente encriptados a través de una clave RSA.

4.3.2 PROBLEMA: DENEGACIÓN DE SERVICIO.

Ya hemos hecho énfasis en los principales peligros a los que se enfrenta la tecnología de "VoIP". Resumiendo, destacan los problemas de Denegación de

Servicio (DoS), que afectan a la disponibilidad del servicio de "VoIP"; o los Accesos No Autorizados que pueden terminar afectando la confidencialidad del servicio (escuchar de forma no autorizada, suplantación de identidad, robos del servicio de voz, redirección, etc.). En este sentido, el uso no autorizado del servicio es factible que genere un impacto económico elevado al realizar llamadas internacionales o de larga distancia.

Desafortunadamente, al inicio del diseño de hardware, software y protocolos para voz, la seguridad no siempre suele ser una prioridad, pero como todos sabemos esto es lo que siempre pasa cada vez que aparece una nueva tecnología. A continuación examinemos algunas opciones que previenen las amenazas sobre esta tecnología.

Una técnica común para mitigar las vulnerabilidades en el servicio de "VoIP" es la protección perimetral (IPS, firewalls, análisis avanzado de protocolos), la cual debe actualizarse para incorporar un nivel de seguridad proactivo adecuado frente a estas amenazas en los servicios de "VoIP"; inclusive hoy existen tecnologías de protección perimetral especializadas en VoIP.

MEDIDA CONTRARESTARIA

La seguridad de cualquier PC se puede mejorar mediante uncortafuegos. Este firewall puede ser configurado con un conjunto de reglas / comandos que resulta en forma flexible de la filtración el tráfico no deseado. Otro enfoque es usar la detección de intrusiones / Prevention System (IDS / IPS).

Sistemas de Detección de Intrusos y Snort.

Un IDS es una herramienta de seguridad que intenta detectar o monitorizar los eventos ocurridos en un determinado sistema informático en busca de intentos de comprometer la seguridad de dicho sistema.

Analiza todo el tráfico y las compara contra una base de datos (firmas de ataques ya conocidos) y si coinciden, el sistema muestra como una alerta, estas alertas pueden ser monitoreadas desde una interfaz web, también se puede configurar para que envie un correo a una cuenta predefinida.

Posee varias características como:

- Los IDS buscan patrones previamente definidos que impliquen cualquier tipo de actividad sospechosa o maliciosa sobre nuestra red o host.
- Los IDS aportan a nuestra seguridad una capacidad de prevención y de alerta anticipada ante cualquier actividad sospechosa. No están diseñados para detener un ataque, aunque sí pueden generar ciertos tipos de respuesta ante éstos.
- Los IDS aumentan la seguridad de nuestro sistema, vigilan el tráfico de nuestra red, examinan los paquetes analizándolos en busca de datos sospechosos y detectan las primeras fases de cualquier ataque como pueden ser el análisis de nuestra red, barrido de puertos, etc.

CREACIÓN DE IPTABLES

El problema más frecuente en las redes Voip es la Denegación de Servicio, una opción para evitar éste problema es implementar un firewall, que permitirá filtrar el tráfico entre la red estableciendo unas reglas de filtrado con las que se decide si una conexión determinada puede establecerse o no, de ésta manera se decide si un paquete pasa, se modifica, se convierte o simplemente se descarta.
Los pasos seguidos son los siguientes:

1. Creamos un script de firewall iptables contiene normas para el filtrado del tráfico no deseado y la aceptación de los paquetes de VoIP tal como se muestra:

```
$IPTABLES -A INPUT -p udp -m state --
state NEW -m --dport 5060:5070 -j QUEUE
$IPTABLES -A INPUT -p udp -m state --
state NEW -m udp --dport 1024:5059 -j QUEUE
$IPTABLES -A INPUT -p udp -m state --
state NEW -m udp --dport 5071:65535 -j QUEUE
```

Después de la configuración de iptables, la siguiente fase fue diseñar un conjunto de reglas. Hay dos conjuntos de normas: las que sólo generan alerta scuando el tráfico malicioso es descubierto y la que da de baja a ciertos paquetes detectados.

La alerta se utiliza principalmente para el tráfico de la red interna esto se hizo como una medida de mitigación de los falsos positivos (donde paquetes legales por error pueden ser etiquetados como tráfico no deseado y se elimina). Las reglas se aplican

para todo el tráfico, así como para los mensajes que podrían ser identificados con ninguna duda siendo maliciosos.
Para la generación de alertas se utilizó un sistema potente denominado Snort el cual conlleva a un proceso de instalación de paquetes necesarios. Que se describen mas adelante.
Después de la instalación del paquete Snort se procede al establecimiento y ejecución de las reglas que permitirán alertar cuando un ataque de denegación de servicio se está efectuando.

Las reglas, permiten eliminar todo tráfico externo que llegase a ingresar al servidor, así como también alerta de los paquetes INVITE que lleguen y de esta manera darnos cuenta de que IP y porque puerto ingresan.

```
# Rules for SIP INVITE flooding
drop ip $EXTERNAL_NET any -> $HOME_NET 5060
(msg:"VOIP INVITE Message Flood";
content:"INVITE"; depth:6; threshold: type
threshold, track by_src, count 300, seconds
10;classtype:attempted-dos; sid:2003192;
rev:1;)

alert ip $HOME_NET any -> $SIP_PROXY_IP 5060
(msg:"VOIP INVITE Message Flood";
content:"INVITE"; depth:6; threshold: type
threshold , track by_src, count 300, seconds
10; classtype:attempted-dos; sid:2003193;
rev:1;)
```

INSTALACIÓN DE SNORT

A continuacion se dará una breve explicación de la instalación y configuración de Snort.

- Instalamos los paquetes necesarios:

 # yum -y install mysql mysql-bench mysql-server mysql-devel php-mysql httpd gcc pcre-devel php-gd gd mod_ssl glib2-devel gcc-c++ bison flex php-pear

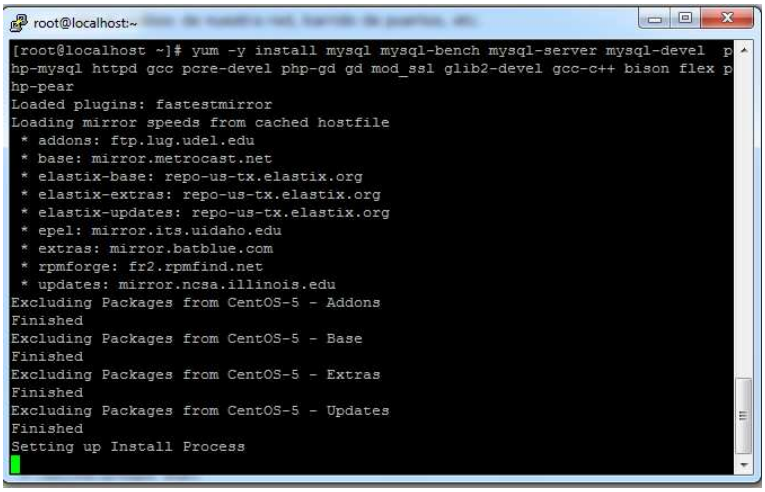


Fig.IV.45. Instalación de paquetes necesarios para Snort.

- Iniciamos los servicios de la base de datos y del apache.

```
# /etc/init.d/httpd start
# /etc/init.d/mysqld start
# chkconfig mysqld on
# chkconfig httpd on
```

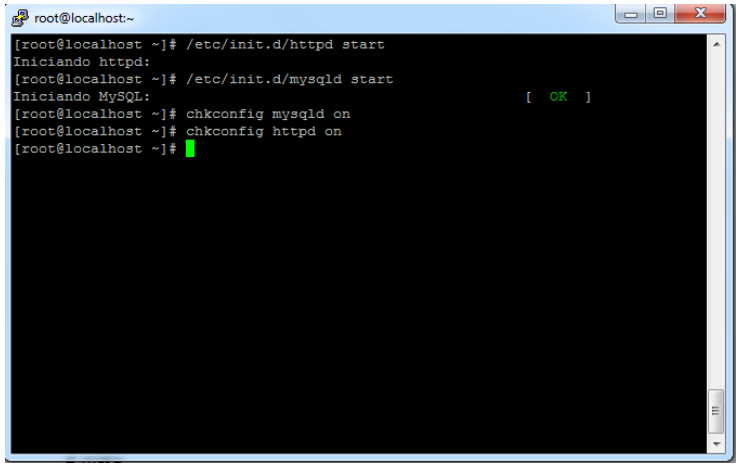


Fig. IV.46. Iniciando los servicios de la base de datos y apache.

- Crearemos nuestro directorio donde pondremos todos los paquetes que vayamos a utilizar.

```
# mkdir /etc/snortinstall
# cd /etc/snortinstall
# wget http://www.tcpdump.org/release/libpcap-1.0.0.tar.gz

#tar –vxfz libpcap-1.0.0.tar.gz
# cd libpcap-1.0.0
#./configure
# make
# make install
# cd ..
```

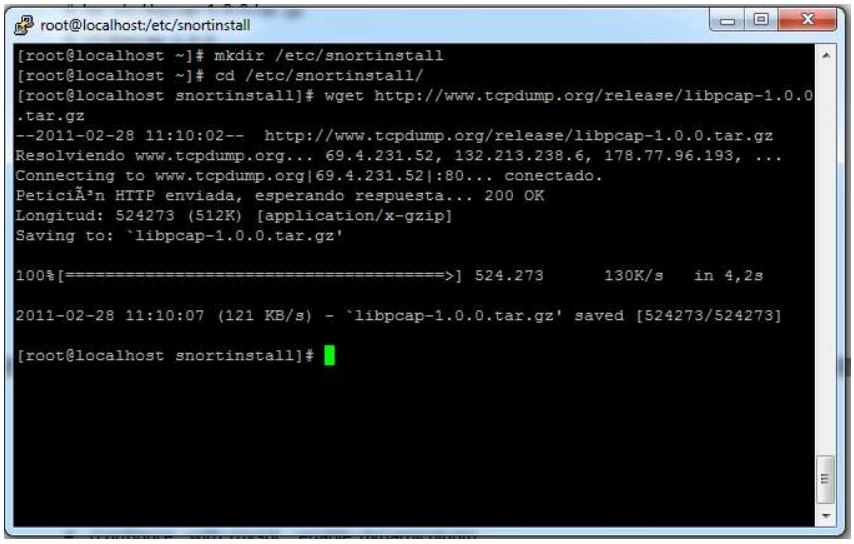


Fig.IV.47. Descargando libpcap-1.0.0.tar.gz

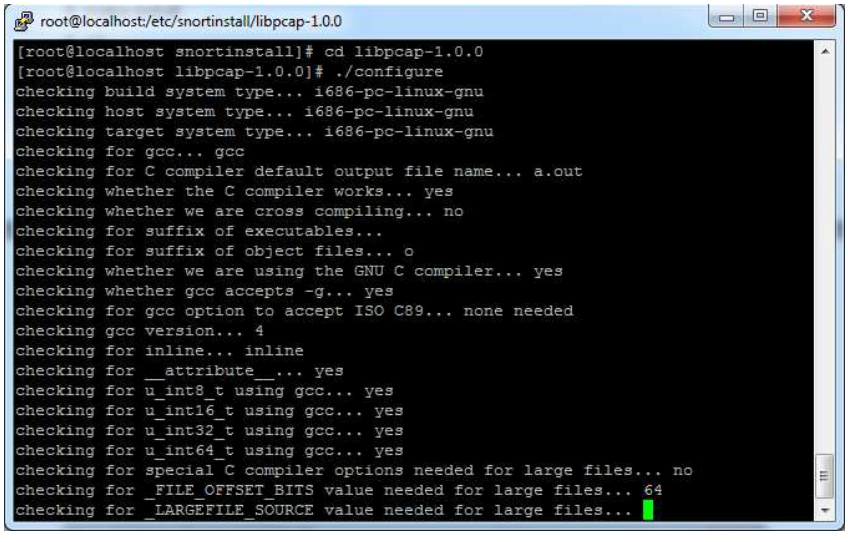


Fig.IV.48. Instalación de libpacap

```
# wget http://dl.snort.org/downloads/752
# tar xzf snort-2.9.0.4.tar.gz
# cd snort-2.9.0.4.
#./configure –with-mysql –enable-dynamicplugin
# make
# make install
```

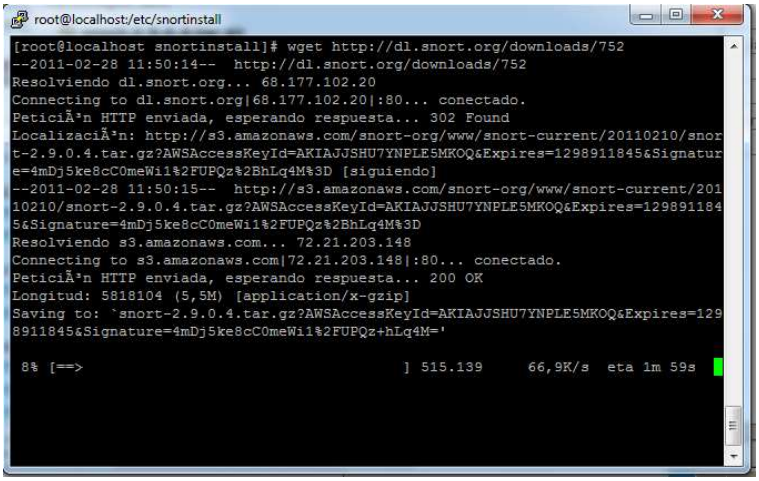


Fig.IV.49. Descargando snort-2.9.0.4.tar.gz

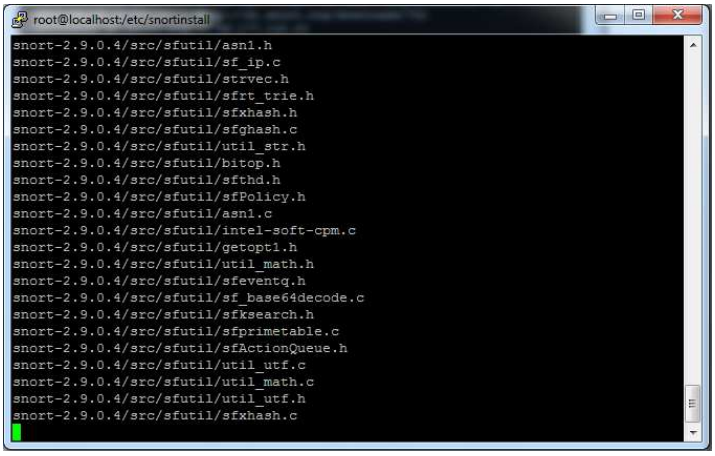


Fig.IV.50. Instalación de snort-2.9.0.4

- Una vez instalado, creamos un usuario Snort en el grupo Snort, creamos el directorio rules donde se agregarán las respectivas reglas, por último creamos el directorio snort bajo /etc y copiamos el instalador.

```
# groupadd snort
# useradd -g snort snort -s /sbin/nologin usuario1
# mkdir /etc/snort
# mkdir /etc/snort/rules
```

```
# mkdir /var/log/snort
# cp /etc/snortinstall/snort-2.9.0.4/* /etc/snort/
```

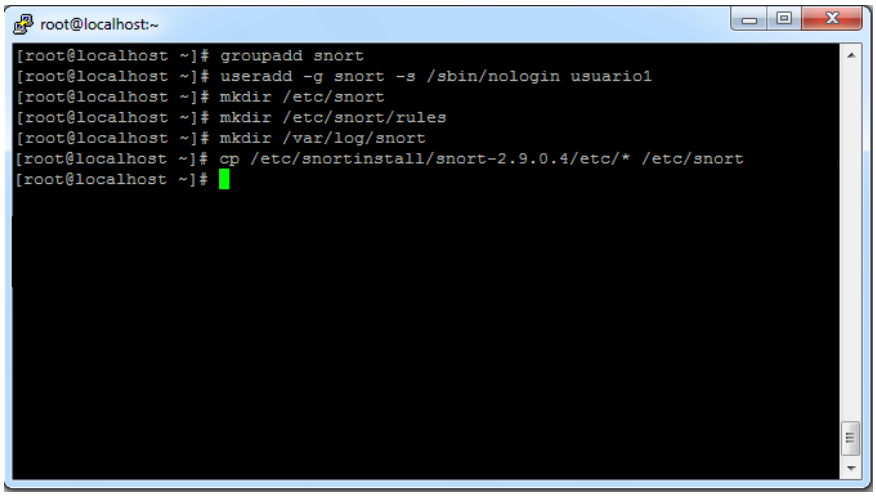


Fig.IV.51. Añadiendo un usuario Snort y copiando Snort a otro directorio.

- Ahora vamos a configurar nuestro Snort.

Accedemos al directorio:

```
# cd /etc/snort/
```

En el archivo snort.conf ingresaremos las reglas que nos permitirán alertar al servidor Elastix de algún ataque como el de inundación de mensajes INVITE.

```
# vi snort.conf
```

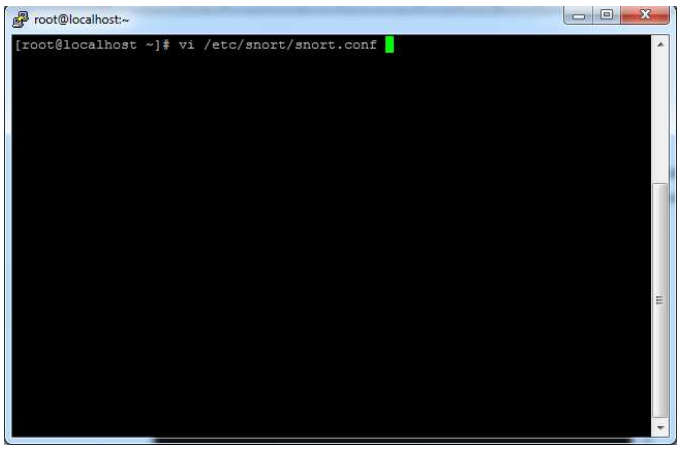


Fig.IV.52. Accediendo al directorio snort.conf

En el archivo snort.conf existe una regla que permite alertar sobre los ataques de inundación de mensajes INVITE hacia el servidor, mostrando el mensaje: "VOIP INVITE Message Flood", lo que nos indica que se está generando el envío de una

gran cantidad de mensajes INVITE mediante la herramienta de denegación de servicio Inviteflood, cuyo ataque lo describimos anteriormente.

A demás elimina cualquier acceso a la red de redes externas, de esta forma controlamos la red evitando accesos no autorizados o desconocidos.

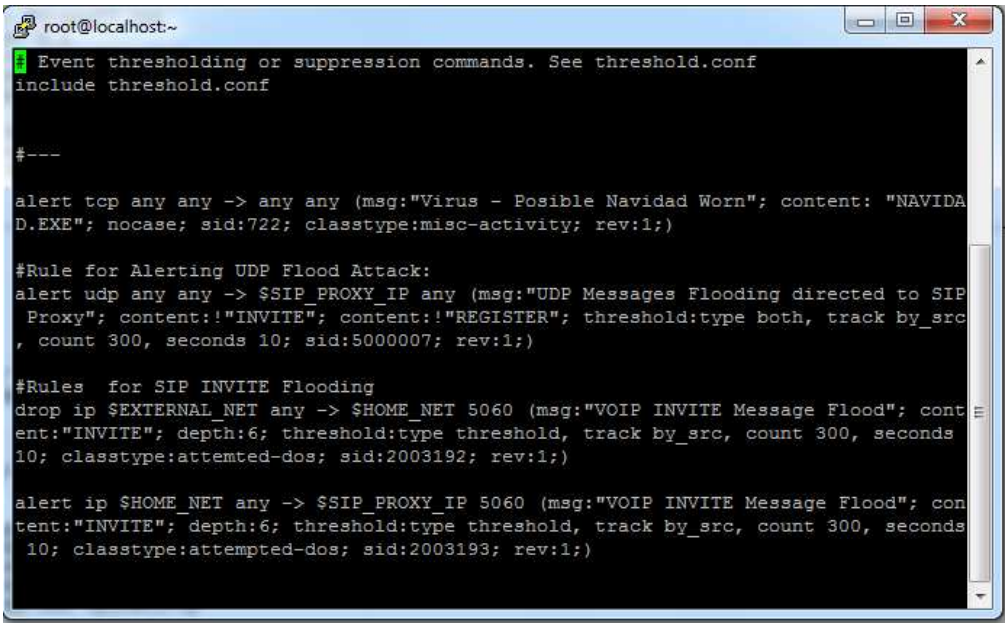


Fig.IV.53. Reglas para la alerta de Inundación de Mensajes INVITE.

- Ahora configuraremos nuestra base de datos mysql para registrar todos los eventos del snort.

```
# mysqladmin -u root password ‘contraseña’

# mysqladmin create snort -p
Enter password:
# cd /etc/snortinstall/snort-2.9.0.4
# mysql -p snort < schemas/create_mysql
Enter password:
# mysql -p
Enter password:

mysql> grant all privileges on snort.* to snort@localhost identified
by ‘contraseña’
```

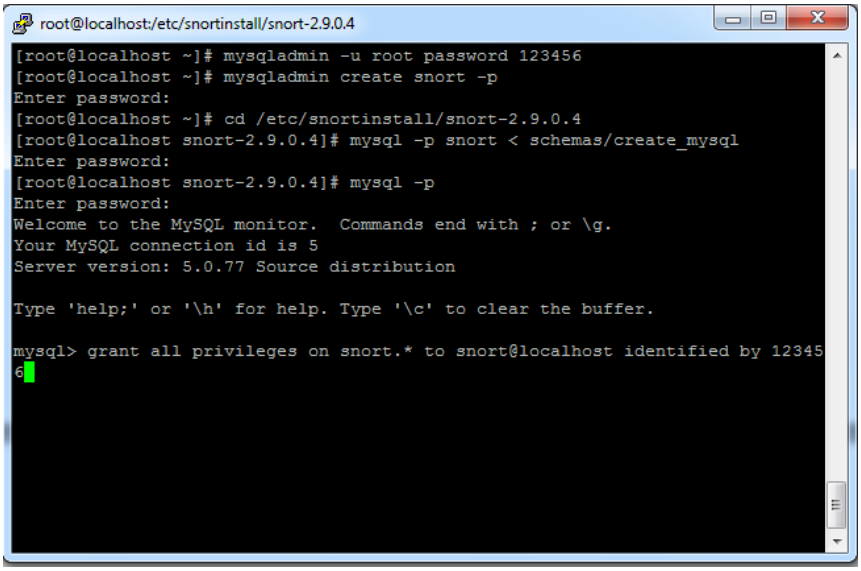


Fig.IV.54. Configuración de Base de datos.

- A continuación vamos a hacer que el snort registre todo en la base de datos mysql, para ello nuevamente editamos el snort.conf descomentamos la línea de output database para que quede de la siguiente manera:

 # vi snort.conf

output database: log, mysql, user=snort password=contraseña dbname=snort sensor_name=LAN host=localhost

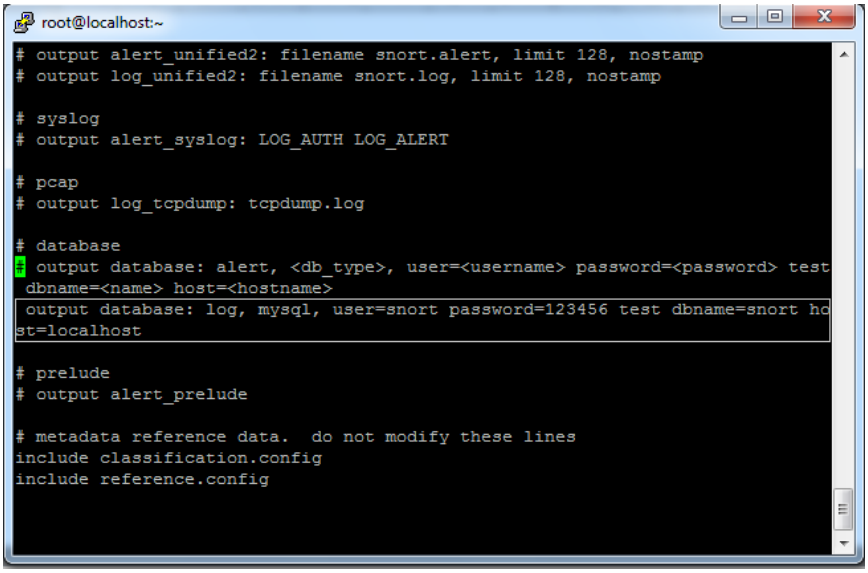


Fig.IV.55. Registro de Base de datos en Snort.

Hecho esto, vamos a configurar la interfaz web para monitorear el IDS.

- Nos ubicamos nuevamente en /etc/snortinstall/

 # cd /etc/snortinstall/

 # pear install –alldeps Image_Graph-alpha Image_Canvas-alpha Image_Color Numbers_Roman

 # wget http://downloads.sourceforge.net/project/adodb/adodb-php5-only/adodb-509a-for-php5/adodb509a.tgz

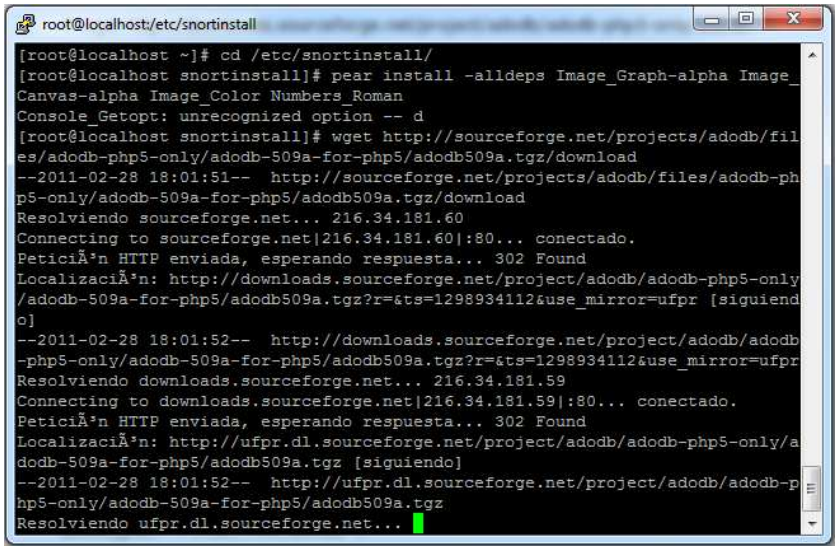


Fig.IV.56. Descarga de adodb

 # wget http://downloads.sourceforge.net/project/secureideas/BASE/base-1.4.4/base-1.4.4.tar.gz

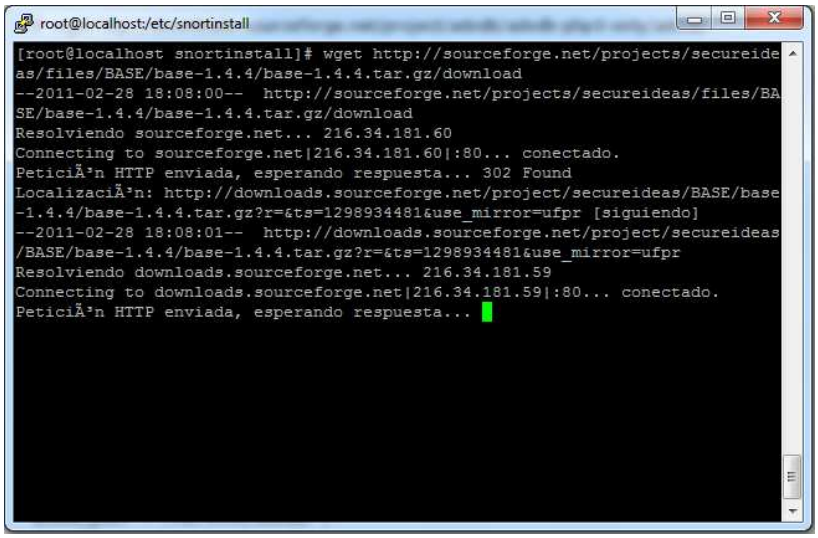


Fig.IV.57. Descarga de base-1.4.4

```
# cd /var/www/
# tar xfz /etc/snortinstall/adodb509a.tgz
# mv adodb5 adodb
# cd html/
# tar xfz /etc/snortinstall/base-1.4.4.tar.gz
# mv base-1.4.4 base
# cd base/
# cp base_conf.php.dist base_conf.php
# vi base_conf.php

……

$BASE_urlpath = '/base';

$DBlib_path = '/var/www/adodb/ ';

$DBtype = 'mysql';
$alert_dbname   = 'snort';
$alert_host     = 'localhost';
$alert_port     = "";
$alert_user     = 'snort';
$alert_password = 'contraseña';

……
```

- Ahora accedemos via web

http://10.1.1.4/base le damos clic en Setup page, luego en create BASE AG finalmente en Man page

- Finalmente iniciamos el servicio de snort, ejecutando de la siguiente manera:

```
#/etc/rc.d/rc.snort start
```

4.3.1.1 RESULTADO:

Después de haber creado las respectivas reglas de permiso o denegación de paquetes que se realizó en la configuración de iptables y de las reglas para alertar de posibles ataques Inviteflood que puedan estar ejecutándose hacia el Servidor, es

necesario poner en marcha la protección del sistema Snort y sus alertas ejecutando:

Log de Snort:
tail -f /var/log/messages

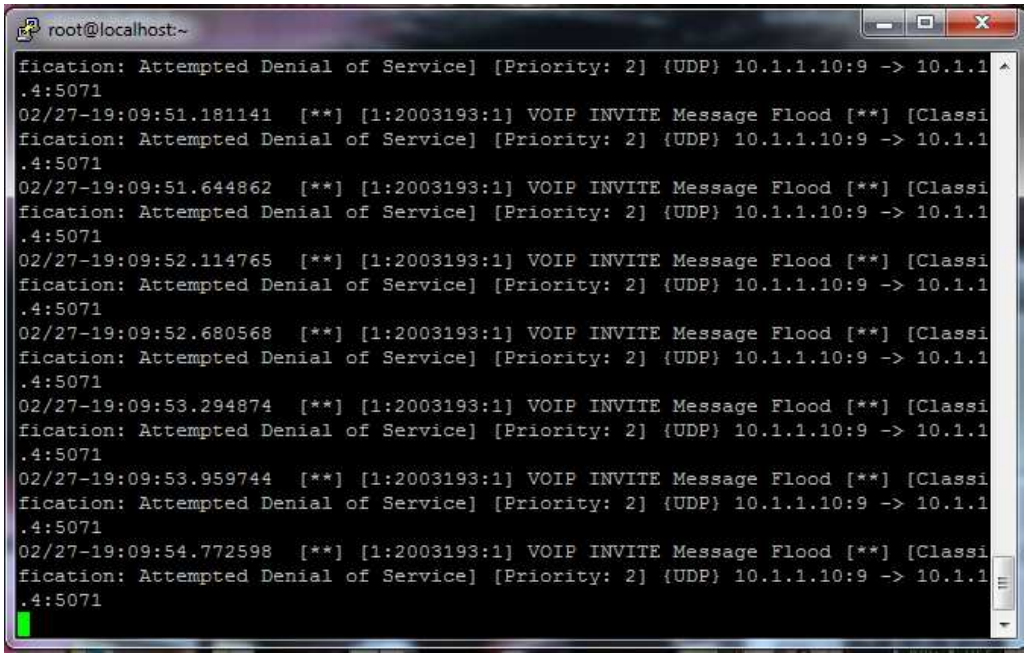


Fig.IV.58. Visualización de alertas mediante Snort.

Como podemos ver se consigue que la inundación de peticiones INVITE sea alertada, indicándonos las direcciones IP origen y destino así como sus respectivos puertos, con lo que podemos tomar las decisiones más adecuadas para evitar la saturación del servidor y con esto detener la denegación del servicio.

Una alternativa para evitar que se sigan recibiendo mensajes **INVITE** al conocer que se está produciendo un ataque es denegar el acceso a la dirección IP la cual está produciendo el ataque esto se haría mediante una regla de iptables asi:

```
#--------Bloqueo de Direcciones IP que Atacan al Servidor---------
echo -e "Bloqueo de Direcciones IP que Atacan al Servidor...$OK"
$IPTABLES -A INPUT -s 10.1.1.10 -j DROP
$IPTABLES -A INPUT -p tcp --dport 9 -j DROP
$IPTABLES -A INPUT -p udp --dport 9 -j DROP
```

Esto permite eliminar cualquier tráfico que venga de la dirección origen del ataque impidiendo así que los paquetes sigan accediendo al servidor.

4.4 Sugerencias Generales de Seguridad.

En los últimos tiempos han aparecido una serie de nuevas herramientas que hace posible a cualquier novato atacar y cometer fraudes en equipos SIP, incluyendo los sistemas basados en Asterisk.
Existen herramientas fácilmente disponibles que hacen un barrido de redes en busca de hosts que ofrezcan servicios SIP, luego, una vez encontrado, realiza un barrido en busca de extensiones y contraseñas.

Exiten ciertas reglas, de aplicación inmediata, que eliminan muchos de los problemas de seguridad, protegiendo al servidor Elastix de los barridos masivos y los ataques posteriores.

1) No aceptar pedidos de autenticación SIP desde cualquier dirección IP. Utilizar las líneas "permit=" y "deny=" de sip.conf para sólo permitir un subconjunto razonable de direcciones IP, alcanzar cada usuario/extensión listado en el archivo sip.conf. Aún aceptando llamadas entrantes desde "anywhere" (via [default]) no se debe permitir a esos usuarios alcanzar elementos autenticados.

2) Estblecer el valor de la entrada "alwaysauthreject=yes" en el archivo sip.conf. Esta opción está disponible desde la versión 1.2 de Asterisk, pero por defecto su valor es "no", lo que puede ser potencialmente inseguro. Estableciendo este valor en "yes" se rechazarán los pedidos de autenticación fallidos utilizando nombres de extensiones válidas con la misma información de un rechazo de usuario inexistente. De ésta forma no facilitamos la tarea al atacante para detectar nombres de extensiones existentes utilizando técnicas de "fuerza bruta".

3) Utilizar claves SEGURAS para las entidades SIP. Este es probablemente la más importante medida de seguridad. Como ya se demostró en los ataques realizados a las red existen programas que generan y prueban claves por fuerza bruta por lo cual nos podemos dar cuenta que se necesita algo más que palabras y números para una clave segura. Usar símbolos, números, una mezcla de letras minúsculas y mayúsculas y al menos 12 caracteres de largo.

4) Bloquear los puertos del Asterisk Manager Interface. Usar "permit=" y "deny=" en manager.conf para limitar las conexiones entrantes sólo a hosts conocidos. Una vez más utilizar claves seguras aquí también, 12 caracteres al menos en una combinación de números, letras y símbolos.

5) Permitir sólo una o dos llamadas por vez por entidades SIP cuando sea posible. Limitar el uso no autorizado de las líneas VoIp, esto también es útil para el caso que usuarios legítimos hagan pública su clave y pierdan control de su uso.

6) Los nombres de usuarios SIP deben ser diferentes que sus extensiones. A pesar de ser conveniente tener una extensión "1234" que mapee a una entrada SIP "1234" la cual es también el usuario SIP "1234", esto también facilita a los atacantes para descubrir nombres de autenticación SIP. En su ligar usar las direciones MAC del dispositivo, o alguna combinación de frases comunes + extensión MD5 hash (por ejemplo: desde el shell prompt, hacer "md5 -s ThePassword5000").

7) Asegurarse que el contexto [default] sea seguro. No permitir que llamadores no autenticados alcancen contestos que les permitan llamar. Permitr sólo una cantidad limitada de llamadas activas pasen por el contexto default (utilizar la función "GROUP" como contador). Prohibir totalmente las llamadas no autenticadas (si es que así lo queremos) estableciendo "allowguest=no" en la parte [general] de sip.conf.

Estos 7 puntos básicos nos protegen en la mayoría de los casos, pero hay otras medidas que se pueden tomar aunque son más complejas.

En resumen, las medidas básicas de seguridad nos protegerán contra la vasta mayoría de los ataques de fuerza bruta basados en SIP. Muchos de los atacantes SIP son "tontos con herramientas", oportunistas que ven una forma fácil de cometer fraudes. Asterisk tiene algunos métodos para prevenir los ataques más obvios a nivel de red, los métodos más efectivos de protección son cuestiones administrativas como la complejidad de las claves y nombres de usuarios.

CAPÍTULO V
ANÁLISIS DE RESULTADOS

A continuación, se mostrarán los resultados de las pruebas realizadas de la implementación del prototipo basado en el estudio del protocolo SIP. Se han probado dos diferentes escenarios:

- Escenario con implementación de seguridades.
- Escenario sin implementación de seguridades.

En estos dos escenarios los pasos que se siguen para la realización de las pruebas de vulnerabilidad son exactamente los mismos, al igual que todo el contexto de comunicación, excepto por la aplicación de las seguridades implementadas como son la activación del Snort y de la OpenVPN.

5.1. Resultados en escenario sin herramientas de seguridad

Se comenzará a explicar el escenario sin la aplicación de seguridades en la red, porque se necesitará después comparar y ver los resultados que arroja con la implementación de los mecanismos de seguridad descritos anteriormente.

Este escenario es el más simple ya que no hay ningún elemento extra que trate de garantizar la calidad de servicio ni mucho menos la seguridad de los paquetes de audio ni de los mensajes que se intercambian en el momento de la comunicación.

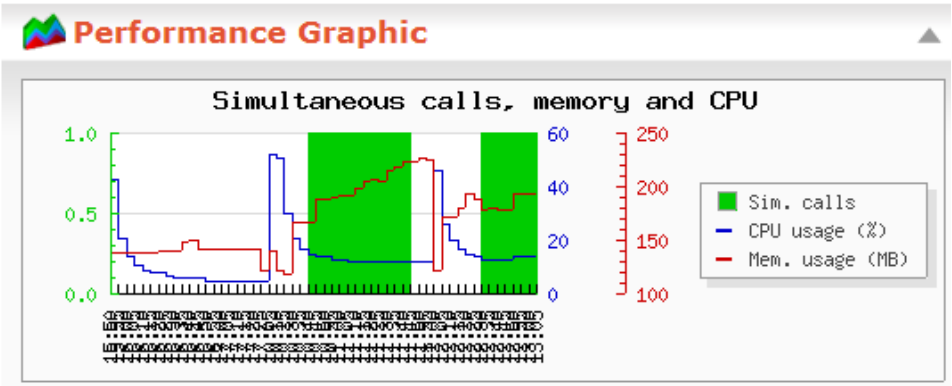


Fig. V.1. Consumo de recursos del sistema sin seguridad

En la Fig.V.1, se puede observar que el consumo de los recursos del sistema en lo que tiene que ver a la memoria llegó a ser del 96% debido a que necesita procesar

una gran cantidad de paquetes de forma casi simultánea a causa del ataque de inundación de peticiones invite, ocasionando que las comunicaciones tarden mucho tiempo en establecerse, llegando hasta el punto de impedir que estas se realicen mientras dura éste.

Lo mismo sucede con el uso del CPU que llegó a ser del 56% en el servidor Elastix.

Otras vulnerabilidades analizadas son la captura de paquetes de audio en la red ya que estos no viajan de forma encriptada pudiendo de esta manera ser capturados por cualquier sniffer como Wireshark y ver toda la información tanto de audio como de los mensajes de autenticación intercambiados durante el inicio de la sesión llegando a ser información muy importante a la cual se le puede dar un uso indebido.

En la Fig.V.3 podemos ver que se capturaron todos los paquetes intercambiados en la sesión VoIP como también las contraseñas de los softphones Fig.V.4, utilizadas como medio de autenticación con el servidor y en especial se pudo capturarlos paquetes RTP los cuales contiene la información de audio que pudo ser extraída sin problemas tal como muestra la Fig.V.5.

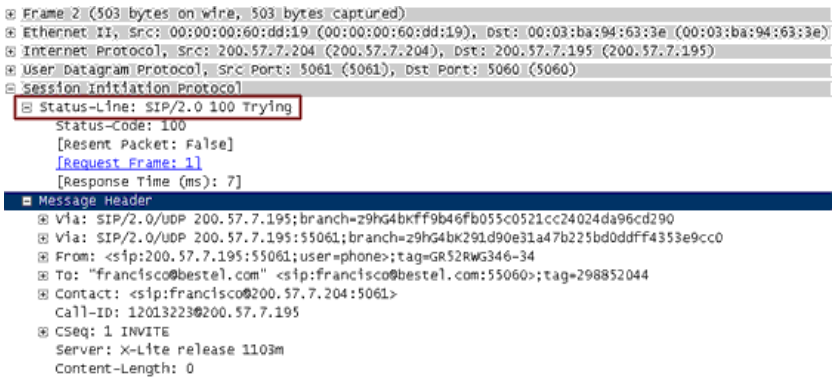


Fig. V.3. Captura de paquetes SIP y RTP.

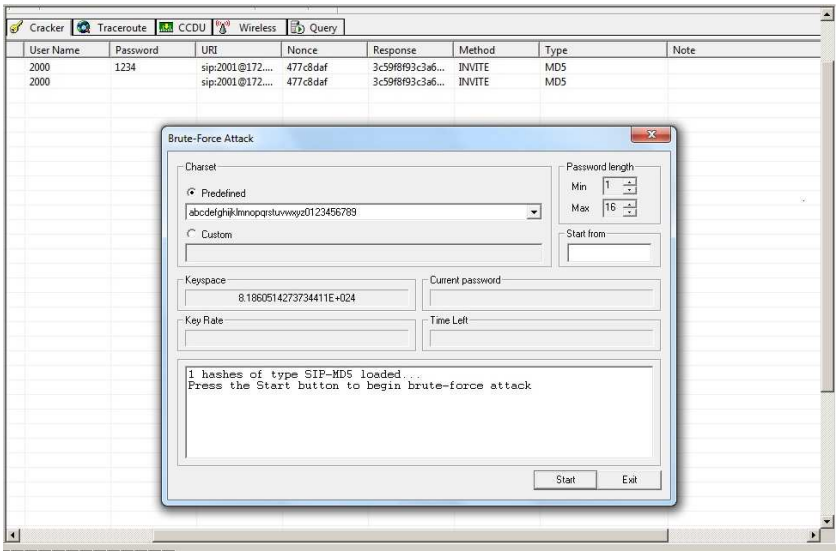


Fig. V.4. Captura de contraseñas de softphones.

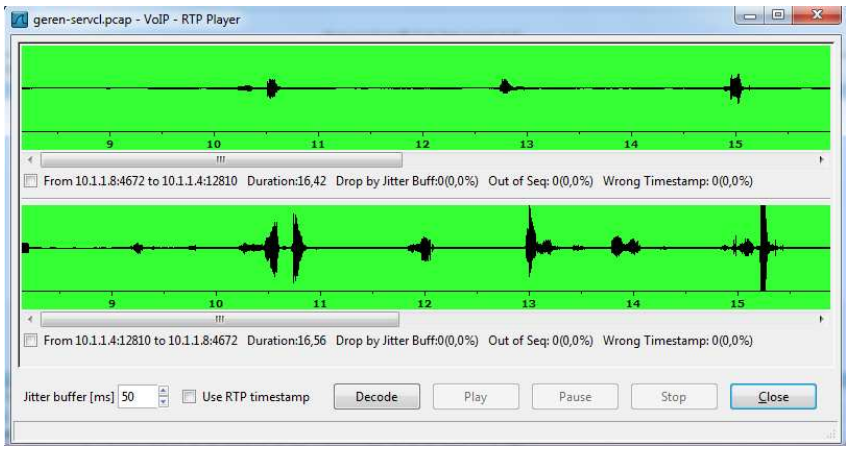


Fig.V.5. Extracción de audio de paquete RTP

5.2. Resultados en escenario con herramientas de seguridad

En este escenario se puso en funcionamiento la herramienta Snort que fue implementada para conocer el tráfico que ingresaba hacia el servidor, ayudándonos de esta manera a observar el ataque de Denegación de Servicio que se estaba realizando teniendo la oportunidad de impedir el acceso de paquetes desde la dirección IP causante del intento de saturación del servidor.

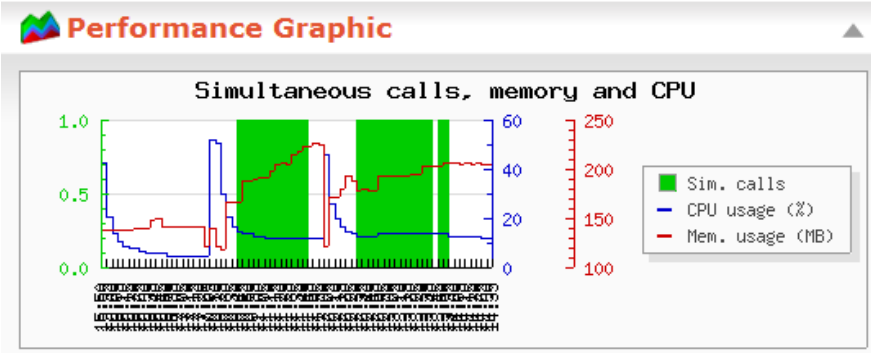


Fig.V.6. Consumo de recursos del sistema con activación de Snort.

En la Fig.V.6, se puede observar que al ser controlado el ataque los niveles de consumo de los recursos del sistema disminuyeron, ya que la cantidad de peticiones INVITE no es muy grande y no tiene mayores problemas en procesar. En cuanto a la cantidad de memoria utilizada llegó a ser del 80%tomando en cuenta todos los procesos que se ejecutan en el servidor, como es la misma herramienta Snort la cual trabaja en tiempo real y necesita de cierta cantidad de recursos para su funcionamiento.

En el caso del uso del CPU llegó a ser del 12% en el servidor Elastix.

Para contrarrestar el problema de la información SIP y RTP que viaja en plano se puso en funcionamiento la OpenVPN creando túneles entre los usuarios y de esta forma mediante el intercambio de llaves entre el servidor y el cliente la información viaja de forma segura impidiendo que cualquier herramienta como la mostrada anteriormente pueda capturar la información intercambiada entre estos tal como muestran las siguientes figuras:

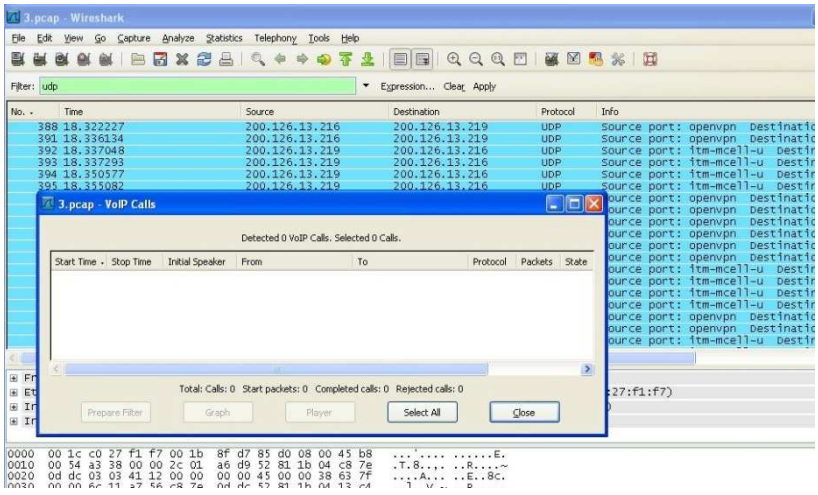


Fig.V.7. Captura de paquetes con el túnel OpenVPN habilitado.

Frente a esto se obtiene resultados óptimos de seguridad, puesto que ya no es posible capturar los paquetes SIP ni RTP que son los necesarios para la realización de los ataques antes escritos, ya que toda la información viaja encriptada.

Después de haber realizado las diferentes pruebas y haber observado su desempeño en función de su seguridad se obtuvieron los siguientes resultados:

5.3. Modelo Estadístico para el Análisis e Interpretación de Datos.

Para el análisis de los resultados se utilizó el método de Comprobación de la Hipótesis CHI Cuadrado en el campo de la estadística no paramétrica, ya que nos interesa probar la hipótesis en base a los datos de una muestra que provienen de una población que tiene una determinada distribución.

La prueba estadística es:

$$\chi^2 = \sum \frac{(Ob - Es)^2}{Es}$$

En donde "**Ob"** es el número de ítems de una determinada característica o eventos observados y **"Es"** es el número teórico esperado de ítems o eventos, de acuerdo con la distribución teórica planteada en la hipótesis nula H_o.

La prueba se realiza con (*n* – 1) grados de libertad, en donde ***n*** es el número de categorías en las que se encuentran las observaciones.

En nuestro caso se tomará en cuenta dos categorías: un escenario antes y uno después de haber aplicado las propuestas de soluciones para determinar si éstas contribuyeron al mejoramiento de la seguridad de nuestra red de VoIP, resultados que ya se explicaron anteriormente.

Sin embargo, cuando tenemos únicamente dos categorías, es decir un solo grado de libertad, o cuando alguna de las categorías tiene un bajo número de observaciones (cinco o menos), la fórmula cambia a:

$$\chi^2 = \sum \frac{(|Ob - Es| - 0.5)^2}{Es}$$

El restar 0.5 de los valores absolutos $|Ob - Es|$ se denomina la **Corrección de Yates** y es necesaria para obtener una mejor aproximación a la distribución teórica planteada.

5.4. COMPROBACIÓN DE HIPÓTESIS

Al realizar las diferentes pruebas de vulnerabilidad mediante ataques a la red, se plantea la relación de los niveles de seguridad de la siguiente manera:

Nivel de seguridad	Puntuación
Seguro	8 – 10
Poco Seguro	5 - 7
Nada Seguro	0 - 4

Tabla V.1. Niveles de Seguridad de la red.

HIPÓTESIS: CON LA PROPUESTA DE SOLUCIÓN ENCONTRADA EN LAS VULNERABILIDADES DEL PROTOCOLO DE SEÑALIZACIÓN SIP DE VOIP SE PRETENDE ESTABLECER SOLUCIONES ÓPTIMAS PARA TENER UNA RED DE TELEFONÍA IP **MÁS** SEGURA.

RESULTADOS

Después de haber realizado las diferentes pruebas mencionadas y haber observado su desempeño en función de su seguridad y utilizando los parámetros señalados anteriormente se tiene los siguientes resultados:

	ANTES(sin propuestas)	**DESPUÉS(con propuestas)**
Ataque1 (Captura de trafico SIP y RTP)	1	9
Ataque2 (Descifrado de contraseñas)	1	8
Ataque3 (Denegación de	1	8

Servicio)		
Resultado	1	8

Tabla V.2. Niveles de Seguridad en las diferentes categorías.

Obtención del valor de la prueba estadística χ^2, con el empleo de la corrección de Yates, a partir de los datos de prueba de seguridad:

CATEGORIA	**OBSERVADO**	**ESPERADO**
Antes(sin propuestas)	1	5
Despues(con propuestas)	8	10

5.5. PLANTEAMIENTO DE HIPÓTESIS NULA Y ALTERNATIVA

Dada esta hipótesis se han cumplido los siguientes objetivos:
Identificar la hipótesis nula y la hipótesis alternativa, expresadas así:

Hipótesis Nula. Denotada por H_0, es la aseveración de la hipótesis planteada

Ho: CON LA PROPUESTA DE SOLUCIÓN ENCONTRADA EN LAS VULNERABILIDADES DEL PROTOCOLO DE SEÑALIZACIÓN SIP DE VOIP SE PRETENDE ESTABLECER SOLUCIONES ÓPTIMAS PARA TENER UNA RED DE TELEFONÍA IP **MÁS** SEGURA.

Con los niveles de seguridad especificados anteriormente se denota la hipótesis nula como Ho=10

Hipótesis Alternativa. Denotada por H_1, es la negación de la hipótesis nula, que de alguna manera difiere de la hipótesis nula.

Hi: CON LA PROPUESTA DE SOLUCIÓN ENCONTRADA EN LAS VULNERABILIDADES DEL PROTOCOLO DE SEÑALIZACIÓN SIP DE VOIP **NO** SE PUDIERON ENCONTRAR SOLUCIONES ÓPTIMAS PARA TENER UNA RED DE TELEFONÍA IP MÁS SEGURA.

La hipótesis alternativa se la denota como Hi:5

Calculo de la prueba estadística χ^2 **(chi cuadrado):**

$$\chi^2 = \sum \frac{\left(|Ob - Es| - 0.5\right)^2}{Es}$$

$$\chi^2 = \left[\frac{\left(|1-5| - 0.5\right)^2}{5} + \frac{\left(|8-10| - 0 - 5\right)^2}{10} \right]$$

$$\chi^2 = \left[\frac{\left(|-4| - 0.5\right)^2}{5} + \frac{\left(|-2| - 0.5\right)^2}{10} \right]$$

$$\chi^2 = 2.675$$

Luego de haber calculado nuestro valor estadístico CHI cuadrado procedemos a determinar si se valida o no la hipótesis planteada.

El nivel de significación que se emplea queda a criterio del investigador, pero por lo general se usa el 5%, (α=5%).

Por lo que usando la tabla A-4 de la distribución Chi-cuadrada, identificamos primero la columna de grados de libertad, en nuestro caso tenemos 1 grado de libertad. Entonces en la cola de la izquierda hacemos 1-0.025=0.975, y la cola de la derecha 0.025.

Los valores en la tabla A-4 (chi cuadrada) son los siguientes:

Grados de libertad	**1-0.025=0.975**	**0.025**
1	0.001	5.024

Tabla V.3. Datos de la tabla A-4 (Anexo V) de la Distribución Chi-Cuadrada.

Luego de analizar los valores conseguidos de acuerdo a la tabla de chi cuadrado, se tienen los dos valores críticos de nuestra distribución Chi-cuadrada. El valor de nuestro estadístico de prueba es de $\chi^2 = 2.675$, que NO está dentro de los valores críticos de la tabla; por lo que se concluye:

Se comprueba que a Hipótesis Nula es verdadera $Ho = 10$ que se interpreta que las soluciones propuestas influyen favorablemente a la contribución del

mejoramiento de la seguridad de nuestra red con el protocolo de señalización SIP en VoIP.

Y se rechaza la Hipótesis Alternativa $Hi = 0$.

De esta manera se ha podido comprobar que la aseveración estadística planteada en esta tesis es congruente con la hipótesis planteada y los objetivos trazados. A continuación se aprecia la gráfica que demuestra esta ponencia.

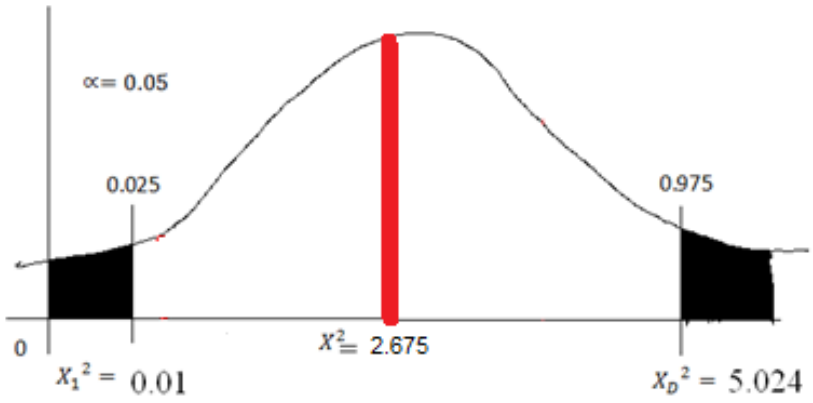


Fig.V.8. Ubicación del Estadístico de Prueba en la Distribución Chi-cuadrada para la prueba de hipótesis.

RESULTADO FINAL

A continuación se presenta la cantidad de vulnerabilidades que se han logrado contrarrestar deduciendo en un 90% la inseguridad de la red, luego de implementar las propuestas.

ANTES	Nº	DESPUÉS	Nº
Captura de información fácilmente	1	La información se ha logrado ocultar impidiendo que cualquier atacante pueda obtener datos importantes.	0 (No existe ataque)
Se obtiene cualquier contraseñas del administrador así como las utilizadas para la autenticación de un usuario agente con el	1	Información no visible para el atacante.	0 (No se logra ataque)

servidor.			
La inundación de paquetes INVITE al servidor que permite que el sistema colapse mediante el uso excesivo de los recursos de memoria y CPU.	1	Cualquier ataque por inundación es alertado por el sistema Snort el cual nos permite tomar las medidas necesarias para contrarrestar el ataque.	1 (Se logra realizar el ataque pero puede ser detenido)
Total	3	Total	0
Porcentaje	100%		1%
Relación numérica	3>1		

Tabla.V.4. Ubicación del Estadístico de Prueba Distribución Chi-cuadrada para la prueba de hipótesis.

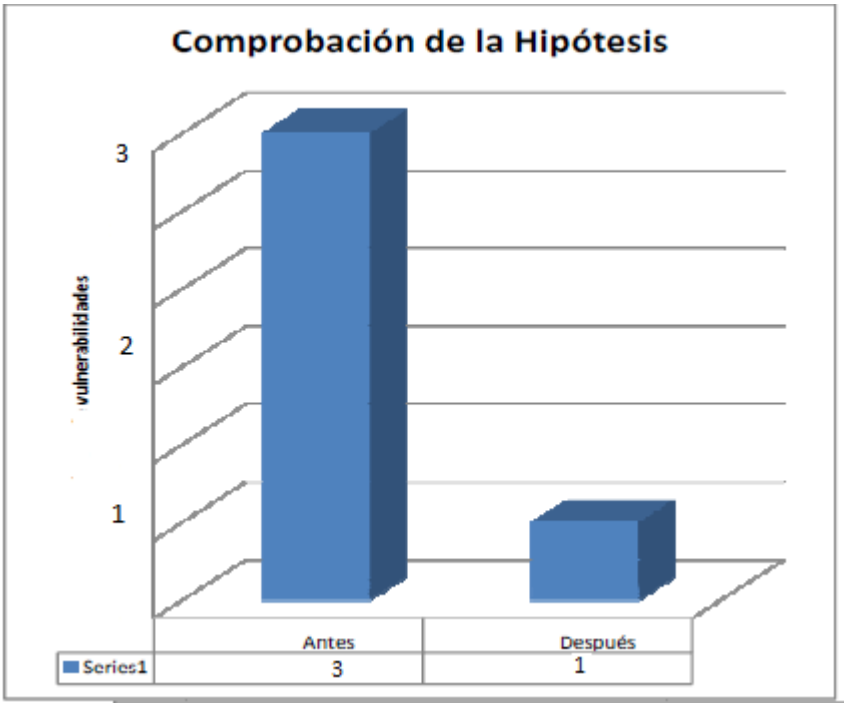


Fig.V.9. Gráfico Ubicación del Estadístico de Prueba Distribución Chi-cuadrada para la prueba de hipótesis.

De esta manera se concluye, que nuestra tesis ha sido validada con respecto a las propuestas planteadas y los resultados obtenidos.

CONCLUSIONES:

1. Tal como se analizó durante todo este proyecto, es imprescindible tomar medidas de seguridad y prevención, durante la implementación de un sistema VoIP.

2. Existen muchas herramientas de alcance libre que pueden perjudicar al Sistema por lo que no es suficiente el correcto funcionamiento del mismo, sino que además considerar las medidas a tomar para no ser víctimas de un intruso mal intencionado.

3. Para implementar un Sistema Voip más seguro, libre de ataques DoS, crackeo de contraseñas, escuchas ilegales, etc, deben ser considerados varios factores como la implementación de: Firewalls, VPN, herramientas de monitoreo de redes como Snort.

4. Las herramientas usadas a lo largo de este proyecto, para realizar los diferentes ataques al sistema VoIP, son eficaces, es decir cumplen con las funciones por las cuales fueron implementadas.

5. La gran ventaja del protocolo SIP no es solo su sencillez en la configuración sino su estabilidad al aumentar nodos que intervienen en la transmisión de voz.

6. La herramienta Snort es un instrumento útil de monitoreo ya que ésta proporciona la información sobre condiciones de red en tiempo real, dando lugar al administrador a tomar las decisiones más adecuadas a los problemas que se presenten en ese momento.

7. La creación de la OpenVPN permitió que la comunicación entre los clientes y servidor se realice de forma segura, impidiendo la captura de paquetes que sirvan para poner en riesgo la red.

8. El inconveniente que se dio en la implementación de la herramienta Inviteflood, fue que, debido a que en primera instancia los paquetes de ésta herramienta fueron descargados por separado, al compilarlos para su instalación, en todas las versiones encontradas de la web, se generaban errores, es decir no estaban correctamente implementados los archivos .c y .h, contenidas en los paquetes, por lo que producía varios errores que tomo mucho tiempo en resolverlos.

RECOMENDACIONES

1. No hay mejor defensa para un Sistema VoIP, que evitar los ataques. Entre las medidas de prevención, a considerar se encuentran:

2. Abrir solo los puertos del servidor que sean necesarios, sobre los que funcionan las aplicaciones que procesa.

3. A pesar de la complejidad de emplear un firewall en VoIP por los múltiples requerimientos que necesita, es una medida excelente para proteger la red de voz.

4. Se recomienda prestar una especial atención a los accesos que se dan en la red, mediante la utilización de herramientas de monitorización de redes.

RESUMEN

Propuesta de Soluciones a las Vulnerabilidades del Protocolo de Señalización SIP en Voz sobre IP, con el propósito de plantear soluciones que logren en alguna medida contrarrestar las falencias que sufre dicho protocolo.

Considerando las características del trabajo, el tipo de investigación que se realizó es analítica porque se realizo un estudio de las vulnerabilidades del protocolo SIP con el fin de proponer mecanismos para brindar mayor seguridad a este tipo de red.

Las herramientas Software utilizadas fueron sniffers como Wireshark, Cain&Abel, y herramientas de denegación de servicio como Inviteflood, herramientas de seguridad OpenVpn, Snort, y algunos comandos del sistema operativo Linux. El hardware utilizado fueron 3 maquinas clientes y un Servidor.

Se analizaron 3 vulnerabilidades del protocolo SIP, el primero interceptación de llamadas o escuchas ilegales que se basa en la captura de paquetes de voz de los cuales se pueden extraer las conversaciones generadas entre los usuarios del servicio, otro problema es el descifrado de contraseñas que mediante la herramienta Cain&Abel es posible obtenerlas, ante estos problemas se implemento una OpenVpn la cual permitió que todo trafico que viaja en la red se transmita de manera encriptada.

Se analizó el gran problema que sufren las redes VOIP que es la denegación de servicio para esto se utilizó la herramienta inviteflood que permite el envío de una gran cantidad de mensajes INVITE propio del protocolo SIP logrando el colapso del servidor, ante esto se propuso un mecanismo de monitoreo mediante la herramienta Snort la cual genera información en tiempo real de los sucesos de la red, ayudando al administrador a monitorear todos los paquetes que ingresan al servidor y de esta manera tomar decisiones más adecuadas y oportunas ante cualquier anomalía registrada.

Al implementar estas herramientas de seguridad la red mejoró en un 90% puesto que es casi imposible capturar tráfico en especial los paquetes RTP, mientras que estando en funcionamiento la herramienta snort se puede actuar de manera oportuna y detener cualquier paquete que esté en contra el rendimiento adecuado del servidor.

Se concluye que los sistemas de seguridad implementados en una red de este tipo ayudan a mejorar de forma efectiva el rendimiento del servidor y su seguridad.

Se recomienda mantenerse actualizado en conocimientos para evitar problemas de seguridad.

SUMMARY

Solution proposal for the vulnerabilities of the signalizing protocol S!P in Voz over *IP,* pretending to plan soiutíons that achieve to some extent counteract the shortcomings.

Considering the features of the work, the type of investigation was analytic, studying íhe vuinerabiiity of the SIP protocol with the aim to come up with a device to provide mayor security in this type of network. The used Software tools were sniffers like Wireshark, Cain&Abel and refusal tools of service like Inviteflood, security tools OpenVpn, Snort and some commands of the operative system Linux. As hardware were used three client machines and a server.

Three vulnerabiliiies of the SIP protocol were analyzed, the first one was interception of calls or eavesdropping based on voice packet capture of which can be pulled out the conversation generated between the service users, another problem is the password cracking by Cain&Abel is possible to obtain. To these problems was implemented a OpenVpn which ailows all network traffic that travels in an encrypted transmitting.

The big problem was analyzed that suffer the network VOIP, the refusal service. The inviteflood tool was used that allows sending a flood of rnessages INVITE characteristic of SIP protocoi achieving the collapse of the server. To this was proposed a device of monitoring by the Snort tool, which generales information in real time of events in the network, supporting so the administrator for monitoring all packages that come in the server and thus to take more timely and appropriate decisions for any reported anomafy.

Implementing these security tools the network improved 90% since it is almost impossible to capture traffic specially RTP packages, while the snort tool in function can act in a timely way and stop any package against the appropriate performance of the server.

It is concluded that the implemented securtiy systems of this type in a network help to improve the effectively performance of the server and its security.

It is recommended to stay updated in knowledge to avoid security problems.

BIBLIOGRAFÍA

1.- LANDIVAR, E., Comunicaciones Unificadas con Elastix., s.ed., s.edt., 2009., Pp. 7-102.

2.- MUÑOZ, A., Elastix a Ritmo de Merengue., s.ed., s.edt., 2010., Pp. 70-233.

3. - **SCHAR**, K., Snort 2.8.6 on Centos 5.5 Installation and Configuration Guide., s.ed., s.edt., 2009., Pp. 1-12.

4.- **SHARIF**, B., Elastix without Tears., s.ed., s.edt., 2008., Pp 30-92.

5.- **GONCALVES**, F., Asterisk PBX Guía de Configuración., 1.ed., Janeiro., s.edt., 2007., Pp. 166-198-256-277.

6.- **TRIOLA**, M., Estadística., 10.ed., México., Pearson-Addison Wesley., 2009., Pp. 363-366-383-397-439.

BIBLIOGRAFIA INTERNET

1.- IPTABLES

http://www.pello.info/filez/firewall/iptables.html

2010-12-20

2.- OPENVPN

http://www.alcancelibre.org/staticpages/index.php/como-openvpn-server-centos5

http://www.howtoforge.com/openvpn-server-on-centos-5.2

http://www.throx.net/2008/04/13/openvpn-and-centos-5-installation-and-configuration-guide/

http://www.voztovoice.org/?q=node/103

2011-01-20

3.- SNORT

http://www.how-to-linux.com/2008/12/install-snort-and-base-on-centos-52/

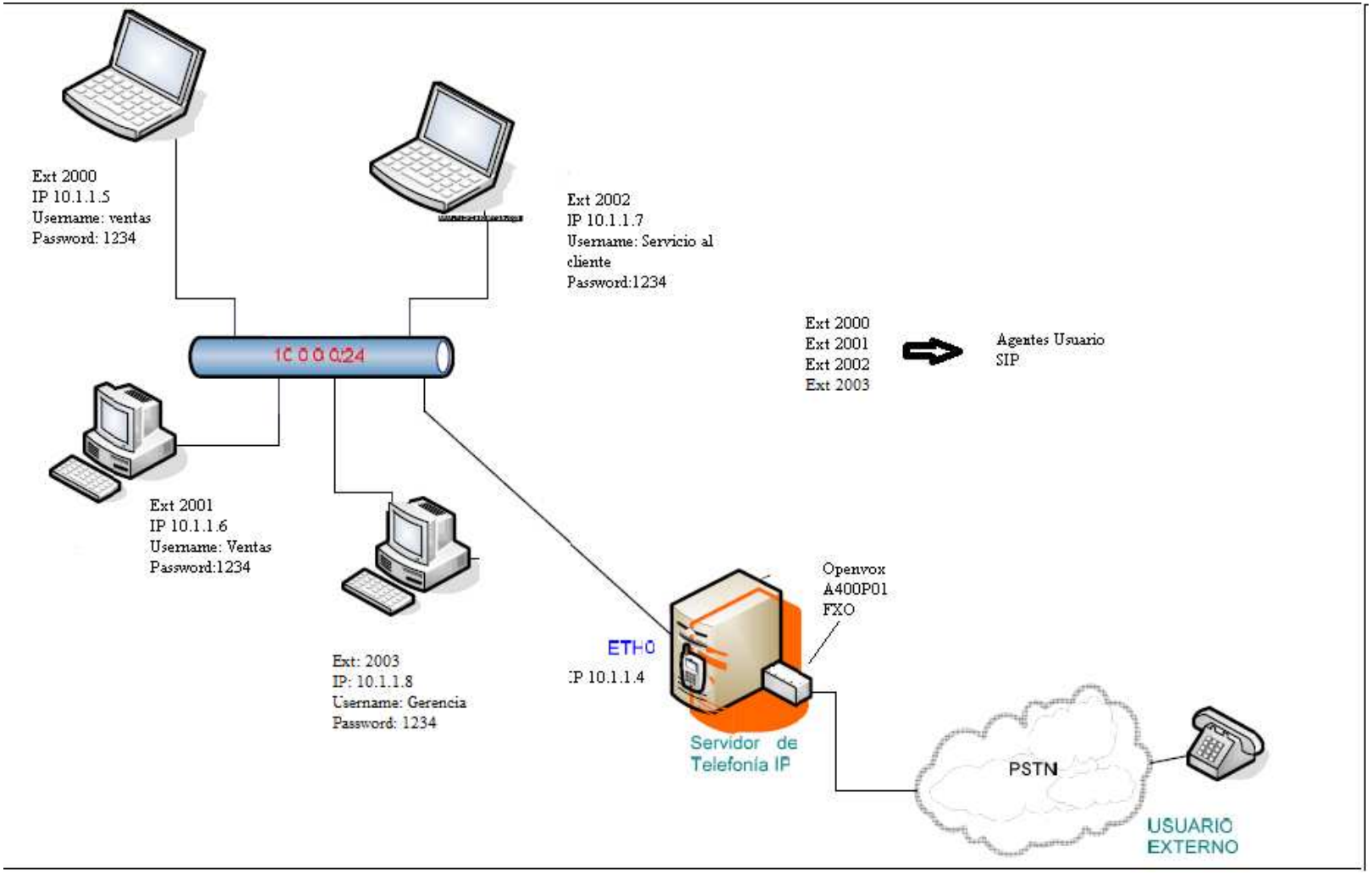
2011-01-20

ANEXOS

ANEXO 1

Red VoIp

RED VOIP


Ext 2000
IP 10.1.1.5
Username: ventas
Password: 1234
Ext 2002
IP 10.1.1.7
Username: Servicio al cliente
Password:1234
10.0.0.0/24
Ext 2000
Ext 2001
Ext 2002
Ext 2003
Agentes Usuario SIP
Ext 2001
IP 10.1.1.6
Username: Ventas
Password:1234
Ext: 2003
IP: 10.1.1.8
Username: Gerencia
Password: 1234
ETH0
IP 10.1.1.4
Openvox
A400P01
FXO
Servidor de Telefonía IP
PSTN
USUARIO EXTERNO

ANEXO 2

Datasheet OpenVox

A400p01

TARJETA OPENVOX A400P01

A400P Datasheet

Modular Analog Telephony Interface Product

Document Rev 0.02., written by:James.zhu@openvox.cn

A400P/A400E is a 4-port analog card and works with PSTN line. It can be used to build a PBX system based on Asterisk Open Source platform.

Key Benefits:

- Modular Design: Up to 4 FXS, FXO or mixed FXS/FXO ports per card
- Scalable: Just add additional cards to extend system
- Easy to use: Full software and hardware compatible with Digium™'s TDM400P. You can use Digium's X100M/S100M module on this card, or use OpenVox FXO-100/ FXS-100 Module on TDM400P.
- World Wide Usable: Configurable line interface to meet global telephone line interface requirements
- High quality with low price
- Application ready: Use Asterisk® to build your IP-PBX/Voicemail system

Features:

- Support Industry Standard: PCI 2.2 and PCI Express (for A400E)
- Both 3.3 V and 5 V PCI slot can be used for A400P
- Support GPL Software driver used with zaptel

Hardware and Software Requirements:

- RAM 128 + MB
- Linux kernel 2.4.X or 2.6.X
- CPU 800+ MHZ
- PCI 2.2 or PCI Express

Physical Information:

Name	Net weight（g）	Size（cm）
A400P	82	13.8*10.2*1.8
A400E	89	13.8*11.1*1.8

Misc:

- Temperature Operation: 0 to 50°C
- Temperature Storage: - 40 to 125°C
- Humidity:10 TO 90% NON-CONDENSING
- Voltage:5/12V,3REN
- Power Dissipation Max:2.77W/11.6W

ANEXO 3

Script de Configuración de Firewall

FIREWALL IMPLEMENTADO PARA CONTRARRESTAR LA DENEGACIÓN DE SERVICIO.

```
#!/bin/sh
#---
# Nombre: firewall.ipt
# Version: 0.1
# Licencia: GNU GPL v1.2
# Directorio: /etc/rc.d/firewall
# Descripcion: Firewall para habilitacion y bloqueo de Servicios.
# Fecha de Creacion: Lunes, 21 de Febrero del 2011.
# Revision: Ing. .
# Fecha de Revision: Martes, 22 de Febrero del 2011.
#---

#-------------------------------------------------------------------------------------
--------------------
#
echo "1" > /proc/sys/net/ipv4/ip_forward
echo "1" > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts
echo "1" > /proc/sys/net/ipv4/icmp_echo_ignore_all
echo "1" > /proc/sys/net/ipv4/tcp_syncookies
echo "1" > /proc/sys/net/ipv4/icmp_ignore_bogus_error_responses
echo "30" > /proc/sys/net/ipv4/tcp_fin_timeout
echo "1280" > /proc/sys/net/ipv4/tcp_max_syn_backlog

# Evitar ataques de spoofing...
echo "1" > /proc/sys/net/ipv4/conf/all/rp_filter
# Deshabilitar la redireccion del ping...
echo "0" > /proc/sys/net/ipv4/conf/all/accept_redirects

/sbin/depmod   -a
/sbin/modprobe iptable_nat
/sbin/modprobe ip_conntrack_ftp
/sbin/modprobe ip_conntrack_irc
/sbin/modprobe ip_nat_ftp
```

```
#
#--------------------------------------------------------------------------------------------
--------------------

#--------------------------------------------------------------------------------------------
--------------------
#---
#       Definicion de Variables Principales.
#---

IPTABLES=/sbin/iptables

#--- Interfaz eth0
OUTERIF=eth0
OUTERIP=10.1.1.4/32
OUTERNET=10.1.1.0/24

LOCALHOST_IP=127.0.0.1/32
STATIC_IP=10.1.1.1/32

# lo - interfaz de loopback
LOO_RED=127.0.0.0/8
# cualquier red
ANY_RED=0.0.0.0/0

INET_IFACE=eth0

REMOTENET=0/0
PRIVPORTS="0:1023"
UNPRIVPORTS="1024:65535"
OK="\033[1;0m [  \033[00;32mOK  \033[1;0m]\033[0m"

#
#--------------------------------------------------------------------------------------------
--------------------

echo -e "Flushing de Reglas por Default:                    $OK"
```

```
# ===>> Flush <<=== #

$IPTABLES -F
$IPTABLES -X
$IPTABLES -t nat    -F
$IPTABLES -t mangle -F
$IPTABLES -t mangle -X

echo -e "Cargando Reglas Generales Para el FireWall:              $OK"

#--------------------------------------------------------------------------------------
--------------------
#---
#       Bloqueo de Ataques Syn.
#---

$IPTABLES -N bad_tcp_packets
$IPTABLES -t filter -A bad_tcp_packets -p tcp ! --syn -m state --state NEW -j LOG -
-log-prefix " Posible ataque SYN: "
$IPTABLES -t filter -A bad_tcp_packets -p tcp ! --syn -m state --state NEW -j DROP
$IPTABLES -t filter -A INPUT -p tcp --dport 80 -j bad_tcp_packets

$IPTABLES -N PKT_FAKE
$IPTABLES -F PKT_FAKE
$IPTABLES -A PKT_FAKE -m state --state INVALID -j DROP
$IPTABLES -A PKT_FAKE -p tcp ! --syn -m state --state NEW -j DROP
$IPTABLES -A PKT_FAKE -f -j DROP

echo -e "Protegiendo de Anti-flooding o inundacion tramas SYN:
$OK"

$IPTABLES -N syn-flood
$IPTABLES -A INPUT -i eth0 -p tcp --syn -j syn-flood
$IPTABLES -A syn-flood -m limit --limit 1/s --limit-burst 4 -j RETURN
$IPTABLES -A syn-flood -j DROP
```

```
$IPTABLES -A FORWARD -p tcp --syn -m limit --limit 1/s -j ACCEPT
$IPTABLES -A FORWARD -p tcp --tcp-flags SYN,ACK,FIN,RST RST -m limit --limit 1/s -j ACCEPT
$IPTABLES -A FORWARD -p icmp --icmp-type echo-request -m limit --limit 1/s -j ACCEPT

echo -e "Chain FORWARD: drop bad packets                                    $OK"
#$IPTABLES -A FORWARD -p tcp ! --syn -m state --state NEW -j LOG --log-prefix "New not syn: "
$IPTABLES -A FORWARD -p tcp ! --syn -m state --state NEW -j DROP

echo -e "Chain FORWARD: enable LOG                                          $OK"
$IPTABLES -A FORWARD -m limit --limit 3/minute --limit-burst 3 -j LOG --log-level DEBUG --log-prefix "IPT FORWARD died: "
# Kill packets which are invalid.
$IPTABLES -A FORWARD -m state --state INVALID -j DROP

#
#-------------------------------------------------------------------------------------------------

#-------------------------------------------------------------------------------------------------
#---
#       Protegiendo contra ataques por ICMP como ping masivo.
#---

#echo -e "Proteccion contra Ataques por ICMP.                                $OK"
#$IPTABLES -A INPUT -i eth0 -p icmp --icmp-type 8 -j DROP
#$IPTABLES -A FORWARD -i eth0 -p icmp --icmp-type 8 -j DROP

#$IPTABLES -A INPUT -p icmp --icmp-type echo-request -m limit --limit 1/s -i eth0 -j ACCEPT #Acepto un ping por segundo.
#---
#       Reglas para bloqueo de SNMP que excedan las 4 sesiones por minuto...
#---
```

```
#$IPTABLES -A INPUT -i eth1 -p tcp -m tcp --dport 25 -m state --state NEW -m recent --set --name DEFAULT --rsource
#$IPTABLES -A INPUT -i eth1 -p tcp -m tcp --dport 25 -m state --state NEW -m recent --update --seconds 60 --hitcount 4 --name DEFAUL
T --rsource -j DROP
#
#--------------------------------------------------------------------------------------------
--------------------
#---
#       Reglas para Control de Trafico de VoIP...
#---
$IPTABLES -A INPUT -p udp -m state --state NEW -m udp --dport 1024:5059 -j QUEUE
$IPTABLES -A INPUT -p udp -m state --state NEW -m udp --dport 5060:5070 -j QUEUE
$IPTABLES -A INPUT -p udp -m state --state NEW -m udp --dport 5071:65535 -j QUEUE

#
```

ANEXO 4

Distribución Chi-cuadrada

Distribución Chi-cuadrada

Fórmulas y tablas
para *Estadística, décima edición*, de Mario Triola

TABLA A-4 Distribución chi cuadrada (χ^2)

Grados de libertad	Área a la derecha del valor crítico									
	0.995	0.99	0.975	0.95	0.90	0.10	0.05	0.025	0.01	0.005
1	—	—	0.001	0.004	0.016	2.706	3.841	5.024	6.635	7.879
2	0.010	0.020	0.051	0.103	0.211	4.605	5.991	7.378	9.210	10.597
3	0.072	0.115	0.216	0.352	0.584	6.251	7.815	9.348	11.345	12.838
4	0.207	0.297	0.484	0.711	1.064	7.779	9.488	11.143	13.277	14.860
5	0.412	0.554	0.831	1.145	1.610	9.236	11.071	12.833	15.086	16.750
6	0.676	0.872	1.237	1.635	2.204	10.645	12.592	14.449	16.812	18.548
7	0.989	1.239	1.690	2.167	2.833	12.017	14.067	16.013	18.475	20.278
8	1.344	1.646	2.180	2.733	3.490	13.362	15.507	17.535	20.090	21.955
9	1.735	2.088	2.700	3.325	4.168	14.684	16.919	19.023	21.666	23.589
10	2.156	2.558	3.247	3.940	4.865	15.987	18.307	20.483	23.209	25.188
11	2.603	3.053	3.816	4.575	5.578	17.275	19.675	21.920	24.725	26.757
12	3.074	3.571	4.404	5.226	6.304	18.549	21.026	23.337	26.217	28.299
13	3.565	4.107	5.009	5.892	7.042	19.812	22.362	24.736	27.688	29.819
14	4.075	4.660	5.629	6.571	7.790	21.064	23.685	26.119	29.141	31.319
15	4.601	5.229	6.262	7.261	8.547	22.307	24.996	27.488	30.578	32.801
16	5.142	5.812	6.908	7.962	9.312	23.542	26.296	28.845	32.000	34.267
17	5.697	6.408	7.564	8.672	10.085	24.769	27.587	30.191	33.409	35.718
18	6.265	7.015	8.231	9.390	10.865	25.989	28.869	31.526	34.805	37.156
19	6.844	7.633	8.907	10.117	11.651	27.204	30.144	32.852	36.191	38.582
20	7.434	8.260	9.591	10.851	12.443	28.412	31.410	34.170	37.566	39.997
21	8.034	8.897	10.283	11.591	13.240	29.615	32.671	35.479	38.932	41.401
22	8.643	9.542	10.982	12.338	14.042	30.813	33.924	36.781	40.289	42.796
23	9.260	10.196	11.689	13.091	14.848	32.007	35.172	38.076	41.638	44.181
24	9.886	10.856	12.401	13.848	15.659	33.196	36.415	39.364	42.980	45.559
25	10.520	11.524	13.120	14.611	16.473	34.382	37.652	40.646	44.314	46.928
26	11.160	12.198	13.844	15.379	17.292	35.563	38.885	41.923	45.642	48.290
27	11.808	12.879	14.573	16.151	18.114	36.741	40.113	43.194	46.963	49.645
28	12.461	13.565	15.308	16.928	18.939	37.916	41.337	44.461	48.278	50.993
29	13.121	14.257	16.047	17.708	19.768	39.087	42.557	45.722	49.588	52.336
30	13.787	14.954	16.791	18.493	20.599	40.256	43.773	46.979	50.892	53.672
40	20.707	22.164	24.433	26.509	29.051	51.805	55.758	59.342	63.691	66.766
50	27.991	29.707	32.357	34.764	37.689	63.167	67.505	71.420	76.154	79.490
60	35.534	37.485	40.482	43.188	46.459	74.397	79.082	83.298	88.379	91.952
70	43.275	45.442	48.758	51.739	55.329	85.527	90.531	95.023	100.425	104.215
80	51.172	53.540	57.153	60.391	64.278	96.578	101.879	106.629	112.329	116.321
90	59.196	61.754	65.647	69.126	73.291	107.565	113.145	118.136	124.116	128.299
100	67.328	70.065	74.222	77.929	82.358	118.498	124.342	129.561	135.807	140.169

De Donald B. Owen, *Handbook of Statistical Tables*, © 1962 Addison-Wesley Publishing Co., Reading, MA. Reproducido con permiso del editor.