Ministère de l'Enseignement Supérieur
et de la Recherche Scientifique
Université Virtuelle de Tunis

UVT
جامعة تونس الافتراضية
UNIVERSITÉ VIRTUELLE DE TUNIS

MEMOIRE

DE STAGE DE FIN D'ETUDES

Pour l'obtention du

«Mastère professionnel en Nouvelles Technologies des Télécommunications et Réseaux (N2TR)»

Présenté par :
AIDA FRIJA

ETUDE ET MISE EN PLACE D'UNE SOLUTION VOIP SECURISEE

Soutenu le :……

Devant le jury :

Président : Mr.(Mme.) ……

Encadreur : Mr. Khaled GHORBEL

Rapporteur : Mr.(Mme.) ……

Membre : Mr.(Mme.) ……

Année Universitaire : 2017/ 2018

www.uvt.rnu.tn

14, Rue Yahia Ibn Omar - 1082 Mutuelleville - Tunis
Tél. : +216 71 28 99 81 / +216 71 89 17 31 - Fax : +216 71 89 26 25

Résumé

Ce PFE traite la mise en place d'une solution de voix sur IP dans une infrastructure téléphonique existe via la solution VoIP open source « Asterisk » au sein de l'entreprise « MAGMA ». Nous exposons en premier lieu les notions de base essentielles pour la compréhension du déroulement de cette technologie ainsi que sa sécurisation. Nous installons ensuite notre solution dans un environnement de test avec le serveur Asterisk, deux clients Softphone.

Nous avons installé la suite de logiciel d'audit et d'attaque linux Khali pour l'écoute du traffic via la voix IP et pour réaliser une série d'attaque visant les vulnérabilité d'une communication via la voix sur IP, suite à ses attaques, nous venons de proposer les mesures de sécurité à implémenter dans l'infrastructure existante.

Abstract

This internship treats with the implementation of a voice over ip solution in a classic existing communication infrastructure via the open source VoIP solution "Asterisk" within the company "MAGMA". First of all, we expose the basic notions essential for understanding the unfolding of this technology as well as its security. We then install our solution in a test environment with the Asterisk server, two Softphone clients.

We installed the Linux Khali audit and attack software suite to listen for IP voice traffic and perform a series of attacks targeting the vulnerability of a voice over ip communication, following its attacks; we have just proposed the security measures to implement in the existing infrastructure.

ملخص

يدرس مشروع التخرج هذا إمكانية وضع الصوت عبر بروتوكول الإنترنت في البنية التحتية للهاتف الموجود عبر استعمال برنامج "الاستركس" داخل شركة "ماقما للإعلامية" أولا ، نحن نكشف المفاهيم الأساسية للكشف عن هذه التكنولوجيا وكذلك أمنها. ثم نقوم بتثبيت الحل في بيئة اختبار مع خادم "الاستركس" قمنا باستخدام مشتركين في هذه الخدمة باستعمال "ترواسكس" وقمنا بإجراء اتصالات بين المستعملين كل في حاسوب. لقد قمنا بتركيب تطبيق "كالي لينكس" للتدقيق والمهاجمة من أجل مراقبة حركة الاتصالات الصوتية عبر بروتوكول الإنترنت وسلسلة من الهجمات التي تستهدف قابلية تأثر الصوت عبر اتصال "ايبي" للهجمات، اقترحنا للتو التدابير الأمنية لتنفيذ في البنية التحتية القائمة باستعمال تطبيق "سنورت".

A propos du stage du projet de fin d'étude

Ce stage a été effectué dans le cadre de l'obtention de mastère professionnelle en nouvelles technologies de la télécommunication et réseaux (N2TR) au sein de la Société MAGMA.

Il s'est déroulé du 1 Février 2018 au 31 Mai 2018 sous l'assistance de l'Université Virtuelle de Tunis et l'encadrement auprès de la société MAGMA.

Au cours du stage, j'ai pu approfondir mes connaissances sur plein de technologies à savoir la voix sur IP, la configuration réseau sous différents systèmes d'exploitation Windows et Linux, la réalisation de plusieurs scénarios d'attaques et d'audit de la solution voix sur ip via la distribution Khali linux.

REMERCIEMENTS

A mes encadreurs à la société **MAGMA**:

- Monsieur Ahmed Haded
- Monsieur Anis Hachani

Aux enseignants de l'UVT :

- Monsieur Khaled GHORBEL, Encadrant UVT.

DEDICACES

A mon cher père

L'homme à qui je dois tout le respect

A ma chère et tendre mère

A toute ma famille

En témoignage de mon profond amour et respect, à qui je souhaite le succès et le bonheur

A ma chère Safia, à tous ceux que j'aime, tous ceux qui m'aiment

Et tous ceux qui me sont chers

J'offre ce travail qui présente le fruit de leurs aides et leur dévouement.

TABLE DE MATIERES

LISTE DES FIGURES

LISTE DES TABLEAUX

INTRODUCTION GENERALE

La Voix sur IP (Voice over IP ou VoIP) est une technologie permettant de transmettre la voix sur un réseau numérique et sur Internet.
La voix sur IP est utilisée avec différentes architectures et des protocoles définissent son fonctionnement, elle dépend de plusieurs contraintes.

La Voix sur IP présente plusieurs avantages mais il faut plus d'efforts pour innover et essayer de réduire les failles et les inconvénients qui y existent encore.

Dans ce cadre, on a proposé de mettre en place une solution Voix sur IP open-source se basant sur le protocole SIP pour le compte de la Société MAGMA tout en prenant les mesures de sécurité nécessaire.

Le but de ce projet de fin d'étude est de comparer les différentes solutions existantes, de déceler leurs limites et de chercher la solution la plus adéquate qui répond aux besoins de la société, ses besoins se résument essentiellement dans la mise en place d'une application vocale qui permet à tous les employés de la société de communiquer aisément et gratuitement entre eux à travers différents départements et ce d'une manière sécurisée.

Ainsi, le présent rapport s'article sur 4 chapitres :

- Le premier chapitre présentera l'organisme d'accueil de la société, une brève description de notre projet ainsi une étude et critique de l'infrastructure existante.
- Le deuxième chapitre comportera une étude des concepts théoriques nécessaires pour la réalisation du projet à savoir, la voix sur IP, le protocole SIP, les attaques qui peuvent menacer une application VoIP ainsi que les problèmes de sécurité.
- Le troisième chapitre sera consacré à la spécification des besoins et une justification des choix envisagés ainsi qu'une conception détaillée de l'application.
- Le dernier chapitre présentera les outils de travail et décrira d'une manière détaillée la mise en place de l'application.

CHAPITRE 1 : PRESENTATION DU CADRE DU PROJET

Introduction

Dans le cadre de la formation du master professionnel en nouvelles technologie des communications et des réseaux au sein de l'Université Virtuelle de Tunis, nous avons effectué notre stage de mémoire de fin d'études au sein de la Société MAGMA, ce stage va me permettre de me mettre en pratique les connaissances théoriques dans un projet réel.

Dans ce premier chapitre, nous présentons le cadre général de notre projet, l'environnement de travail à savoir l'organisme d'accueil (MAGMA).

Nous exposons ensuite une description de notre projet en précisant son contexte et son objectif, après on présentera une étude et critique de l'infrastructure existante

1. Présentation de la société

La société **MAGMA** Incorporation développe des logiciels pour le compte de tiers, fait la maintenance applicative, gère à distance des plateformes de service et propose des solutions de maintenances informatiques destinées à tous les domaines professionnels.

La société MAGMA propose à ses clients plusieurs services et produits à très forte valeur.

1.1. Le développement des logiciels informatiques

La société informatique MAGMA propose une panoplie de produits et services pour développer des programmes et des logiciels qui répondent exactement aux besoins des entreprises à savoir les logiciels :

- De gestion des terminaux de paiement électroniques (TPE),
- De gestion intégrée (ERP)
- De caisses,
- De gestion de stock,
- De gestion de ressource humaine,
- De rapprochement comptable (entre vos ventes et votre relevé bancaire),
- De gestion comptable,
- De facturation et de gestion des achats,
- De gestion de la relation client (CRM)

1.2. La maintenance informatique

La société MAGMA dispose de spécialistes en maintenance informatique hardware et software (postes travail, imprimantes …), elle assure les services listés ci-dessous à savoir :

- La gestion complète des parcs informatiques.
- La gestion de la maintenance du matériel informatique (Ordinateur de bureau, PC portable, imprimante, caisses enregistreuses…)
- La gestion des mises à jour de toutes les applications et les programmes informatique Anti-virus, drivers, navigateurs, caisses enregistreuses …)
- La gestion de stock de matériel et de consommable
- La gestion de la relation avec les fournisseurs et ce en contrôlant la qualité et les délais d'intervention des services après ventes.

Ci-dessous un aperçu sur la structure organisationnel de la société Magma

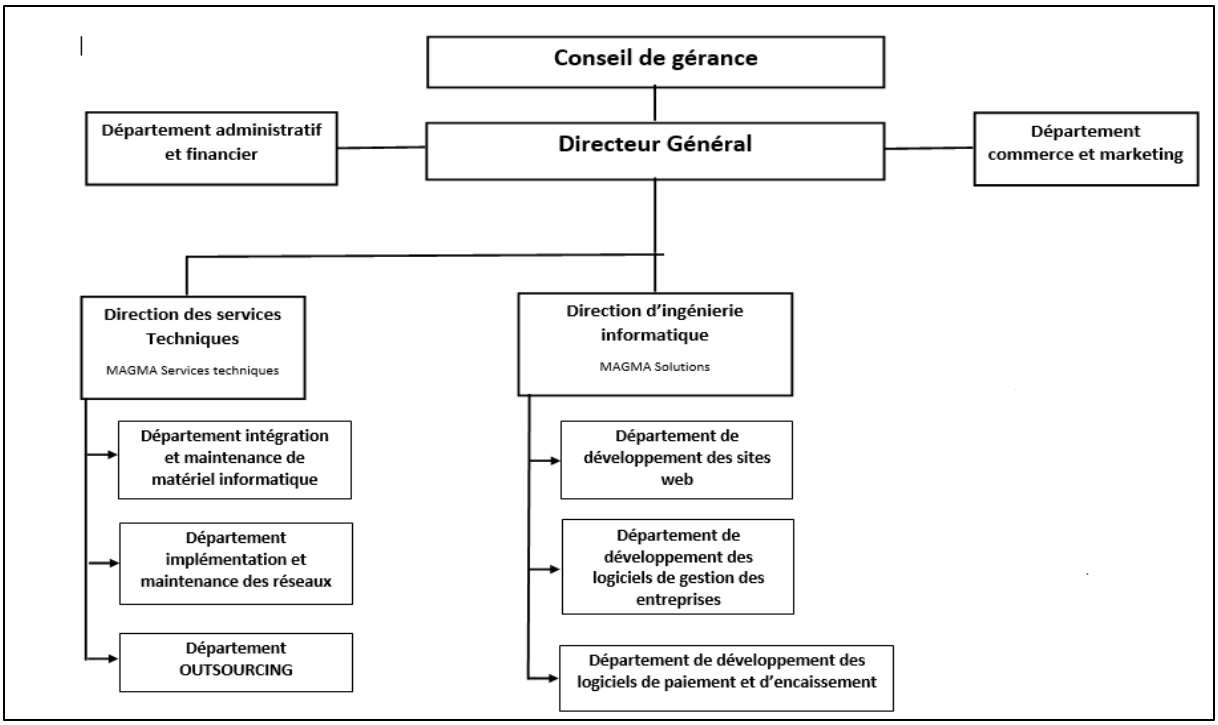

Figure 1 : Structure organisationnel de l'entreprise

2. Présentation du projet

Le projet consiste à la mise en place d'une plateforme de téléphonie sur IP sécurisé basée sur un serveur SIP open source intégré avec l'infrastructure existante. Cette plateforme sera exploitée pour gérer les différentes communications téléphoniques dans l'entreprise

2.1. Étude de l'existant

Dans le but d'assurer la communication téléphonique entre tous ses agents à l'intérieur de l'entreprise, la société MAGMA a mis en place une plateforme téléphonique classique (RTC). Ce réseau est exploité entre les différents départements, nous allons présenter une étude de la solution existante et dégager ses limites, on va proposer ainsi des solutions pour ces problèmes.

2.1.1. L'infrastructure existante

Le parc informatique de la société est constitué d'un routeur connecté via un fournisseur de service internet, d'un Firewall, des switches et des postes de travail interconnectés au sein de réseaux locaux LAN et WAN comme le montre la figure ci-dessous.

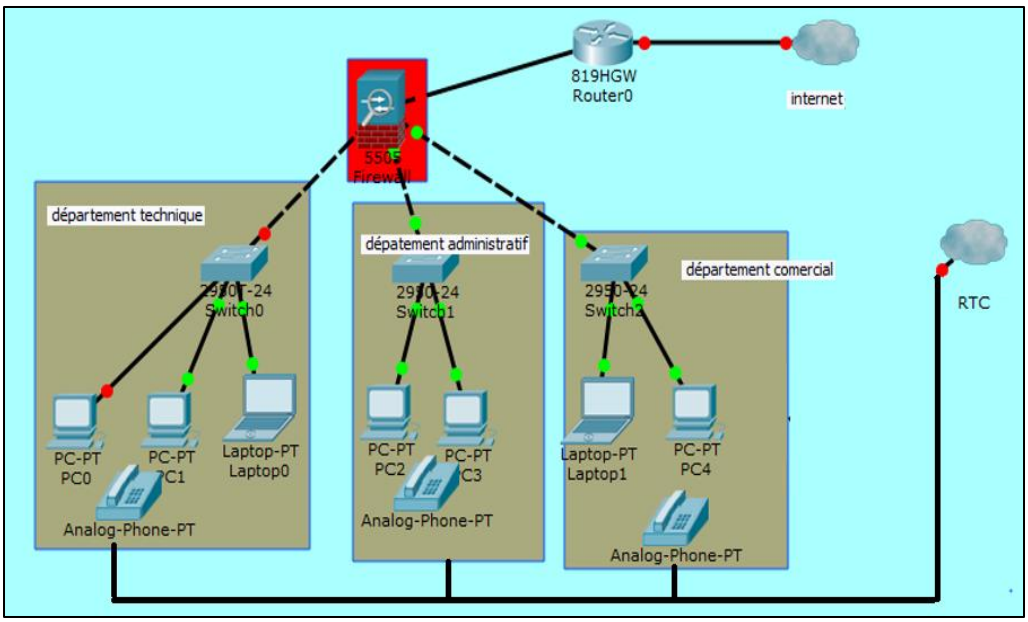

Figure 2: Architecture du réseau informatique existant

2.1.2. Le Réseau Téléphonique public Commuté RTC

Utilisant le principe de la commutation de circuits, le réseau téléphonique met en relation deux abonnés à travers une liaison dédiée pendant tout l'échange (**voir figure**3). Un canal de communication est ouvert entre eux et l'intégralité de cette bande passante est réservée à ces deux interlocuteurs. RTC est structuré en trois zones comme indique le schéma ci-dessous, chaque zone correspond à un niveau de concentration et en principe de taxation. [1]

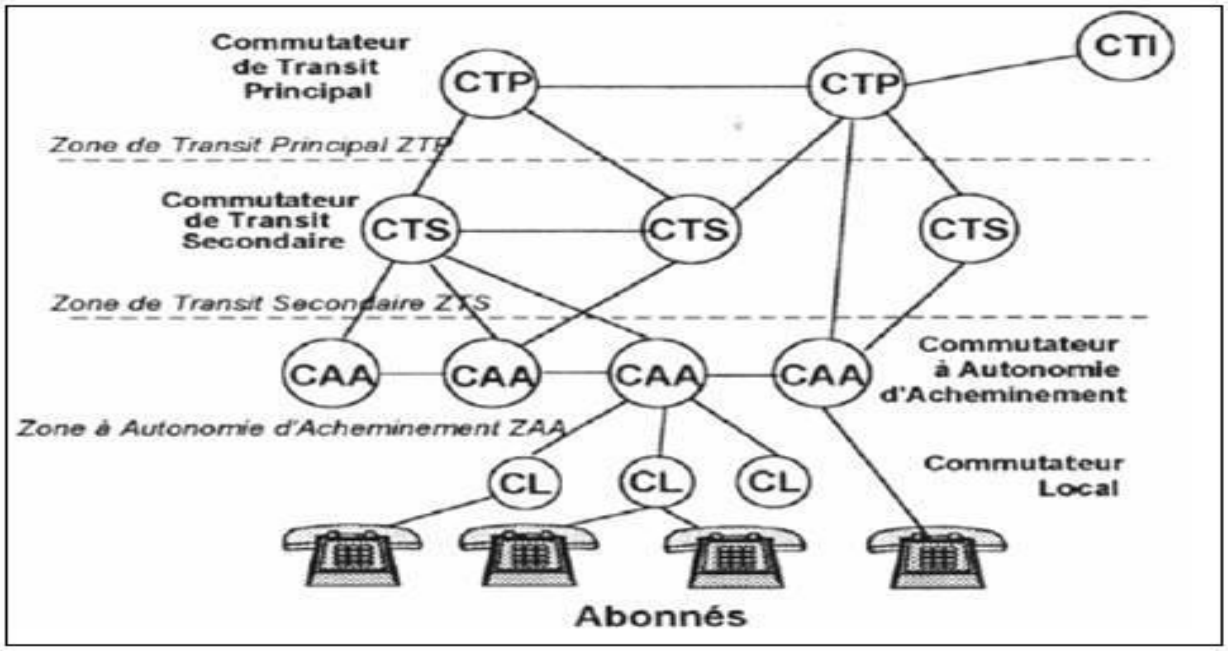

Figure 3: Architecture d'un réseau RTC

On distingue :

- **La Zone à Autonomie d'Acheminement (ZAA)** : C'est la zone la plus basse de la hiérarchie. Elle comporte un ou plusieurs Commutateurs à Autonomie d'Acheminement (CAA) qui eux-mêmes desservent des Commutateurs Locaux (CL).
- **La Zone de Transit Secondaire (ZTS)** : Cette zone comporte des Commutateurs de Transit Secondaire (CTS). Ces derniers assurent le brassage des circuits lorsqu'un CAA ne peut atteindre directement le CAA destinataire.
- **La Zone de Transit Principal (ZTP)** : Cette zone assure la commutation des liaisons longues distances. Chaque ZTP comprend un Commutateur de Transit Principal (CTP). Au moins un CTP est relié à un Commutateur de Transit Internationale (CTI).

2.2. Critique de l'existant

Le Réseau téléphonique Commuté est très sollicité ce qui entraine occasionnellement quelques défaillances et difficultés de fonctionnement, Nous allons expliquer dans ce paragraphe les différents problèmes à savoir

- Le cout : vu que la direction technique et administrative de la société sont séparés chacun dans un département à part, les employés de la société préfèrent se communiquer via le réseau RTC mieux que se déplacer, on note aussi que tous les employés doivent disposer d'un appareil téléphonique, comme conclusion la société aura à payer les frais

de l'achat des appareils téléphonique ainsi à payer les frais du aux communications établi à l'intérieur de la société via le réseau RTC

- Limitation du débit : La bande passante du RTC (300-4000Hz) aussi son rapport signal/bruit (40dB en moyenne) limitela qualité du signal analogique transmis, ce qui se traduit par une limitation du nombre de bits que l'on peut faire passer par unité de temps.
- Un encombrement au niveau du câblage.
- Ruptures et perturbations de la communication.

2.3. SOLUTION ENVISAGEABLE

La mise en place d'une solution VoIP sécurisée, basée sur l'usage du serveur ASTERISK au sein de l'entreprise ouvre des nouvelles perspectives : Minimiser le coût des appels, élargir les variétés d'appels tels que visioconférence et visiophonie, dégager la meilleure disponibilité en utilisant l'IP phones et l'amélioration de la qualité de service

2.3.1. Nouvelle architecture

La figure ci-dessous nous montre un aperçu sur la nouvelle architecture proposés après avoir ajouté le matériel ainsi le software permettant d'établir une communication en interne via la voix IP,on propose dans cette nouvelle architecture l'ajout d'un serveur ASTERISK liée à un switch qui permettra de gérer la téléphonie interne dans la société.

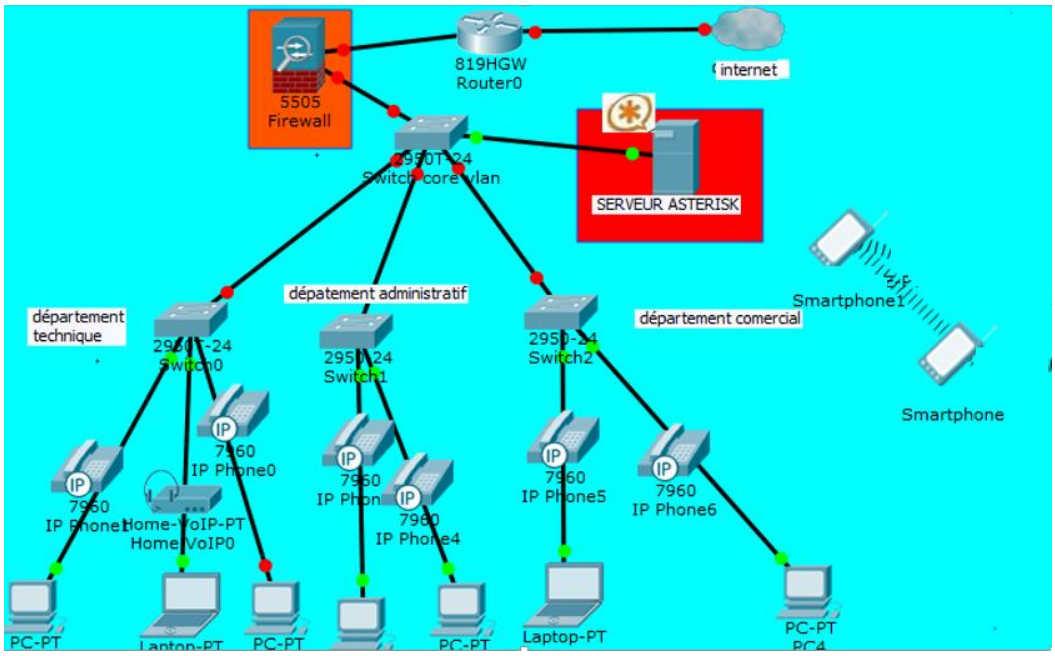

Figure 4: Architecture proposé

2.3.2. Avantages de la solution

Cette application offre plusieurs avantages par rapport à la téléphonie classique

- Installation et maintenance simplifiées (un seul réseau) : un seul câblage, un abonnement, et une maintenance allégée.
- Organisation simple : l'utilisateur se déplace avec son terminal et le branche où il veut dans le réseau.
- Réduction des coûts de télécommunications : les communications sont gratuitesau sein du réseau de l'entreprise, même sur sites distants.
- Gain de temps et d'argent : les communications téléphoniques intégrant le multimédia (audio et vidéoconférence).
- Convergence fixe-mobile : plus de collaboration et de mobilité. Grâce à l'interconnexion des téléphones mobiles avec les téléphones fixes de l'entreprise, vos GSM sont reliés en permanence avec la plateforme IPBX, en 3G et/ou Wifi.
- Elargissement des fonctionnalités avec le matériel périphérique IP : audioconférence IP et vidéo-parlophonie.

CONCLUSION

Dans ce chapitre nous avons présenté la société MAGMA et les orientations du projet à mener, nous avons mené une critique sur l'infrastructure existante avec notre proposition d'implémentation de la solution Voix sur ip, dans le chapitre suivant présente les différents concepts théoriques sur lesquels se base notre projet.

CHAPITRE 2 : LA NOTION THEORIQUE ET LA SECURISATION DE LA VOIX SUR IP

Introduction

Dans ce chapitre nous allons présenter la VoIP ainsi son historique, nous allons aussi évoquer toute technologie y relié avec, ainsi le volet de la sécurité.

La VoIP se réfère à la diffusion du flux de la voix sur les réseaux Internet. Le protocole Internet IP fut conçu à l'origine pour la gestion de réseau de données puis après son succès, le protocole a été adapté à la gestion de la voix.

1. Le Processus du traitement de la voix IP

L'utilisation de la VoIP a pour but de minimiser le coût des communications, offrir des services de données, de voix, et d'images.

La VoIP peut faciliter des tâches et fournir des services qu'il serait difficile ou coûteux de mettre en œuvre en utilisant le réseau RTC traditionnel.

Dans la paragraphe ci-dessous, nous allons présenter le processus du traitement de la VoIP.

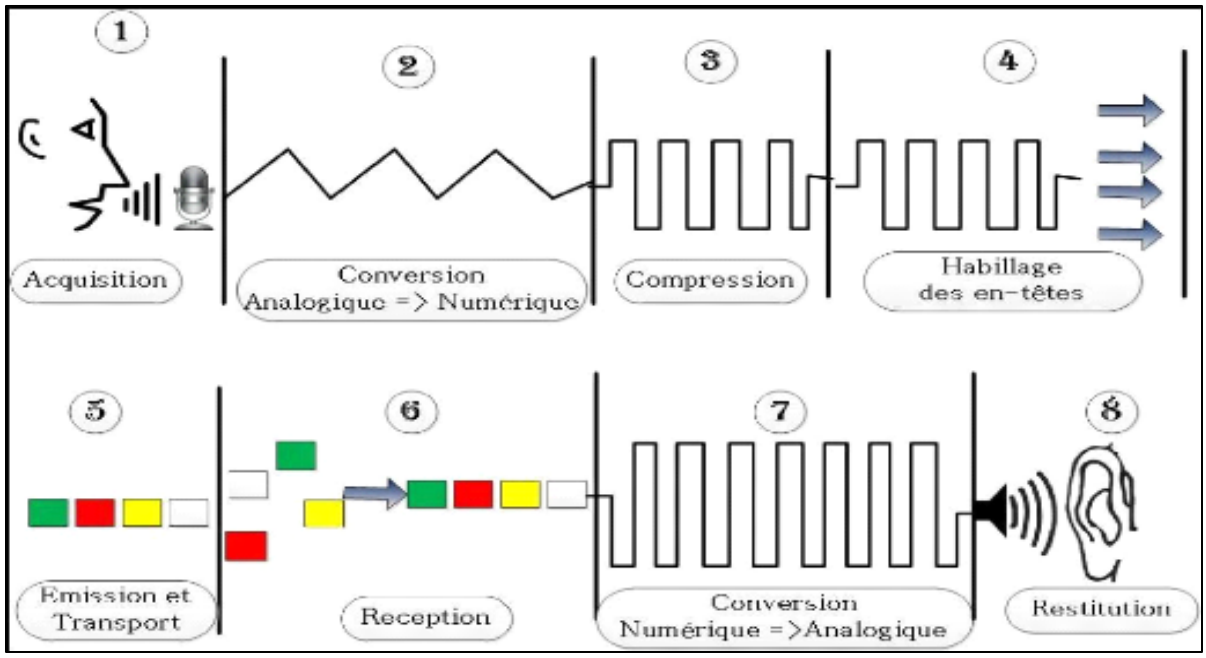

Figure 5 : Processus de traitement de la voix sur IP [2]

Le traitement de la voix sur IP passe par plusieurs étapes à savoir :

- **L'acquisition :** C'est la première étape qui consiste à détecter la voix via un périphérique (téléphone ….)
- **La numérisation :** La bande voix qui est un signal électrique analogique utilisant une bande de fréquence de 300 à 3400 Hz. Ce signal doit d'abord être converti sous forme numérique suivant le format PCM (Pulse Code Modulation) ou G.711 à 64 Kbps.

- **La compression :** Cette opération consiste à réduire la taille physique de blocs d'informations numériques en utilisant un algorithme de compression.
- **L'habillage des entêtes** : le signal numérisé et compressé va être après découpé, en ajoutant des entêtes, il faut prendre en compte l'ordre du réassemblage du paquet, le type du trafic de synchronisation.
- **L'émission et transport :** C'est l'acheminement jusqu'au destinataire dans des paquets IP en utilisant les protocoles du routage.
- **La réception :** La réception des informations émis pendant la transaction
- **La conversion numérique/analogique :** C'est l'étape inverse de la numérisation
- **La restitution :** Résultat finale l'écoute de la voix

2. Les Protocoles utilisés par la VoIP

Un protocole est un langage commun utilisé par l'ensemble des acteurs de la communication pour échanger des données. Dans cette partie on va parler des protocoles de transport de la voix et des protocoles de la signalisation

2.1. Les Protocoles de transport de la voix

Il y a de nombreux protocoles de couches inférieures à celle qui contient l'information voix parmi lesquels TCP (Transmission Control Protocol), UDP (User Datagramme Protocol) et RTP (Real Time Protocol), RTCP (Real Time Control Protocol).

2.1.1. Le protocole RTP

Le protocole RTP (Real-**t**ime **T**ransport) assure la gestion des flux multimédia en mode UDP, il permet aussi la transmission en temps réel des données audio et vidéo sur des réseaux IP et il est utilisé Les appels téléphoniques simples, les audio ou les visioconférences.

Le Protocole **RTP** permet l'identification de type de l'information transportée, l'ajout des numéros de séquence des donnés émise ainsi le contrôle l'arrivée des paquets à la destination

2.1.2. Le protocole RTCP

Le protocole de contrôle (RTCP : Real Time Control Protocol) assure la bonne qualité de service des communications RTP, il permet l'envoi d'un rapport sur la qualité de service(QoS), l'identification et le contrôle de la session

2.2. Les Protocoles de Signalisation

Plusieurs approches sont utilisées aujourd'hui pour assurer les services de la voix sur IP.

Le protocole H323, SIP et MGCP, sont des normes dont les spécifications doivent être respectées par les appareils de téléphonie sur IP pour assurer l'interopérabilité.

2.2.1. Le protocole SIP

Le protocole SIP est un protocole d'établissement de sessions multimédia, conçu pour l'Internet. SIP est un protocole client/serveur, sa fonction principale est l'établissement de session entre deux ou plusieurs utilisateurs ou plus généralement entre des systèmes possédant des adresses de type URI (Uniform Resource Identifier).

Le protocole SIP assure :

- La localisation des terminaux (usagers).
- Détermination de la disponibilité des participants (accessibilité).
- Détermination de la capacité ou des paramètres des terminaux.
- La gestion de l'établissement et le contrôle de la session.

Pour fonctionner, SIP se base sur une architecture comportant des principaux acteurs

Ci-dessous une description détaillée des différentes entités

- **L'entité Terminal Utilisateur**

Le terminal est l'élément dont dispose l'utilisateur pour appeler et être appelé. Il doit donc permettre de composer des numéros de téléphone. Il peut se présenter sous la forme d'un composant logiciel (un programme lancé à partir d'un ordinateur).

Le terminal est appelé UA (User Agent). Il est constitué de deux sous-entités à savoir la partie cliente, appelée UAC (User Agent Client) qui est chargée d'émettre les requêteset la partie serveur, appelée **UAS** (User Agent Server), qui est en écoute, reçoit et traite les requêtes. C'est l'**UAS** qui répond à un appel. L'association des requêtes et des réponses entre deux entités de type **UA** constitue un dialogue.

- **L'entité Serveur Proxy** (SIP Proxy Server)

Un serveur proxy a la charge de router les messages SIP.

- **L'entité Serveur d'enregistrement** (Registrar Server)

Lors de l'activation d'un terminal dans un réseau, la première action initiée par celui-ci consiste à transmettre une requête d'enregistrement auprès du serveur d'enregistrement afin de lui indiquer sa présence dans le réseau.

C'est la requête REGISTER, que l'utilisateur envoie à destination du serveur d'enregistrement. Celui-ci sauvegarde cette position en l'enregistrant auprès du serveur de localisation. L'enregistrement d'un utilisateur est constitué par l'association de son identifiant.

- **L'entité Serveur de Redirection (Redirect Server)**

Le serveur de redirection (Redirect Server) agit comme un intermédiaire entre le terminal client et le serveur de localisation. Il est sollicité par le terminal client pour contacter le serveur de localisation afin de déterminer la position courante d'un utilisateur.

- **L'entité Serveur de localisation**

Le serveur de localisation (Location Server) joue un rôle complémentaire par rapport au serveur d'enregistrement en permettant la localisation de l'abonné. Ce serveur contient la base de données de l'ensemble des abonnés qu'il gère.

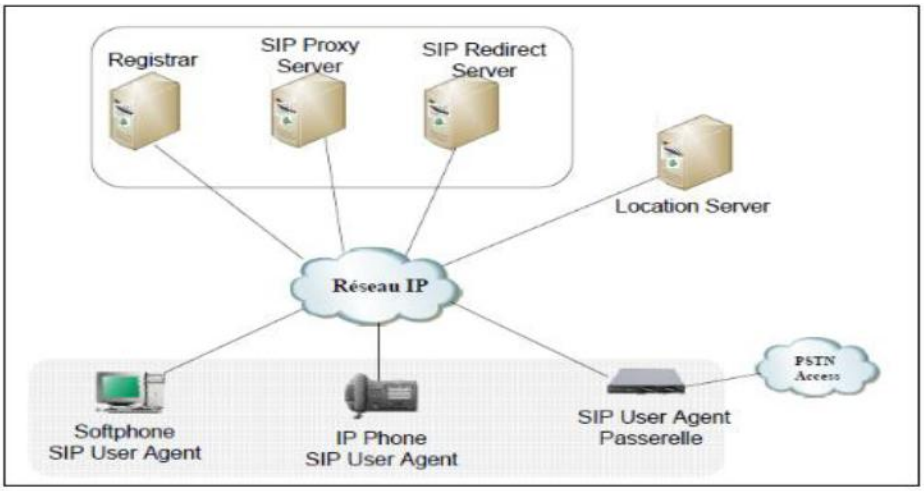

Figure 6 : ARCHITECTURE SIP [3]

Passons maintenant à étudié Les principaux types et formats du message SIP qui sont des réponses ou bien des demandes (Des Requêtes SIP).

- INVITE : Pour l'ouverture d'une session.
- MESSAGE : Défini dans la [RFC 3428], pour l'envoi de messages instantanés.
- NOTIFY : Défini dans la [RFC 3265], pour l'envoie de notifications d'évènements.
- OPTIONS : Permet d'obtenir les capacités du terminal distant.
- PRACK : Défini dans la [RFC 3262], elle assure la transmission fiable des réponses
- Provisoires (nécessaire pour l'interfonctionnement avec le réseau mobile « GSM », par exemple).
- REFER : Défini dans la [RFC 3515], elle permet le transfert ou la redirection d'appels.
- SUBSCRIBE : Définie dans la [RFC 3265], pour recevoir une notification d'événement.
- UPDATE : Définie dans la [RFC 3311], pour la mise à jour des paramètres de la session (en cours de dialogue).

- ACK : Pour confirmer la réponse finale (ex. 200 OK).
- BYE : Pour libérer l'appel.
- CANCEL : Pour annuler une requête précédente.
- INFO : Définie dans la [RFC 2976], pour le transport d'informations supplémentaires (ex. tonalités DTMF), ces informations ne changent pas l'état général de l'appel.

La figure ci-dessous décrit l'établissement d'une communication à travers le protocole SIP [4].

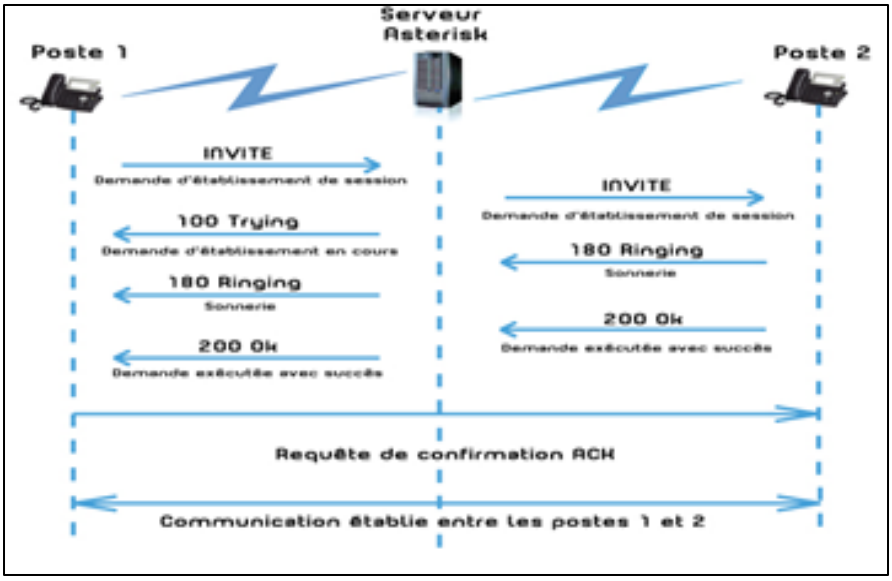

Figure 7 :scénario de communication (dialogue Sip)

- Une requête INVITE de l'utilisateur au serveur.
- Le proxy envoie un TRYING 100 pour arrêter les diffusions et rediriger la demande à l'utilisateur poste2.
- L'utilisateur poste2 envoie une sonnerie 180 lorsque le téléphone se met à sonner, et il est également réacheminer par le mandataire à l'utilisateur.
- Enfin, le message 200 OK correspond à accepter le processus (la réponse utilisateur B de conversation).La communication est établie

2.2.2. Le protocole H323

H.323 regroupe un ensemble de protocoles de communication de la voix, de l'image et de données sur IP. C'est un protocole développé par l'UIT-T qui le définit comme : « systèmes de communication multimédia en mode paquet ».

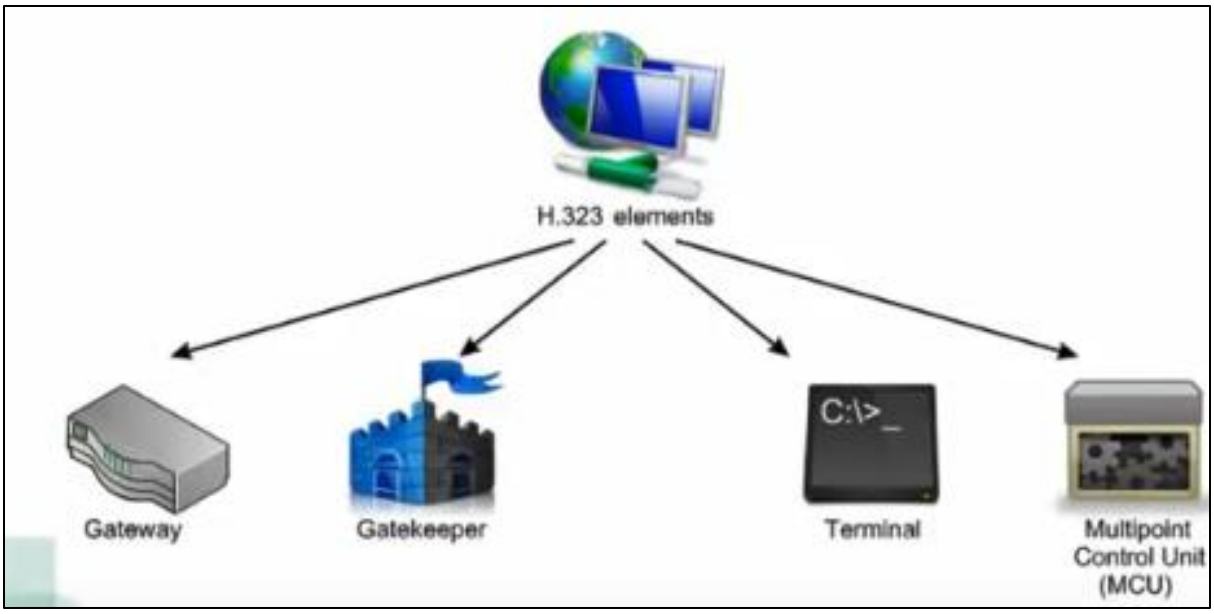

Figure 8 : Les principaux acteurs du protocole h323

- Les terminaux : participation à une session multimédia
- Les passerelles **Gateway** : assure l'interconnexion entre le réseau h323 et les autres réseaux téléphoniques (RTC, SIP…) Les portiers **Gatekeeper** : se charge de l'enregistrement des clients et s'occupe des traductions d'adresse (numéro de tel, adresse IP).
- Unité de contrôle multipoint **Les MCU (Multipoint Control Unit)** : permet au client de se connecter aux sessions des conférences de donnés.

Passons maintenant à expliquer le déroulement de la session H323 entre deux utilisateurs via un Gatekeeper [5].

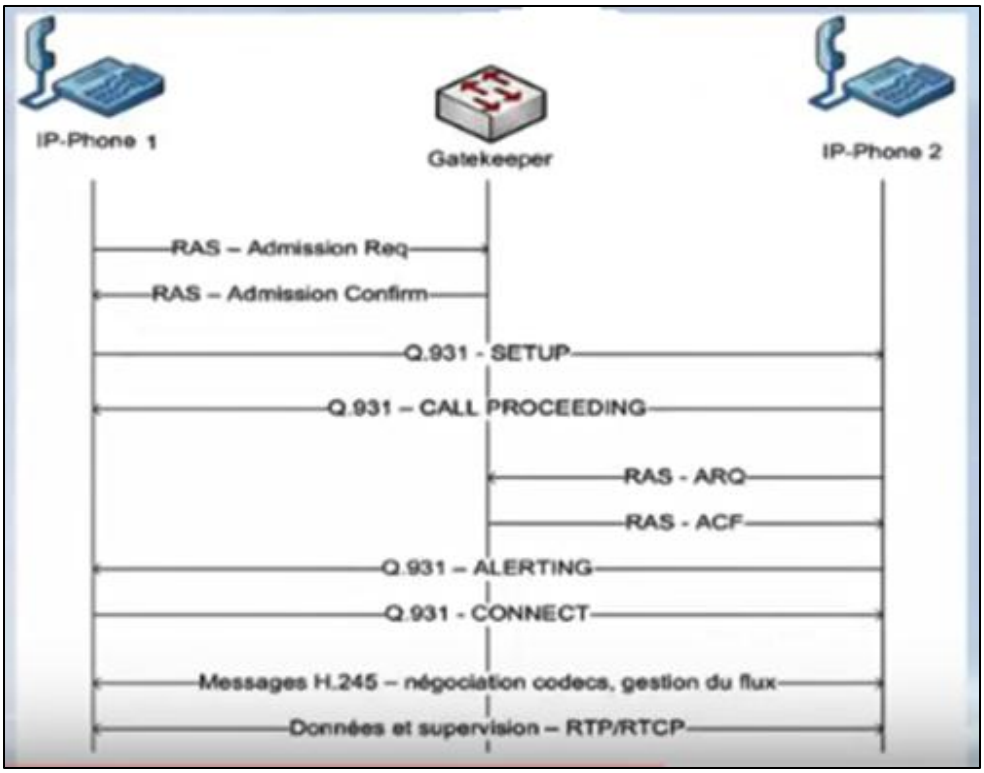

Figure 9 : communication téléphonique avec h323

Comme montre la figure ci-dessous, une communication H.323 se déroule en cinq phases :

1- L'établissement d'appel.

2- L'échange de capacité.

3- réservation éventuelle de la bande passante à travers le protocole RSVP (Ressource réservation Protocol), l'établissement de la communication audio-visuelle.

4- L'invocation éventuelle de services en phase d'appel (par exemple, transfert d'appel, changement de bande passante, etc.).

5- Enfin la libération de l'appel.

On va citer quelques avantages et inconvénients du protocole H323

Un Support Multipoint : la possibilité de faire des conférences multipoint en utilisant une structure centralisée de type MCU (Multipoint Control Unit) ou en mode ad-hoc.

La gestion de la bande passante : le protocole H.323 permet la meilleur gestion de la bande passante, pour assurer le bon fonctionnement des applications indiquées sur le LAN, H323 pose des limites au flux audio/vidéo. La possibilité qu'un terminal H.323 procède à l'ajustement de la bande passante et la modification du débit en fonction du comportement du réseau en temps réel (perte de paquets**,** latenceet gigue).

Support Multicast : Le protocole H.323 donne la possibilité de faire des transmissions en multicast.

Flexibilité : une conférence H.323 peut inclure des terminaux hétérogènes (studio de visioconférence, PC, téléphones…) qui peuvent partager selon le cas, de la voix de lavidéo et même des données grâce aux spécifications T.120.

La complexité de mise en œuvre : les problèmes d'architecture en ce qui concerne la convergence des services d'Internet et de téléphone, plus qu'un manque de souplesse etde modularité.H323 Comprend plusieurs options susceptibles implémentées d'une façon différentes par les constructeurs donc la possibilité d'avoir des problèmes d'interopérabilité.

2.2.3. Comparaison entre SIP et H323

Ci-dessous un tableau de comparaison entre les deux fameux protocoles IP.

Tableau 1 : Tableau de comparaison H323 et SIP

	H323	**SIP**
Nombres d'échange pour établir la connexion	6 à 7 aller-retour	1 à 5 aller-retour
Complexité	Elevée	Faible
Implémentation de nouveaux services	NON	OUI
Protocole de transport	TCP	TCP ou UDP
Coût	Elevé	Faible
Avantages	Maturitédu protocole.	Simple à mettre en œuvre. messages écrits en clair.

3. Les codeurs et décodeurs audio de la voix sur IP

Le codec est une abréviation pour Codeur/Décodeur. Un codec est basé sur un algorithme qui permet la compression des données qu'on lui donne. Il s'agit d'un procédé permettant de compresser et de décompresser un signal, de la vidéo oude l'audio, souvent en temps réel. Le codec permet une réduction de la taille du fichier original. Le codec compresse et numérise la voix de l'émetteur, ainsi les données numériques sont encapsulées dans des paquets IP et acheminées vers le destinataire. A la destination grâce au même codec décompresse et restitue le son. Il On distingue des codecs sans pertes et des codecs à pertes.

Un codec à pertes distingue les parties moins importantes des informations et les supprime pour gagner en taille.

Un codec sans pertes tout le signal est transformé en binaire et le décodage restitue des données parfaitement identiques à celles données en entrée. Ce type de codecs est utilisé quand la qualité de la restitution est importante.

Codec	Débit (Kbs)	Type de codeur	Délai algo. (ms.)	Qualité (score MOS)
G.711 (UIT-T)	64	« forme d'onde » (PCM)	0.125	4.2
G.726 (UIT-T)	16/24/32/40	« forme d'onde » (ADPCM)	0.125	2/3.2/4/4.2
G.728 (UIT-T)	16	« ABS » (LD-CELP)	2.5	4
G.729 (UIT-T)	8	« ABS » (CS ACELP)	15	4
G.723.1 (UIT-T)	6.3/5.3	« ABS » (MP-MLQ/CS-ACELP)	37.5	3.9/3.7
G.722 (ITU-T)	48/56/64	« forme d'onde » (ADPCM)	1.5	<4.1
G.722.1 (ITU-T)	24/32	« forme d'onde » (MLT)	40	5
G.722.2 (ITU-T)	6.6…23.85	« ABS » (CELP)	25	<4.5
GSM fr (ETSI)	13	« ABS » (RPE-LTP)	20	3.71
GSM hr (ETSI)	5.6	« ABS » (VCELP)	20	3.85
GSM efr (ETSI)	13	« ABS » (AS-ACELP)	20	4.43

Figure 10:Caractéristiques des principaux codeurs de parole

G.711 : Ce codec est le premier à avoir été utilisé dans la VoIP. Même si il existe maintenant des codecs nettement plus intéressants, celui-ci continue d'être implémenté dans les équipements à des fins de compatibilité entre marques d'équipements différentes.

G.722 : A la différence du G.711, ce codec transforme le spectre jusqu'à 7kHz ce qui restitue encore mieux la voix. Les débits que ce codec fournit sont 48,56 ou 64kbit/s. Une des particularités est de pouvoir immédiatement changer de débit. Ceci est fortement appréciable lorsque la qualité du support de transmission se dégrade.

G.722.1 : Dérivé du codec précédent, celui-ci propose des débits encore plus faibles (32 ou 24kbit/s). Il existe même des versions propriétaires de ce codec fournissant un débit de 16kbit/s.

G.723.1 : C'est le codec par défaut lors des communications à faible débit. On distingue deux modes. Le premier, un débit de 6,4kbit/s et le deuxième un débit de 5,3kbit/s [5].

4. Etude de la sécurisation de la voix sur IP

Dans ce volet, nous dériverons des attaques qui menacent la VoIP, et nous détaillerons quelques-uns. Nous finirons par une description des bonnes pratiques pour sécuriser les communications de type voix sur IP.

Les attaques sur les réseaux VoIP peuvent être classées en deux types à savoir **les attaques externes** sont lancées par des autres personnes que celle qui participe à l'appel, et ils se produisent généralement quand les paquets VoIP traversent un réseau peu fiable et/ou l'appel passe par un réseau tiers durant le transfert des paquets, ainsi **Les attaques internes** s'effectuent

directement du réseau local dans lequel se trouve l'attaquant, Lesystème VoIP utilise l'Internet, et particulièrement le protocole IP. De ce fait les vulnérabilités de celui-ci. [8]

4.1. Les attaques sur le protocole VOIP

Les protocoles de la VoIP utilisent UDP et TCP comme moyen de transport et par conséquent sont aussi vulnérables à toutes les attaques contre ces protocoles, telles le détournement de session (TCP) (session Hijacking) et la mystification (UDP) (Spoofing), etc.

Les types d'attaques les plus fréquentes contre un system VoIP sont :

4.2. L'attaque par suivie des appels

Appelé aussi Call tracking, cette attaque se fait au niveau du réseau LAN/VPN et cible les terminaux (soft/hard phone). Elle a pour but de connaître qui est en train de communiquer et quelle est la période de la communication. L'attaquant doit récupérer les messages INVITE et BYE en écoutant le réseau et peut ainsi savoir qui communique, à quelle heure, et pendant combien de temps.Pour réaliser cette attaque, L'attaquant doit être capable d'écouter le réseau et récupérer les messages INVITE et BYE.

4.3. Le Sniffing

Un reniflage (Sniffing) peut résulter un vol d'identité et la récupération des informations confidentielles, aussi bien des informations sur les systèmes VoIP. Ces informations peuvent être employées pour mettre en place une attaque contre d'autres systèmes ou données.

L'IP sniffing est une attaque passive, il est décrit comme le suivant,

1. L'intrus est placé sur un réseau.
2. l'intrus met sa station en mode écoute.
3. la station récupère l'ensemble du trafic échangé sur le réseau.
4. L'intrus utilise un analyseur de protocoles réseau à l'insu des administrateurs du réseau.

4.4. Le déni de service (DOS : Denial of service)

L'attaque en déni de service consiste à surcharger le serveur Web de requêtes jusqu'à ce qu'il ne puisse plus suivre et s'arrête. Bloquant ainsi les communications internes, externes et aussi le système d'information.

Par exemple un nombre trop important de messages SIP INVITE ou de simples messages ICMP peuvent créer une situation de déni de service.Cette pratique vise à rendre un tel service sur un réseau indisponible, cette attaque peut être effectuée sur plusieurs couches du modèle OSI :

- **Attaque à travers la couche réseau**

IP Flooding : consiste à envoyer des paquets IP vers une même destination de telle sorte que le traitement de ces paquets empêche une entité du réseau de traiter les paquets IP légitimes.

- **Attaque à travers la couche transport**

L'UDP Flooding Attacks :

Le principe c'est l'envoie d'un grand nombre de requêtes UDP vers une machine pour saturer le trafic transitant sur le réseau.

TCP SYN floods :

Cette attaque se base sur le protocole TCP exactement lors de l'établissement de la connexion entre les interlocuteurs, le scénario se fait comme suit :

Le client envoie un paquet SYN au serveur, Le serveur répond avec un paquet SYN-ACK, Le client envoie un paquet ACK au serveur.

L'attaque consiste en **l'envoie d'un grand nombre de paquets SYN.** La victime va alors répondre par un message SYN-ACK d'acquittement. Pour terminer la connexion TCP, la victime ensuite va attendre pendant une période de temps la réponse par le biais d'un paquet ACK final qui ne sont jamais envoyés, et par la suite, la mémoire système se remplit rapidement et consomme toutes les ressources disponibles à ces demandes non valides. Le résultat final est que le serveur, le téléphone, ou le routeur ne sera pas en mesure de faire la distinction entre les faux SYN et les SYN légitimes d'une réelle connexion VoIP.

- **Attaque à travers la couche applications**

SIP Flooding : c'est une attaque qui touche les terminaux tels que les téléphones IP via les mécanismes du protocole SIP et les attaques DOS citant :

- **Attaque dos via la requête CANCEL**

C'est un exemple de déni de service lancé contre l'utilisateur, l'attaquant surveille l'activité du proxy SIP et attend qu'un appel arrive à un utilisateur spécifique. Une fois que l'utilisateur reçoit la requête INVITE par son dispositif, alors l'attaquant envoie immédiatement une requête CANCEL, cette requête provoque une erreur sur le dispositif de l'appelé et bloque l'appel. [6]

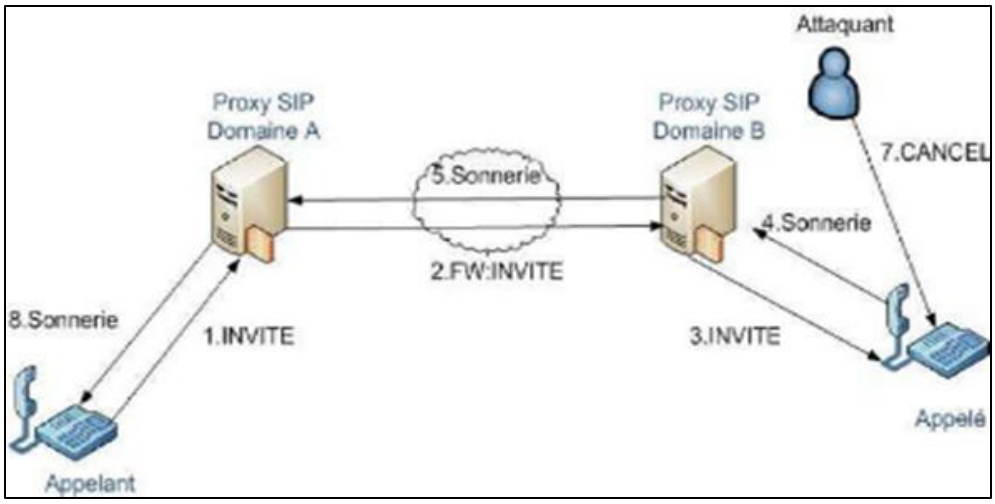

Figure 11:Attaque Dos avec la méthode cancel

4.5. Attaque par écoute clandestine

Cette attaque consiste à écouter et à décoder la conversation entre deux utilisateurs.

Le principe de l'écoute clandestine est montré dans la figure comme suit :

1. La détermination des adresses MAC des victimes (client-serveur) par l'attaquant.
2. L'attaquant envoie une requête ARP au client, pour l'informer du changement de l'adresse MAC du serveur VoIP.
3. L'attaquant envoi une requête ARP au serveur, pour informer le changement de l'adresse MAC du client.
4. Désactiver la vérification des adresses MAC sur la machine d'attaque afin que le trafic puisse circuler entre les 2 victimes.

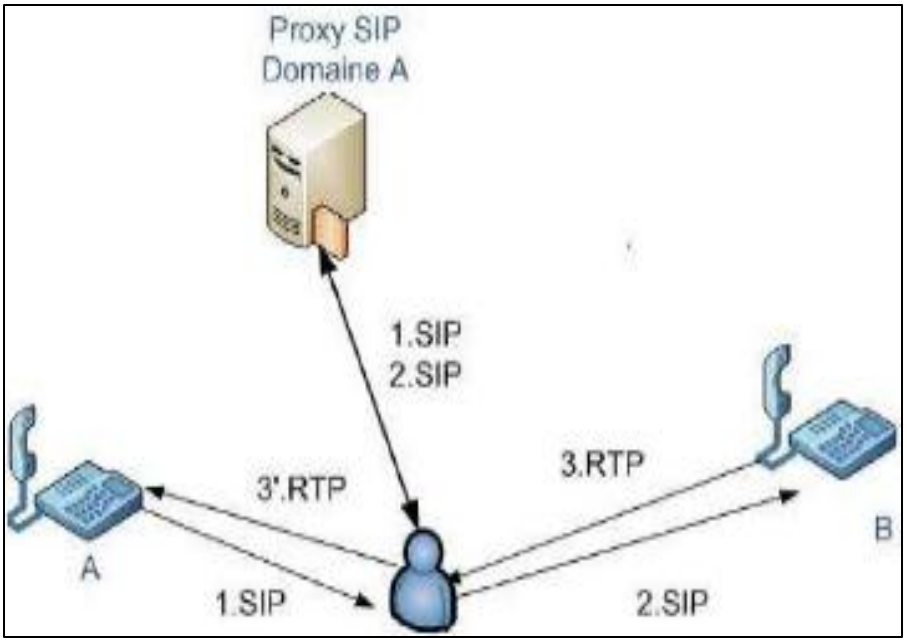

Figure 12:scénario du l'écoute clandestine

4.6. Attaque par la compromission de serveurs

Cette attaque vise à contrôler le serveur SIP afin d'avoir le pouvoir de changer n'importe quel paramètre relatif à l'appel et d'implanter n'importe quel code malveillant (vers, virus...) dans le serveur SIP.

4.7. Les bonnes pratiques de sécurité

Ci-dessous on va présenter les bonnes pratiques d'implémentation d'une solution de VoIP

4.7.1. La protection physique

Il est conseillé que les équipements critiques de la VoIP (serveurs) soient dans une salle informatique équipée et bien sécurisé par un système d'alarme, un anti-incendie, de la vidéo surveillance, d'un accès par badge et d'un onduleur.

4.7.2. La protection des postes de travail pour les soft phones

La sécurisation d'un soft phone contre les codes malveillants et l'usurpation d'identité par exemple par l'utilisation des mots de passe contenant plus de 10 chiffres.

4.7.3. L'utilisation des pare-feu

Un pare-feu aide et assure le contrôle du trafic entrant et sortant du réseau, ce dernier permet de réduire les attaques de déni de service en filtrant les ports et les appels à travers le réseau IP.

4.8. Les mesures de sécurités

Les vulnérabilités existent au niveau applicatif, protocole et systèmes d'exploitation. Pour cela, on a découpé la sécurisation aussi en trois niveaux :

-Sécurité au niveau protocolaire

-Sécurité au niveau applicatif

-Sécurité au niveau système de l'exploitation.

4.8.1. Les mesures de sécurité au niveau protocolaire

Consiste à implémenter les mesures de sécurité nécessaire pour combler les lacunes au niveau protocolaire, prenant un exemple, les services de sécurités offertes par SRTP (version sécurisé du protocole RTP)

- La confidentialité des données RTP.
- L'authentification et la vérification de l'intégrité des paquets RTP.
- La protection contre le rejeu des paquets, chaque client SIP tient à jour une liste de tous les indices des paquets reçus et bien authentifiés.

4.8.2. Les mesures de sécurité au niveau système de l'exploitation.

Le système dans lequel on héberge notre application serveur est ciblé, ce qui présente un risque d'affectation des fichiers de configuration contenant des informations sur les clients enregistrés. Il faut prendre plusieurs mesures de sécurités pour le protéger à savoir :

- L'utilisation d'un système d'exploitation stable tout en installant les derniers mis à jours recommandés.
- L'utilisation d'un mot de passe formé de plusieurs combinaisons de lettre, de chiffres et de ponctuations.

4.8.3. Sécurité au niveau applicatif

Pour sécuriser le serveur, on recommande :

- L'utilisation d'une version stable contenant les derniers mis à jours recommandés par le fournisseur aussi bien la partie client et serveur.
- La création d'un environnement de test dans lequel on va tester les mises à jour des applications utilisé et ce avant de leurs installation dans un environnement de production.
- A ne pas utiliser la configuration par défaut qui sert juste à établir des appels. Elle ne contient aucune mesure de sécurité.
- A ne pas installer les Softphones dans le serveur.

Pour notre application, la sécurité c'est une étape primordiale, après des recherches, la société a choisi Snort système de détection d'intrusion réseau ou NIDS, Snort permet de surveiller les données de package envoyées et reçues via une interface réseau spécifique. Il permet aussi de détecter les menaces ciblant les vulnérabilités de votre système à l'aide de technologies de détection et d'analyse de protocole basées sur des signatures.

Il existe plusieurs endroits où nous pouvons mettre en place notre NIDS.

Le schéma ci-dessous illustre un réseau local ainsi que les trois positions que peut y prendre un IDS [7].

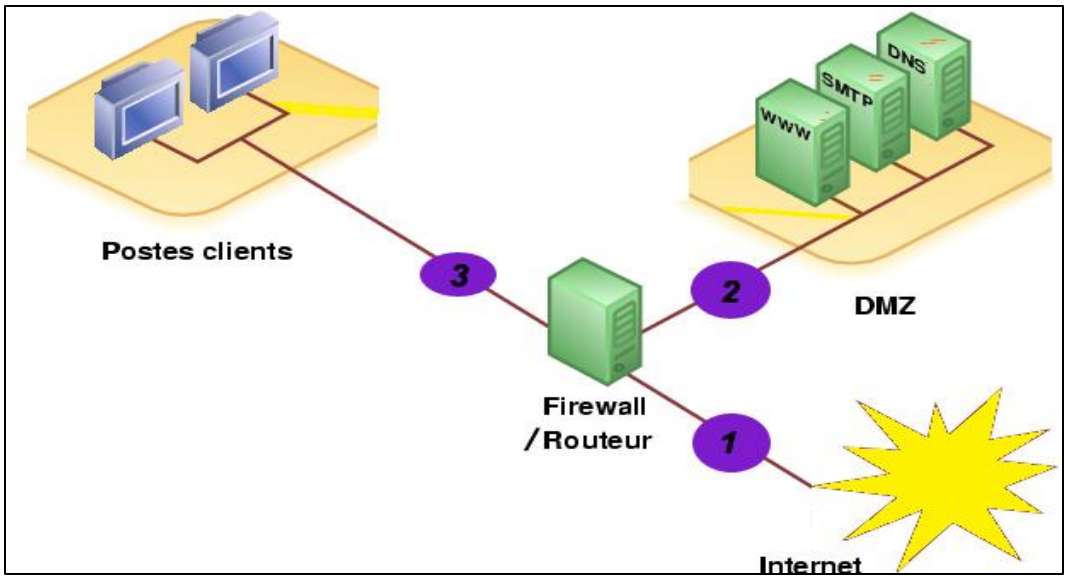

Figure 13: les différents emplacements de Snort

En se basant sur la figure ci-dessous, nous pouvons mettre en place Snort

- **Juste avant le routeur internet**

  Ici, notre NIDS va détecter l'ensemble des attaques frontales provenant de l'extérieur, en amont du firewall.

- **Dans le DMZ**

  Ici, notre NIDS est placé sur la DMZ (Zone dématérialisé), il détectera les attaques qui n'ont pas été filtrées par le firewall et qui relèvent d'un certain niveau de compétence.

- **Avec les postes clients**

  Ici, notre NIDS va détecter les attaques internes, provenant du réseau local de l'entreprise. Il peut être judicieux d'en placer un à cet endroit étant donné le fait que 80% des attaques proviennent de l'intérieur.

Conclusion

Dans ce chapitre, on a présenté le principe de la VoIP, nous avons présenté les deux fameux protocoles de la voix IP à savoir le protocole SIP et le protocole H232, après, nous avons décrit dans la voix IP les attaques et les vulnérabilités au niveau protocolaire, applicatif et système de d'exploitation.

Enfin, on a décrit les bonnes pratiques et on a suggéré les bonnes mesures de sécurité.

Dans le chapitre suivant, on présentera Spécification des besoins et conception

CHAPITRE 3 : SPECIFICATION DES BESOINS ET CONCEPTION

Introduction

Après avoir présenté des notions théoriques de la VoIP dans le chapitre 2, ce chapitre met l'accent sur les besoins auxquels notre application VoIP via serveur IP PBX(ASTERISK) doit répondre.

Nous allons présenter en premier lieu les besoins fonctionnels et non fonctionnels, puis nous allons présenter la partie conception.

1. Les besoins fonctionnels

Les besoins fonctionnels ou besoins métiers représentent les actions que le système doit exécuter, le projet doit couvrir principalement les besoins fonctionnels suivants :

- **La gestion des utilisateurs :** permet l'ajout, la suppression, la modification des utilisateurs (client SIP) par un administrateur.
- **La gestion des appels :** permet l'envoie et la réception des appels VoIP.
- **La gestion des connexions :** permet l'interconnexion entre l'administrateur et les clients SIP aussi entre eux.
- **La gestion d'un serveur SIP.**

Tableau 2: Les besoins fonctionnels globales

Utilisateur	Opérations
L'administrateur	Authentification (Login et mot de passe) Enregistrer informations client La configuration du serveur Astrerisk Ajouter, supprimer, modifier des utilisateurs. Vérifier la fiabilité et la connexion
Le client SIP	Authentification (Login et mot de passe) Recevoir, émettre… des appels Consulter des services téléphoniques

2. Les besoins non fonctionnels

Après avoir déterminé les besoins fonctionnels, nous présentons ci-dessous l'ensemble des besoins non fonctionnels qui sont des exigences qui ne concernent pas spécifiquement le

comportement du système mais plutôt identifient des contraintes internes et externes à respecter pour garantir la performance du système.

- **La modularité de l'application :**

  L'application doit être claire pour permettre des futures évolutions ou améliorations.

- **L'ergonomie :**

  L'application offre une interface conviviale et facile à utiliser.

- **La sécurité :**

  L'application doit respecter la confidentialité des données.

- **La performance :**

  Un logiciel doit être avant tout performant c'est-à-dire à travers ses fonctionnalités, répond à toutes les exigences des usagers d'une manière optimale.

- **La rapidité de traitement :**

  En effet, vu le nombre important des appels quotidiennes, il est impérativement nécessaire que la durée d'exécution des traitements s'approche le plus possible du temps réel.

3. La modélisation des besoins

Pour mieux s'approcher à la réalisation de notre application « VOIP », on doit traduire les besoins fonctionnels et non fonctionnels sous forme de diagrammes qui expliquent mieux l'interaction utilisateur-application ou application-systèmes de vérification. Le but de la conceptualisation est de comprendre et structurer les besoins du client .Il ne faut pas chercher l'exhaustivité, mais clarifier, filtrer et organiser les besoins.

3.1. Étude conceptuelle

Le modèle conceptuel doit permettre une meilleure compréhension du système il doit servir d'interface entre tous les acteurs du projet. Pour implémenter les diagrammes de l'application, on va utiliser la méthodologie de conception **UML** « UnifiedModelingLanguage, ou Langage de Modélisation Unifié », L'UML est l'outil le plus fréquemment utilisé dans le monde de la modélisation et conception Orienté Objet, il offre une démarche simple et claire dans la modélisation d'un tel projet et il se base sur plusieurs diagrammes dont chacun à ses propriétés et ses valeurs ajoutés pour réaliser une meilleure conception du projet, parmi ces diagrammes dont on va utiliser durant notre projet, on peut citer :

- **Le diagramme de paquetage**

  Ce diagramme permet de découper l'application en grand blocs.

- **Le Diagramme des cas d'utilisation**

  Ce diagramme permet d'illustrer les cas d'utilisations des utilisateurs du système.

- **Le Diagramme de classe**

  Ce diagramme permet de convertir les différents utilisateurs et cas d'utilisation en classes, il a comme objectif de détailler les interactions déroulantes entre ses dernières sous formes de relation et de distinguer les paramètres de chaque cas ou utilisateur.

- **Le Diagramme de Séquences**

  Ce diagramme permet de représenter le déroulement de chaque opération tout en synchronisant avec les différents opérateurs et systèmes (internes ou externes).

3.1.1. Le diagramme de paquetage

A ce niveau, on va découper notre application en blocs ou packages selon les besoins déclarés, chaque package représente un domaine d'utilisation de l'application.

Pour chaque package on va lui affecter l'utilisateur qui va le gérer et le relier avec des autres packages s'il y a une relation entre eux, ci-dessous le digramme de paquetage de notre système.

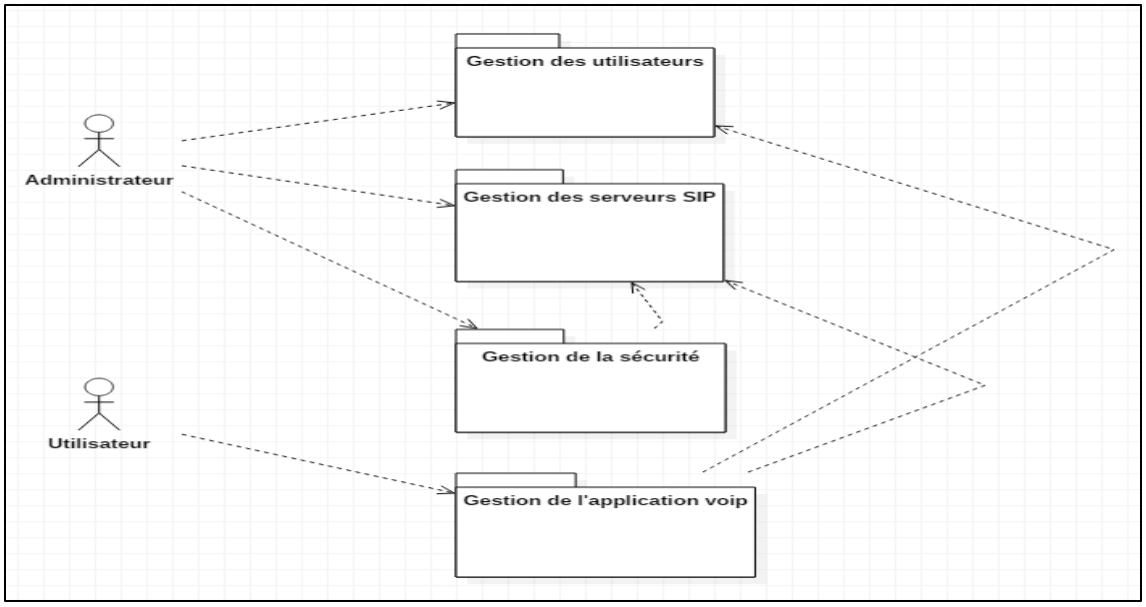

Figure 14: Digramme de paquetage de notre système

Ci-dessous un tableau descriptif du diagramme de paquetage.

Tableau 3 : Descriptif du diagramme de paquetage

Package	Acteur	Package en relation avec
Gestion des utilisateurs	L'administrateur	Gestion des serveurs SIP
Gestion des serveurs SIP (asterisk, freepbx)	L'administrateur	
L'administration du serveur Snort	L'administrateur	
L'administration de l'application VoIP (les Softphone)	L'administrateur Les utilisateurs	Gestion des serveurs SIP, Gestion des utilisateurs

Selon notre tableau récapitulatif, on note également que l'administrateur assure la gestion des utilisateurs et ce à travers le serveur Sip, il assure aussi l'administration du serveur Sip, Snort ainsi les Softphones.

3.1.2. Digramme des Cas d'Utilisation

Le diagramme des cas d'utilisation explique les différentes opérations entre l'utilisateur et le système.

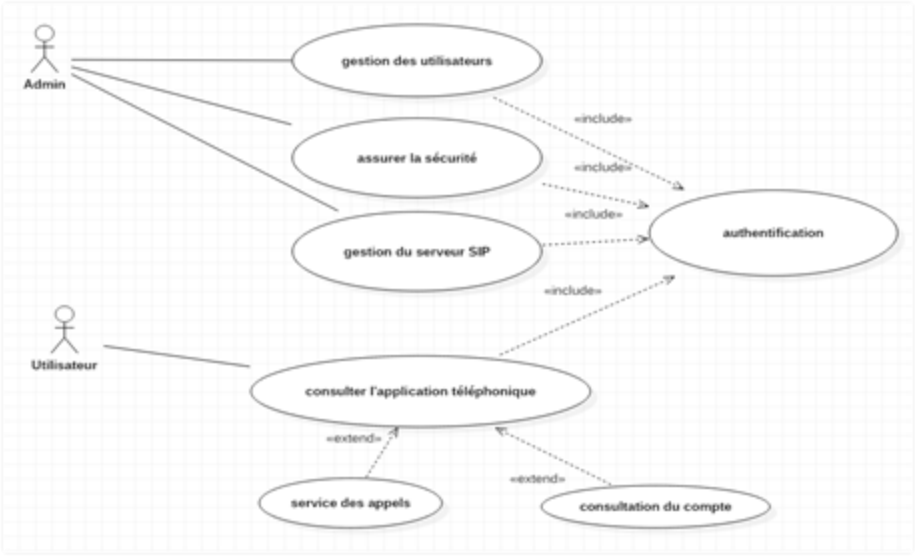

Figure 15 : Diagramme de cas d'utilisation globale

La figure ci-dessous présente les différentes fonctionnalités de notre application VoIP et les interactions entre les intervenants qui sont :

- **L'administrateur :** c'est lui qui gère les trois opérations qui suivent :

  La gestion des utilisateurs, la gestion de la sécurité et la gestion du serveur SIP, il joue le rôle du leader.

- **L'utilisateur :** il est le bénéficiaire de cette application peut consulter le service des appels ou la consultation du son compte (c'est le cas « extend »).

  On note bien ici que tous les cas d'utilisations nécessitent l'authentification de l'utilisateur (« include »)

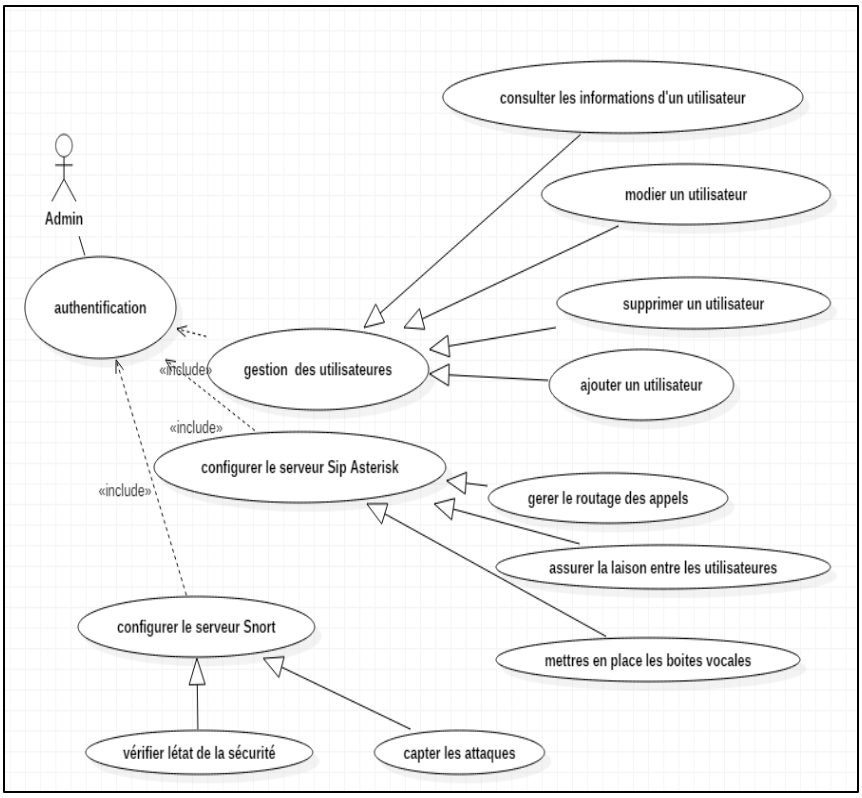

Figure 16 : Diagramme du cas d'utilisation « administrative »

La figure ci-dessous présente en détail les taches exécutées par l'administrateur après avoir établir la phase de l'authentification à savoir :

- **La gestion des utilisateurs**

  L'administrateur peut consulter les informations, supprimer et ajouter des utilisateurs

- **La configuration du serveur SIP Asterisk**

  Ici, l'administrateur assure la mise en place du serveur SIP qui lui permet de gérer le routage des appels, la liaison entre les différents utilisateurs et la mise en place des boites vocales.

- **La configuration le serveur Snort**

  L'administrateur assure la mise en place du serveur Snort qui lui permet de vérifier l'état de la sécurité et détecter les attaques qui peuvent menacer notre application VoIP

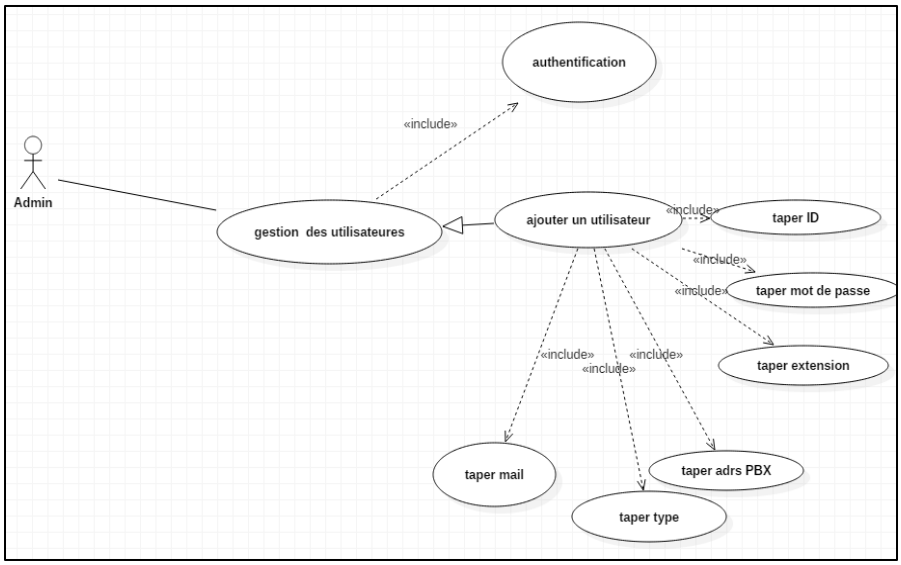

Figure 17 : Diagramme de cas d'utilisation « ajout des utilisateurs »

La figure ci-dessus montre bien que l'administrateur peut ajouter un utilisateur après avoir remplir les champs obligatoires à savoir :

- L'ID (identité déterminant propre à chaque client)
- Le mot de passe (qui est confidentiel)
- L'extension (un numéro du tel)
- L'adresse du PBX (adresse IP fixe)
- L'email

➔(« include »)

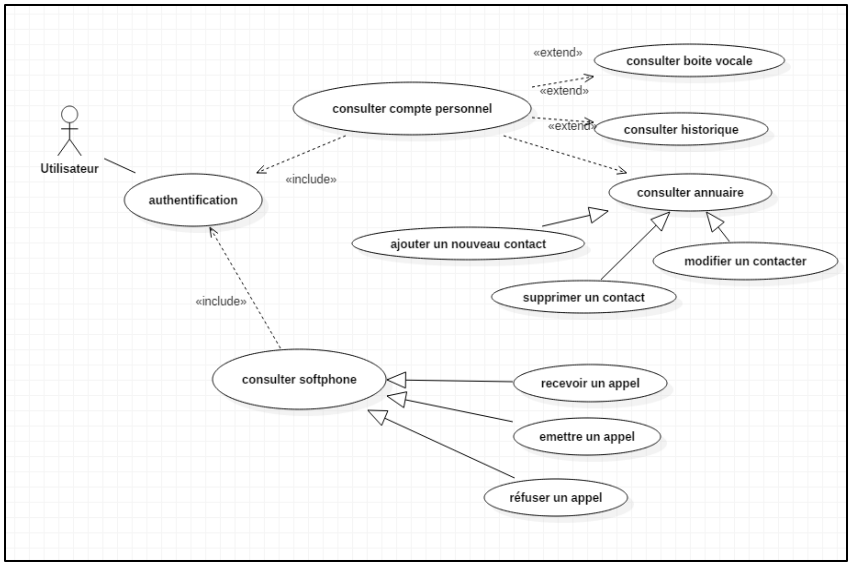

Figure 18 : Diagramme de cas d'utilisation « Utilisateurs »

Comme le montre la figure (figure 18) après l'authentification l'utilisateur peut consulter son compte pour faire le suivie de son historique, consulter sa boite vocale, consulter son annuaire et la gérer ses contacts.

L'utilisateur peut également effectuer des appels via la VoIP.

3.2. Conception détaillée

3.2.1. Digramme de classe

Le diagramme suivant représente le diagramme de classe de la VoIP.

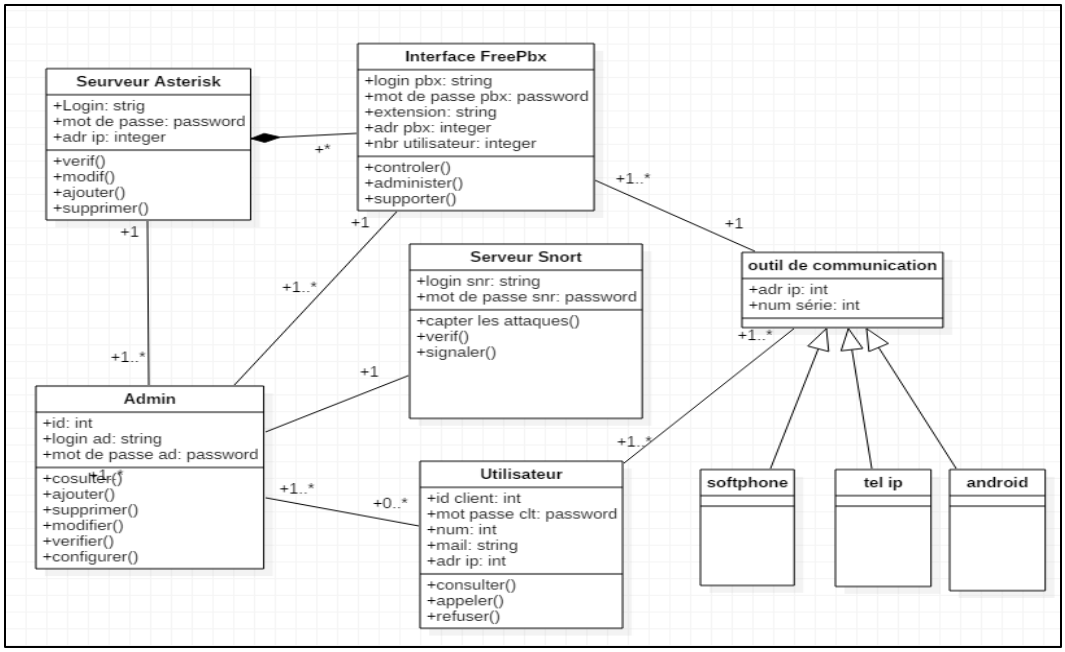

Figure 19 :Le diagramme de classe

Dans cette étape nous allons détailler chaque classe dans un tableau, citons les méthodes et les opérations.

Pour la classe « asterisk » Le serveur Asterisk est représenté par cette classe, les principales fonctionnalités offertes sont :

Tableau 4 : La classe serveur Astrerisk

Champ	**Désignation**
Login	Login du serveur
Mot de passe	Mot de passe du serveur
Adr IP	Adresse IP fixe du serveur
Vérif. () :	permet de vérifier les données provenant des clients s'ils sont compatibles avec ceux qui sont dans les fichiers de configuration ou non.
Ajouter () :	Ajouter un utilisateur
Supprimer () :	Supprimer un utilisateur
Modifier () :	Modifier un utilisateur

Pour la classe « Freepbx » Le serveur Freepbx est représenté par cette classe, les principales fonctionnalités offertes sont :

Tableau 5 : La classe Freepbx

Champ	**Désignation**
Login	Login du serveur
Mot de passe	Mot de passe du serveur
Extension	Extension d'utilisateur
Adr pbx	Adresse IP du serveur
Nbr utilisateur	Le nombre des utilisateurs
Contrôler () : Administrer () : Consulter () :	Contrôler uniquement l'application Gérer toute l'application Consulter uniquement l'application

Tableau 6: La classe utilisateur

Champ	**Désignation**
Id client	Un identifiant de la personne
Mot de passe clt	Mot de passe donné a chaque utilisateur
Num	Numéro du téléphone
Mail	mail de la personne
Adr	Adresse de la personne
Consulter () : Appeler () Refuser () :	Consulter annuaire, boite vocal et les contacts Appeler d'autre utilisateur Refuser des appels téléphoniques

Tableau 7: La Classe Admin

Champ	**Désignation**
Id	CIN de la personne
Login	Nom de la personne
Mot de passe	Prénom de la personne
Gérer () : Vérifier () : Configurer () :	Ajouter, supprimer et modifier les utilisateurs Vérifier les comptes utilisateurs Configurer l'application

3.2.2. Diagrammes de séquences

Le diagramme de séquence permet de représenter les vues dynamiques du système. En effet, il montre les collaborations entre les objets selon un point de vue temporel en mettant l'accent sur la chronologie des envois de messages.

Dans cette partie, on va décrire quelque scénario pour mieux comprendre le fonctionnement de la VoIP.

Le serveur SIP Asterisk gère les appels téléphoniques entre les utilisateurs.

Chaque utilisateur possède un numéro de téléphone unique.

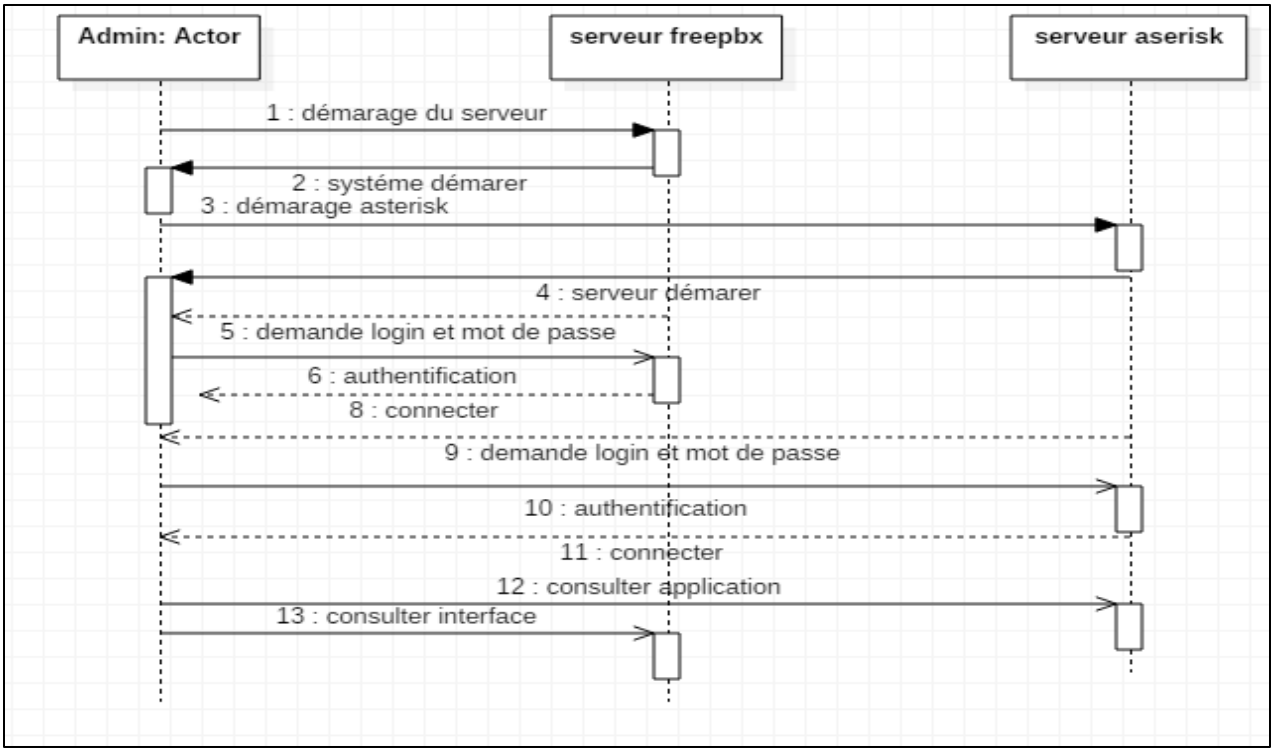

Figure 20: Diagramme de séquences de l'authentification

Pour qu'un administrateur puisse consulter l'application, le système effectue les opérations suivantes :

1-L'administrateur doit démarrer le serveur Asterisk

2-l'administrateurs'authentifie

3-Le système vérifie les paramètres saisis de l'administrateur

Si les paramètres sont valides, l'administrateur sera connecté

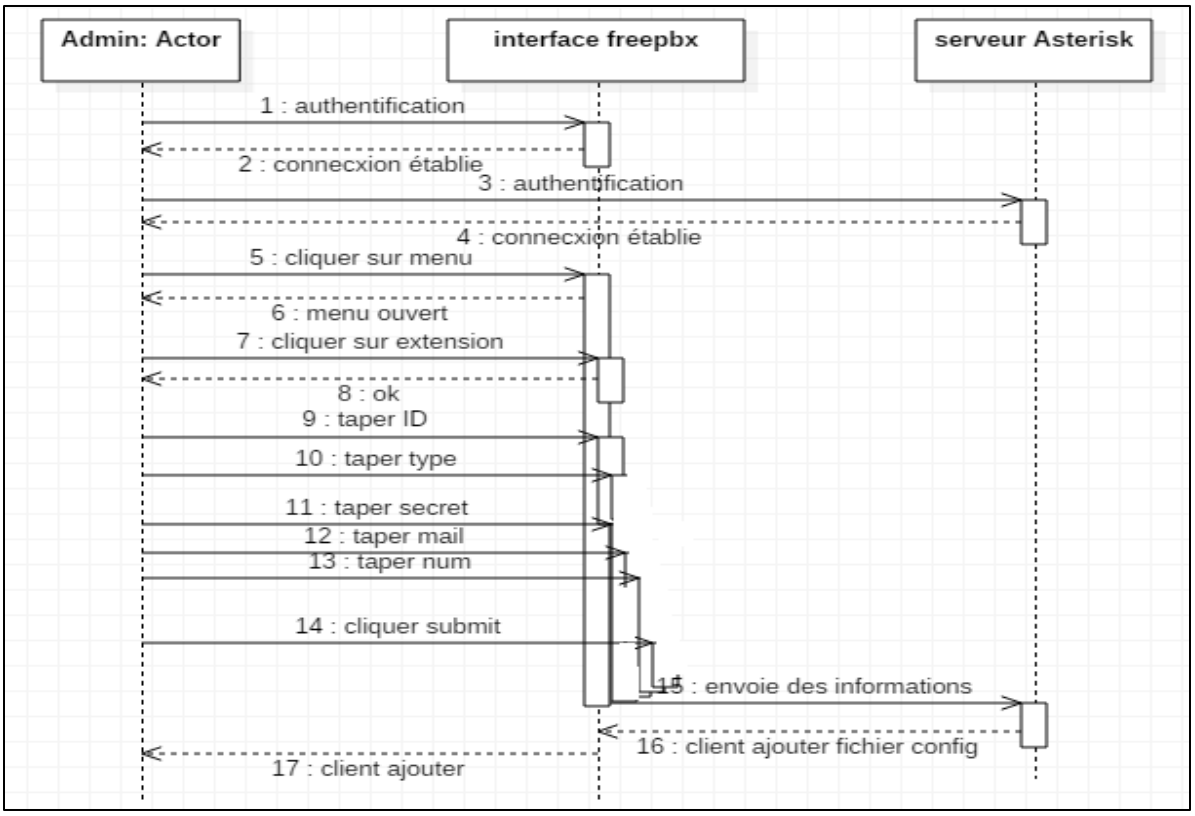

Figure 21 : Diagramme de séquences ajouter un utilisateur

Pour qu'un administrateur peut ajouter des clients : les étapes suivantes doivent se faire entre l'administrateur et le système :

1- L'administrateur doit principalement se connecter au système par une demande d'authentification.
2- Le système lui confirme l'authentification.
3- L'administrateur doit remplir les champs obligatoire (ID, type, secret, num, mail) pour chaque utilisateur.
4- L'administrateur valide l'envoie des informations au serveur asterisk via interfaçage freepbx.
5- Le système lui confirme l'ajout.

Pour qu'un utilisateur peut réaliser une communication il y a des scénarios à suivre ci-dessous la figure du diagramme de séquence.

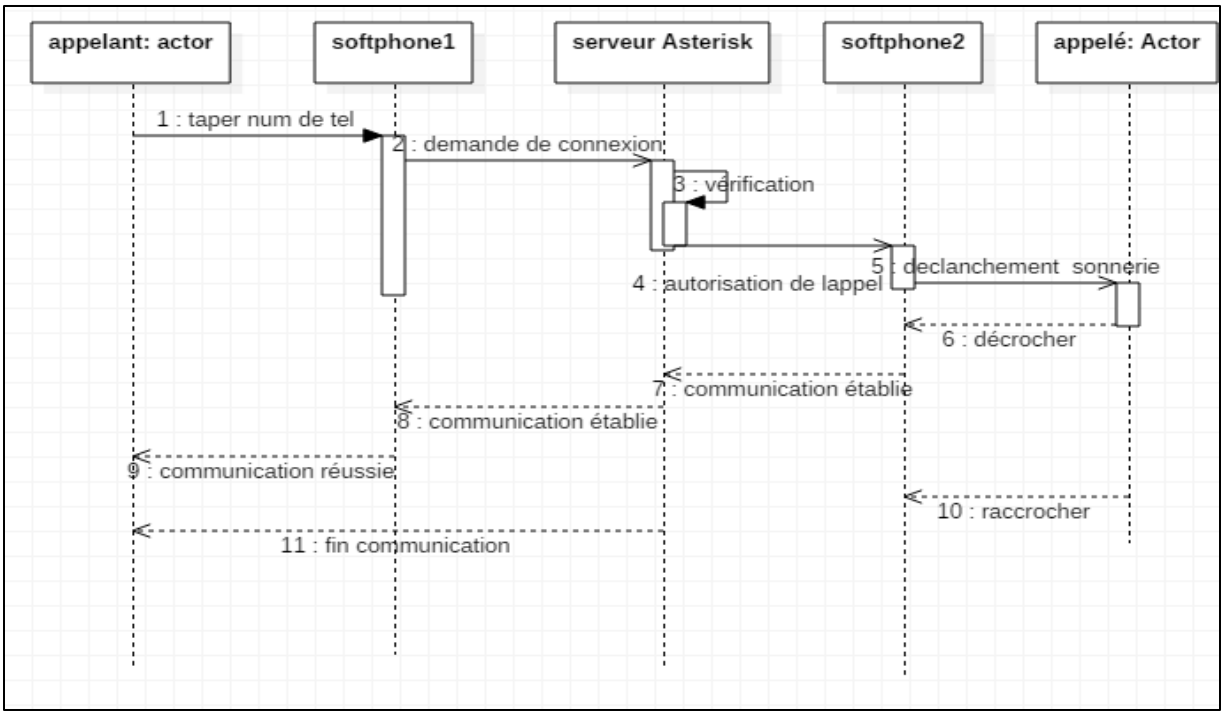

Figure 22: Diagramme de séquences communication réussie

Chaque utilisateur possède un numéro de téléphone unique.

1- L'utilisateur compose le numéro souhaité.

2- Le serveur établit une connexion avec le poste cible.

3- Le système Autorisation de l'appel vers le destinataire.

4- Déclenchement de la sonnerie chez l'appelé.

5- Etablissement de la communication.

Si le poste de l'appelé est occupé, un signal prévient l'appelant, une fois que l'appelé devient disponible, ce dernier peut visiter sa boite de messagerie vocale et écouter les messages reçus.

Conclusion

Dans ce chapitre, nous avons présenté les besoins fonctionnels et non fonctionnels auxquels notre application VoIP via serveur IP PBX(ASTERISK) doit répondre, après nous avons aussi présenté la partie conception à travers de différents digramme à savoir le digramme de classe et de séquence, dans le prochain chapitre, nous allons présenter la phase réalisation de l'application web ainsi que la phase de test et de validation effectué.

CHAPITRE 4 : REALISATION

Introduction

Après avoir présenté la partie réservée à la spécification des besoins et conception, on présentera la phase de réalisation de mon projet, on entame cette partie par la présentation de l'environnement matériel et logiciel, puis, on présentera les différents choix techniques adoptés, ensuite, on présentera les tâches réalisées.

1. Environnement de travail

1.1. Environnement matériel

Afin de bien réaliser ce projet, on a utilisé un pc portable DELL ayant la configuration suivante :

- Processeur Intel Core i7 2670QM CPU 2.2 GHZ (64 bits).
- 8 Go de RAM.
- Disque du de 500 Go.
- Système d'exploitation équipé de Windows 8.1 Professionnel (64bit)

1.2. Environnement logiciel

Du point de vue logiciel, on a travaillé avec plusieurs systèmes d'exploitation à savoir Windows 8.1, Windows XP et Ubuntu dans lesquelles son a installé les outils nécessaires pour la réalisation de ce travail à savoir :

- L'analyseur de paquets Wireshark
- Softphone 3CX utilise pour le test des appels téléphonies.
- VMware Workstation pour la création des machines virtuelles.

2. Les taches réalisées

- Préparation de l'environnement de travail issue avec l'installation du VMware Workstation 14.
- Installation, configuration et intégration du serveur SIPAsterisk sous Ubuntu 14.04.
- Installation, configuration et intégration du serveur freepbx sous 16.04.
- Installation et lancement des appels avec Softphone 3cx sous Windows 8, Windows XP et Android.
- Installation, lancement des attaques et analyses des paquets avec Wireshark sous Khali linux.
- Installation, configuration et détection des attaques avec Snort sous Ubuntu.

La figure suivante présente l'environnement de travail avec les différentes machines installées dedans.

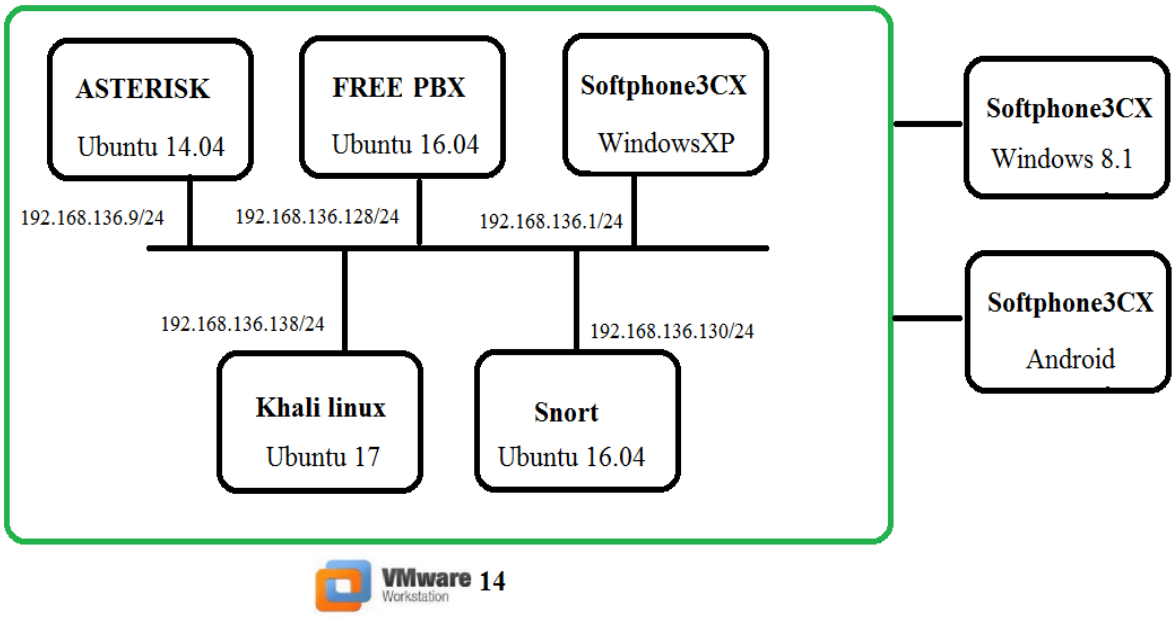

Figure 23: Schéma globale du travail réalisé

3. La mise en place de l'application

3.1. Préparation de l'environnement du travail

L'interface d'installation du VMware Workstation 14 se présente comme suit :

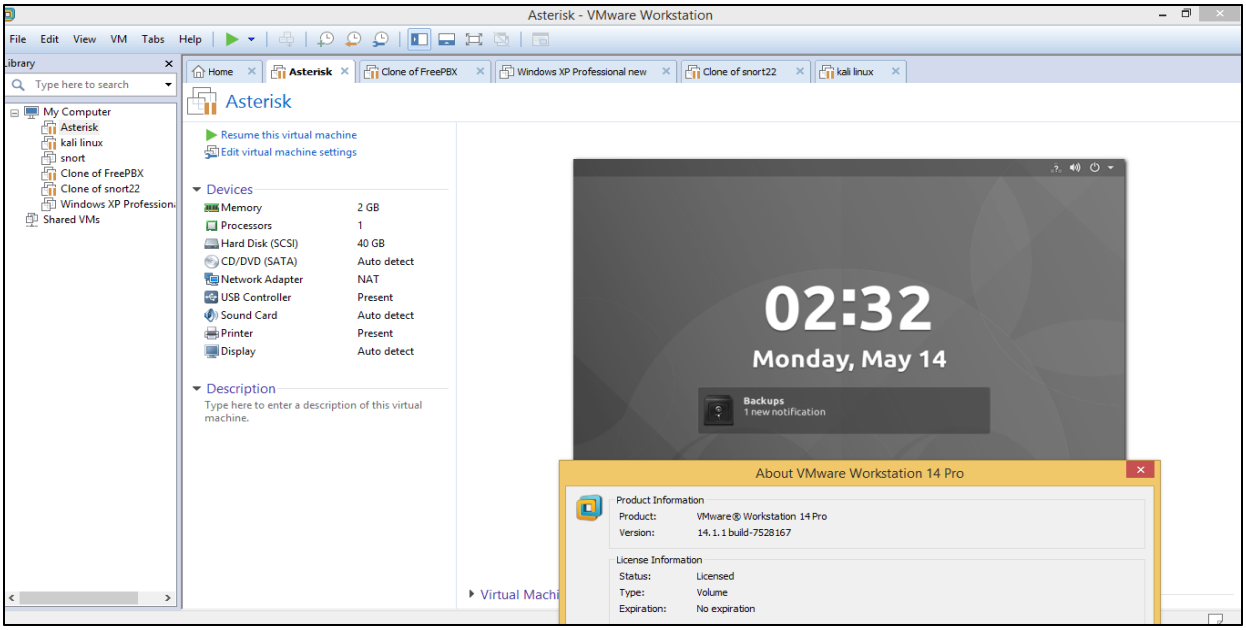

Figure 24: Environnement du travail avec VMware Workstation 14

Dans notre environnement de travail, on a eu recourt à attribuer à chaque machines une adresse IP statique comme le montre la figure ci-dessous

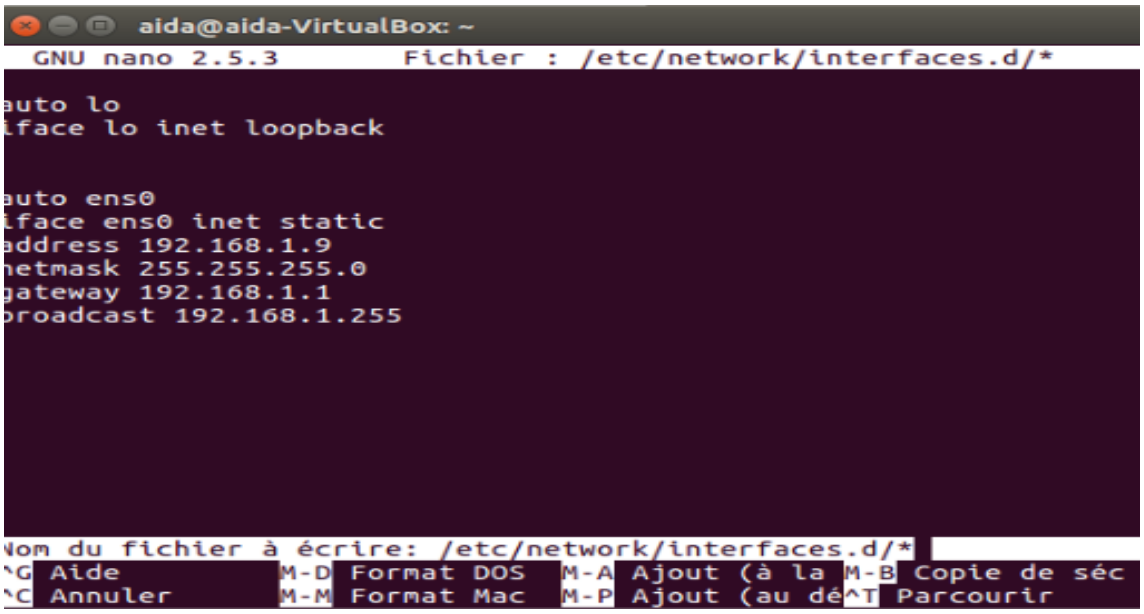

Figure 25: Fixation d'adresse IP sur une machine Ubuntu

3.2.Mise en place du serveur ASTERISK

Dans ce qui suit, on va décrire les étapes de l'installation, de la configuration et de l'intégration du serveur sip Asterisk sous Ubuntu 14.04.

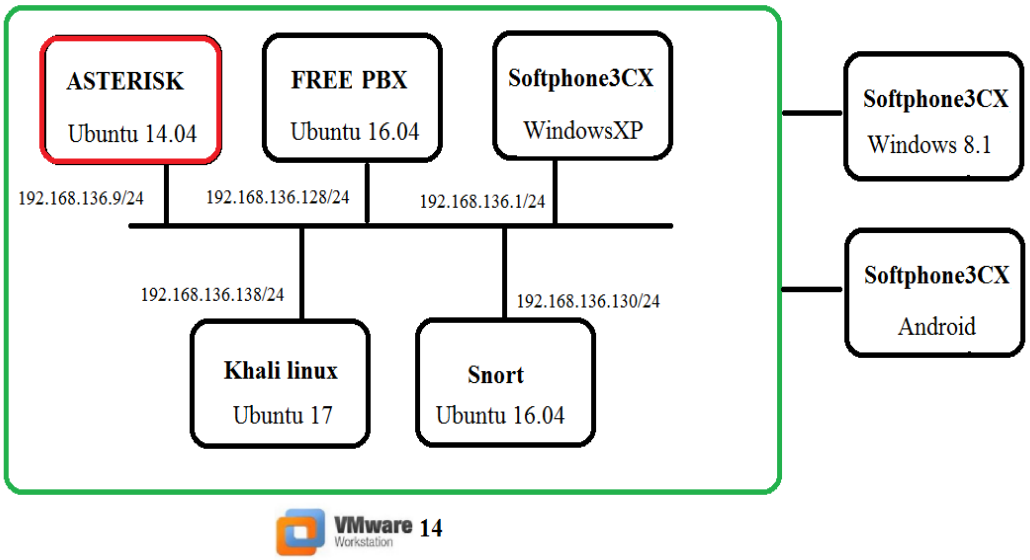

Figure 26: Emplacement du serveur Asterisk dans l'environnement de travail

Le Serveur SIPAsterisk est un logiciel libre qui implémente un central téléphonique. Le logiciel permet à un certain nombre de téléphones connectés d'échanger des appels, et de les relier au réseau téléphonique mondial. [8]

3.2.1. Les étapes de l'installation du serveur Asterisk

Ci-dessous l'ensemble des commandes nécessaire pour l'installation du serveur Asterisk

Mis à jours du système

root@AIDA:~# Apt update

root@AIDA:~# Apt upgrade

root@AIDA:~# reboot

Téléchargement de la source

root@AIDA:# cd /usr

root@AIDA:/usr #cd /src

root@AIDA:/usr/src # wget https://downloads.asterisk.org/pub/telephony/asterisk/asterisk-14-current.tar.gz

root@AIDA:/usr/src#

Wget https://downloads.asterisk.org/pub/telephony/libpri/libpri-current.tar.gz

root@AIDA:/usr/src#

wgethttps://downloads.asterisk.org/pub/telephony/dahdi-linux-complete/dahdi-linux-complete-current.tar.gz

Installation des packages

root@AIDA:/usr/src# apt install build-essential wget libssl-dev libncurses5-dev libnewtt-dev libxml3-dev linux-headers-$(uname -r) libsqlite3-dev uid-dev libjansson-dev

Extraction des packages

root@AIDA:/usr/src # tar xvf asterisk-13-current.tar.gz

root@AIDA:/usr/src # tar xvf libpri-current.tar.gz

root@AIDA:/usr/src # tar xvf dahdi-linux-complete-current.tar.gz

Installation de la librairie DAHDI

root@AIDA:/usr/src/dahdi-linux-complete-2.11.1#

root@AIDA:/usr/src/dahdi-linux-complete-2.11.1# make

root@AIDA:/usr/src/dahdi-linux-complete-2.11.1# make install

root@AIDA:/usr/src/dahdi-linux-complete-2.11.1# make config

Installation de la librairie libpri

root@AIDA:/usr/src# cd libpri-1.6.1

root@AIDA:/usr/src/libpri-1.6.1# make

root@AIDA:/usr/src/libpri-1.6.1# make install

Installation d'asterisk

root@AIDA:/usr/src # cd asterisk-13.16.2/

root@AIDA:/usr/src/asterisk-13.16.2 #. /configure

root@AIDA:/usr/src/asterisk-13.16.2# make menuselect

root@AIDA:/usr/src/asterisk-13.16.2# make

root@AIDA:/usr/src/asterisk-13.16.2# make install

root@AIDA:/usr/src/asterisk-13.16.2# make samples

root@AIDA:/usr/src/asterisk-13.16.2# make config

Lancement Asterisk

root@AIDA:/usr/src/asterisk-13.16.2# systemctl start asterisk

3.2.2. La mise en marche du serveur Asterisk

Après avoir installé notre serveur Asterisk, il nous reste qu'a le lancer et ce à travers la commande systemctl status astersisk.service comme le montre la figure ci-dessous.

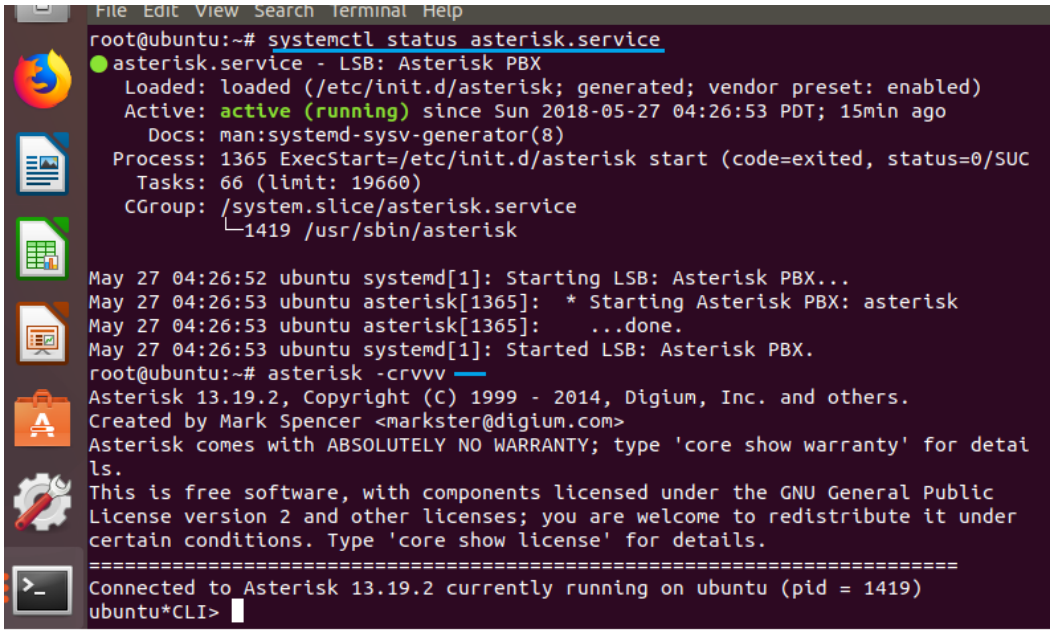

Figure 27: Lancement du serveur Asterisk

La commande Asterisk –c permet la connexion au console CLI d'Asterisk

La commande Asterisk –v permet le paramétrage de la quantité de sortie

3.3.Mise en place du freepbx

Freepbx est un outil de configuration graphique très convivial pour le logiciel de téléphonie libre ASTERISK, il permet de gérer la plateforme coté administrateur. C'est également le logiciel utilisé dans la distribution Trixbox et Elastix.

Dans ce qui suit on va décrire les étapes de l'installation, de la configuration et del'intégration du serveur freepbx sous 16.04 [9].

3.3.1. Instalation freepbx

L'installation de freepbx comme par l'installation des paquets nécessaire et ce à travers les commaandes ci-dessous :

```
apt-get install -y build-essential linux-headers-`uname -r` openssh-server apache2 mysql-server\mysql-client bison flex php5 php5-curl php5-cli php5-mysql php-pear php5-gd curl sox libncurses5-dev libssl-dev libmysqlclient-dev mpg123 libxml2-dev libnewt-dev sqlite3\
 libsqlite3-dev pkg-config automake libtool autoconf git unixodbc-dev uid uid-dev\
 libasound2-dev libogg-dev libvorbis-dev libcurl4-openssl-dev libical-dev libneon27-dev libsrtp0-dev, libspandsp-dev libmyodbc
```

Ci-dessous l'emplacement de notre freepbx

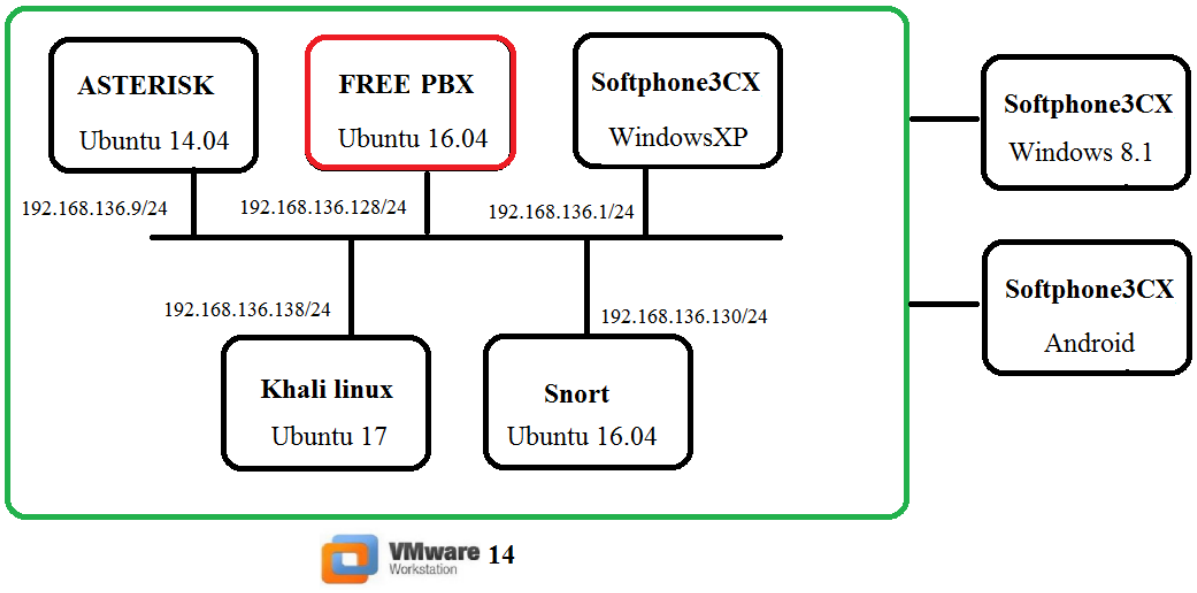

Figure 28 : Emplacement du Freepbx dans l'environnement de travail

Grâce à l'interface graphique on n'a pas besoin de gérer les utilisateurs manuellement avec le fichier sip.conf d'Asterisk, il suffit d'accéder à l'interface freepbx d'administration après avoir s'identifié (fig.30), avec interface freepbx va nous permettre de gérer les utilisateurs.

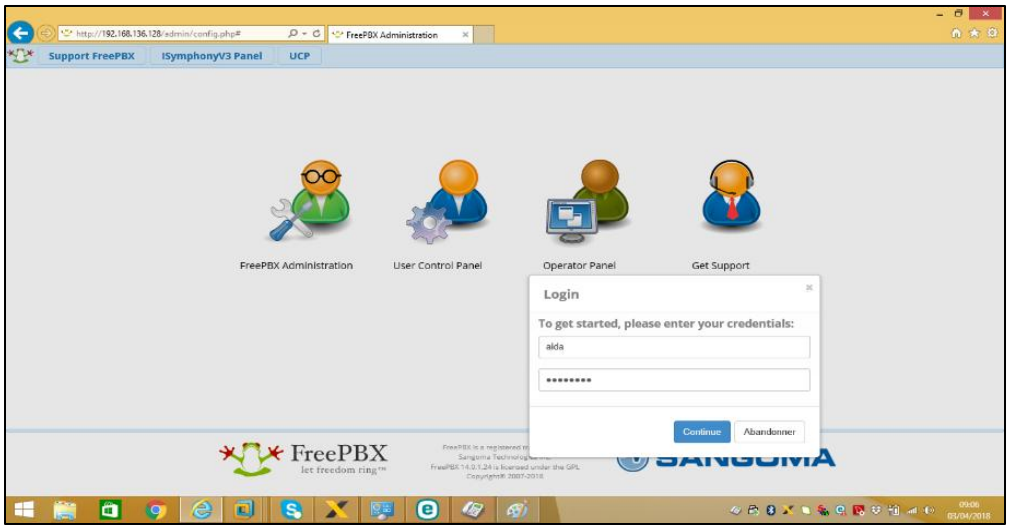

Figure 29: Interface freepbx

Les services freepex se présentent comme suit :

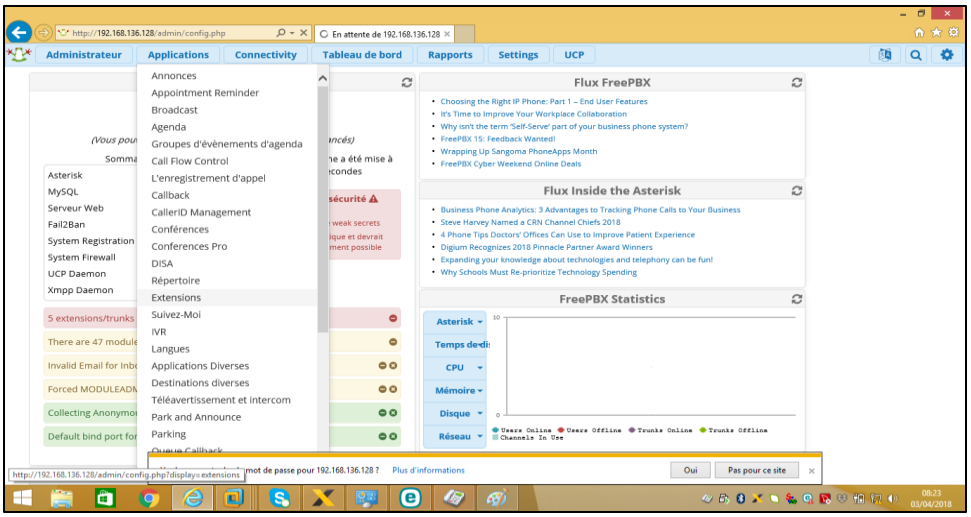

Figure 30: les services freepbx

3.3.2. L'ajout d'un client sip avec freepbx

Parmis les services du freepex l'ajout des clients sip se présentent comme suit

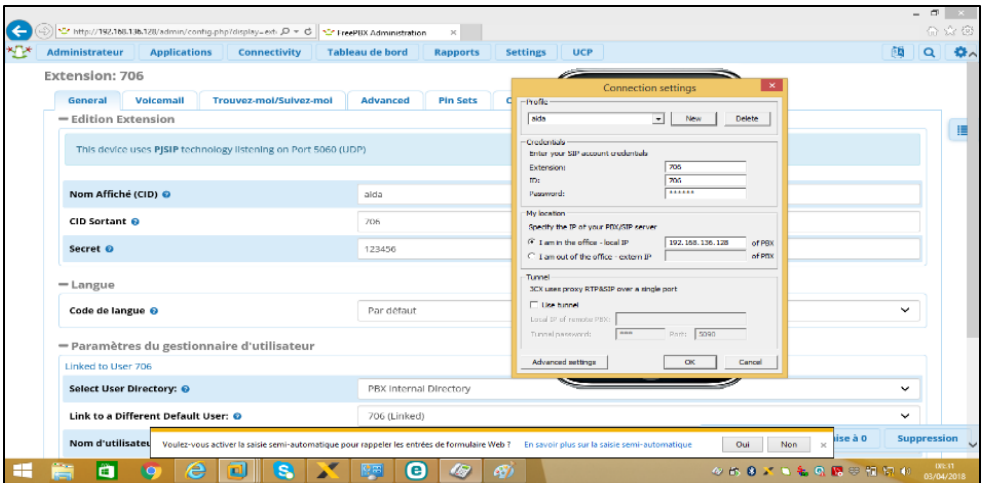

Figure 31: Ajout d'un client sip

Un utilisateur softphone est appelé client SIP, il suffit donc de remplir les champs sépcifiques pour chaque utilisateurs en tappant : l'identifiant du client appelé client id,le nom ,le mot de passe appelé secret, ainsi l'une adresse ip du serveur asterisk ,on procéde ensuite à la vérification de toutes les informations concernant chaque utilisateur qui posséde un mot de passe propre a lui et enfin on clique sur submit pour enregistrer le client.

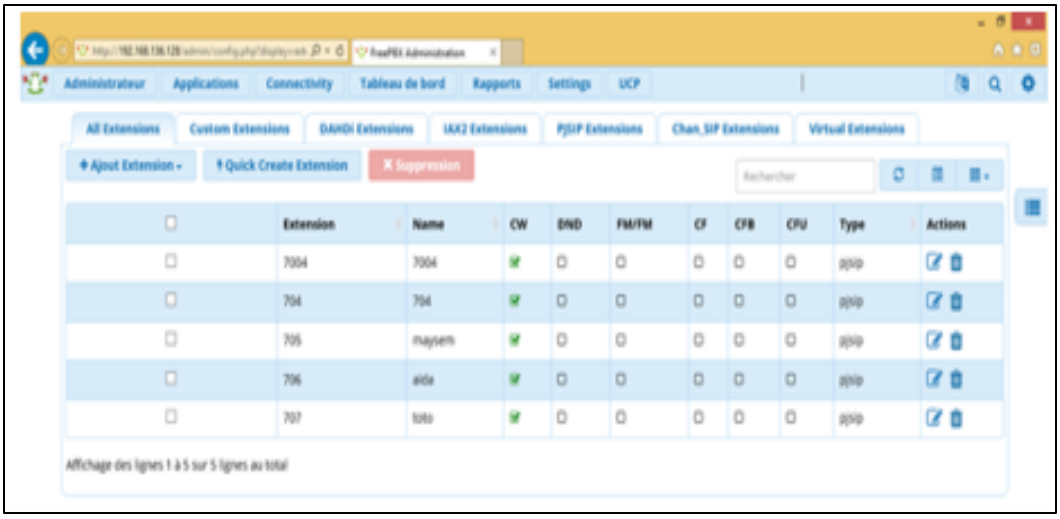

Figure 32: Liste des utilisateurs

Cette interface a le role d'une base de donnés bien définit qui subit a chaque fois une mise a jour des utilisateurs,on a deux types de clients, sdes clients pjsip pour les softphones etdes clients chansip pour les appareils androids, c'est une interface pratique ,conviviale et facile a manipuler.

3.4. Mise en place des Softphones

On va décrire Installation et lancement des appels avec Softphones 3cx sous Windows 8, Windows XP et Android.

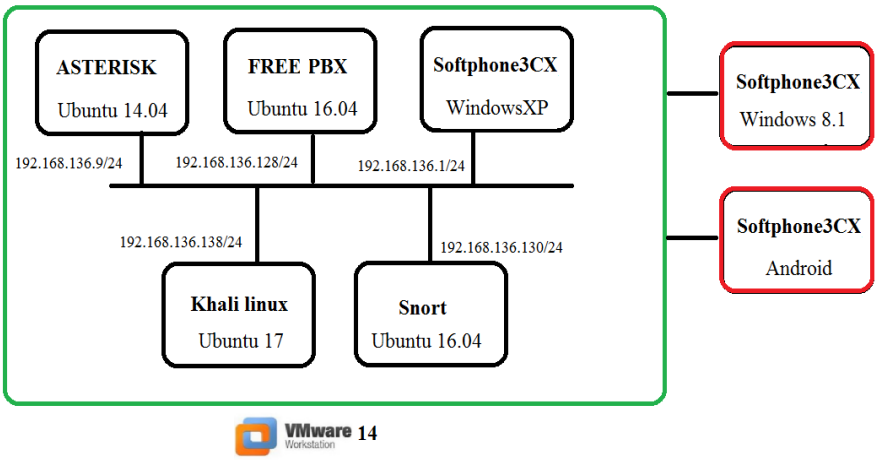

Figure 33 : Emplacement du Softphone 3cx dans l'environnement de travail

Un Softphone est un type de logiciel utilisé pour faire de la téléphonie par Internet depuis un ordinateur plutôt qu'un téléphone.

Chaque utilisateur a la possibilité de télécharger le Softphone (version Android ou version Windows) suivant le terminal utilisé. La figure ci-dessous représente l'interface utilisateur du logiciel 3cx phone.

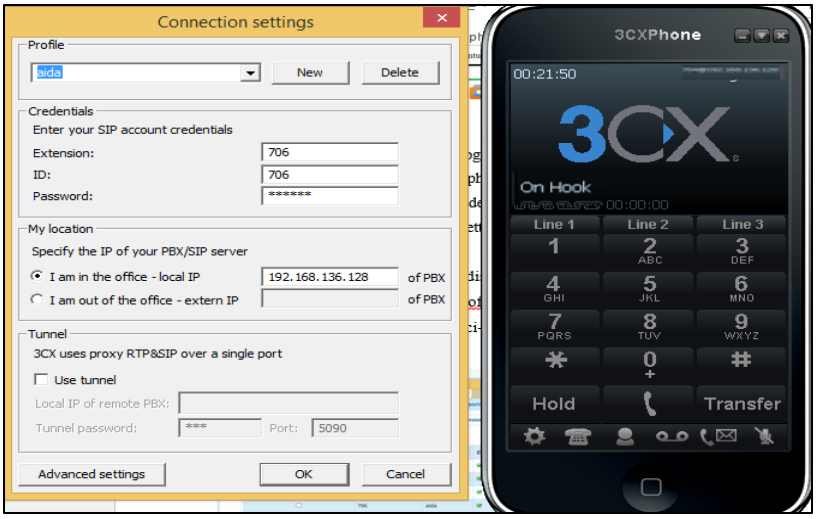

Figure 34 : Configuration d'un Softphone 3cx mode On Hook

Chaque utilisateur à des champs propre à savoir :

- Le champ Profile dans lequel on ajoute nom de l'utilisateur
- Le camp Extension dans lequel on ajoute numéro du tel exemple 704
- Le champ Id dans lequel on ajoute un identifiant

- Le champ Password dans lequel on ajoute secret mot de passe
- Le champ Adresse IP dans lequel on ajoute l'adresse IP du serveur Asterisk.

Figure 35 : Softphone et freepbx

La figure ci-dessous montre un test d'un appel réussi entre deux Softphone 3cx qui sont installés le premier sur Windows XP et le deuxième sur Windows 8 communication.

Figure 36 :Test d'un appel entre deux Softphone

L'utilisateur quia une extension 706 a le nom aida effectue un appel avec l'utilisateur Haithem qui a une extension 704, il suffit de composer le numéro de l'appelé, si la ligne est libre, une sonnerie se déclenche chez le récepteur avec l'affichage du numéro de l'appelé.

Ci-dessous un Test réussi d'un appel entre deux téléphones Android.

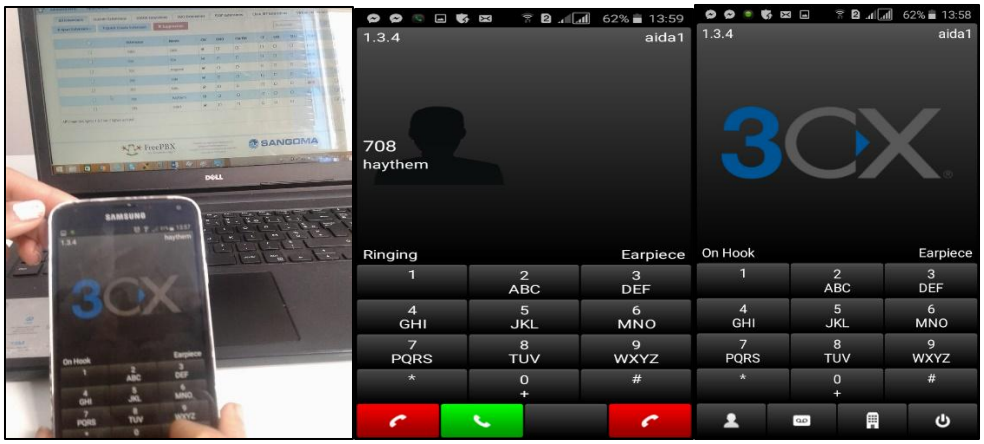

Figure 37: Test d'un appel entre deux téléphones Android

Après le téléchargement du 3cx Softphone pour Android, il suffit de se connecter au réseau pour qu'un utilisateur puisse accéder à sa boite vocale via son Softphone, il tape 9998, le répondeur lui informa de l'état de sa boite, et il peut écouter s'il y a des messages vocaux.

Si un utilisateur appelle un autre utilisateur non disponible, un message de notification du message vocale sera envoyé à la boite mail du l'appelé.

4. Attaque contre la solution VoIP

Nous avons listé quelques attaques possibles sur la VoIP et aussi les méthodes de sécurisation. Des logiciels d'attaques de degré variable du danger, nous allons dans cette partie se concentrer sur l'écoute clandestine et l'identification des identités des clients sip aussi leur mot de passe à l'aide du logiciel open source nommé WIRESHARK en utilisant KHALI LINUX, et nous allons par la suite présenter les solutions à réaliser.

4.1. Installation, lancement des attaques et analyses des paquets avec Wireshark sous Khali linux

Ci-dessous l'emplacement de la distribution khali linux dédiée à l'audit de sécurité et aux tests de pénétration.

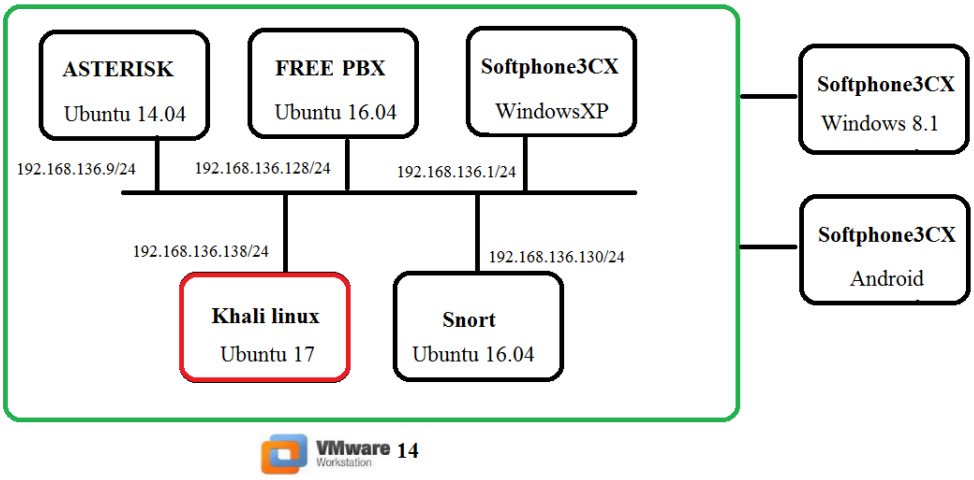

Figure 38: Emplacement de Khali linux dans l'environnement de travail

Khali linux est une distribution GNU/Linux basée sur Debian regroupant plus de 6008 programmes d'analyse de sécurité préinstallés à savoir Wireshark (un analyseur de paquets), John the Ripper (un outil de cassage de mots de passe) et Sipcrack (une suite logicielle permettant de cracker le protocole sip).

Figure 39 : Interface du système d'exploitation khali linux

4.2.L'écoute clandestine avec Wireshark

Dans le cadre de notre projet, on a utilisé Wireshark pour l'analyse des paquets réseaux et l'écoute des appels téléphonique via la voix sur IP.

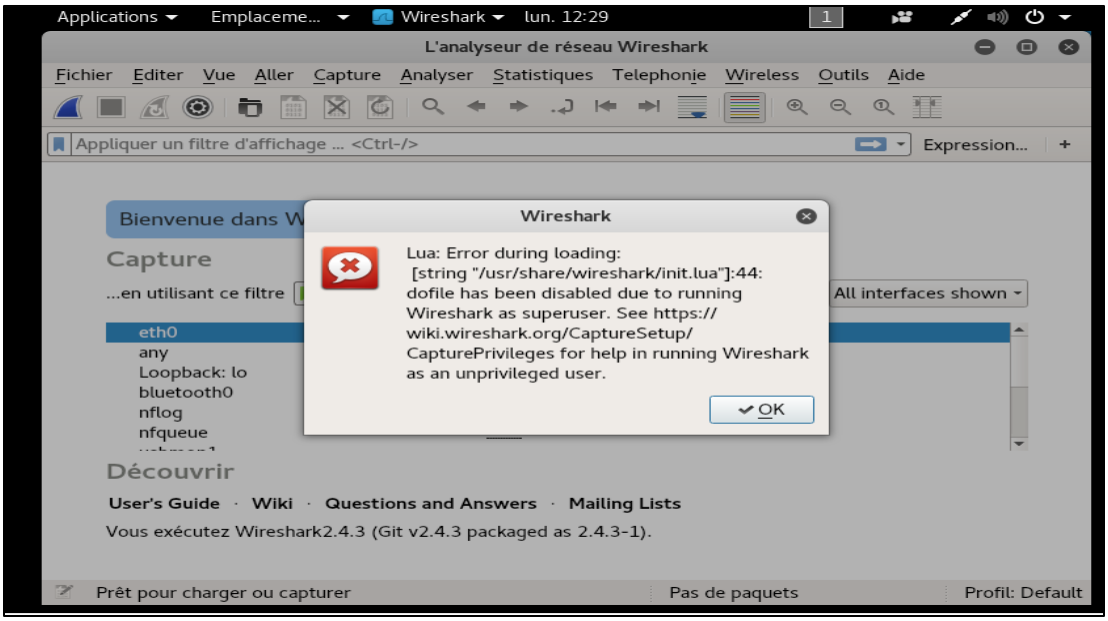

Figure 40: Wireshark

La figure suivante présente des exemples des paquets capturés par Wireshark à savoir les adresses IP, les numéros de ports, et d'autres informations.

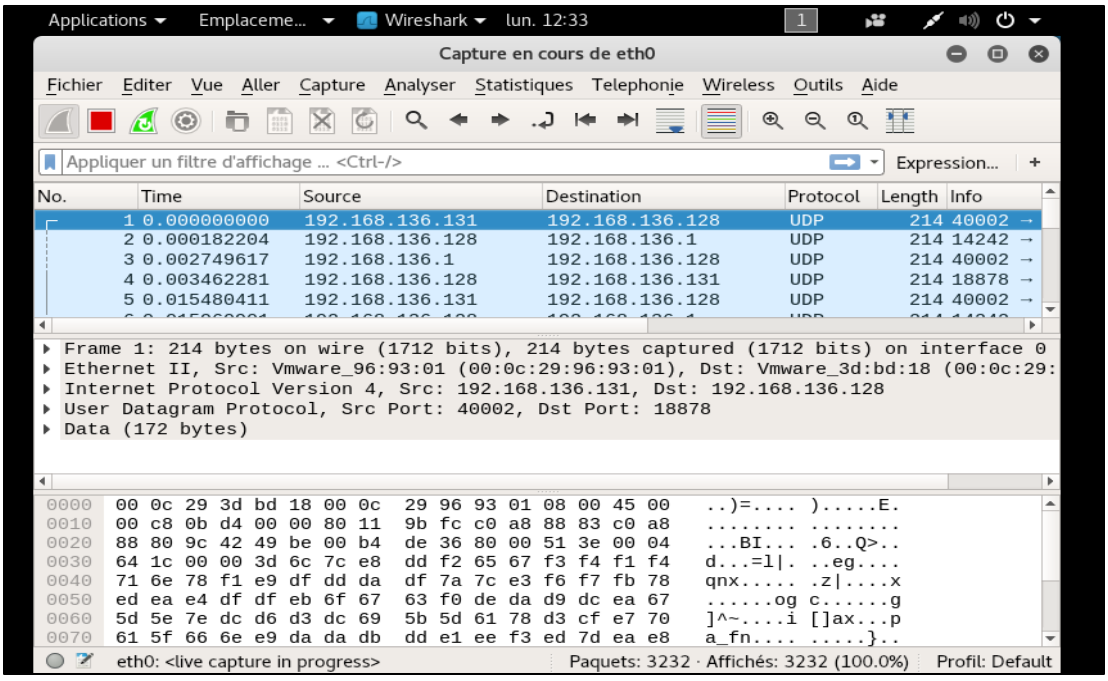

Figure 41: Capture des paquets

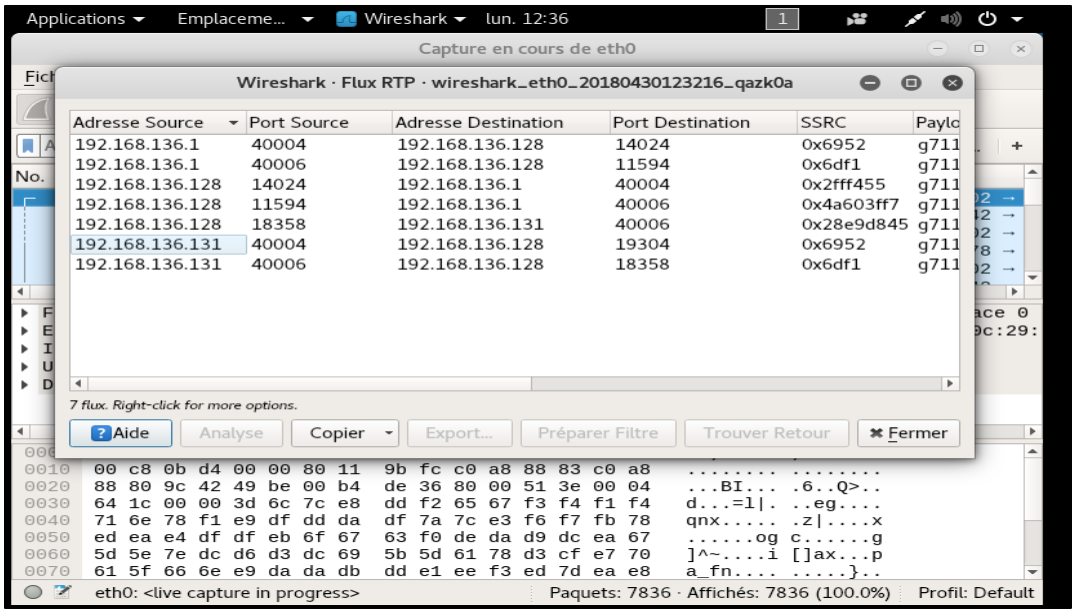

Figure 42 : Capture des trafics RTP

L'outil Wireshark, permet d'écouter une communication entre deux clients Sip (Softphone) en décodant les paquets RTP envoyés lors d'une communication en temps réel.

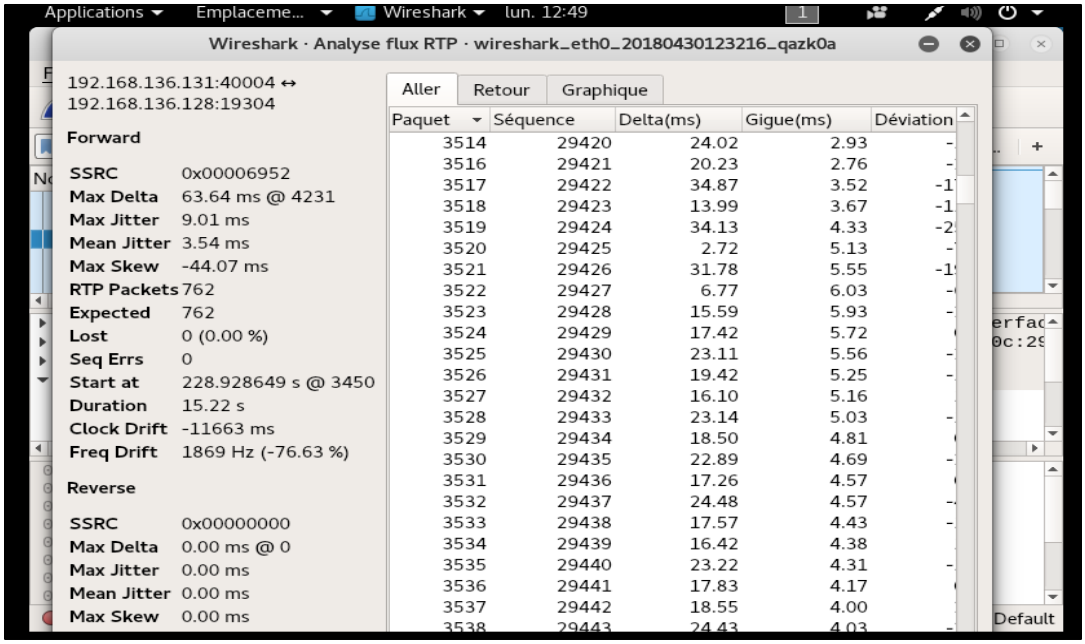

Figure 43: Description détaillé d'analyse du flux RTP

Avec Wireshark, on a pu récupérer les paquets RTP et faire l'écoute de la conversation téléphonique établie entre deux clients Sip comme l'indique la figure ci-dessous.

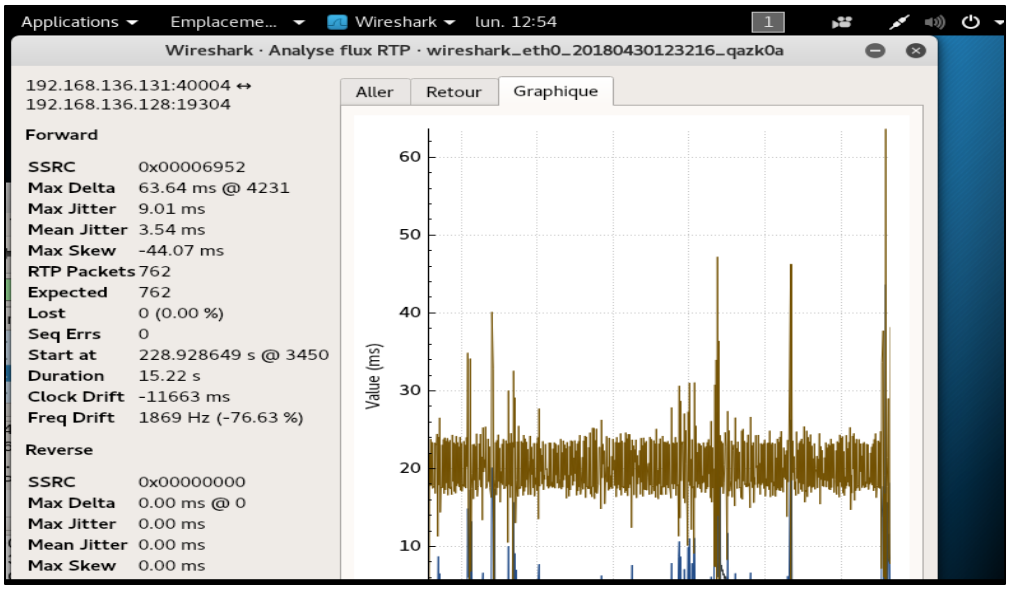

Figure 44: Décodage des paquets RTP

4.3.Ecoute du traficSip avec Khali linux(SIPdump)

La figure ci-dessous montre l'écoute du trafic SIP

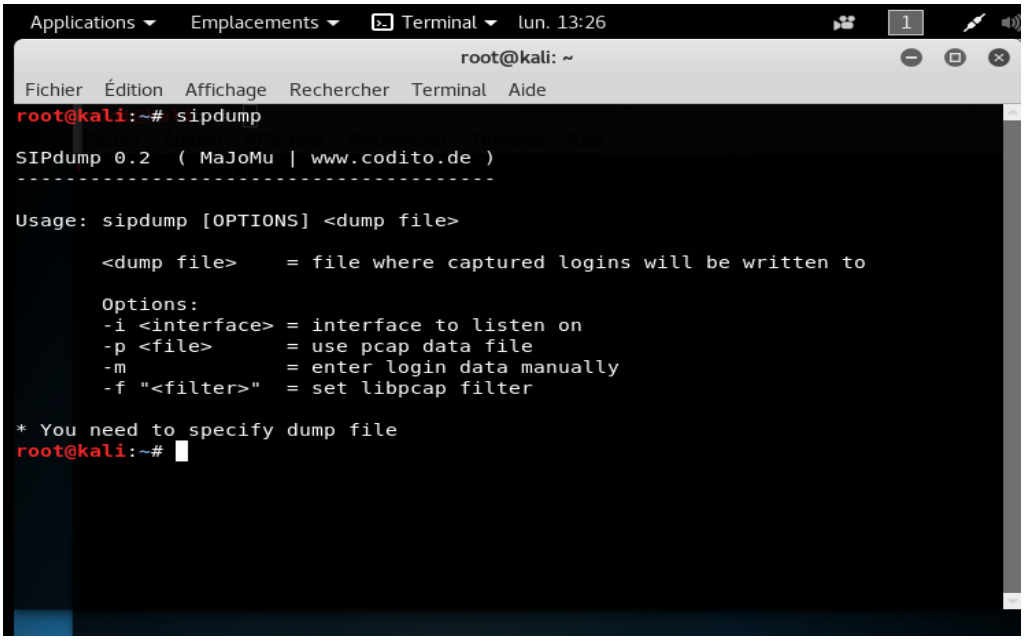

Figure 45 :Ecoute du traficSip avec Khali linux

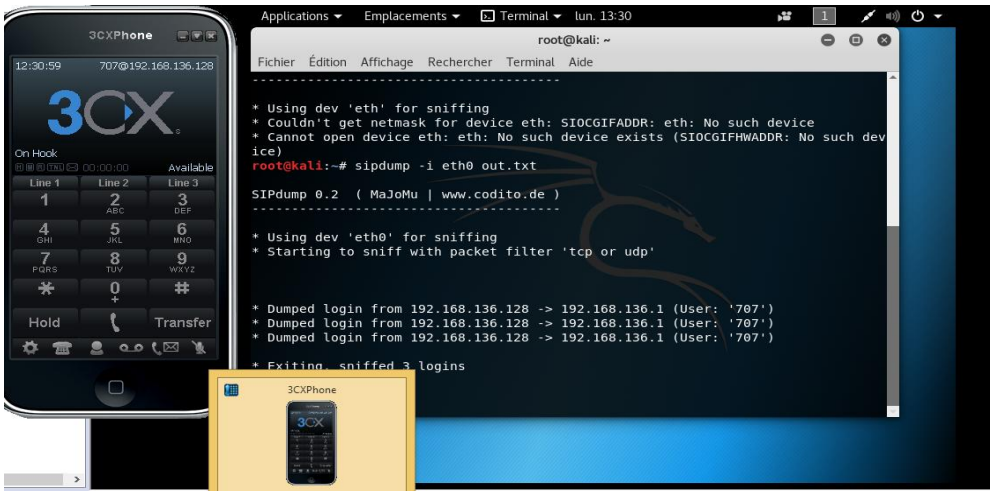

Figure 46 : Ecoute de l'interface réseau eth0

La figure ci-dessous montre que non seulement afficher les adresses ip de la communication via voix ip, mais aussi consulter des informations très importante à tel que les identifiants des clients SIP.

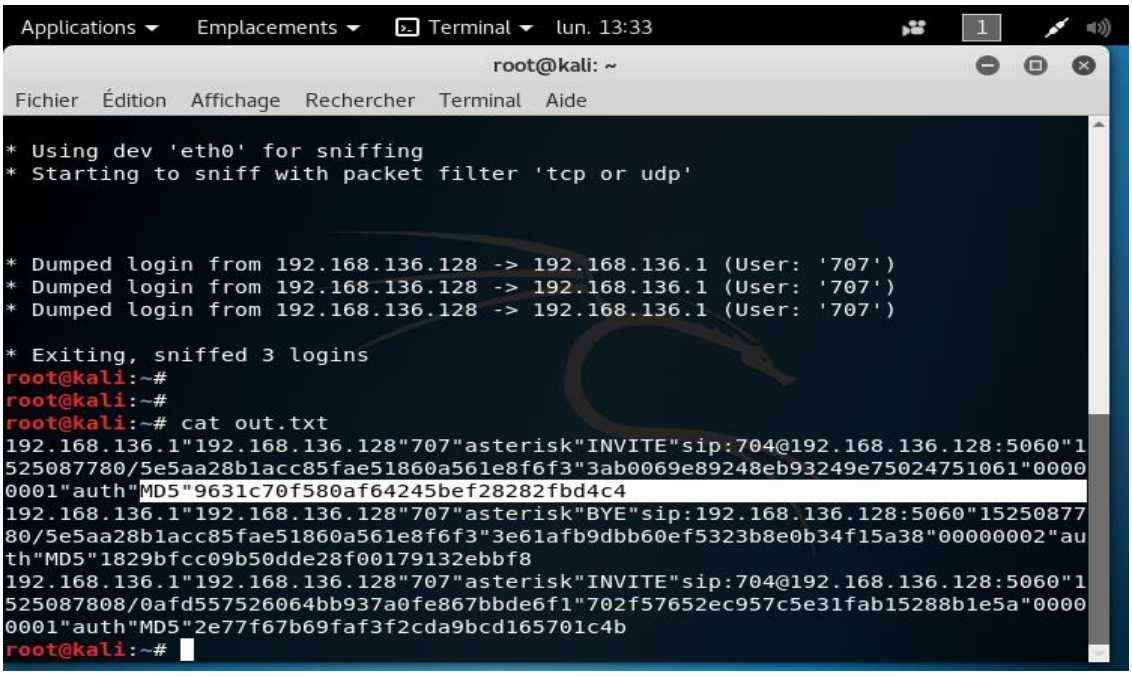

Figure 47: Affichage des mots passe des clients SIP

La figure ci-dessous montre un cas plus avancé qui consiste à afficher les mots de passe des clients sip haché en MD5.

Nous pouvons ainsi décoder les mots de passe en utilisant l'utilitaire Sipcrack ou bien en utilisant des sites internet offrant ce service.

La figure suivante présente un exemple de décodage d'un mot passe du client Sip.

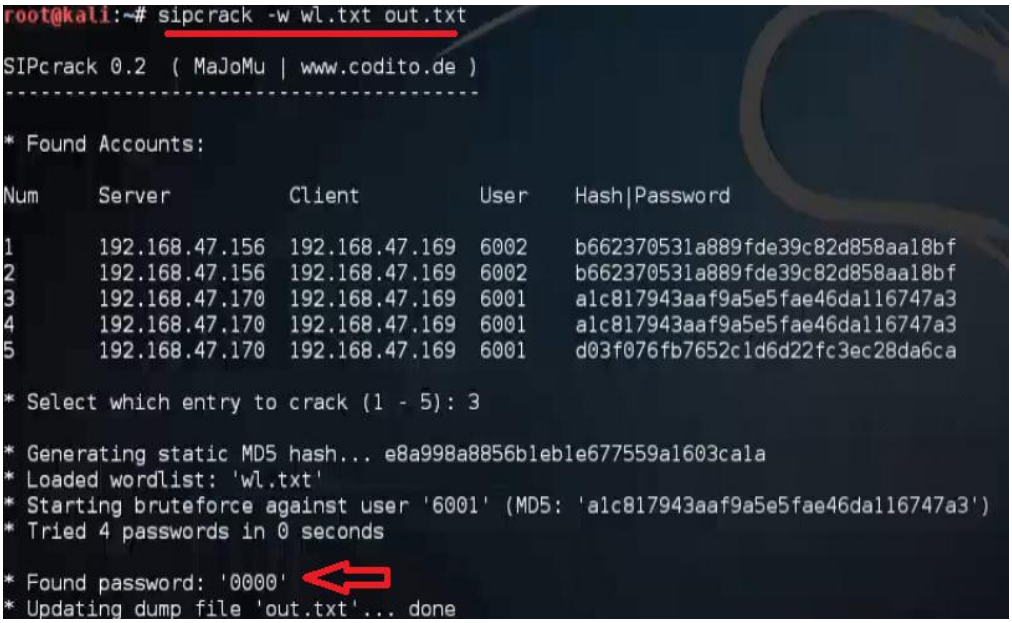

Figure 48: Décodage d'un mot de passe

La figure ci-dessous montre un Exemple d'attaque avec l'utilitaire invite flood.

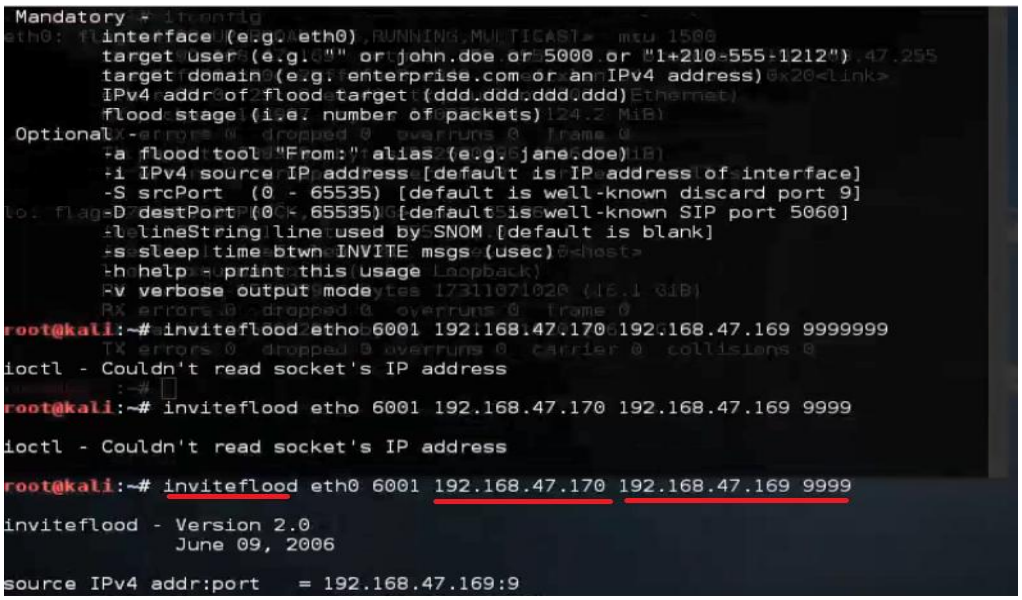

Figure 49: Attaque invite flood

Invite flood est un outil qui permet d'effectuer un débordement de message SIP / SDP INVITE sur UDP / IP pour effectuer une attaque DOS (Deny of Service). Cet outil est utilisé pour inonder une cible avec des messages de demande INVITE, tant que cet outil continue d'inonder le PBX, il empêche les clients de passer des appels téléphoniques

5. Solutions pour la sécurisation

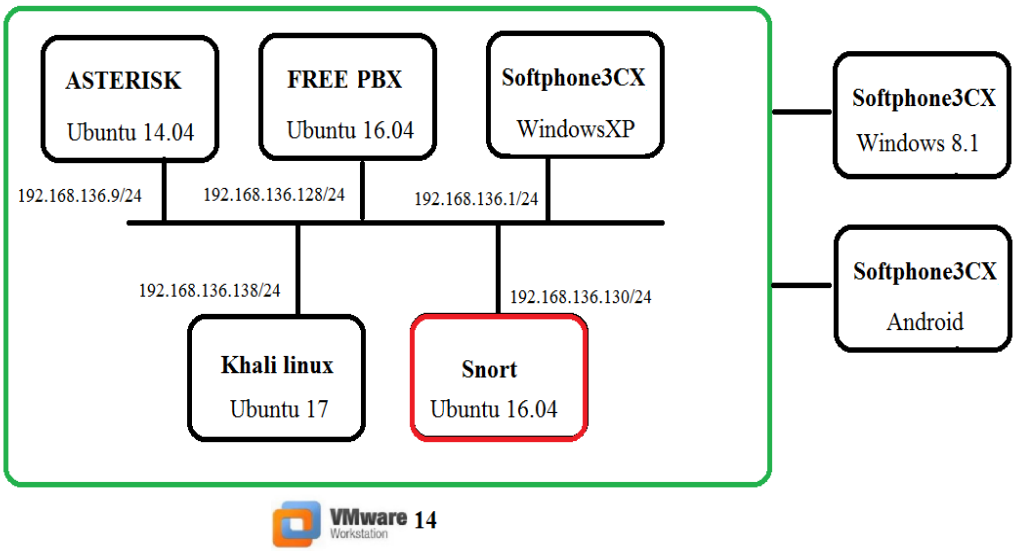

Figure 51 : Emplacement de Snort dans l'environnement de travail

Les attaques que nous avons testées lors de ce projet sont un témoin signalant l'importance de la sécurisation du serveur Asterisk.

La société Magma a suggère d'installer Snort comme système de détection d'intrusion, ce dernier permet d'analyser le trafic réseau de type IP, il peut être configuré pour Fonctionner en quatre modes :

- **Le mode sniffer,** dans ce mode, SNORT lit les paquets circulant sur le réseau et les affiche d'une façon continue sur l'écran ;
- **Le mode « packet logger »,** dans ce mode SNORT journalise le trafic réseau dans des répertoires sur le disque
- **Le mode détecteur d'intrusion réseau (NIDS)**, dans ce mode, SNORT analyse le trafic du réseau, compare ce trafic à des règles déjà définies par l'utilisateur et établi des actions à exécuter.
- **Le mode Prévention des intrusions réseau (IPS)**, c'est SNORT-inline.

5.1.Installation et configuration de Snort

Installation Snort

Installation des packages source

Wget https ://www.snort.org/downloads/snort/daq-2.0.6.tar.gz

Wget https://www.snort.org/downloads/snort/snort-2.9.11.1.tar.gz

Tar xvzf daq-2.0.6.tar.gz

cd daq-2.0.6

./configure && make && sudo make install

tar xvzf snort-2.9.11.tar.gz

cd snort-2.9.11

./configure --enable-source fire && make && sudo make install

Instalation des rules

wget https://www.snort.org/downloads/comunity/comunity-rules.tar.gz -O comunity-rules.tar.gz

tar -xvzf community.tar.gz -C /etc/snort/rules

La figure ci-dessous montre les étapes de la configuration et de l'installation de SNORT.

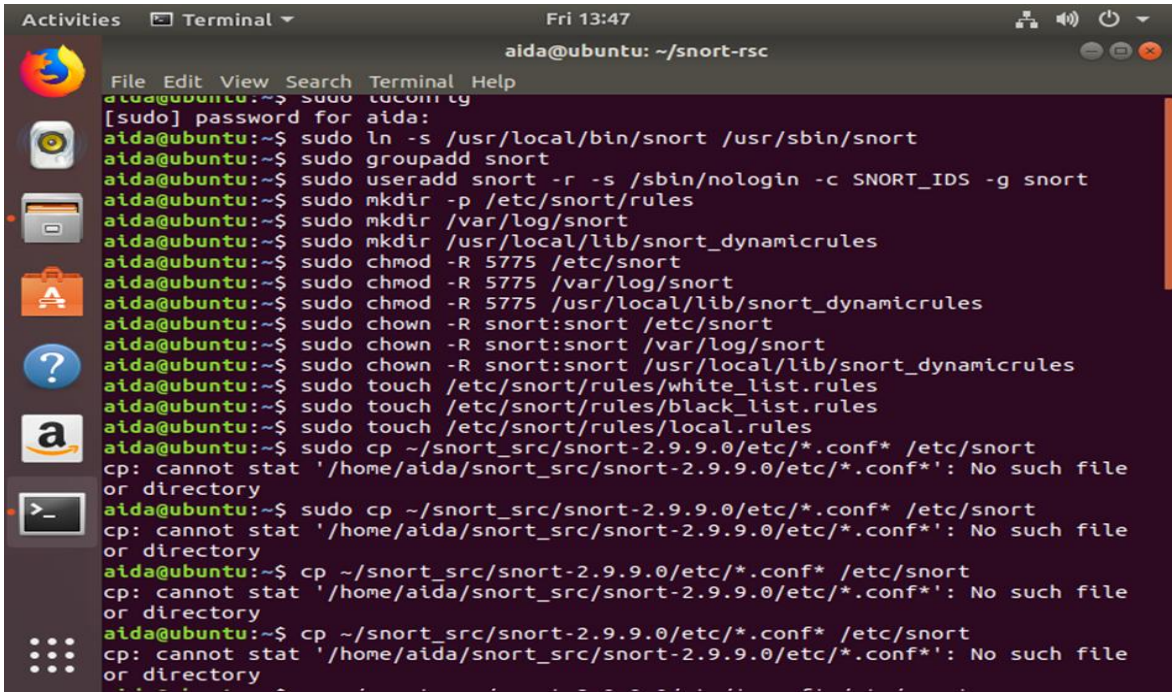

Figure 50: Installation du snort

Après avoir installé et configuré Snort, il nous reste à le démarrer et ce avec la commande service snortd start

La figure ci-dessous montre le démarrage de Snort

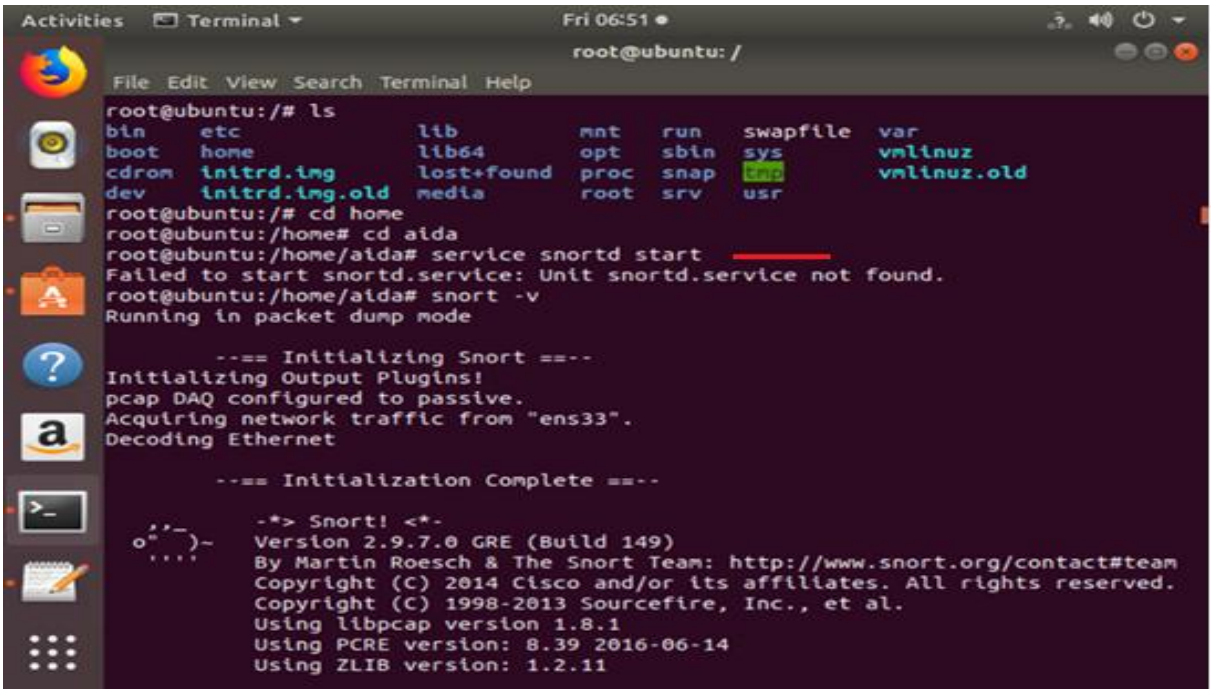

Figure 51: Démarage de snort

5.2.Détection des attaques avec Snort sous Ubuntu

5.2.1. Snort mode sniffer

C'est le mode basic, il permet de lire et afficher à l'écran les paquets TCP/IP circulant sur le réseau.

La configuration du snort se réalise en tappant les comandes suivantes :

root@ubuntu:/home/ aida # **snort –v**

Cette commande permet d'exécuter et d'afficher les entêtes des paquets TCP/IP.

root@ubuntu:/home/ aida # **snort –vd**

Cette commande permet d'exécuter SNORT et d'afficher tout le paquet TCP/IP (entête et données).

root@ubuntu:/home/ aida # **snort –vde**

Cette commande permet d'exécuter SNORT et d'afficher tout le paquet TCP/IP (entête et données).

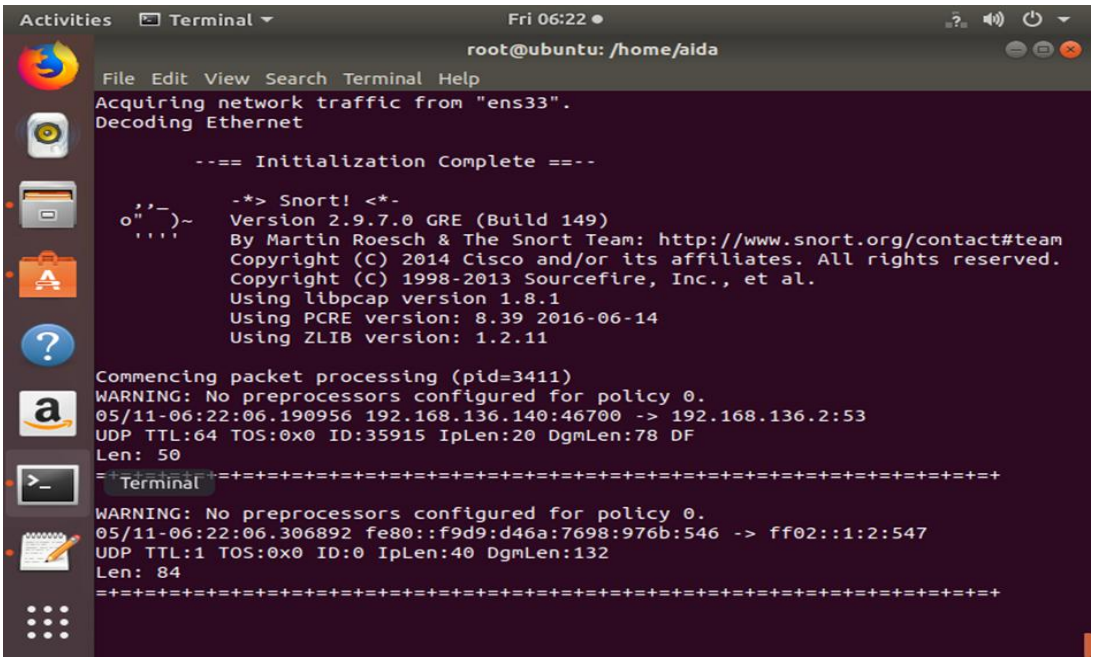

Figure 52: La commande snort –vd

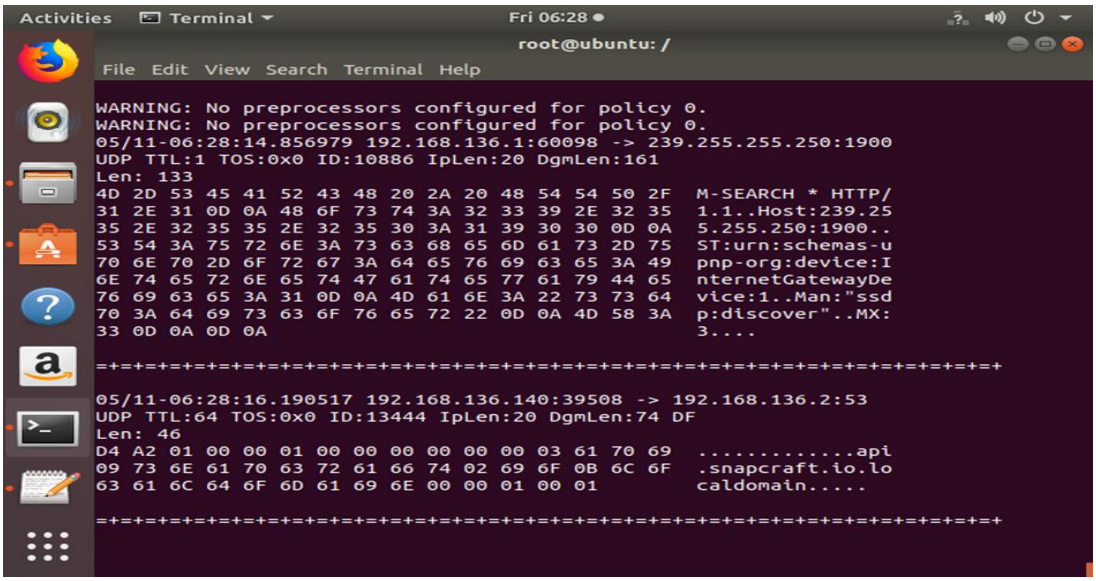

Figure 53: commande snort –vde

5.2.2. Snort en mode « packet-logger »

Dans ce mode SNORT journalise le trafic réseau dans des répertoires sur le disque :

[root@ ubuntu:/home/ aida]# snort –dev –l ./log

Cette commande permet d'exécuter SNORT et d'enregistrer ses logs dans le répertoire **log**, il faut créer au préalable le dossier log.

La société vise à faire fonctionner Snort en mode IDS (intrution detection système) et IPS (intrution prevention système)

Conclusion

A traves ce chapitre, on a mis en œuvre la conception abordée au niveau du chapitre précédant .On a commencé par présenter l'environnement matériel et logiciel de travail, par la suite, on a énuméré l'ensemble des taches réalisées en général et en détail.

Actuellement, la société opère dans le même bâtiment, la solution implémenté prend en considération l'évolution de la taille de l'entreprise, en effet notre solution, permet d'assurer des communications et ce à travers des sites distants tout en ajoutant les technologies nécessaires à savoir la connexion de deux réseaux locaux distant et ce avec la technologie VPN (Virtual Private Network).

CONCLUSION GENERALE

La VoIP via Asterisk est une technologie émergente utilisé par plusieurs entreprises vu les multiples avantages qu'elle présente. Ainsi, le marché de la VoIP ne cesse depuis quelques années de s'étendre et de créer par la suite un environnement concurrentiel intense.

Dans une première étape, nous nous sommes intéressés à l'étude de cette technologie avec ses différents protocoles. Dans une deuxième étape, nous avons étudié les problèmes de sécurité de la voix sur IP, les attaques et les bonnes pratiques possibles pour les attaques citées ainsi nous avons présenté une étude conceptuelle pour cette solution. Comme troisième étapes, nous avons installé et configuré une solution de VoIP utilisant le serveur Asterisk et de deux clients SoftPhone. En dernière étape, nous avons testé une attaque de sécurité contre la solution installée, et nous avons proposé quelques solutions pour la sécuriser.

Ce projet a été une expérience fructueuse qui nous a permis de mieux s'approcher du milieu professionnel et d'enrichir nos acquis reçus en VoIP. Cette expérience nous a permis de bien améliorer notre capacité d'analyse et de résolution de problème et ce avec les moyens de bord, elle nous a permis aussi de bien s'intégrer dans une équipe hétérogène et ce en améliorant les capacités personnel de communication.

BIBLIOGRAPHIE

[1] http://www.frameip.com/voip/#22-8211-principe-du-rtc

[2] https://www.memoireonline.com/07/13/7238/m_Mise-en-place-dun-service-de-voip-avec-Trixbox9.html

[3] https://www.memoireonline.com/10/13/7591/Etude-d-une-offre-technique-innovante-de-telephonie-sur-IP--Camtel-Cameroun.html

[4] https://search.yahoo.com/search?ei=utf-8&fr=tightropetb&p=communication+h323&type=103807_112717

[5] https://www.memoireonline.com/10/13/7591/m_Etude-d-une-offre-technique-innovante-de-telephonie-sur-IP--Camtel-Cameroun21.html

[6] http://www-igm.univ-mlv.fr/~dr/XPOSE2004/IDS/IDSSnort.html

[7] https://www.memoireonline.com/09/13/7361/m_Etude-dimplementation-dune-solution-VOIP-securisee-dans-un-reseau-informatique-dentrepr44.html
R. Bouzaida, «Étude et Mise en place d'une solution VoIP sécurisée,» 2010-2011.

[8] https://www.memoireonline.com/09/13/7361/m_Etude-dimplementation-dune-solution-VOIP-securisee-dans-un-reseau-informatique-dentrepr44.html

[En ligne]. Available: http://blogs.digium.com/2012/11/14/how-to-install-asterisk-11-on-ubuntu-12-4-lts/. [Accès le 25 2 2015].

[9] /https://wiki.freepbx.org/display/FOP/Installing+FreePBX+13+on+Ubuntu+Server+14.04.2+LTS

[10] http://www.freepbx.org/

[11] https://www.snort.org

ACRONYME

A

ADSL= Asymmetric Digital Suscriber Line

ARP = Address Resolution Protocol

C

CLI =Command Line Integration

D

DOS = Deny of Service

G

GK = Gatekeeper

GW = Gateway

I

IP = Internet Protocol

IPBX = Private Branch Exchang

L

LAN = Local Area Network

M

MAC = Media Access Control

MCU = Multipoint Control Unit

O

OS = Operating System

P

PABX = Private Automatic Branch eXchange

PBX= Private Branch eXchange

R

RTC = Réseau Téléphonique de Commuté

RTP = Real-Time Transport Protocol

RTCP = Real-time Transport Control Protocol

S

SIP = Session Initiation Protocol

SRTP = Secure Real-time Transport Protocol

T

TCP = Transport Control Protocol

TLS = Transport Layer Security

U

UDP = User Datagram Protocol

UML = Unified Modelling Language

V

VoIP = Voice over Internet Protocol

VPN = Virtual Private Network

W

WAN = World Area Network