TABLE DES MATIERES

LISTE DES FIGURES

LISTE DES TABLEAUX

ACRONYMES :

ACL = ACCESS CONTROL LIST

ANRT = Agence National des Régulations de Télécoms.

ARP = Address Resolution Protocol

DDoS = Distributed Denial of Service

DHCP = Dynamic Host Configuration Protocol

DNS = Domain Name System

DoS = Deny of Service

GSM = Global System for Mobile Communications

HTTP = HyperText Transfer Protocol

IAX = Inter-Asterisk Exchange

ICMP = Internet Control Message Protocol

IETF = Internet Engineering Task Force

IP = Internet Protocol

LAN = Local Area Network

MD5 = Message Digest 5

MIKEY = Multimedia Internet KEYing

MKI = Master Key identifier

MGCP = Media Gateway Control Protocol

PABX = Private Automatic Branch eXchange

PSTN = Public Switched TelephoneNetwork

QoS = Quality of Service

RTCP =Real Time Control Protocol

RTP = Real Time Protocol

SIP = Session Internet Protocol

TDM =Time Division Multiplex

ToIP =Téléphonie Over IP

TOS =Type of Service

UIT = Union Internationale des Télécommunications

VLAN =Virtuel LAN

VoIP = Voice Over IP

WAN = Wide Area Network.

LE CAHIER DE CHARGE:

Missions

Mise en place d'une solution open source sécurisée pour les services VoIP.

- Etude technique de l'existant.
- Etude de différentes solutions open source disponibles.
- Choix de la solution VoIP open source.
- Mise en place technique de la solution.
- Simulations des attaques contre la solution VoIP mise en place.
- Mise en œuvre de la politique de sécurité.
- Vérification de la sécurité implémentée.

Technologies: Asterisk Elastix, Backtrack, Softphones(x-lite), Wireshark, Sipvicious, Openvpn,..

INTRODUCTION GENERALE :

La téléphonie a connu ces dernières années une véritable révolution avec l'émergence de la téléphonie sur IP, qui apporte néanmoins certains inconvénients comme la problématique de la sécurité. Puisque, la téléphonie sur IP cumule les vulnérabilités de la téléphonie classique et celles des réseaux informatiques. Ainsi, en déployant ou en adoptant une solution de ToIP, les entreprises et les particuliers exposent leurs systèmes à de nouvelles menaces.

Compte tenu de l'étroite intégration avec l'infrastructure informatique, la sécurité des flux de la voix doit être examinée parallèlement à l'administration des systèmes et des périphériques, en particulier avec l'émergence des solutions IP qui renforcent le besoin de sécurité et de fiabilité.

Pour cela, la sécurité de la solution VOIP/TOIP doit couvrir toute l'infrastructure réseau, incluant les outils et les équipements de gestion des communications et des utilisateurs, le système d'exploitation sur lesquels sont installés ces outils, et les protocoles de signalisation et de transport de données. Il faut même se protéger contre les personnes malveillantes. Mieux on sécurise, moins il y a de risques.

Au cours de ce stage, j'ai pu m'intéresser principalement à la VoIP en entrant au support technique.

Le but de ce stage est de faire comprendre et confronter les aspects techniques (le fonctionnement des équipements, la Configuration, la sécurisation VoIP…) et humains.

Organisation de rapport :

La présentation des travaux s'organise en 4 chapitres que nous synthétisons de la façon suivante :

Chapitre 1 – Contexte général et L'état de l'art de la VoIP : Ce chapitre explicite les notions sur les quelles s'appuie le projet .Il présente l'organise d'accueil, ces services et son domaine d'activités, la problématique et le planning adopté pour la réalisation de ce projet .ET d'autre part la présentation de la technologie de la VoIP et son principe de fonctionnement et architecture adopté .

Chapitre 2 – Attaques contre la VoIP et les stratégies de sécurisation : Ce chapitre présente les fameuses d'attaque qui menacer la sécurité contre la VoIP et les différentes solutions possibles pour la sécurisation notre systèmes.

Chapitre 3 – Etude des solutions disponibles : Une étude comparative entre les différent IPBX libre disponible et étude des différents soft phones.

Chapitre 4 – Mise en place technique de la solution : Dans ce chapitre une mise en place technique, mécanisme, configuration de serveur, et les scénarios d'attaque et les solutions proposé pour sécuriser notre infrastructure, puis testes et les résultats.

Finalement, on fini ce travail par une conclusion général, un Limitations et Perspectives.

CHAPITRE 1 : CONTEXTE GENERAL & ETAT DE L'ART DE LA VOIP

I. Contexte général :

1. Introduction :

L'objectif de ce chapitre est de présenter d'une part, l'Organisme d'accueil, ces services et son domaine d'activité et d'autre part, le projet de fin d'études objet du présent rapport, la problématique, et le planning adopté pour la réalisation de ce projet .

2. Présentation de High Tech-service:

HighTech –service est une société de services informatiques spécialisée dans le support, le conseil, la maintenance informatique & réseaux, l'installation ADSL-SDSL, la téléphonie IP et IPBX mono et multi-sites, pour professionnels, artisans, commerçants, PME-PMI, grands comptes, collectivités.

HighTech emploie actuellement environ 100 agents, gère et exploite un réseau de 1907 Km à voie unique et 370 Km à double voie. Ce réseau comporte également 528 Km de voies de service et 201 Km de ligne d'embranchement particulier reliant diverses entreprises au réseau national.

Raison sociale	HighTech –service
Siege social	charguia 2
Directeur général	M. Khlie Mohamed Rabie
Effectif	plus de 100
Tel	71934254/ 71934255/ 71934256
Fax	71934254
Site-web	www.Hightech-service.tn

Tableau 1:Présentation de High tech-service

3. Missions de High Tech-service:

High Tech est présent à l'international dans toutes les grandes zones géographiques dynamiques. En Tunisie, nous sommes présents avec près de 200 collaborateurs répartis sur l'ensemble du territoire national. A travers notre organisation, nous nous définissons comme un acteur global capable d'apporter à la fois son expertise technologique et un modèle de gestion de projets adaptés aux exigences de compétitivité de tous les acteurs mondiaux de l'industrie. En Afrique, nous sommes un

des partenaires privilégiés de l'industrie aéronautique et spatiale, High Tech s'affirme également dans les secteurs de la Défense, de l'Energie, des Télécoms & Média, et Transports.

Pour répondre au mieux aux attentes du marché, High Tech a développé un éventail d'expertises qui s'appuie sur son département, High Tech, véritable incubateur d'innovations. Nous développons et industrialisons des solutions à forte valeur ajoutée dans les domaines des objets connectés, des systèmes multi-agents collaboratifs, du Big Data et du cyber sécurité.

High Tech renforce son activité principalement dans les secteurs de l'Energie, de l'Industrie et dans les domaines tels que les systèmes connectés, les capteurs intelligents et la sécurité.

C'est ainsi que les nouvelles missions de High Tech-service s'articulent autour des axes suivants :

Sur le plan commercial :

Les nouvelles missions de High Tech-service sur le plan commerciales sont ambitieuses, on peut en citer :

- Une meilleure maîtrise des coûts.
- Le développement de l'activité de l'entreprise par une connaissance approfondie des besoins de la clientèle.
- L'offre de produits compétitifs répondant à leurs desiderata, l'amélioration de la qualité, information, sécurité, fréquence, régularité, tarifs...

Sur le plan organisationnel :

Sur le plan organisationnel, les efforts de High Tech-service sont d'autant plus importants :

- La mise en œuvre de mesures organisationnelles et de méthodes de gestion modernes visant l'efficacité, l'économie et l'optimisation des moyens de production.
- L'optimisation de la gestion des stocks et des charges de fonctionnement en maîtrisant les coûts de maintenance des installations fixes et du matériel roulant
- La valorisation des ressources humaines et la rationalisation des effectifs avec refonte du cadre de travail.
- L'adoption d'une culture d'entreprise fondée sur l'esprit de rentabilité et le principe de recherche de gisements de progrès pour la satisfaction des clients.
- L'amélioration de l'image de marque de High Tech-service en associant son nom à la compétence, à la qualité, à la sécurité et à l'efficacité.

Sur le plan technique :

High Tech-service focalise ses efforts techniques essentiellement sur audit informatique et Maintenance :

- Connaître les systèmes informatiques est le point de départ indispensable pour tous projets d'avenir.
- Installer une nouvelle application ou un nouveau serveur.

- Procéder aux dépannages de vos équipements informatiques.
- Installer des matériels ou logiciels.
- Installer et paramétrer vos réseaux d'entreprise .
- Solutions de maintenance informatique sur site.

4. Organisation et structure :

La structure de High Tech-service se manifeste par sa nature hierachico-fonctionnelle. En effet, par son caractère, elle est organisé hiérarchiquement mais les impératifs de son activité font qu'il est organisé aussi par fonctions et ce, dans un souci de compétitivité et d'efficacité.

J'ai effectué mon stage au sein de la **direction des systèmes d'informations**, dans le **département infrastructure SI** au **service réseaux et support SI.**

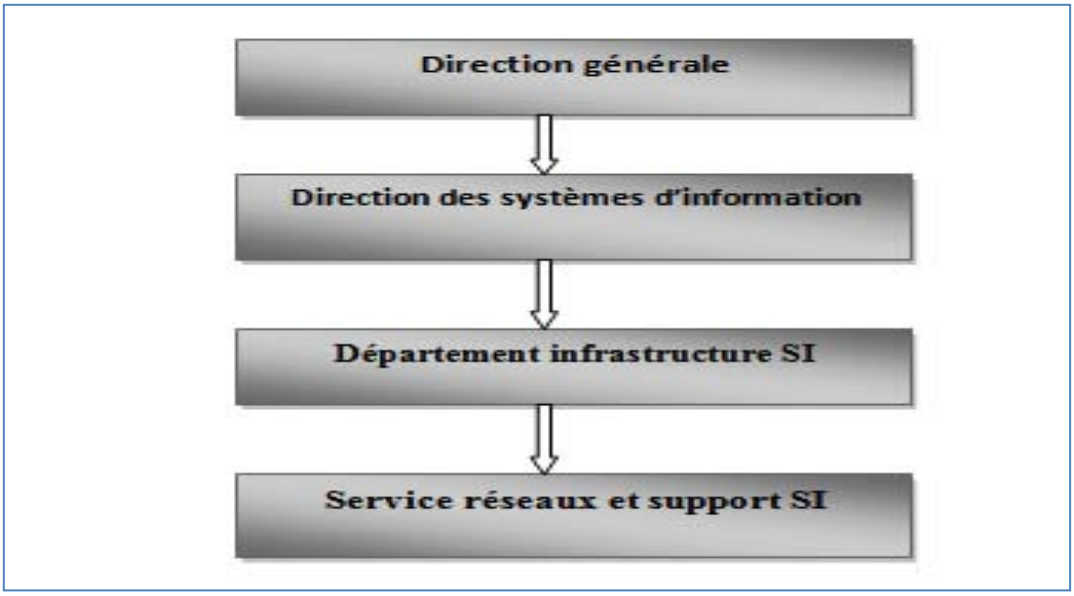


Figure 1:Organigramme de la Direction des Systèmes d'information.

Présentation de la direction des systèmes d'informations :

La Direction des systèmes d'Information a le rôle d'étudier, mettre en place, et maintenir des systèmes informatiques fiables (matériel et logiciel) permettant d'autoriser les procédures administratives et techniques, développer des applications de gestion permettant d'accroître les rendements et d'aider à la prise de décision conformément aux besoins exprimés par l'utilisateur .

Département Infrastructure SI :

Ce département prend en charge plusieurs missions notamment :

- Contribuer à la définition de la stratégie de développement du SI en cohérence avec celle de l'entreprise.

- Développer et maintenir l'infrastructure technique des systèmes d'informations.
- Assurer la production informatique, et instaurer progressivement une gouvernance des SI au niveau de HighTech-service.

Service Réseaux et Support SI :

Le service Réseaux & Support SI est l'entité en charge du maintien du bon fonctionnement du réseau de HighTech et de ses équipements. Les interventions du service concernent tout ce qui est supervision. Cependant il est aussi responsable de faire des études de renouvèlement des équipements et installations réseaux.

5. Présentation de la problématique :

High Tech-service, comme toute autre entreprise, souhaite bénéficier de la technologie de la VoIP en installant une solution sécurisée, vu l'augmentation du nombre des utilisateurs dans la majorité de ses sites, le cout exorbitant des communications, et les contraintes d'interconnexion et de câblage (réduction des taches de brassage). Cette solution doit améliorer la sécurité des flux de la voix, assurer la confidentialité des appels, et la gestion facile via une interface web.

6. Les objectifs du travail demandé :

Pour répondre à ces contraintes, le travail à réaliser est la mise en place d'une solution open source sécurisée pour les services voix. Pour cela, j'ai procédé comme suit:

- Une étude sur les protocoles de VoIP et des architectures existantes.
- Une étude des vulnérabilités et des attaques de sécurité sur les divers composants d'une infrastructure VoIP dans des réseaux LAN.
- Une étude pour déterminer la solution Open source de téléphonie sur IP la plus adaptée High Tech-service afin de la mettre en place.

Les entreprises, bénéficiant de cette solution, seront capables de mettre en place une plateforme de VoIP assez flexible, peu couteuse, et protégée contre les attaques de l'intérieur du réseau comme de l'extérieur.

7. La solution Open Source :

Suite au cahier de charges, j'utiliserai une solution open source pour la voix sur IP, ceci pour plusieurs raisons à savoir :

• La question de confiance

L'Open Source remet la confiance dans les mains du consommateur qui a tout loisir d'analyser le produit qu'on lui donne : en cela, il répond aux soucis de transparence qu'on trouve dans les sociétés contemporaines.

Il permet aussi d'éliminer les difficultés rencontrées à l'usage des nouvelles technologies en les rendant, de fait, plus accessibles à la compréhension de tous.

L'Open Source s'adapte parfaitement au travail collaboratif, car il permet à tous les acteurs d'avoir accès au même niveau d'information, sans que personne ne puisse revendiquer un rôle de gestion des droits des uns et des autres.

• L'Open Source et son support

Une contrainte du projet est de trouver un logiciel où la communauté du monde Open Source est très active. Il est alors relativement aisé de trouver des informations, voire de se faire aider sur un problème particulier, par le biais de forums et mailing listes.

• L'aspect budgétaire

L'intérêt de l'Open Source est qu'il permet également de faire des économies de part de la gratuité du produit mais également le fait d'éviter l'achat de matériel couteux.

8. Planning adopté :

La planification est parmi les phases d'avant projet les plus importantes. Elle consiste à déterminer, ordonnancer les tâches du projet et à estimer leurs charges respectives. Mon projet s'est articulé en quatre Mois (Février Mars Avril Mai Juin).

- **Ressources humaines :**

  Les gens qui ont participé à ce travail sont :

  Encadrant-interne Mr .Slim ALOUI

  Encadrant-externe Mr . Hassen SEDDIK

  Stagiaire Mr.Ahmed AOUADI

- **Ressources logiciels :**

Durant mon projet j'ai utilisé une panoplie d'outils informatiques à savoir :

VMware, Windows Seven , Linux, Backtrack, ASTRISK freePBX ,ELASTIK, X-lite, Sipvicious, Adito VPN, OpenVPN, Heartbeat, fail2ban, Nmap, Wireshark, Sivus …

- **Ressources budgétaires :**

L'estimation de la durée est à 80 jours ouvrables en prenant en compte les jours fériés. (5 jours en Février + 21jours en Mars +22 jours en Avril + 22 jours en Mai + 7jours en Juin - 1jour « Le 1 mai »).
Cout : 80jrs x Tarif journalier moyen = 0 DT (vu que le tarif journalier moyen est à Zéro dinar « cas de stagiaire à HighTech –service »).

Pour mener à bien mon projet, j'ai commencé par un planning prévisionnel, sauf que j'ai passé beaucoup plus de temps dans la partie de la sécurisation de la solution.

- **Chronogramme :**

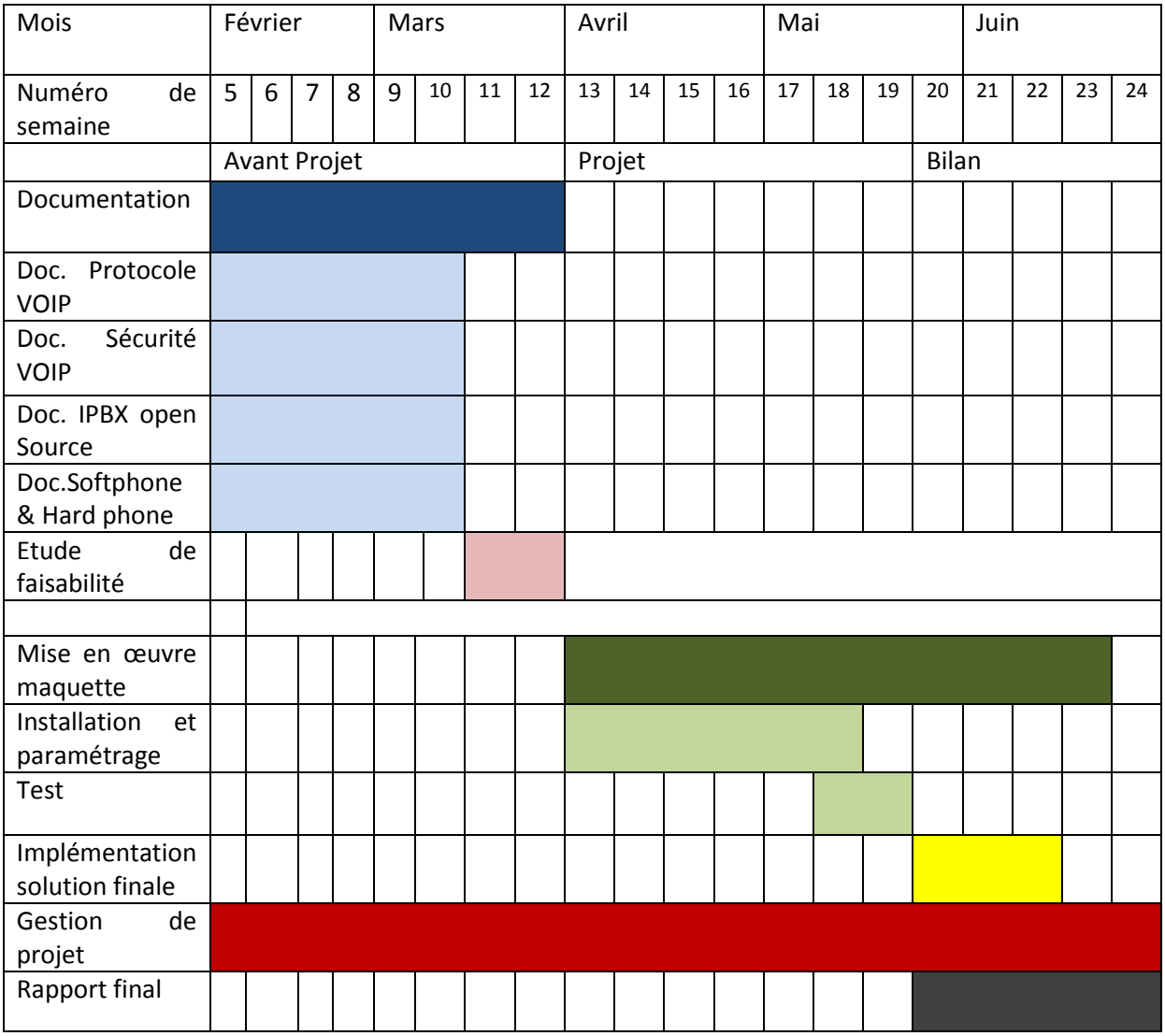


Figure 2: Planning prévisionnel de travail

II. Etat de l'art de la VoIP :

1. Introduction :

La Voix sur IP (VoIP ou Voice over Internet Protocol) consiste à transmettre une conversation vocale sur un réseau au protocole IP (Internet Protocol) c'est-à- dire sur un réseau de données par opposition à une transmission sur le réseau téléphonique classique ou réseau téléphonique commuté (RTC).

IP présente la caractéristique de transporter des données sous forme de paquets. La voix est donc digitalisée, compressée, envoyée par paquets de données sur le réseau conformément au protocole IP. Les données reçues sont décompressées et converties en voix audible.

Tous types de réseau IP peuvent donc être utilisés, réseaux privés ou réseau internet public, ainsi que tous types d'accès au réseau, Frame Relay, ATM, sans fil, fibre…

2. Avantages de la VoIP :

La VoIP offre de nombreuses nouvelles possibilités aux opérateurs et utilisateurs qui bénéficient d'un réseau basé sur IP. Les avantages les plus marqués sont les suivants.

- **Réduction des coûts:**

En déplaçant le trafic voix RTC vers le réseau privé WAN/IP les entreprises peuvent réduire sensiblement certains coûts de communications. Réductions importantes mises en évidence pour des communications internationales, ces réductions deviennent encore plus intéressantes dans la mutualisation voix/données du réseau IP inter-sites (WAN).

Dans ce dernier cas, le gain est directement proportionnel au nombre de sites distants.

- **Un réseau voix, vidéo et données (triple Play) :**

En positionnant la voix comme une application supplémentaire du réseau IP, l'entreprise ne va pas uniquement substituer un transport opérateur RTC à un transport IP, mais simplifier la gestion des trois réseaux (voix, données et vidéo) par ce seul transport. Une simplification de gestion, mais également une mutualisation des efforts financiers vers un seul outil. Concentrer cet effort permet de bénéficier d'un réseau de meilleure qualité, plus facilement évolutif et plus disponible, pourvu que la bande passante du réseau concentrant la voix, la vidéo et les données soit dimensionnée en conséquence.

- **Plus de fonctionnalité standard incluse :**

Puisque le réseau VoIP est basé sur un logiciel, il est plus simple pour les développeurs de le concevoir, d'ajouter et d'améliorer les jeux de fonctionnalités. C'est pourquoi la plupart des réseaux VoIP comportent des fonctionnalités riches et variées, y compris l'opérateur automatique, le répondeur, les appels en file d'attente et bien d'autres. Ces options sont souvent coûteuses avec les systèmes propriétaires.

- **Aucun branchement téléphonique séparé n'est nécessaire :**

Un réseau VoIP vous laisse connecter le matériel téléphonique directement au port réseau informatique standard (qu'il peut partager avec l'ordinateur adjacent). Les solutions téléphoniques peuvent être installées directement sur le PC. Cela signifie qu'il n'y a aucun réseau de branchement séparé à installer et maintenir pour le réseau téléphonique, vous donnant ainsi une plus grande flexibilité pour l'ajout d'utilisateurs/d'extensions. Si vous emménagez dans des locaux et n'avez pas encore installé les prises téléphoniques, vous pourrez faire des économies substantielles en installant uniquement un réseau informatique.

- **Adaptabilité :**

Les systèmes propriétaires sont difficiles à Tunis : l'ajout de lignes téléphoniques ou d'extensions nécessite souvent des mises à jour du matériel très coûteuses. Dans certains cas vous devrez renouveler l'intégralité de votre réseau téléphonique. Il n'en est pas de même avec le réseau VoIP : un

ordinateur normal peut facilement gérer un grand nombre de lignes téléphoniques et d'extensions, il suffit d'ajouter des téléphones à votre réseau.

Motivations	Pourcentage
Réduction de coûts	70%
Nécessité de standardiser l'équipement	66%
Hausse de la productivité des employés	65%
Autres bénéfices de productivité	64%
Hausse du volume d'appels à traiter	46%
Autres facteurs	50%

Tableau 2: Motivations pour déployer la VoIP.

3. Principe de Fonctionnement et Architecture :

3.1 Fonctionnement :

La voix sur IP (Voice over IP) caractérise l'encapsulation d'un signal audio numérique (La voix) au sein du protocole IP. Cette encapsulation permet de transporter la voix sur tout réseau compatible TCP/IP. Le transport de la voix sur un réseau IP nécessite au préalable sa numérisation. Il convient alors de récapituler les étapes nécessaires à la numérisation de la voix avant d'entrer dans les détails de la VoIP.Le principe de la voix sur IP est de faire circuler sur Internet, grâce au protocole IP, des paquets de données correspondant à des échantillons de voix numérisée. Reste ensuite à acheminer ces paquets dans le bon ordre et dans un délai raisonnable pour que la voix soit correctement restituée.

Le processus de la numérisation de la voix est schématisé par la figure suivante :

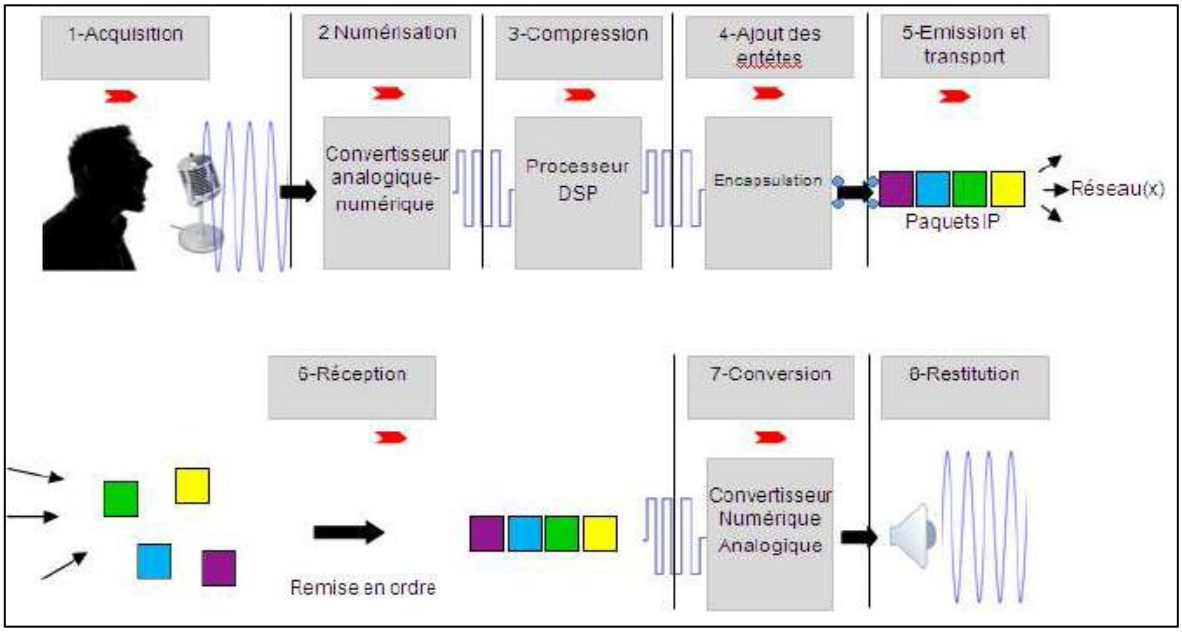


Figure 3: Le principe de fonctionnement de la VoIP

Etapes de transformation de la voix :

La première étape consiste à capter la voix à l'aide d'un micro, qu'il s'agisse de celui d'un téléphone ou d'un micro casque. La voix passe alors dans un convertisseur analogique numérique qui réalise deux tâches distinctes :

• **L'échantillonnage du signal sonore**, c'est-à-dire un prélèvement périodique de ce signal ;

• **La quantification**, consiste à affecter une valeur numérique (en binaire) à chaque échantillon. Plus les échantillons ne sont codés sur un nombre de bits important, meilleure sera la qualité de la conversion.

Généralement, la voix est échantillonnée à 8 kHz et chaque échantillon est codé sur 8 bits, ce qui donne un débit de 64 kbit/s (norme G711 [1]).

Numérisation : dans le cas où les signaux téléphoniques à transmettre sont sous forme analogique, ces derniers doivent d'abord être convertis sous forme numérique suivant le format PCM (Pulse Code Modulation) à 64 Kbps.

Compression: le signal numérique PCM à 64 Kbps est compressé selon l'un des formats de codec (compression / décompression) puis inséré dans des paquets IP .

Décompression: côté réception, les informations reçues sont décompressées. Il est nécessaire pour cela d'utiliser le même codec que pour la compression puis reconverties dans le format approprié pour le destinataire.

Le principe de la voix sur IP est de faire circuler sur Internet, grâce au protocole IP, des paquets de données correspondant à des échantillons de voix numérisée. Reste ensuite à acheminer ces paquets dans le bon ordre et dans un délai raisonnable pour que la voix soit correctement restituée.

Le signal une fois numérisé peut être traité par un DSP (Digital Signal Processor) qui effectue la compression, c'est-à-dire réduire la quantité d'informations (bits) nécessaire pour l'exprimer. Plusieurs normes de compression / Décompression (Codecs) sont utilisées pour la voix.

L'avantage de la compression est de réduire la bande passante nécessaire pour transmettre le signal. Mais ce gain peut se faire au détriment de la qualité sonore. Celle-ci peut être mesurée sur une échelle allant de 1 à 5, appelée échelle MOS (Mean Opinion Score) qui varie de 1 à 5 où 5 (score théorique) désigne une qualité parfaite. La note peut varier entre 1 (mauvais) et 5 (excellent, comparable à la version d'origine). Cette technique est issue de la téléphonie analogique

Qualité de l'appel	Score
Excellent	5
Bonne	4
Moyenne	3
Dégradée	2
Mauvaise	1

Tableau 3 : MOS et qualité de transmission de la voix

L'objectif d'un codec est la transformation d'un signal analogue vers un signal numérique et vice-versa. Ici, le codec transforme donc le signal de la voix en données numériques facilement transportables sur un réseau. Après de transport, le même codec se charge de retransformer le signal numérique vers un signal analogique. Parmi les principaux codecs décrits par l'UIT (Union Internationale des Télécommunications), on peut citer :

· **G711** [1] : compresse le signal à un débit de 64 kbit/s. Cette norme, largement supplantée par les suivantes, continue néanmoins à servir de référence en termes de fidélité au signal.(Score MOS de4,2)

· **G722** [2] : Cette norme, connue également sous l'appellation SB-MICDA (Modulation et Codage Différentiel Adaptatif à Sous-Bandes), propose trois niveaux de débits : 64,56, ou 48 kbit/s. Ses principaux avantages sont de coder le spectre sonore jusqu'à 7000 Hz et d'être très rapide (délai algorithmique de 1,5 ms). Son score MOS en 64kbit/s est de 4.

· **G723.1** [3] : Il s'agit d'une norme particulièrement adaptée à transmissions basse débits puisqu'elle fonctionne à 6,4 kbit/s ou 5,3 kbit/s. La contre partie est une moindre qualité (scores MOS respectivement de 3,9 et 3,7).

· **G 729** [4] : Avec les normes de la famille G723, G729 est le codec le plus utilisé pour la VoIP. Il fonctionne à un débit de 8 kbit/s et obtient un score MOS de 4.0, ce qui correspond à la qualité téléphonique requise. Comme G723.1, il ne permet pas la transmission des signaux fax ou fréquences vocales (DTMF, Dual Tone Multi Frequency).

Plus le MOS est élève plus le codec est de meilleur qualité (Figure 4).

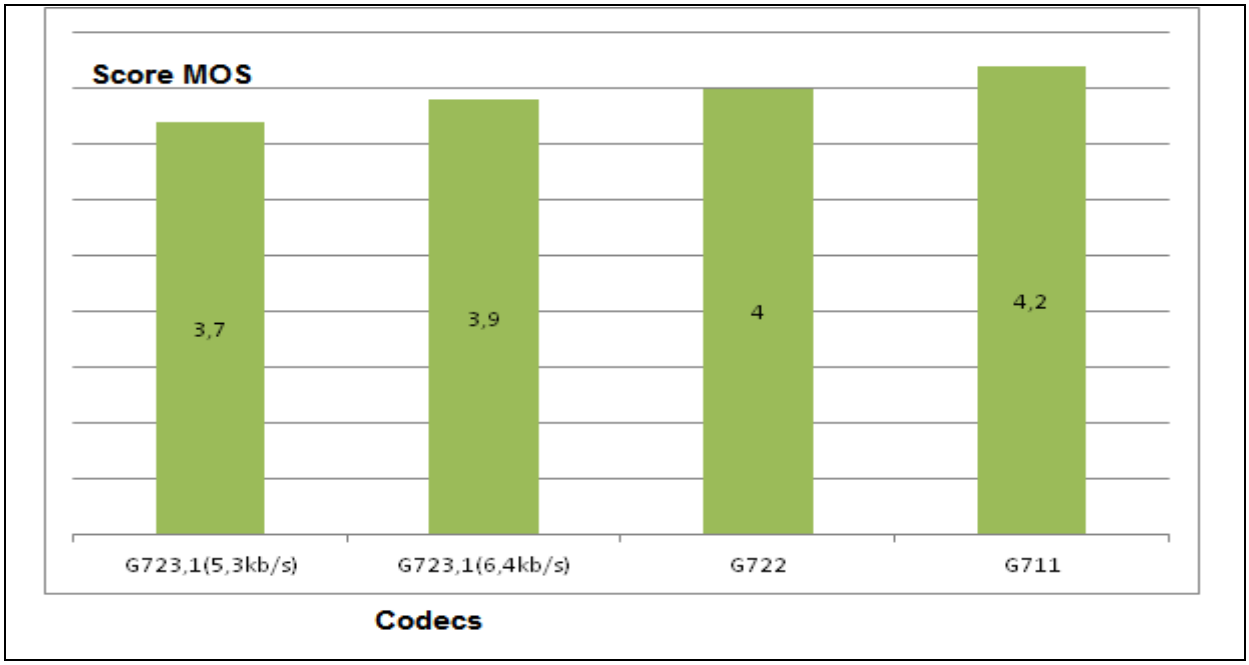


Figure 4:Echelle MOS des différents codecs.

Les données brutes qui sortent du DSP doivent encore être encapsulées avant d'être converties en paquets de données à expédier sur le réseau.

Les paquets sont ensuite acheminés depuis le point d'émission pour atteindre le point de réception sans qu'un chemin précis soit réservé pour leur transport. Ils vont transiter sur le réseau (réseau local,

réseau étendu voire Internet) en fonction des ressources disponibles et arriver à destination dans un ordre indéterminé. Lorsque les paquets arrivent à la destination, il est essentiel de les replacer dans le bon ordre et assez rapidement. Faute de quoi une dégradation de la voix se fera sentir.

La conversion numérique permet de transformer les données reçues sous forme de série discrète en un signal électrique continu.la voix peut être captée par le haut-parleur du casque, du combiné téléphonique ou de l'ordinateur.

3.2 Architecture :

Plusieurs cas de figures peuvent se présenter :

- **PC To PC**

Si les deux correspondants possèdent un PC équipé en conséquence (micro, écouteur), ils pourront communiquer à condition de connaître leurs adresses IP respectives.

Figure 5:Communication PC to PC

- **PC to Phone/Phone to PC**

Si un correspondant utilisant un PC souhaite appeler une personne sur son téléphone, il doit passer par un fournisseur de service sur Internet. Ce dernier met en place une passerelle, entre Internet et le RTC (réseau téléphonique commuté), qui gèrera les échanges de données. Dans le sens inverse, le correspondant peut contacter la passerelle de son téléphone.

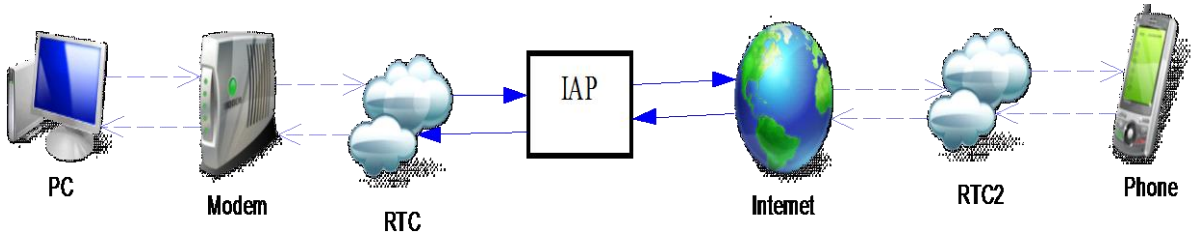


Figure 6:Communication PC to Phone

- **Phone to Phone**

Si les deux correspondants possèdent chacun un téléphone normal (analogique, ils devront chacun passer par une passerelle. Ensuite, les deux passerelles communiquent entre elles par un réseau de type Internet.

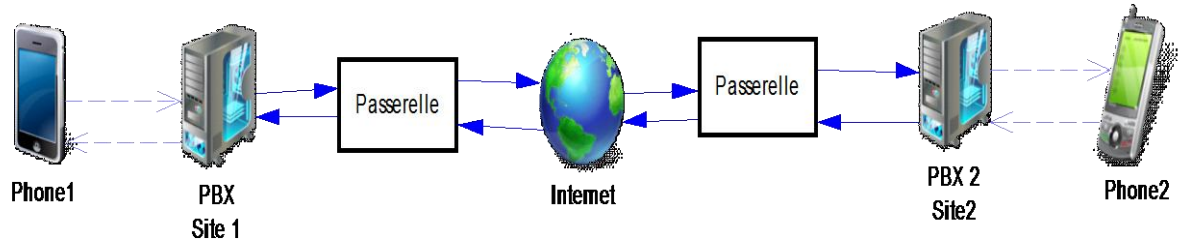


Figure 7:Communication Phone to Phone

4. Différence entre VoIP /ToIP :

La VoIP est une technique qui permet la communication par la voix (audio ou vidéo) , sur des réseaux compatibles IP, que ce soit un réseau privé ou Internet, filaire (câble, ADSL, fibre optique) , ou non filaire (satellite, wifi, GSM,3G) . La VoIP comprend donc les communications de PC à PC, dans lequel chaque utilisateur utilise le logiciel adéquat .Les communications peuvent également passer entre un PC et un téléphone, dans lesquelles le PC se transforme en téléphone, grâce à des logiciels spécifiques, appelées « Softphone ».

La TOIP est une catégorie de communication en voix sur IP, et concerne des échanges de téléphone à téléphone. Les téléphones IP ou les IP-phones, sont alimentés par courant, à la différence des cellulaires, et sont capables de numériser la voix pour la transmettre sur des réseaux IP, et inversement, rassembler les paquets entrants pour interpréter la voix reçue. La TOIP circule surtout sur des réseaux privés (LAN, VPN) ou publics.

En bref la TOIP est basée sur la VOIP mais la VOIP offre des services et applications multiples : couplage téléphonie –informatique (CTI), visioconférence sur IP, orientation des appels, messagerie vocale unifiée…

La VOIP résulte de la convergence entre voix, données et vidéo (triple Play), ce qui permet d'avoir un réseau unique par lequel ces trois éléments peuvent circuler. La TOIP, pour sa part restera toujours de la téléphonie pure.

5. Architecture VoIP :

La VoIP étant une nouvelle technologie de communication, elle n'a pas encore de standard unique. En effet, chaque constructeur apporte ses normes et ses fonctionnalités à ses solutions. Les trois principaux protocoles sont H.323, SIP et MGCP/MEGACO. Il existe donc plusieurs approches pour offrir des services de téléphonie et de visiophonie sur des réseaux IP.

L'architecture d'un réseau de téléphonie IP, comprend toujours des terminaux, un serveur de communication et une passerelle vers les autres réseaux. Chaque norme a ensuite ses propres caractéristiques pour garantir une plus ou moins grande qualité de service. L'intelligence du réseau est aussi déportée soit sur les terminaux, soit sur les passerelles/ contrôleur de commutation, appelées Gatekeeper. On retrouve les éléments communs suivants :

- **L'autocommutateur privé (IPBX)**

Sa mission est de gérer les appels internes et de relier les postes téléphoniques du site avec le réseau extérieur. Dans le cas où l'autocommutateur traite directement les conversations comme des flux de paquets IP, on parle d'IPBX.

- **Gatekeeper**

Le Gatekeeper est le dispositif chargé d'autoriser ou d'interdire l'accès au réseau et d'allouer une certaine bande passante à un appel. Il joue donc un rôle clé dans la sécurisation et la qualité de service

des communications .le Gatekeeper assure également la traduction entre les adresses IP et les numéros de téléphone dans l'entreprise, et route les appels.

- **Passerelle (media Gateway)**

Comme son nom l'indique, la passerelle fait le pont entre le protocole IP utilisé en interne ou sur le WAN et le réseau téléphonique public TDM (Time Division Multiplexing).

- **Téléphones**

Effectivement, les téléphones restent un équipement indispensable de la téléphonie sur IP. Selon les architectures, des téléphones classiques pourront être utilisés (cas des déploiements hybrides, décrit au chapitre 3), des téléphones IP (IP phones), des téléphones logiciels embarqués sur l'ordinateur de l'utilisateur (softphones) ou encore des terminaux mobiles pour réseau WiFi (Wifi phones) ou mixte WiFi / GSM.

- **Autres équipements**

Pour compléter la solution, on trouve fréquemment des équipements complémentaires comme une console d'administration pour le superviseur du réseau, un serveur de taxation, un pare feu (indispensable), un serveur de messagerie vocale ou messagerie unifiée, etc. …

6. Les protocoles de la VoIP :

Il faut distinguer entre deux types de protocoles VoIP: les protocoles de signalisation et de mise en relation des clients (H323, SIP, MGCP et IAX) et les protocoles de transport des données multimédia (RTP, RTCP). Globalement, la pile de protocoles est présentée dans la (figure 8).

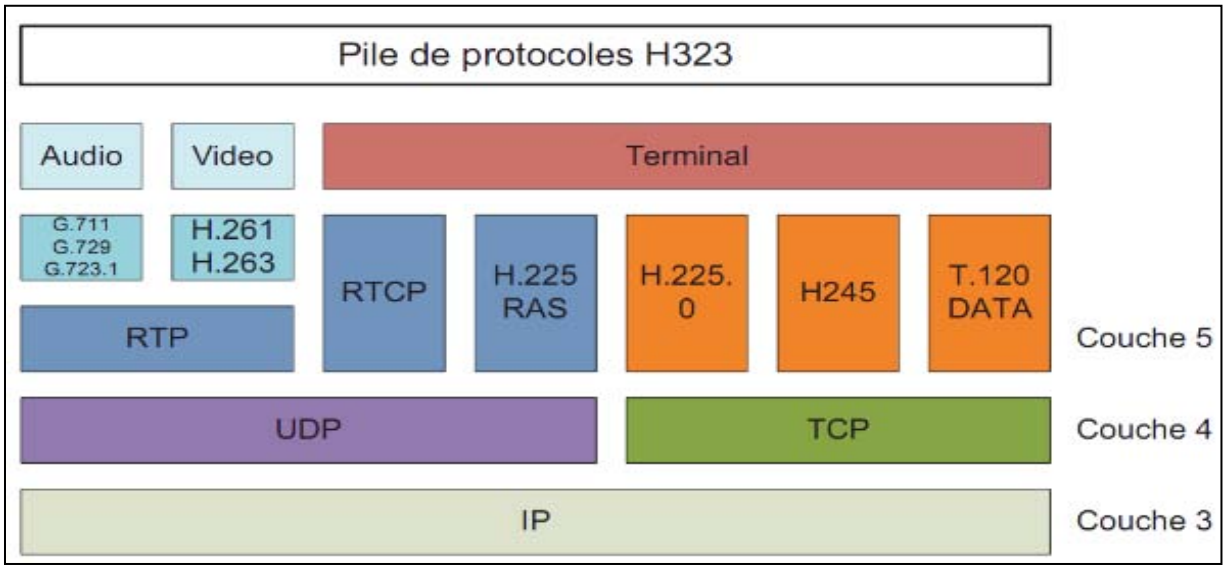


Figure 8: les protocoles de la VoIP

6.1 Les protocoles de signalisation :

- **H323 :**

Ce fût en 1996 la naissance de la première version voix sur IP appelée H323 [5]. Issu de l'organisation de standardisation européenne ITU-T sur la base de la signalisation voix RNIS (Q931), ce standard

regroupe un ensemble de protocoles de communication de la voix, de l'image et de données sur IP. Plus qu'un protocole, H.323 ressemble d'avantage à une association de plusieurs protocoles différents et qui peuvent être regroupés en trois catégories : la signalisation, la négociation de codec, et le transport de l'information. Les messages de signalisation sont ceux que l'on envoie pour demander d'être mis en relation avec une autre personne, indiquant que la ligne est occupée, que le téléphone sonne… Cela comprend aussi les messages que l'on envoie pour signaler que tel téléphone est connecté au réseau et qu'il peut être joint.

En H.323, la signalisation s'appuie sur le protocole RAS (Remote Access Service) pour l'enregistrement et l'authentification, et le protocole Q.931 pour l'initialisation et le contrôle d'appel.

Alors que, la négociation est utilisée pour se mettre d'accord sur la façon de coder les informations qu'on va s'échanger.

Il est important que les téléphones (ou systèmes) parlent un langage commun s'ils veulent se comprendre. Il serait aussi préférable, s'ils ont plusieurs alternatives de langages qu'ils utilisent. Il peut s'agir du codec le moins gourmand en bande passante ou de celui qui offre la meilleure qualité. Le protocole utilisé pour la négociation de codec est le H.245.

Le transport de l'information s'appuie sur le protocole RTP (Real Time transport Protocol) qui transporte la voix, la vidéo ou les données numérisées par les codecs. On peut aussi utiliser les messages RTCP pour faire du contrôle de qualité, voire demander de renégocier les codecs si, par exemple, la bande passante diminue.

En résumé, une communication H.323 se déroule en cinq phases :

1. Établissement d'appel.
2. Échange de capacité et réservation éventuelle de la bande passante à travers le protocole RSVP (Ressource réservation Protocol).
3. Établissement de la communication audio-visuelle
4. Invocation éventuelle de services en phase d'appel (par exemple, transfert d'appel, changement de bande passante, etc.)
5. Libération de l'appel.

- **SIP :**

SIP (Session Initiation Protocol) est un protocole normalisé et standardisé par l'IETF qui a été conçu pour établir, modifier et terminer des sessions multimédia. Il se charge de l'authentification et de la localisation des multiples participants. Il se charge également de la négociation sur les types de média utilisables par les différents participants en encapsulant des messages SDP (Session Description Protocol).

SIP ne transporte pas les données échangées durant la session comme la voix ou la vidéo. SIP étant indépendant de la transmission des données, tout type de donnés et de protocoles peut être utilisé pour cet échange. SIP remplace progressivement H323. Ceci est justifié par les différents atouts de ce standard. Il s'agit d'un protocole :

• **Ouvert** : les protocoles et documents officiels sont détaillés et accessibles à tous en téléchargement.

• **Flexible** : SIP est également utilisé pour tout type de sessions multimédia (voix, vidéo, mais aussi musique, réalité virtuelle, etc.)

• **Simple** : SIP est simple et très similaire à http. En effet, le client envoie des requêtes au serveur, qui lui renvoie une réponse.

Les Différentes méthodes sont utilisées pour gérer une conversation téléphonique :

• REGISTER : enregistrement du téléphone IP sur son proxy SIP,

• INVITE : demande l'établissement d'une session avec le téléphone appelé,

• RING : l'établissement de l'appel a été fait, le téléphone sonne.

• ACK : Confirmation de l'établissement de la session entre les deux IP Phones suite au décrochage du poste appelé. Les deux IP Phones sont désormais en point à point à ce stade et utilisent le protocole RTP pour transférer la voix.

• BYE : L'un des interlocuteurs raccroche et déclenche l'envoie de cette information au deuxième IP Phone (cette méthode est la source d'une attaque sur le protocole SIP : le reset perpétuelle d'une conversation).

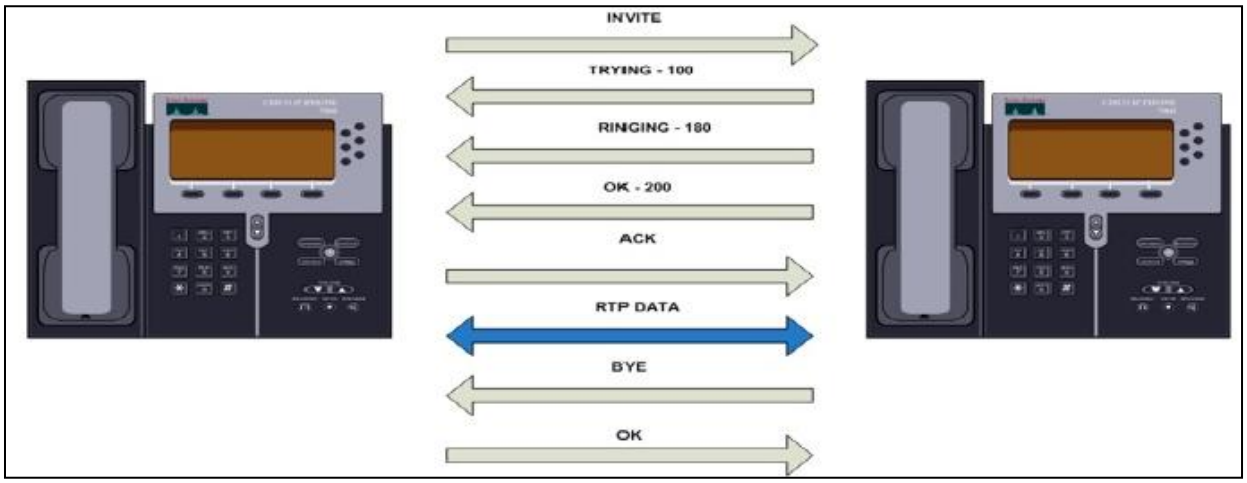


Figure 9:Processus d'appel entre deux clients SIP

Puisque le travail demandé sera effectué via le protocole SIP, on s'attardera un peu à expliquer les aspects et les caractéristiques qui font de ce protocole un bon choix pour l'établissement des sessions. Les principales caractéristiques du protocole SIP sont:

Fixation d'un compte SIP :

Il est important de s'assurer que la personne appelée soit toujours joignable. Pour cela, un compte SIP sera associé à un nom unique. Par exemple, si en tant qu'utilisateur d'un service de voix sur IP, vous disposez d'un compte SIP et que chaque fois que vous redémarrez votre ordinateur, votre adresse IP change, vous devez cependant toujours être joignable. Votre compte SIP doit donc être associé à un serveur SIP (proxy SIP) dont l'adresse IP est fixe. Ce serveur vous allouera un compte et vous permettra d'effectuer ou de recevoir des appels quelques soit votre emplacement. Ce compte sera identifiable via votre nom (ou pseudo).

Changement des caractéristiques durant une session :

Un utilisateur doit pouvoir modifier les caractéristiques d'un appel en cours. Par exemple, un appel initialement configuré en « voice-only » (voix uniquement) peut être modifié en « voix plus vidéo ».

Différents modes de communication :

Avec SIP, les utilisateurs qui ouvrent une session peuvent communiquer en mode point à point, en mode diffusif ou dans un mode combinant ceux-ci. Mode Point à point : on parle dans ce cas là « d'unicast » qui correspond à la communication entre 2 machines.

Mode diffusif : on parle dans ce cas là de « multicast » (plusieurs utilisateurs via une unité de contrôle MCU – Multipoint Control Unit).Combinatoire : combine les deux modes précédents. Plusieurs utilisateurs interconnectés en multicast via un réseau à maillage complet de connexion.

Gestion des participants :

Durant une session d'appel, de nouveaux participants peuvent joindre les participants d'une session déjà ouverte en participant directement, en étant transférés ou en étant mis en attente (cette particularité rejoint les fonctionnalités d'un PABX par exemple ou l'appelant peut être transféré vers un numéro donné ou être mis en attente).

Adressage :

Les utilisateurs disposant d'un numéro (compte) SIP disposent d'une adresse ressemblant à une adresse mail (sip:numéro@serveursip.com). Le numéro SIP est unique pour chaque utilisateur.

Codes d'erreurs :

Une réponse à une requête est caractérisée, par un code et un motif, appelés respectivement code d'état et raison phrase. Un code d'état est un entier codé sur 3 digits indiquant un résultat à l'issue de la réception d'une requête. Ce résultat est précisé par une phrase, textbased (UTF-8), expliquant le motif du refus ou de l'acceptation de la requête. Le code d'état est donc destiné à l'automate gérant l'établissement des sessions SIP et les motifs aux programmeurs. Il existe 6 classes de réponses et donc de codes d'état, représentées par le premier digit :

• **1xx** = Information - La requête a été reçue et continue à être traitée.

• **2xx** = Succès - L'action a été reçue avec succès, comprise et acceptée.

• **3xx** = Redirection - Une autre action doit être menée afin de valider la requête.

• **4xx** = Erreur du client - La requête contient une syntaxe erronée ou ne peut pas être traitée par ce serveur.

• **5xx** = Erreur du serveur - Le serveur n'a pas réussi à traiter une requête apparemment correcte.

• **6xx** = Echec général - La requête ne peut être traitée par aucun serveur.

Sécurité et Authentification :

Les messages Sip peuvent contenir des données confidentielles, le protocole Sip possède 3 mécanismes de cryptage :

· Cryptage de bout en bout du Corps du message Sip et de certains champs d'en-tête sensibles aux attaques.

· Cryptage au saut par saut (hop by hop) afin d'empêcher des pirates de savoir qui appelle qui.

· Cryptage au saut par saut du champ d'en-tête Via pour dissimuler la route qu'a empruntée la requête.

De plus, à fin d'empêcher à tout intrus de modifier et retransmettre des requêtes ou réponses Sip, des mécanismes d'intégrité et d'authentification des messages sont mis en place. Et pour des messages Sip transmis de bout en bout, des clés publiques et signatures sont utilisées par Sip et stockées dans les champs d'en-tête Autorisation. Une autre attaque connue avec Tcp ou Udp est le « deny of service », lorsqu'un Proxy Server intrus renvoie une réponse de code 6xx au client (signifiant un échec général, la requête ne peut être traitée). Le client peut ignorer cette réponse. S'il ne l'ignore pas et émet une requête vers le serveur "régulier" auquel il était relié avant la réponse du serveur "intrus", la requête aura de fortes chances d'atteindre le serveur intrus et non son vrai destinataire.

Avantages et inconvénients du protocole SIP :

Le protocole possède plusieurs avantages parmi lesquels :

· Son Ouverture : les protocoles et documents officiels sont détaillés et accessibles à tous en téléchargement.

· Standard : l'IETF a normalisé le protocole et son évolution continue par la création ou l'évolution d'autres protocoles qui fonctionnent avec SIP.

· Simple : SIP est simple et très similaire à http.

· Flexible : SIP est également utilisé pour tout type de sessions multimédia (voix, vidéo, mais aussi musique, réalité virtuelle, etc.).

· Téléphonie sur réseaux publics : il existe de nombreuses passerelles (services payants) vers le réseau public de téléphonie (RTC, GSM, etc.) permettant d'émettre ou de recevoir des appels vocaux.

· Points communs avec H323 : l'utilisation du protocole RTP et quelques codecs son et vidéo sont en commun.

Par contre une mauvaise implémentation ou une implémentation incomplète du protocole SIP dans les User Agents peut perturber le fonctionnement ou générer du trafic superflu sur le réseau. Un autre inconvénient est le faible nombre d'utilisateurs : SIP est encore peu connu et utilisé par le grand public, n'ayant pas atteint une masse critique, il ne bénéficie pas de l'effet réseau.

- **MGCP :**

Le protocole MGCP (Media Gateway Control Protocol) sert à l'échange de message de signalisation entre un contrôleur de passerelles de médias et des passerelles réparties dans un réseau IP. Pour l'établissement et la libération des connexions, MGCP se sert de signaux et d'événements. La standardisation de MGCP a été stoppée pour faire place à MEGACO/H.248 (Media Gateway Control Protocol), protocole élaboré en collaboration entre l'IETF et l'UIT.Ce nouveau

standard n'étant pas dérivé de MGCP, la migration vers MEGACO/H.248 semble très difficile. Les instructions de base d'une communication MGCP sont les suivantes :

1. CRCX (Create Connection) ordonne l'ouverture d'une connexion et transmet le message IAM (du protocole SS7 du réseau RNIS) vers sa destination.
2. L'ouverture de connexion est confirmée avec les messages ACK (Acknowledge).
3. MDCX (Modify Connection) permet de transmettre à la passerelle de gauche le numéro de port UDP choisi par la passerelle de droite.
4. Les messages ACM (Address Complete) et ANM (Answer Message) du SS7 permettent d'indiquer de bout en bout que la sonnerie retentit, respectivement, que l'usager appelé a répondu.
5. La libération de la connexion est effectuée au moyen des messages DLCX (Delete Connection) et ACK, pour le protocole MGCP, et de REL (Release) et RLC (Release Complete), pour le SS7.

La figure 10 détaille les phases d'une communication MGCP.

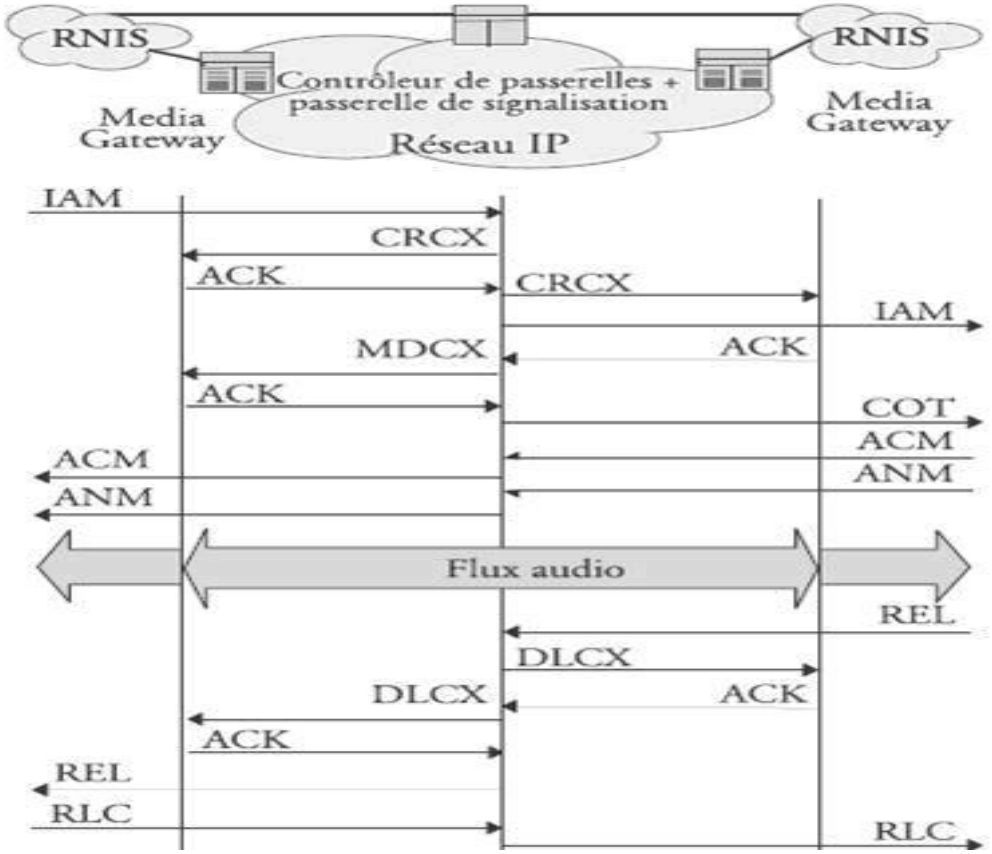


Figure 10: les phases d'une communication MGCP

- **IAX :**

Inter-Asterisk Exchange a été créé par l'équipe de développement du serveur IPBX Asterisk. Il permet de faire transiter voix et vidéo sur des débits plus faibles. D'autre part, il évite les problèmes de NAT posés par SIP car il n'utilise qu'un port UDP. Il est de plus en plus utilisé même s'il est encore jeune, pas normalisé et pas implémenté sur tous les équipements.

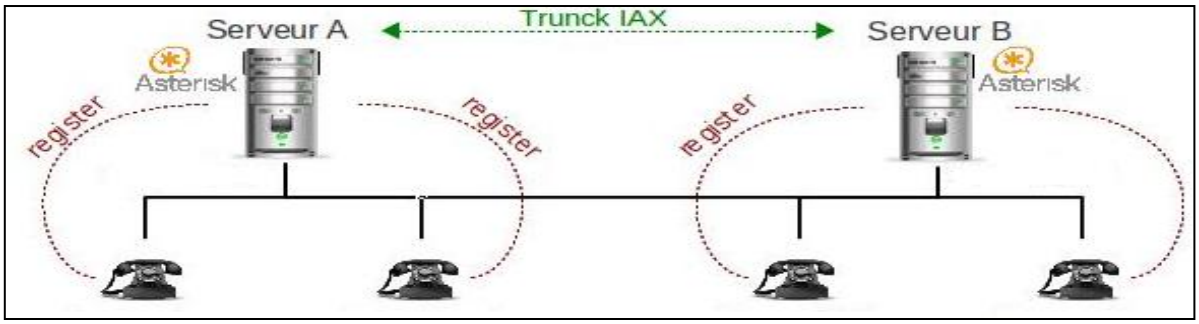


Figure 11:Echange de données entre plusieurs serveurs Asterisk

- **SCCP :**

Il s'agit d'un protocole propriétaire de Cisco mis en place pour éviter le protocole H323 trop compliqué à mettre en place. Il est très léger, utilise peu de bande passante et est principalement utilisé pour les communications entre les téléphones et le call manager, ainsi que pour le contrôle des conférences.

6.2 Les protocoles de transport :

La téléphonie sur IP nécessite le transfert de la voix en temps réel. Sur le réseau Internet, ce mécanisme n'est pas implémenté à la base. Pour effectuer un appel, il faut donc utiliser des protocoles spécifiques pour le transport des informations en temps réel : RTP (Real Time Protocol) / RTCP (Real Time Control Protocol), normalisés IETF (RFC 3550 & 3650).

Ils assurent le transport de la voix en temps réel.

RTP (Real time Transport Protocol) [6] : Il est pour le but de transmettre sur Internet des données qui ont des propriétés temps réel (audio, vidéo etc.). RTP permet d'organiser les paquets à l'entrée du réseau et de les contrôler à la sortie.

RTCP (Real time Transport Control Protocol) [7] :C'est un protocole de contrôle utilisé conjointement avec RTP pour contrôler les flux de données et la gestion de la bande passante. RTCP véhicule périodiquement des informations de bout en bout pour renseigner sur la qualité de service de la session.L'utilisation de RTP/RTCP se fait généralement au-dessus d'UDP. RTP et RTCP peuvent utiliser aussi bien le mode Unicast (point à point) que le mode Multicast (multipoint). Chacun deux utilise un port séparé d'une paire de ports. RTP utilise le port pair et RTCP le port impair immédiatement supérieur.

7. La QoS de la VoIP :

La qualité de service est un ensemble de caractéristiques de performance de service qui sont perçues et exprimées par l'utilisateur. Elle se manifeste par des paramètres pouvant prendre des valeurs qualitatives, c'est à dire qui ne peuvent pas être mesurées directement mais perceptibles par l'utilisateur ou bien se traduit par des valeurs quantitatives qui sont directement observées et mesurées aux points

d'accès. Il est intéressant de noter qu'on ne parle de la qualité de service que s'il y a une dégradation de la performance d'un réseau VoIP. Pour mesurer la QoS, on peut se baser sur des paramètres tels que :

7.1 Le temps de latence :

La latence est le décalage entre le temps écoulé entre l'envoi d'un paquet et sa réception par le destinataire. Plus la latence est important, plus le transfert est long et sera donc décalé.

Pour garantir une communication optimale, la maîtrise du délai de transmission est un élément essentiel, qui permet de bénéficier d'un véritable mode conversationnel et minimiser la perception d'écho. La durée de traversée d'un réseau IP dépend du nombre d'éléments réseaux traversés (et du débit sur chaque lien), du temps de traversée de chaque élément et du délai de propagation de l'information.

L'UIT a défini quatre classes qui permettent de caractériser, à titre indicatif, la qualité de transmission en fonction du retard de transmission dans une conversation téléphonique. Ces chiffres concernent le délai total de traitement, et pas uniquement le temps de transmission de l'information sur le réseau.

Classe n°	**Délai par sens**	**Interprétation**
1	0 à 150 ms	Acceptable pour la plupart des conversations.
2	150 ms à 300 ms	Acceptable pour des conversations faiblement interactives
3	300 ms à 700ms	Devient pratiquement une conversation half duplex.
4	>700 ms	Inutilisable

Tableau 4: Les quatre classes caractérisant la qualité de transmission.

La limite supérieure «acceptable» pour une communication téléphonique, se situe entre 150 et 200 ms par sens de transmission (en considérant à la fois le traitement de la voix et le délai d'acheminement).

7.2 La gigue :

La variation de temps de transit, ou gigue de phase, est la conséquence du fait que tous les paquets contenant des échantillons de voix ne vont pas traverser le réseau à la même vitesse.

Cela crée une déformation de la voix. La gigue de phase est indépendante du délai de transit. Le délai peut être court et la gigue importante ou inversement. La gigue est une conséquence de congestions passagères sur le réseau, ce dernier ne pouvant plus transporter les données de manière constante dans le temps. La valeur de la gigue va de quelques ms à quelques dizaines de ms.

Pour compenser la gigue, on utilise des tampons (mémoire : buffer) qui permettent de lisser l'irrégularité des paquets. Le fait d'insérer des buffers augmente le temps de latence, leur taille doit donc être soigneusement définie, et si possible adaptée de manière dynamique aux conditions du réseau. La dégradation de la qualité de service due à la présence de gigue se traduit par une combinaison des deux facteurs cités précédemment: le délai et la perte de paquets. Pour pallier à ces paramètres, il existe deux principales approches :

- Réserver une bande passante exclusivement au transfert de la voix : Cette solution est possible dans le cas des réseaux locaux (type Intranet) mais il n'est pas possible de l'appliquer lorsque le réseau TCP/IP Internet intervient dans la communication.

-Prioriser les flux : Chaque routeur traversé décide s'il prend en compte ou pas le champ de priorisation (champ TOS) propre à chaque type de données.

Gigues (ms)	Qualité perçue
<40	Excellente qualité (non détectable)
40 -75	Qualité acceptable
>75	Inacceptable

Tableau 5: Tolérance à la gigue en VoIP [8]

7.3 La perte de paquets :

La transmission de la voix par paquets s'appuie sur le protocole RTP (real-time transport Protocol). Ce dernier permet de transmettre sur IP les paquets de voix en reconstituant les informations même si la couche de transport change l'ordre des paquets. Il utilise pour cela des numéros de séquence et s'appuie sur UDP.

Les contraintes temps réel de délai de transit rendent inutile la retransmission des paquets perdus : même retransmis un datagramme RTP arriverait bien trop tard pour être d'une quelconque utilité dans le processus de reconstitution de la voix.

En voix sur IP on ne retransmet donc pas les données perdues. Ces pertes de données VoIP sont dues aux congestions sur le réseau, qui entraînent des rejets de paquets tout au long du réseau, ou à une gigue excessive qui va provoquer des rejets de paquet dans les buffers de gigue du récepteur, ceux-ci ne pouvant pas accueillir tous les paquets arrivés en retard.

Une perte de données régulière mais faible est moins gênante en voix sur IP que des pics de perte de paquets espacés mais élevés. En effet l'écoute humaine s'habituera à une qualité moyenne mais constante et en revanche supportera peu de soudaines dégradations de la QoS.

Plus un paquet de voix contient une longue durée de parole plus cet effet est accentué d'où la nécessité de choisir un bon codec audio (de faible débit).

Le taux de perte en VoIP est typiquement de quelques pourcents ou dixièmes de pourcent.

III. Conclusion :

Durant ce chapitre, on a présenté la technologie de la VoIP, ses avantages, ses protocoles, son principe de fonctionnement, et son architecture. On a pu alors déduire que la VoIP est la solution la plus rentable pour effectuer des conversations : Cette technologie, même si elle n'est pas encore mature, permet l'émergence de services performants et beaucoup moins coûteux, tant pour les entreprises que pour les particuliers.

CHAPITRE 2 : ATTAQUES CONTRE LA VOIP ET LES STRATEGIES DE SECURISATION

I. Introduction :

La course à la réduction des coûts d'une entreprise implique bien souvent la migration du service de téléphonie vers la Voix sur IP, ce choix séduit par le retour sur investissements des communications. Cependant de nombreux paramètres sont bien souvent oubliés ou ignorés.

Mis à part la surcharge du réseau de l'entreprise et la migration de nombreux équipements, la confidentialité des communications et l'efficacité des plans de secours sont remis en cause.

La convergence numérique va introduire de nouveaux services et par conséquent, de nouvelles vulnérabilités et de nouveaux vecteurs d'attaques.

Dans ce chapitre, je décris des attaques qui menacent la VoIP, et je détaille quelques-unes, je termine par une description des stratégies de sécurisations des communications de type voix sur IP.

II. Les attaques contre la VoIP :

1. Attaques sur les protocoles de communication :

Un appel téléphonique VoIP est constitué de deux parties : la signalisation, qui instaure l'appel, et les flux de media, qui transporte la voix.

La signalisation, en particulier SIP, transmet les entêtes et la charge utile (Payload) du paquet en texte clair, ce qui permet à un attaquant de lire et falsifier facilement les paquets. Elle est donc vulnérable aux attaques qui essaient de voler ou perturber le service téléphonique, et à l'écoute clandestine qui recherche des informations sur un compte utilisateur valide, pour passer des appels gratuits par exemple.

VoIP doit être configuré manuellement pour laisser le port 5060 ouvert, créant un trou pour des attaques contre les éléments qui écoutent l'activité sur ce port.

Le protocole RTP, utilisé pour le transport des flux multimédia, présente également plusieurs vulnérabilités dues à l'absence d'authentification et de chiffrage. Chaque entête d'un paquet RTP contient un numéro de séquence qui permet au destinataire de reconstituer les paquets de la voix dans l'ordre approprié. Cependant, un attaquant peut facilement injecter des paquets artificiels avec un numéro de séquence plus élevé.

En conséquence, ces paquets seront diffusés à la place des vrais paquets. Généralement, les flux multimédias contournent les serveurs proxy et circulent directement entre les points finaux. Les menaces habituelles conte le flux de la voix sont l'interruption de transport et l'écoute clandestine.

Les protocoles de la VoIP utilisent TCP et UDP 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 système VoIP seront détaillées dans les sections suivantes.

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

Le ou déni de service (Denial-of-service) [9] est une attaque très évoluée visant à rendre muette une machine en la submergeant de trafic inutile. Il faut savoir que ce sont des attaques qui ont pour seul objectif d'empêcher le bon fonctionnement d'un système, contrairement à d'autres attaques dont le but est de récupérer des informations ou encore de prendre le contrôle d'un système.

Il peut y avoir plusieurs machines à l'origine de cette attaque (c'est alors une attaque distribuée : DDoS) qui vise à anéantir des serveurs, des sous réseaux, etc. D'autre part, elle reste très difficile à contrer ou à éviter. Le DDoS est un type d'attaque qui coûte très cher puisqu'il interrompt le cours normal des transactions pour une entreprise.

Il existe de nombreuses façons pour faire planter une machine ; la différence se situe auniveau des intentions du hacker, c'est-à-dire savoir si le déni de service est intentionnel ou s'il n'est que la résultante d'une attaque plus agressive visant à détruire une machine.

Une attaque de type DoS peut s'effectuer à plusieurs niveaux soit :

2.1 Couche réseau :

IP Flooding [10]: Le but de l'IP Flooding est d'envoyer une multitude de paquets IP vers une même destination de telle sorte que le traitement de ces paquets empêche une entité du réseau (un routeur ou la station destinatrice) de traiter les paquets IP légitimes. Si l'IP Flooding est combiné à l'IP Spoofing, il est impossible, pour le destinataire, de connaître l'adresse source exacte des paquets IP. De ce fait, à moins que le destinataire ne limite ses échanges avec certaines stations, il lui est impossible de contrer ce type d'attaques.

Fragmentation des paquets IP : Par la fragmentation des paquets, il est possible de rendre horsservice de nombreux systèmes d'exploitation et dispositif VoIP par le biais de la consommation des ressources. Il existe de nombreuses variantes d'attaques par fragmentation, parmi les plus populaires teardrop, opentear, nestea, jolt, boink.

2.2 Couche transport :

L'UDP Flooding [11] : Le principe de cette attaque est qu'un attaquant envoie un grand nombre de requêtes UDP vers une machine. Le trafic UDP étant prioritaire sur le trafic TCP, ce type d'attaque peut vite troubler et saturer le trafic transitant sur le réseau et donc consomme plus de bande passante. Presque les dispositifs utilisant le protocole SIP fonctionnent au dessus du protocole UDP, ce qui en fait des cibles potentiels.

TCP SYN floods est une attaque visant le protocole TCP et plus exactement la phase d'établissement de connexion. Celle ci consiste en trois sous étapes :

- 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. C'est là le coeur de l'attaque parce que les ACK final ne seront 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.

2.3 Couche application :

Dans le cas du protocole SIP, une attaque DoS (SIP flooding) peut être directement dirigée contre les utilisateurs finaux ou les dispositifs tels que téléphones IP, routeurs et proxy SIP, ou contre les serveurs concernés par le processus, en utilisant le mécanisme du protocole SIP ou d'autres techniques traditionnelles de DoS. Il existe différentes formes d'attaques DoS, on peut citer :

DoS de type CANCEL :

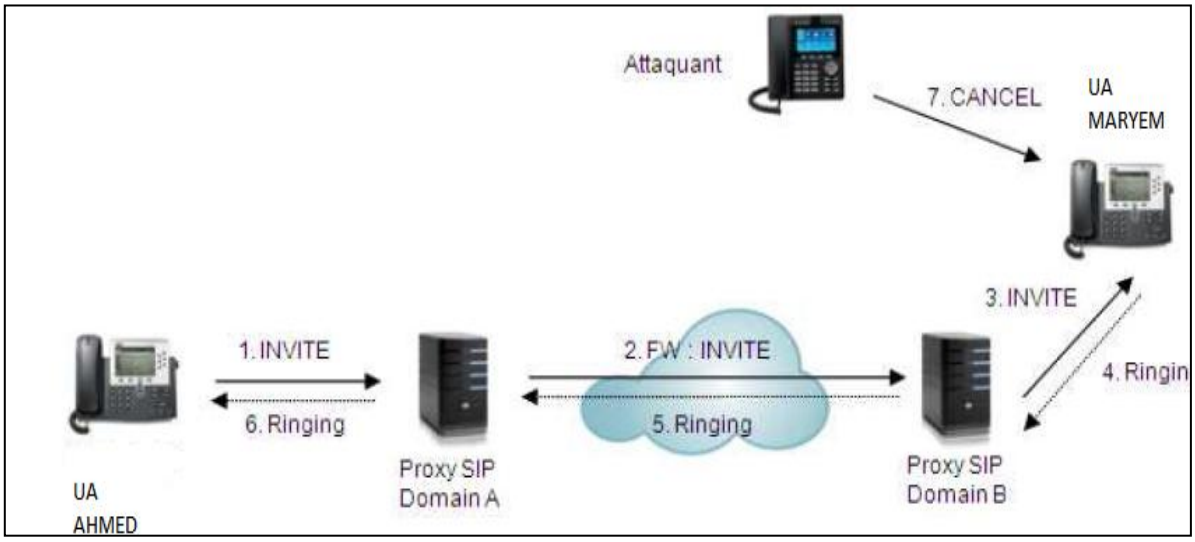


Figure 12:Scénario d'attaques DOS de type CANCEL [12]

C'est un type de déni de service lancé contre l'utilisateur. L'attaquant surveille l'activité du proxy SIP et attend qu'un appel arrive pour un utilisateur spécifique. Une fois que le dispositif de l'utilisateur reçoit la requête INVITE, l'attaquant envoie immédiatement une requête CANCEL.
Cette requête produit une erreur sur le dispositif de l'appelé et termine l'appel. Ce type d'attaque est employé pour interrompre la communication.
La figure (6) montre un scénario d'attaque DoS CANCEL, l'utilisateur (UA : User Agent)
AHMED initie l'appel, envoie une invitation (1) au proxy auquel il est rattaché. Le proxy du domaine A achemine la requête (2) au proxy qui est responsable de l'utilisateur Mehdi. Ensuite c'est le proxy du domaine B qui prend le relais et achemine la requête INVITE (3) qui arrive enfin à destination.
Le dispositif de MARYEM, quand il reçoit l'invitation, sonne (4). Cette information est réacheminée jusqu'au dispositif de AHMED. L'attaquant qui surveille l'activité du proxy SIP du domaine B envoie

une requête CANCEL (7) avant que Mehdi n'ait pu envoyer la réponse OK qui accepte l'appel. Cette requête annulera la requête en attente (l'INVITE), l'appel n'a pas lieu. L'activité du proxy SIP du domaine B envoie une requête CANCEL (7) avant que MARYEM n'ait pu envoyer la réponse OK qui accepte l'appel. Cette requête annulera la requête en attente (l'INVITE), l'appel n'a pas lieu.

DoS de type BYE

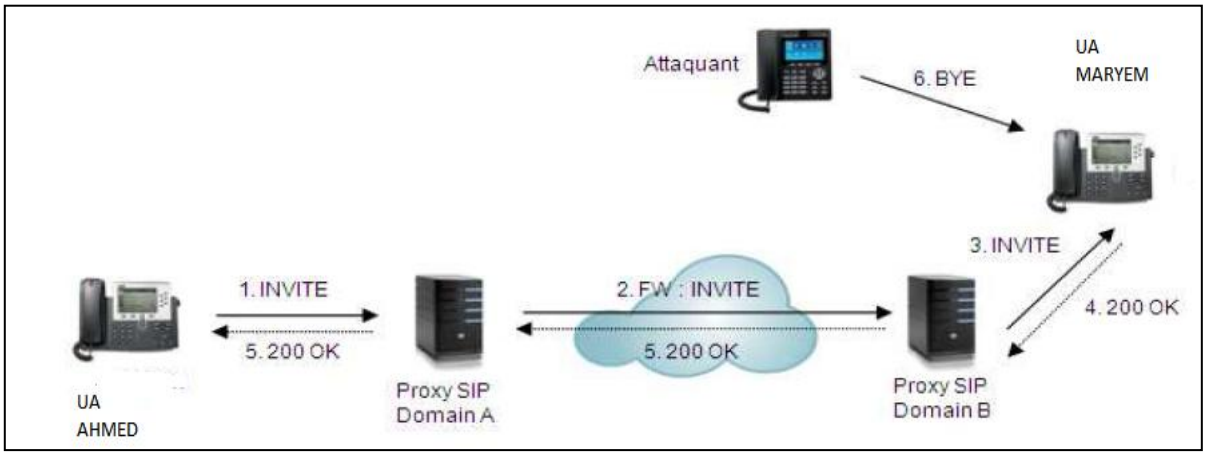


Figure 13:Scénario d'attaques DOS de type BYE [13]

Un autre type d'attaque lancée contre les utilisateurs est le déni de service par requête BYE.

Cette dernière est envoyée soit à l'appelant, soit à l'appelé, peut être utilisé pour perturber l'appel à n'importe quel moment de la communication.

C'est exactement le même scénario de la figure(6) sauf que dans ce cas-ci, l'attaquant attend qu'une réponse positive acceptant l'appel (4) soit envoyée par MARYEM pour lancer son attaque. Dès que la 200 OK est envoyée, l'attaquant envoie une requête BYE à l'un des participants ou même aux deux, ce qui terminera l'appel sans que les communiquant n'y puissent rien.

3. L'écoute clandestine (Eavesdropping) :

L'Eavesdropping est l'écoute clandestine d'une conversation téléphonique. Un attaquant avec un accès au réseau VoIP peut sniffer le trafic et décoder la conversation vocale. Des outils tels que VOMIT (Voice Over Misconfigured Internet Telephones) permettent de réaliser cette attaque. VOMIT convertit les paquets sniffés en fichier .wav qui peut être réécouté avec n'importe quel lecteur de fichiers son. Le principe de l'écoute clandestine est le suivant :

- Déterminer les adresses MAC des victimes (client serveur) par l'attaquant.
- Envoi d'une requête ARP non sollicitée au client, pour l'informer du changement de l'adresse MAC du serveur VoIP à l'adresse MAC de l'attaquant.
- Envoi d'une requête ARP non sollicitée au serveur, pour l'informer du changement de l'adresse MAC du client à l'adresse MAC de l'attaquant.
- Désactiver la vérification des adresses MAC sur la machine d'attaquant afin que le trafic puisse circuler entre les 2 victimes.

4. Sniffing :

C'est une technique servant à espionner le trafique d'un système en surveillant et en copiant les paquets non crypté circulant dans le réseau cible.

Un reniflage (Sniffing)[14] peut avoir comme conséquence un vol d'identité et la révélation d'informations confidentielles. Il permet également aux utilisateurs malveillants perfectionnés de rassembler des informations sur les systèmes VoIP. Qui peuvent par exemple être employées pour mettre en place une attaque contre d'autres systèmes ou données. Plusieurs outils requis pour le Sniffing, y compris pour le protocole H.323 et des plugins SIP, sont disponibles en open source. La plus part des attaques se base sur cette technique d'où son utilité et importance dans la suite. Les sniffer les plus utilisés sont : TCP dumps, dsniff, LAN watch.

5. Suivie des appels :

Appelé aussi Call tracking, cette attaque se fait au niveau du réseau LAN 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,

6. Les spams :

Le spam, pourriel ou polluriel est une communication électronique non sollicitée. Trois formes principales de spams sont jusqu'à maintenant identifiés dans SIP.

6.1 Call Spam :

Ce type de spam est défini comme une masse de tentatives d'initiation de session (des requêtes INVITE) non sollicitées. Généralement c'est un client qui lance, en parallèle, un grand nombre d'appels.

6.2 IM (Instant Message) Spam :

Ce type de spam est semblable à celui de l'e-mail. Il est défini comme une masse de messages instantanés non sollicitées. Les IM spams sont pour la plupart envoyés sous forme de requête
SIP. Ce pourraient être des requêtes INVITE avec un entête très grand, ou des requêtes
INVITE avec un corps en format texte ou HTML. Bien-sûr, l'IM spam est beaucoup plus intrusif que le spam email, car dans les systèmes actuels, les IMs apparaissent automatiquement sous forme de pop-up à l'utilisateur.

6.3 Présence Spam :

Ce type de spam est semblable à l'IM spam. Il est défini comme une masse de requêtes de présence (des requêtes SUBSCRIBE) non sollicitées. L'attaquant fait ceci dans le but d'appartenir à la liste

blanche d'un utilisateur afin de lui envoyer des messages instantanés ou d'initier avec lui d'autres formes de communications. L'IM Spam est différent de la présence Spam dans le fait que ce dernier ne transmet pas réellement de contenu dans les messages.

7. Détournement d'appel (Call Hijacking) :

Le Call Hijacking consiste à détourner un appel. Plusieurs fournisseurs de service VoIP utilisent le web comme interface permettant à l'utilisateur d'accéder à leur système téléphonique. Un utilisateur authentifié peut changer les paramètres de ses transferts d'appel à travers cette interface web. C'est peut être pratique, mais un utilisateur malveillant peut utiliser le même moyen pour mener une attaque. Par exemple quand un agent SIP envoie un message INVITE pour initier un appel, l'attaquant envoie un message de redirection 3xx indiquant que l'appelé s'est déplacé et par la même occasion donne sa propre adresse comme adresse de renvoi. A partir de ce moment, tous les appels destinés à l'utilisateur sont transférés et c'est l'attaquant qui les reçoit. Un appel détourné en lui-même est un problème, mais c'est encore plus grave quand il est porteur d'informations sensibles et confidentielles.

III. Les vulnérabilités de l'infrastructure VoIP :

Plusieurs dispositifs de la VoIP, dans leur configuration par défaut, peuvent avoir une variété de ports TCP et UDP ouverts. Les services fonctionnant sur ces ports peuvent être vulnérables aux attaques DoS.Ces dispositifs sont configurés pour télécharger périodiquement un fichier de configuration depuis un serveur par TFTP ou d'autres mécanismes. Un attaquant peut potentiellement détourner ou mystifier cette connexion et tromper le dispositif qui va télécharger un fichier de configuration malveillant à la place du véritable fichier.

1. Les Attaques contre les téléphones IP :

Un pirate peut compromettre un téléphone IP, un softphone et autres programmes ou matériels clients. Généralement, il obtient les privilèges qui lui permettent de commander complètement la fonctionnalité du dispositif.

Compromettre un téléphone IP, peut être fait à distance ou par un accès physique au dispositif. Le pirate pourrait modifier les aspects opérationnels d'un tel dispositif, en changeant son système d'exploitation. Ainsi la présence de l'attaquant ne sera pas remarquée.

Par ailleurs, un firmware du téléphone IP est modifié de manière malveillante peut être téléchargé et installé, les modifications faites à la configuration des logiciels de téléphonie IP peuvent permettre:

_ Aux appels entrants d'être réorientés vers un autre point final sans que l'utilisateur soit au courant.

_ Aux appels d'être surveillés.

_ A l'information de la signalisation et/ou les paquets contenant de la voix d'être routés vers un autre dispositif et également d'être enregistrés et/ou modifiés.

_ De compromettre la disponibilité du téléphone IP. Par exemple, ce dernier peut rejeter automatiquement toutes les requêtes d'appel, ou encore, éliminer tout déclenchement de notification tel qu'un son, une notification visuelle à l'arrivée d'un appel. Les appels peuvent également être interrompus à l'improviste

_ Des backdoors pourraient été installés

Les softphones ne réagissent pas de la même façon aux attaques comparés à leur homologues téléphones IP. Ils sont plus susceptibles aux attaques dues au nombre de vecteurs inclus dans le système, à savoir les vulnérabilités du système d'exploitation, les vulnérabilités de l'application, les vulnérabilités du service, des vers, des virus

2. Les attaques contre les serveurs VoIP :

Un pirate peut viser les serveurs qui fournissent le réseau de téléphonie sur IP, compromettre une telle entité mettra généralement en péril tout le réseau de téléphonie dont le serveur fait partie. Par exemple, si un serveur de signalisation est compromis, un attaquant peut contrôler totalement l'information de signalisation pour différents appels, ces informations sont routées à travers le serveur compromis.

Avoir le contrôle de l'information de signalisation permet à un attaquant de changer n'importe quel paramètre relatif à l'appel. Si un serveur de téléphonie IP est installé sur un système d'exploitation, il peut être une cible pour les virus, les vers, ou n'importe quel code malveillant.

IV. Les vulnérabilités du système d'exploitation :

Ces vulnérabilités sont pour la plupart relatives au manque de sécurité lors de la phase initiale de développement du système d'exploitation (sur lequel on configure notre serveur VoIP), et ne sont découvertes qu'après le lancement du produit. Une des principales vulnérabilités des systèmes d'exploitation est le buffer overflow. Il permet à un attaquant de prendre le contrôle partiel ou complet de la machine. Les dispositifs de la VoIP tels que les téléphones IP, Call Managers, Gateway et les serveurs proxy, héritent les mêmes vulnérabilités du système d'exploitation ou du firmware sur lequel ils tournent.

Il existe une centaine de vulnérabilités exploitables à distance sur Windows et même sur Linux. Un grand nombre de ces exploits sont disponibles librement et prêts à être téléchargés sur l'Internet.

V. Les solutions de sécurité :

Avant de présenter les solutions de sécurité, il convient de rappeler les définitions des propriétés de sécurité :

-L'intégrité [15] : C'est un service cryptographique qui permet de s'assurer que l'information n'a été ni altérée ni modifiée, par des personnes non autorisées, pendant sa transmission ou son stockage

-l'authentification [16] : C'est un service cryptographique qui permet de s'assurer de l'identité de l'expéditeur de l'information, et par conséquent, de confirmer son identité.

-**La confidentialité** : C'est un service cryptographique qui permet d'assurer le secret des informations afin qu'elles ne soient ni rendues accessibles, ni divulguées à un utilisateur, une entité ou un processus non autorisé

-**La non répudiation** : C'est un service cryptographique qui permet d'obtenir la preuve de l'émission ou de la réception d'une information ; l'expéditeur et le destinataire ne peuvent ainsi en nier l'envoi ou la réception. Il empêche donc le reniement d'actions ou de messages

-**La signature numérique** (ou signature électronique) :C'est un service cryptographique permettant de vérifier l'authenticité de l'expéditeur ainsi que l'intégrité du message reçu, et d'en assurer la non répudiation (Services d'authentification, d'intégrité et de non répudiation)

- **le non rejeu** : éviter de mémoriser puis de re-injecter les données dans le réseau

- **l'anonymat** : capacité du système à masquer l'identité de l'usager ;

Ces propriétés de sécurité permettent de décrire les objectifs qu'il faut fixer pour protéger son système, compte tenu de ses besoins et des menaces.

La stratégie de sécurité repose sur quatre piliers : la sécurisation des éléments actifs qui composent la solution, l'utilisation de l'infrastructure pour empêcher les malveillances, la protection des échanges protocolaires et des communications et la surveillance active. Ainsi, une fois la stratégie est définie, les solutions sont plutôt nombreuses. Elles sécurisent, soit la couche infrastructure et/ou la couche logicielle.

1. Mise en place de VLAN :

Un VLAN est un réseau local regroupant un ensemble de machines de façon logique et non physique, grâce aux réseaux virtuels (VLANs) il est possible de s'affranchir des limitations de l'architecture physique (contraintes géographiques, contraintes d'adressage, ...) en définissant une segmentation logique (logicielle) basée sur un regroupement de machines grâce à des critères (adresses MAC, numéros de port, protocole, etc.).

Le VLAN permet de définir un nouveau réseau au-dessus du réseau physique et à ce titre offre les avantages suivants :

- Plus de souplesse pour l'administration et les modifications du réseau car toute l'architecture peut être modifiée par simple paramétrage des commutateurs.
- Gain en sécurité car les informations sont encapsulées dans un niveau supplémentaire et éventuellement analysées.
- Réduction de la diffusion du trafic sur le réseau.

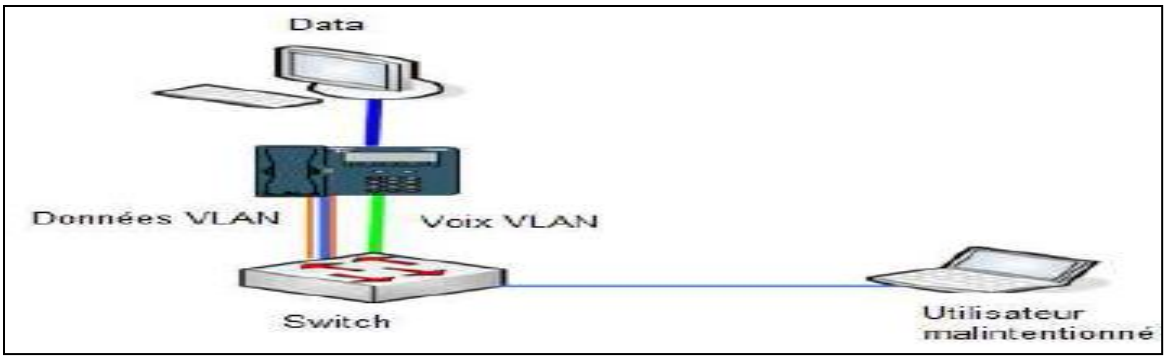


Figure 14:le cloisonnement des VLAN (séparation data et voix)

2. Sécurisation protocolaire :

- **Utilisation de SRTP :**

SRTP est conçu pour sécuriser la multiplication à venir des échanges multimédias sur les réseaux. Il couvre les lacunes de protocoles de sécurité existants comme IPsec (IP Security), dont le mécanisme d'échanges de clés est trop lourd. Il aussi est bâti sur le protocole temps réel RTP (Real Time Transport Protocol). Il associe aussi une demi-douzaine de protocoles complémentaires. Il est donc compatible à la fois avec des protocoles d'initiation de session de voix sur IP tel que SIP (Session Initiation Protocol), ainsi que le protocole de diffusion de contenu multimédia en temps réel RTSP (Real Time Streaming Protocol). Mais, surtout, il s'adjoint les services du protocole de gestion de clé MIKEY (Multimedia Internet KEYing).Avec une gestion de clé appropriée, SRTP est sécurisé pour les applications unicast et multicast de RTP. En théorie, SRTP est une extension du protocole RTP dans lequel a été rajoutée des options de sécurité. En effet, il a pour but d'offrir plusieurs implémentations de cryptographie tout en limitant l'overhead lié à l'utilisation des chiffrements. Il propose des algorithmes qui monopoliseront au minimum les ressources et l'utilisation de la mémoire.Surtout, il permet de rendre RTP indépendant des autres couches en ce qui concerne l'application de mécanismes de sécurité. Pour implémenter les différents services de sécurité précités, SRTP utilise les composants principaux suivants :

Une clé maîtresse utilisée pour générer des clés de session; Ces dernières seront utilisées pour chiffrer ou pour authentifier les paquets. Une fonction utilisée pour calculer les clés de session à partir de la clé maîtresse. Des clés aléatoires utilisées pour introduire une composante aléatoire afin de contrer les éventuels rejet ou effets de mémoire. SRTP utilise deux types de clés : clef de session et clef maîtresse. Par « clef de session » nous entendons une clef utilisée directement dans les transformations cryptographiques; et par « clef maîtresse », nous entendons une chaîne de bit aléatoire à partir desquelles les clefs de sessions sont dérivées par une voie sécurisé avec des mécanismes cryptographiques.

- **Utilisation de tunnels IPSec :**

Les différentes solutions de tunneling présentent toutes des avantages et des inconvénients pour la VoIP avec ses nombreuses exigences. IPSec, qui travaille sur la couche réseau, permet d'assurer une

plus grande fiabilité des informations. Notons par exemple que le problème des en-têtes SRTP modifiables n'est plus un souci ici.

Cependant, le coût de cette solution est parfois considérable, tant sur le plan des ressources matérielles que sur le trafic réseau. IKE (Internet Key Exchange) permet alors de remplacer MiKEY et d'assurer la gestion des clefs pour l'ensemble des communications VoIP.

La surcharge engendrée par IPSec peut être minimisée en configurant le tunnel pour traiter uniquement les flux de voix sur IP (pour des machines/protocoles fixés).Un atout intéressant est la possibilité d'utiliser la totalité des soft phones disponibles puisqu'ils n'ont plus à gérer la sécurité des échanges (SRTP/MiKEY...).

Les tunnels simplifient le déploiement de la VoIP sécurisée, mais ne peuvent pas être employés sur de larges infrastructures ou sur des soft phones peu puissants.

- **Authentification et chiffrement SSL / TLS :**

Transport Layer Security (TLS), anciennement nommé Secure Socket Layer (SSL), est un protocole de sécurisation des échanges sur Internet. Par abus de langage, on parle de SSLpour désigner indifféremment SSL ou TLS.SSL fonctionne suivant un mode client-serveur. Il fournit quatre objectifs de sécurité :

- L'authentification du serveur ;
- La confidentialité des données échangées (ou session chiffrée)
- L'intégrité des données échangées ;
- De manière optionnelle, l'authentification du client.

- **Protection contre DoS :**

Les contre-mesures sont très compliquées à mettre en place et très ciblées vis-à-vis du type de déni de service envisagé. En effet, d'un point de théorique, la plupart des attaques visant à créer des dénis de service sont basées sur des services ou protocoles normaux sur Internet.

S'en protéger reviendrait à couper les voies de communications normales avec Internet, alors que c'est bien là la raison d'être principale des machines concernées (serveurs web, etc...).

Il reste tout de même la possibilité de se protéger contre certains comportements anormaux, comme une tentative de flooding, un trop grand nombre de paquets ou de requêtes de connexion provenant d'un petit nombre de machines. Mais cela implique beaucoup de choses en fait : il faut monitoire le trafic (ce qui est loin d'être simple, du fait de la quantité de données qui transitent), établir des profils types de comportement et des écarts tolérables au delà desquels on considérera que l'on a affaire à une attaque; il faut également définir les types d'attaques auxquelles on souhaite se protéger (analyses de risques à l'appui) car il est impossible de toutes les prévoir.

- **Installer un pare-feu :**

Si un pirate parvient bel et bien à se connecter au réseau sans fil, il peut en principe lancer une attaque ARP contre toutes les stations dans son sous réseau.

Toutefois, certains pare-feux savent détecter ces attaques et les empêcher : l'idéal est que ce type de pare-feu soit intégré à chaque AP, de sorte que le pirate ne puisse même pas attaquer les autres stations associées au même AP. Sinon, on devra se contenter d'un parefeu installé entre l'AP et le réseau filaire, pour au moins protéger le réseau filaire contre les attaques provenant du réseau.

- **IDS :**

Il n'est pas très courant de trouver des outils de détection d'intrusion pour des solutions de voix sur IP. La quantité de faux positifs dus à l'observation du flux RTP pourrait être plus que conséquente. Bien qu'elle permette de détecter des dénis de service par exemple, la détection d'intrusion se ramène souvent à de la détection de fraude.

3. Filtrage des adresses MAC :

Pour éviter que n'importe qui se connecte sur les ports d'un switch, il est possible de faire un contrôle sur les adresses MAC des machines connectées sur chaque port.

Une simple commande permet d'activer cette sécurité sur l'interface concernée.

La définition des adresses MAC autorisées sur un port donné peut se faire de deux façons :

- Par adresse MAC fixée en spécifiant explicitement l'adresse MAC à qui l'on souhaite donner l'accès dans la commande au Switch.

Switch(config-if) # switchport port-security mac-address

- Par apprentissage de l'adresse MAC source de la première trame qui traversera le port via l'option « sticky mac ».

Switch(config-if) # switchport port-security mac-address sticky

VI. Conclusion :

Dans ce chapitre, on a présenté les fameuses attaques qui peuvent menacer la sécurité de notre serveur VoIP, et les différentes solutions possibles pour remédier à ces attaques.La voix sur IP devient jour après jour plus ciblée, donc il faut mettre en place une stratégie de sécurité assez solide, afin de mieux protéger notre réseau VoIP.

CHAPITRE 3 : ETUDE DES SOLUTIONS DISPONIBLES

I. Introduction :

Ce chapitre traite l'étude de comparaison des différents IPBX open source existants. Elle permet de voir et de comparer les caractéristiques de ces IPBX afin d'en retenir un que j'utiliserai pour réaliser la maquette, cette étude doit pouvoir démontrer quel est l'IPBX le plus adapté.

II. Étude des différents serveurs de communication Open Source :

Il existe plusieurs IPBX open source disponibles sur le marché, les plus intéressants sont les suivants :

Le premier IPBX c'est **Asterisk Elastix** qui a été créé par Mark Spencer qui est aussi le fondateur de la société DIGIUM. Il y a encore quelques mois, personne n'avait entendu parler d'Asterisk. Seul un cercle très fermé de puristes de la VoIP le connaissait. Aujourd'hui, Asterisk est prononcé par toutes les langues.

Asterisk est le projet IPBX Open Source qui possède la plus grosse communauté de développeurs. Il est facile de trouver sur Internet des packages ajoutant des fonctionnalités ou de télécharger des fichiers de configuration. La documentation y est aussi très présente. De plus il est compatible avec les protocoles VoIP du moment à savoir H323, MGCP, SIP et aussi IAX2 (Inter Asterisk eXchange). et possède toutes les fonctionnalités que l'on attend d'un IPBX

Le deuxième IPBX c'est **Sipx** qui est un autocommutateur IP libre pour Linux, il fournit la Plu part des fonctionnalités ou services d'un autocommutateur (PABX) classique. Il peut se connecter avec le réseau téléphonique commuté (RTC) par l'intermédiaire des passerelles de VoIP. Sipx fonctionne avec des téléphones ou passerelles utilisant le protocole SIP (Session Initiation Protocol). Ce logiciel est développé par des programmeurs de Pingtel réunis au sein de SIPFoundry.

Avec **SIPx,** Asterisk n'est plus le seul projet IPBX open source en course. SIPx est en effet le plus gros concurrent d'Asterisk.

Le dernier IPBX c'est **YATE** qui est un logiciel d'origine Roumaine dont l'acronyme signifie Yet Another Telephony Engine. Développé en C++ pour Windows, il a été porté sur les systèmes Linux.

Ce qui a eut comme conséquence que YATE ne sait fonctionner qu'avec des cartes d'interface de cette marque. YATE peut être utilisé à la fois en temps que client ou serveur. Le mode client est un softphone écrit en java. Il peut réaliser la fonction de passerelle entre le réseau public et le réseau IP ou entre un PC et un téléphone.

Le tableau 6, montre les fonctionnalités de tous les IBPX disponibles sur le marché.

	SIPx	Bayonne	Yate	Asterisk	SER
Utilisation de SIP et RTP	Oui	Oui	Oui	Oui	Oui
Compatibilité Softphone freeware	Oui	Oui	Oui	Oui	Oui
Faisabilité d'une maquette	Faisable	Faisable	Faisable	Faisable	Faisable
Documentation	Oui	Faible	Faible	Oui	Faible
Protocoles supportés	SIP	SIP H323	SIP	SIP IAX/IAX2 MGCP H323 SCCP …	SIP

Tableau 6:Les différents IPBX libres disponibles

On constate que Asterisk est le produit le plus intéressant du marché, le logiciel libre le plus répandu et qui possède une communauté extrêmement importante. Intéressant pour obtenir de l'aide et pour l'évolutivité et la pérennité du produit. Il est interopérable avec tous les systèmes, même les plus compliqués d'une entreprise.

On préconise donc l'IPBX Asterisk, qui possède de larges possibilités protocolaires SIP, MGCP, et une interface d'administration globale qui facilite sa configuration.

III. Étude des différents Softphones :

Un softphones est un logiciel que l'on utilise pour faire de la téléphonie sur Internet depuis son ordinateur, les interfaces de ces softphones sont souvent simples d'utilisation et très complètes puisque toutes les fonctionnalités qui existent sur des téléphones classiques existent aussi sur les softphones.

Pour cette étude, on compare les quartes softphones compatibles avec le serveur VoIP Asterisk.

Le premier c'est **X-lite** qui est un utilitaire gratuit de connexion à Internet via le protocole SIP (Session Initiation Protocol). Il propose une interface simple et intuitive qui permet de télécharger des fichiers multimédias : vidéo et audio. La lecture de ces derniers est possible.

L'utilisateur peut effectuer des appels vidéo (vidéo conférence) et envoyer des messages instantanés.

Le deuxième est **Sjphone** qui permet de discuter avec un interlocuteur possédant un softphone fonctionnant sur PC, PDA, téléphone supportant l'IP ou distributeur de services de téléphonie par Internet (ITSP). La connexion peut se faire par fil ou par l'intermédiaire des téléphones mobiles.

Il soutient les normes SIP et H.323 et est entièrement inter-fonctionnel avec la plupart des fournisseurs de VOIP et fournisseurs de service principaux.

Express Talk est le troisième softphone à étudier, il fait partie de la famille des softphones.

Cette catégorie désigne les programmes qui permettent de transformer un ordinateur en téléphone. Le principal avantage de cette technique est de permettre une réduction non négligeable du coût des communications.

Le programme arbore une interface à l'esthétique classique, mais efficace. Lors de nos tests, même sans utiliser de micro casque, l'interlocuteur n'a souffert d'aucun écho. Cette caractéristique est primordiale pour un programme de ce type. La qualité d'écoute quant à elle s'est montrée tout bonnement excellente.

Le dernier softphone dans notre étude et le **SipXphone** qui est la retranscription logicielle des téléphones Pingtel. Tous deux utilisent le même programme Java. La version du programme Java des sipXphone étant un peu plus récente que celle des Pingtel, il existe des petites différences dans l'affichage des menus et la présentation des touches du téléphone. L'installation et la configuration de sipXphone est donc quasiment identique à celle des Pingtel.

Le tableau 3, résume et compare toutes fonctionnalités de ces softphones.

	X-lite	Sjphone	Express Talk	SipXphone
Plate forme	Windows Linux MAC OS X	Windows Linux MAC OS X Pocket PC	Windows MAC OS X	Windows CentOS Linux
Interface graphique	Simple	Très complète	Elégante et simple	Compliqué
Nombre de lignes supportées	2	3	4	Conférence possible
Protocoles utilisés	SIP	SIP H .323	SIP	SIP
Messagerie	Oui	Non	Non	Oui

Tableau 7:Comparaison des différents softphones

Après cette comparaison des softphones Open source disponibles sur Internet, j'ai trouvé que X-lite était le plus économique et le plus simple de configuration et d'utilisation.

IV. Etude sur les Hardphones :

L'implémentation d'un système téléphonique IP dans une entreprise nécessite l'utilisation de téléphones très spécifiques: Le Téléphone IP. Ils sont raccordés à une prise murale du réseau informatique et alimentés par une source de courant ou bien alimentés directement par la prise murale

en utilisant des switch POE. La plupart des téléphones IP sont compatibles avec Asterisk (Cisco, Linksys, Aastra,Alcatel).

J'ai choisit de ne pas procéder à une comparaison des différents hardphones, vu que Hight tech-service adopte déjà le matériel Cisco, les hardphones ayant la marque Cisco Spa 942 .

Figure 15: le hard phone Cisco Spa 942

Les touches de raccourcis se trouvent au niveau du téléphone, 4 boutons aux côtés du voyant appelé Softkey permettant de gérer simplement ce téléphone.

• 4 Boutons multi-fonctionnel sur le coté de l'écran

• Codecs: G711a, G711μ, G726, G729a, G723.1.

• Configuration: HTTP, TFTP, Menu de configuration.

• Switch Intégré: Oui.

• Alimentation: PoE ou Externe.

• Multiligne: Oui .

Si on souhaite utiliser un téléphone analogique, il faut utiliser un adaptateur ATA

Figure 16:le Grand Stream Adaptateur SIP ATA-286

L'adaptateur permet de transformer un téléphone analogique en téléphone SIP. Il est pourvu d'une prise RJ11 à raccorder au téléphone analogique et d'une prise RJ45 à raccorder au réseau TCP/IP.

Avec cet adaptateur, Il est possible d'appeler un téléphone classique depuis un téléphone IP et appeler un téléphone IP depuis un téléphone classique.

V. Étude du schéma de câblage :

On peut choisir 2 types de câblage soit avec un Switch PoE ou avec un Switch non POE.

Il serait recommandé dans notre cas d'utiliser un switch PoE qui permet d'alimenter les appareils qui y sont reliés à l'autre bout de courant électrique. Cette technique est très intéressante, car en fait c'est la prise réseau qui alimente les téléphones IP. Le seul inconvénient est qu'il coûte plus cher qu'un Switch non POE. La figure 11 montre la solution de câblage adoptée.

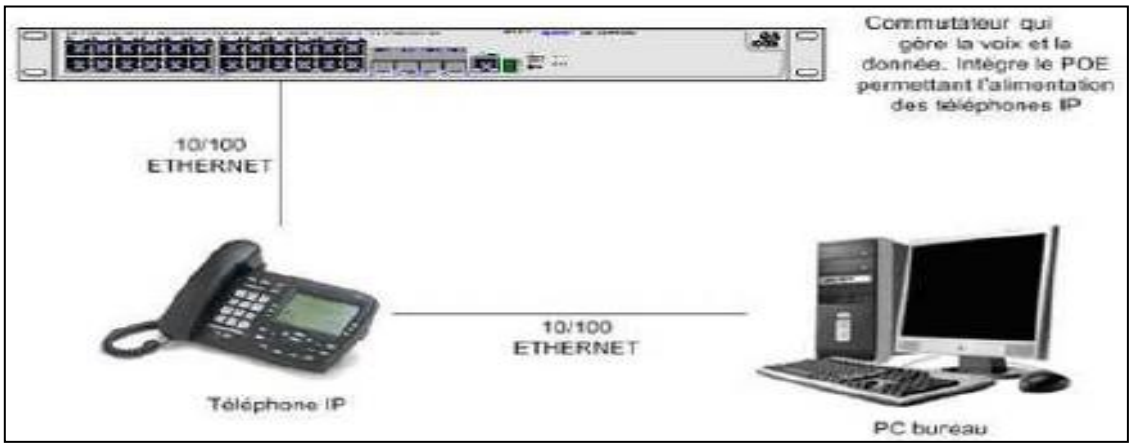


Figure 17:Solution de câblage adoptée

Ainsi, la maquette qu'on propose de mettre en oeuvre doit permettre, la communication entre les clients SIP (Softphone) et /ou (Hardphone) via un IPBX Asterisk sous Linux.

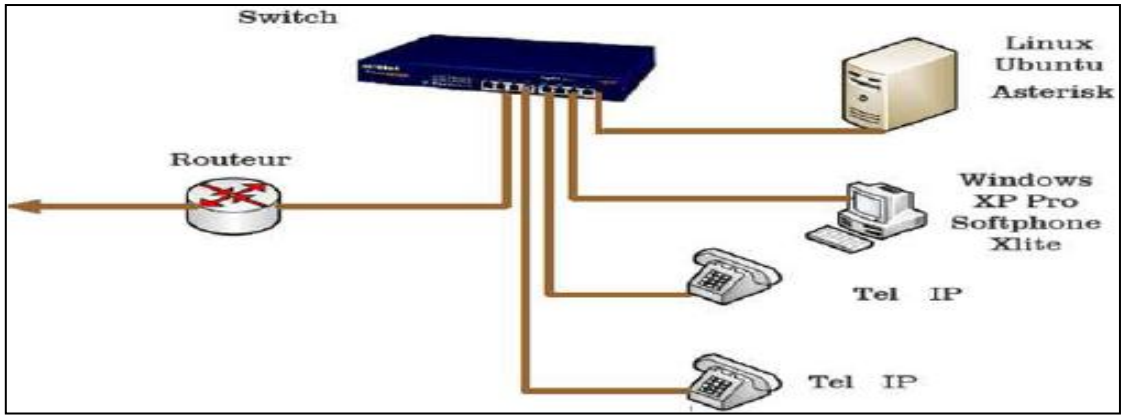


Figure 18:La maquette proposée

VI. Conclusion :

Ce chapitre nous a permis de choisir Asterisk Elastix comme l'IPBX Open source le plus intéressant du marché, le plus adapté et le softphone X-lite de Xten dans sa version gratuite qui s'appuie sur le protocole SIP géré le serveur Elastix IPBX.

Asterisk possède des fonctionnalités puissantes lui permettant de s'imposer dans l'avenir.

CHAPITRE 4 : MISE EN PLACE TECHNIQUE DE LA SOLUTION

I. Introduction :

Dans ce chapitre, je ‘arrêtée sur les techniques, mécanismes et configurations à mettre en place dans le but de démarrer le serveur VoIP, puis présenter des scénarios d’attaques réalisées contre la solution déployée, (dans le but de montrer la vulnérabilité de la solution) ensuite montrer les solutions implémentées pour sécuriser notre infrastructure.

II. Présentation de server Elastix :

Elastix est une solution logicielle qui intègre les meilleurs outils disponibles pour les PABX basés sur Asterisk dans une interface simple et facile à utiliser. Elle ajoute aussi ses propres paquets d'utilitaires et devenir la meilleure solution logicielle disponible pour la téléphonie Open Source. Les avantages d'Elastix sont la fiabilité, la modularité et la facilité d'utilisation. Ces caractéristiques ajoutées au fort pouvoir de rapports font de lui le meilleur choix pour implémenter un PABX basé sur Asterisk. Les fonctions fournies par Elastix sont nombreuses et variées. Elastix intègre plusieurs suites logicielles, chacune incluant ses propres ensembles de grandes fonctions.

1. L’installation d’Elastix :

Insérez le CD d'installation Elastix au démarrage de la machine. Après le démarrage, l'écran suivant apparaitra :

Figure 19:Installation Elastix au démarrage de la machine

Procéder à la sélection du type de clavier correspondant à votre langue.

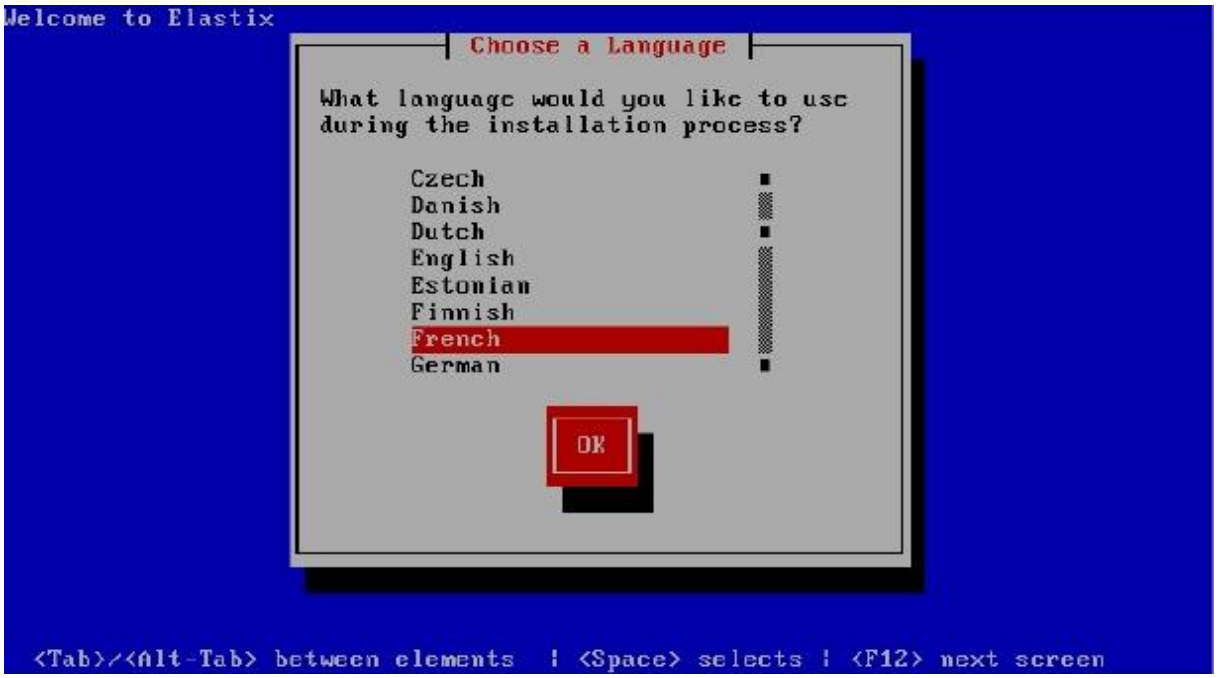


Figure 20:Sélection le type de clavier

Entrez le mot de passe qui sera utilisé par l'administrateur Elastix. Ayez à l'esprit que c'est une partie critique de la sécurité du système.

Figure 21:Authentification système avec mot de passe

Note: Les écrans suivants fourniront des détails de l'installation automatique du CD. Premièrement, une vérification des dépendances nécessaires pour l'installation est requise :

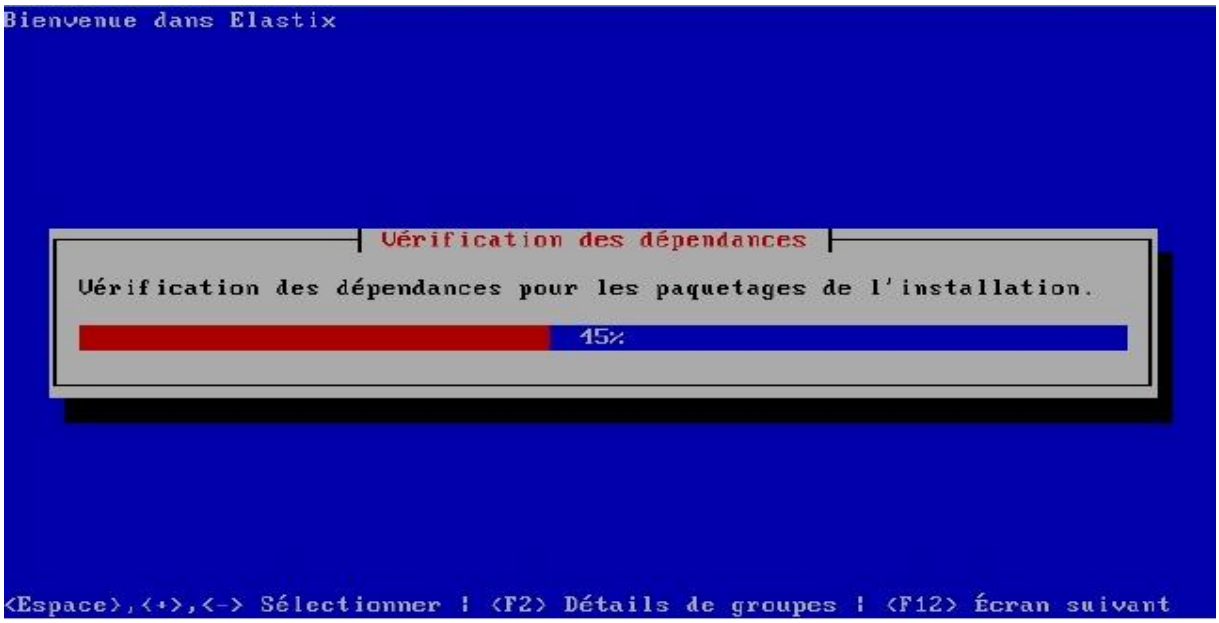


Figure 22:Vérification des dépendances

Ensuite, l'installation continuera et vous verrez quelque chose comme ceci au démarrage :

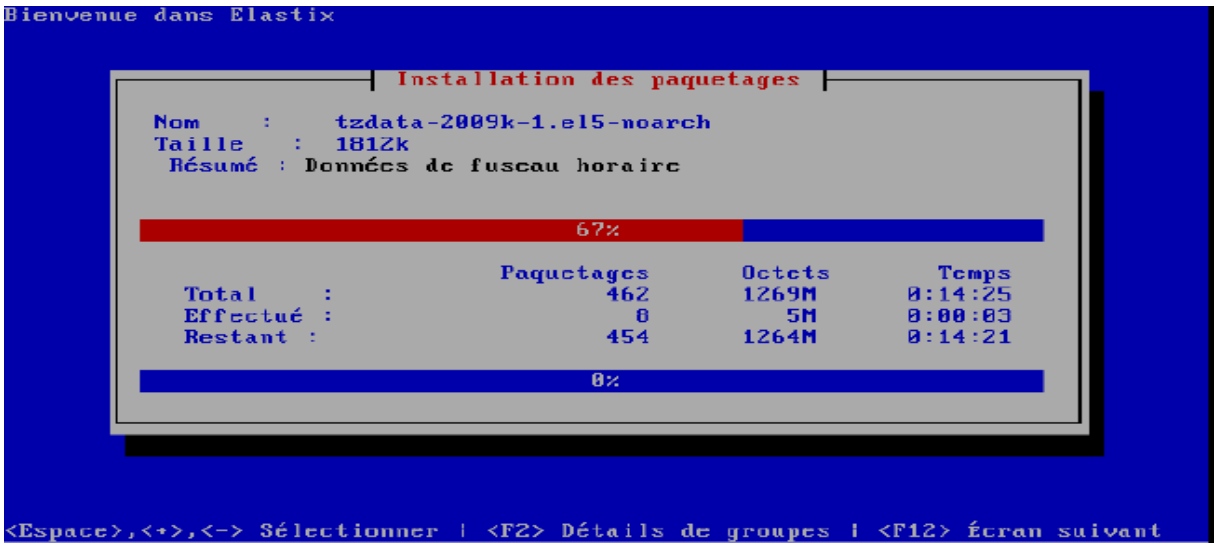


Figure 23:Installation des paquetages

Après que l'installation soit terminé, Identifiez vous en tant qu'utilisateur root et entrez le mot de passe spécifié au début de l'installation.

Login : root

Password : **********

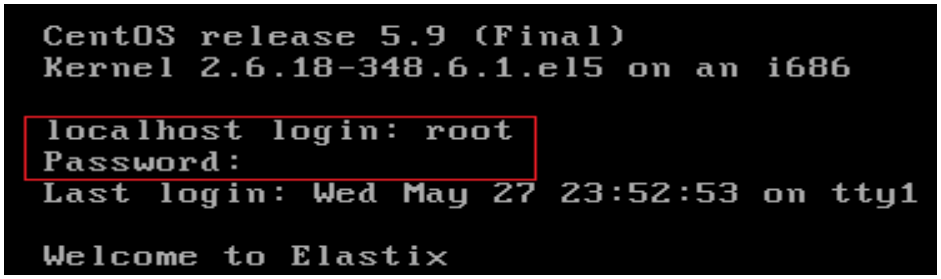


Figure 24:Server authentifiée par « login et password »

Ici on doit spécifier les paramètres réseau sur lequel notre serveur va fonctionner. On modifie le fichier **ifcfg-eth0** avec la commande.

 # vi /etc/sysconfig/network-scripts/ifcfg-eth0

Le fichier doit contenir ceci:

DEVICE=eth0

BOOTPROTO=static

TYPE=Ethernet

IPADDR=192.168.137.128

NETMASK=255.255.255.0

BROADCAST= 192.168.137.255

NETWORK= 127.0.0.1

NOZEROCONF=yes

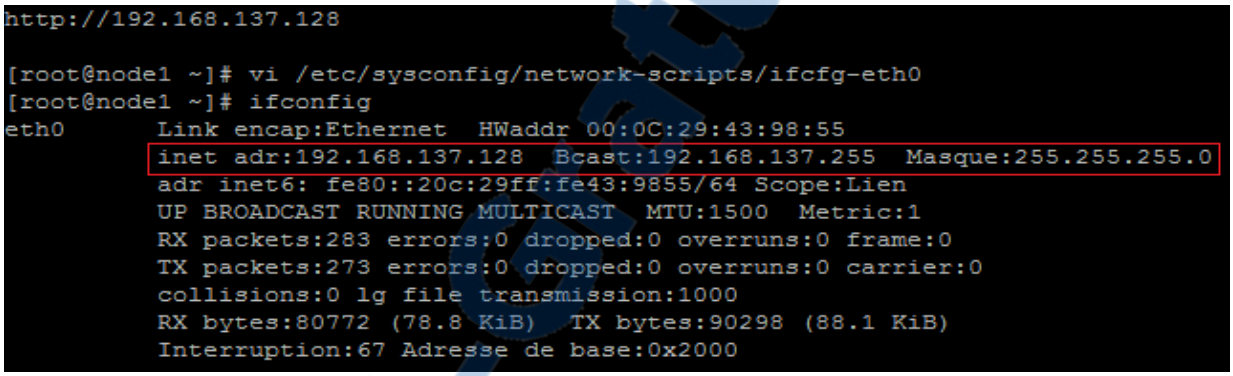


Figure 25:les paramètres réseau sur lequel notre serveur va fonctionner

2. Accès au serveur :

Maintenant le serveur est prés d'être accessible à partir de n'import quel point dans le réseau via une adresse IP qu'on l'a attribué et un navigateur.

Figure 26:Adresse Réseaux de server Elastix

Login et mot de passe par défaut :

Login: admin

Mot de passe: palosanto

Figure 27:Login et mot de passe de notre server Elastix

3. Tableau de bord d'interface Elastix :

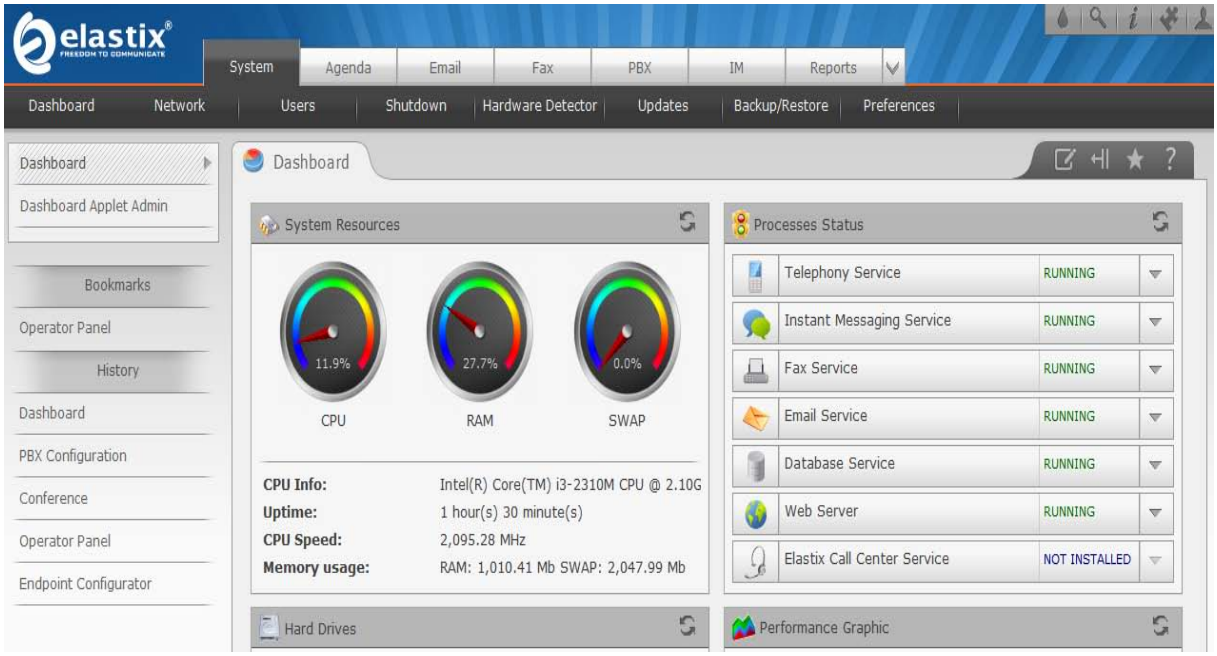


Figure 28:Interface Elastix

4. Configuration Elastix PBX :

Création d'une nouvelle extension

Cet espace est pour les combinés, logiciels de téléphonie, pagers, ou n'importe quoi d'autre qui peut être considéré comme 'extension' dans le contexte classique PABX. Définir et éditer des extensions est probablement la tâche la plus commune effectuée par un administrateur de PABX, et de surcroit, vous allez trouver que vous deviendrez très familier avec cette page. Il y a 4 types de dispositifs supportés - SIP, IAX2, ZAP et 'Personnalisé.

Pour créer une "Nouvelle Extension", allez au menu "PBX" qui par défaut, arrive à la section "Configuration PABX"; dans cette section, choisissez l'option "Extensions" sur le panneau gauche. Maintenant vous pouvez créer une nouvelle extension.

Figure 29: Ajouter Extension

Tout d'abord, choisissez le dispositif parmi les options disponibles:

•Generic SIP Device : SIP est le protocole standard pour les combinés VoIP et ATA.

•Generic IAX2 Device : IAX est le 'Protocole Inter Asterisk', un nouveau protocole supporté par seulement quelques périphériques (eg, téléphones basés PA1688, et les IAX et ATA).

•Generic ZAP Device : ZAP est un périphérique matériel connecté à votre machine Asterisk (Eg, carte TDM400, TE110P).

•Other (Custom) Device : Personnalisé est un 'fourre-tout' pour n'importe quel périphérique non standard (eg H323). Il peut aussi être utilisé pour "mapper" une extension vers un numéro "externe". Par exemple, pour router l'extension 211 vers 1-800-555-1212, vous pourriez créer une extension personnalisée 8000 et dans la boite de texte "dial" vous pourriez entrer Local/18005551212@outbound-allroutes.

Une fois que le périphérique correct à été choisi, cliquez sur “Submit”.

Note: Maintenant vous devez procéder au renseignement des champs nécessaires (obligatoire) pour créer une nouvelle extension. Continuez à entrer les informations correspondantes :

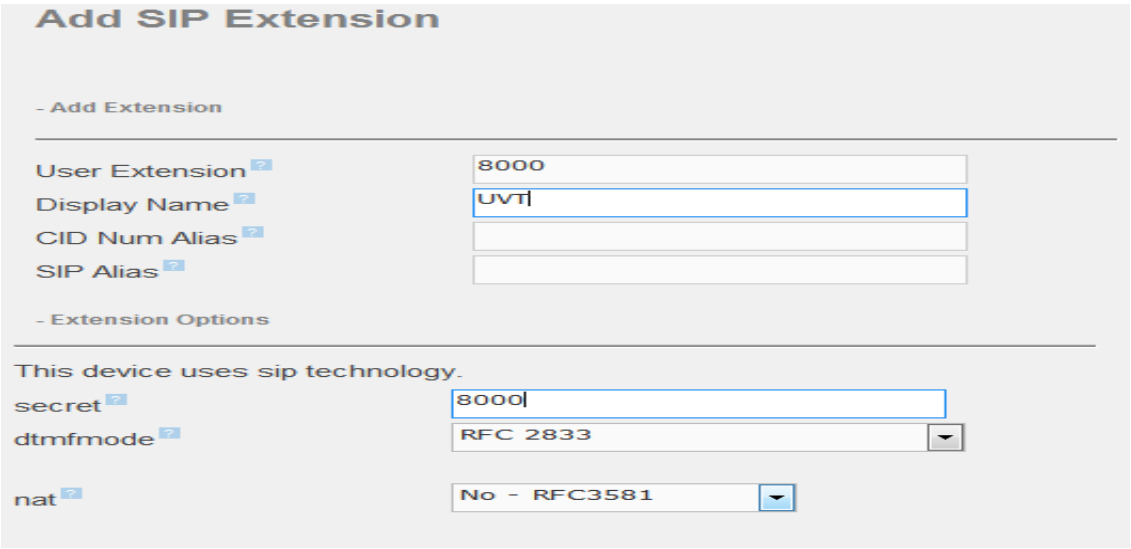


Figure 30:Extension ajouter

•User Extension : Elle doit être unique. C'est le numéro qui peut être appelé de n'importe qu'elle autre extension, ou directement du réceptionniste numérique s'il est activé. Elle peut être de n'importe qu'elle longueur, mais conventionnellement, un numéro de 3 ou 4 chiffres est utilisé.

•Display Name : Le nom d'identification de l'appelant pour les appels de cet utilisateur affichera ce nom. Entrez seulement le nom, pas le numéro.

•Secret : C'est le mot de passe utilisé par le périphérique téléphonique pour s'authentifier sur le serveur Asterisk. Il est habituellement configuré par l'administrateur avant de donner le téléphone à l'utilisateur, et il n'est pas nécessaire qu'il soit connu par l'utilisateur. Si l'utilisateur utilise un logiciel de téléphonie, alors il aura besoin de ce mot de passe pour configurer son logiciel

5. Configuration de logiciel de téléphonie :

En configurant un logiciel de téléphonie, notre but est d'avoir un PC connecté qui autorise les mêmes fonctions qu'un téléphone traditionnel. Pour ceci, vous aurez besoin d'installer un logiciel qui convertit votre PC en téléphone. Toute fois, un micro et un casque sont nécessaires. Il y a beaucoup de logiciels de téléphonie, et parmi eux, il y a les suivants.

***XtenLite**: Ce logiciel fonctionne uniquement avec des extensions SIP, il est également compatible multi-plateforme, et vous pouvez le télécharger ici :http://www.xten.com/index.php?menu=download.

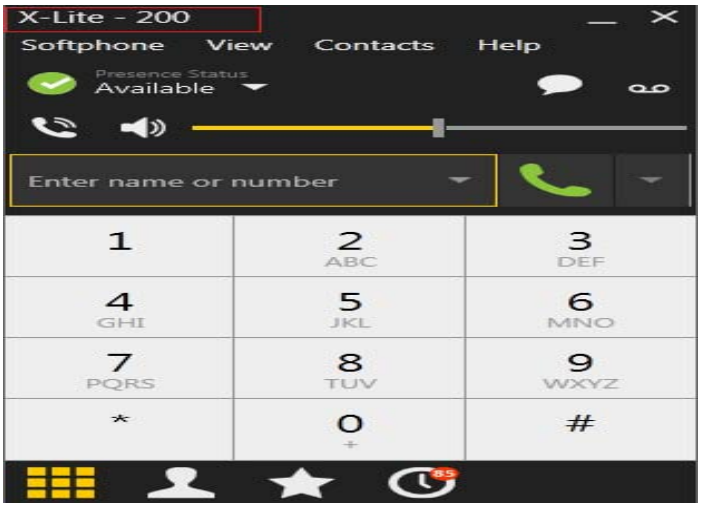


Figure 31:Démarrage de X-lite

Pour ajouter le compte, il faut cliquer sur **Softphone** puis **Account Setting**, il faut ensuite remplir ces champs:

Display Name : « Votre Nom » dans notre cas c'est 200

User name : Votre N° de téléphone Elaxtix dans notre cas c'est 200

Password : Le mot de passe que vous avez défini.

Domain : l'adresse IP de notre serveur Elastix .

Et finalement on coche « Register with domain and receive incoming calls ».Voila notre poste client est prêt.

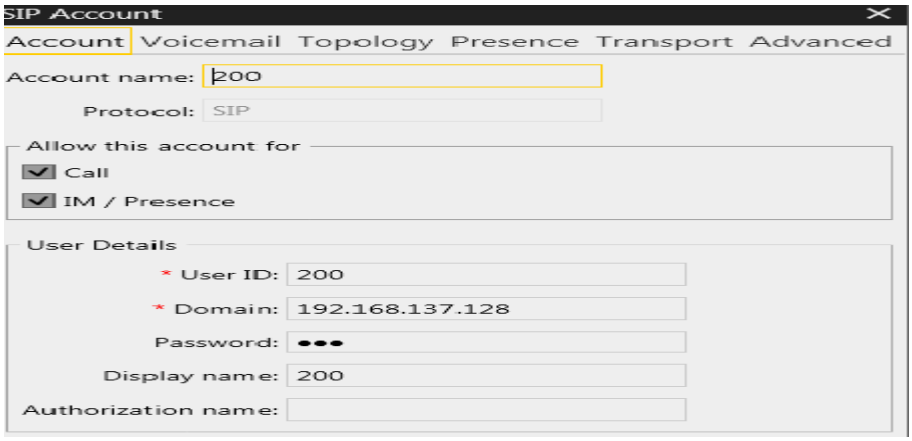


Figure 32:Configuration du compte SIP "200"

IDEFISK: Ce logiciel fonctionne avec des extensions SIP et IAX, et il est compatible multi-plateforme. Vous pouvez le télécharger ici :http://www.asteriskguru.com/idefisk/ .
Une fois que vous avez téléchargé et installé IDEFISK, procédez à sa configuration.
Pour ceci, cliquez sur l'icone qui ressemble à un outil et créez une extension SIP. Dans cet exemple, l'extension 100 est configurée et il est supposé que l'adresse IP assignée au système est 192.168.137.128

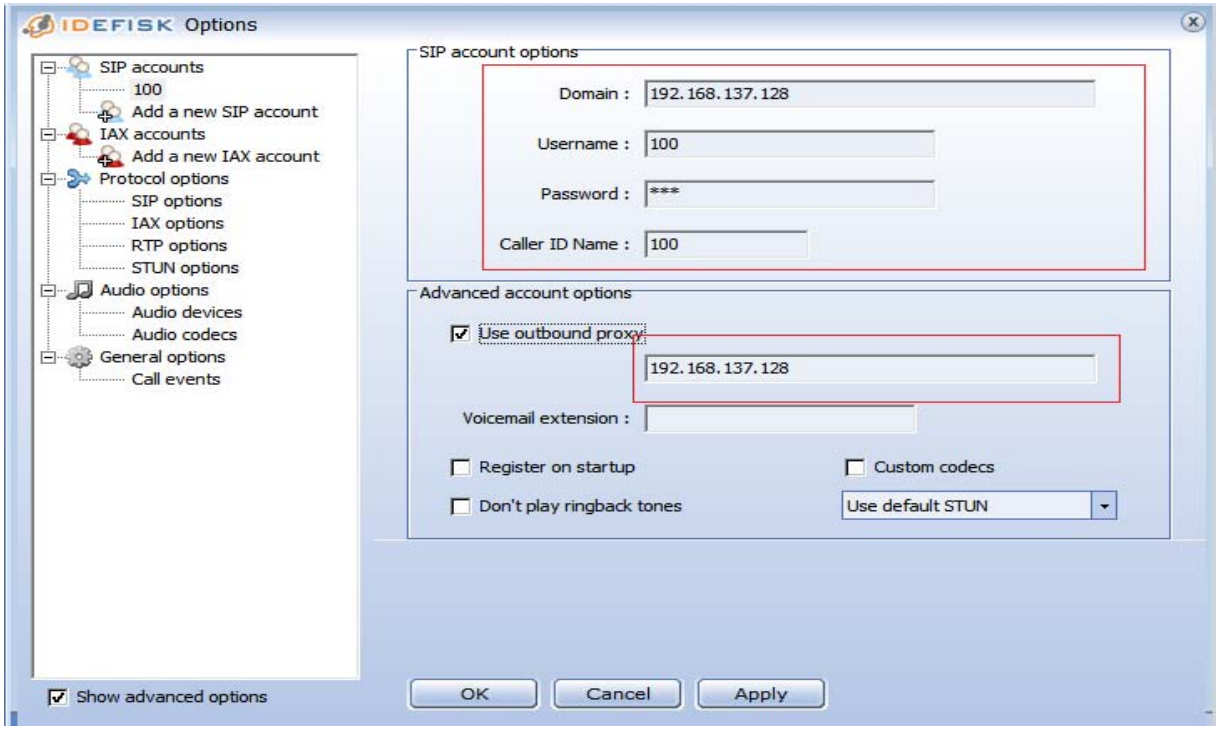


Figure 33:Configuration du compte SIP "100"

Ensuite, on sélectionner “Audio Codecs” et sélectionnez tous les codecs disponibles. Vous appliquez les changements et cliquez sur le bouton “Register”, donc le téléphone s'enregistre dans le système.

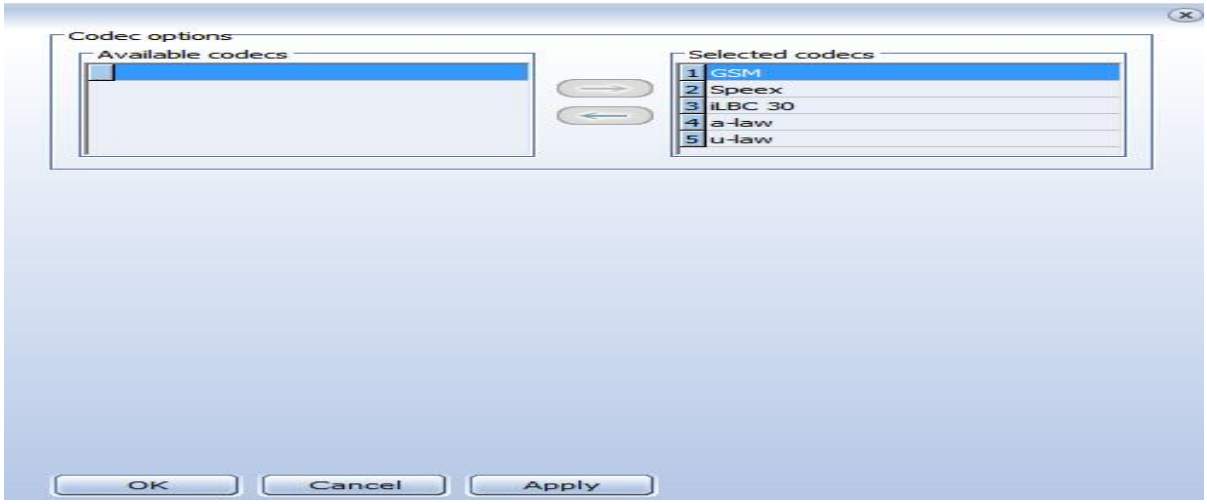


Figure 34:Sélections les Codecs

Finalement, vous pouvez passer un appel d'une extension à une autre.

III. Vérification et Test de communication VoIP :

L'étape finale, consiste à tester la plate-forme principale d'Elastix, on peut vérifier l'état des équipements SIP en ouvrant notre navigateur avec le chemin suivant: http://192.168.137.128 /main .En haut de la page à droite on peut lire « Operator Panel », on visualise le nombre des comptes SIP actifs.

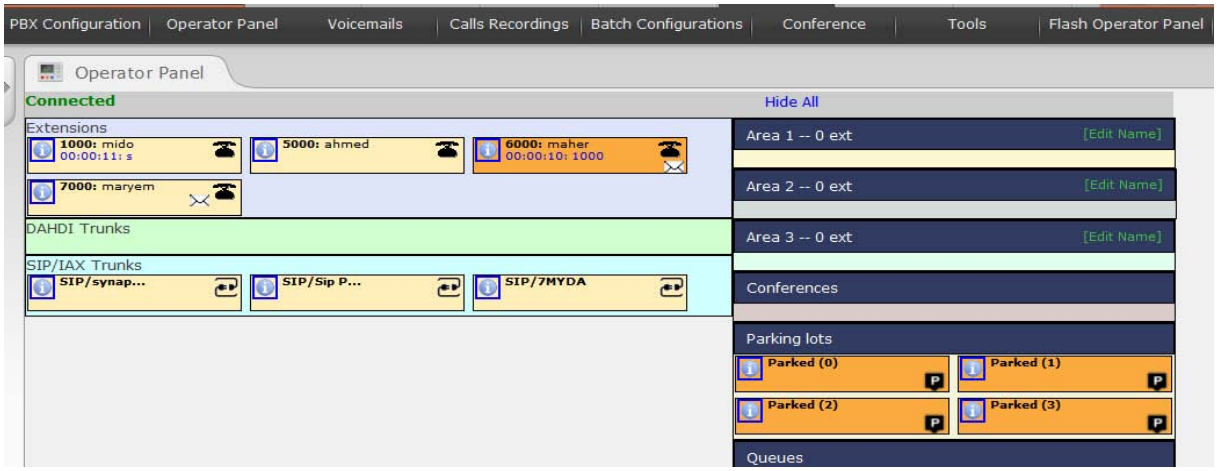


Figure 35:vérification SIP actifs

Maintenant on a une interface pour appeler par Asterisk, on choisit le profil à appeler, on aura une sonnerie et un message vocal.le client SIP 100 a pu établir un appel vers le client SIP 200.

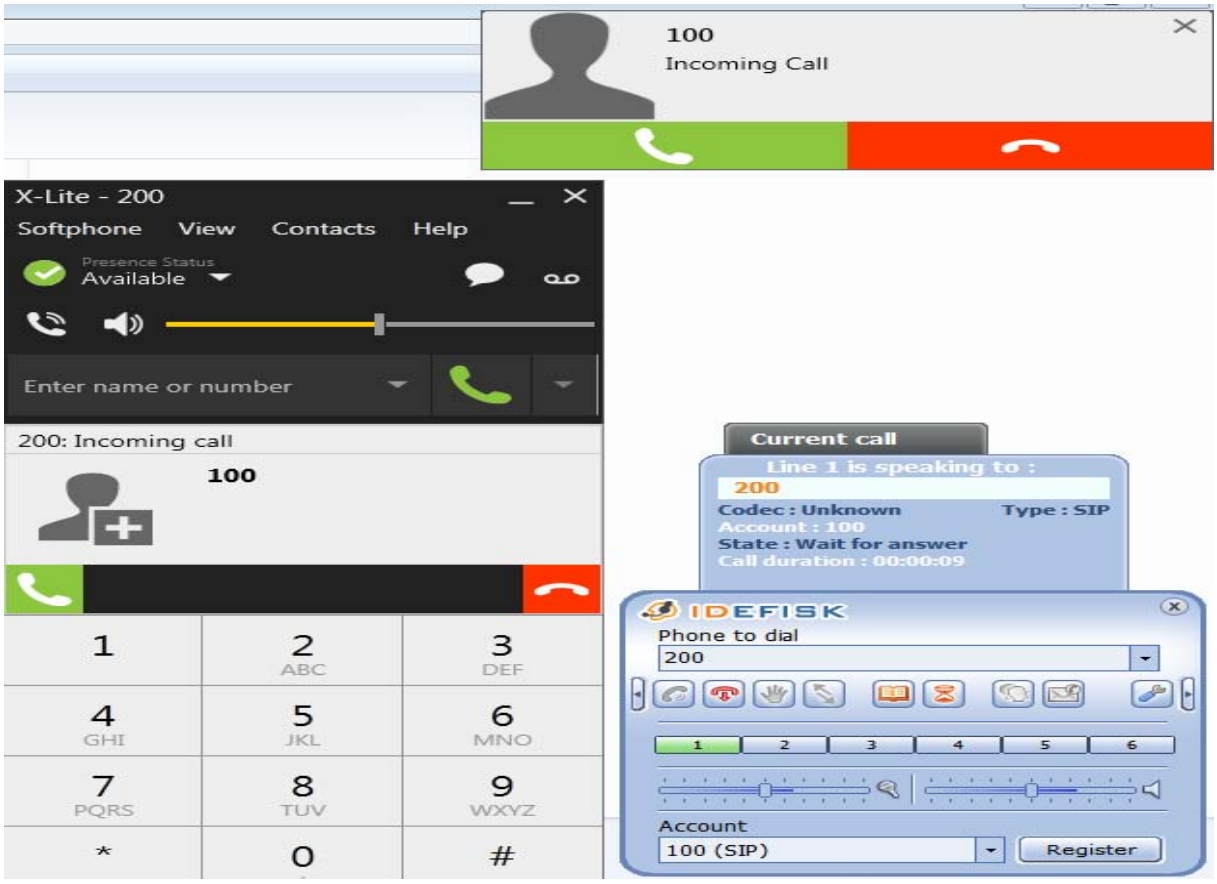


Figure 36:Test de Communication entre les clients X-lite

IV. Scénarios d'attaques contre la VoIP :

1. Collecte d'informations :

Des statistiques montrent qu'une attaque à l'aveugle sur un système distant est dans 99% des cas totalement inefficace. Il est absolument nécessaire d'entamer une collecte d'informations sur le système visé, dans le but d'élargir ses possibilités d'attaques et de s'offrir ainsi plus de flexibilité sur le choix des méthodes d'attaque, la stratégie est aussi importante que la manœuvre elle-même.

Le rassemblement des masses de données sur un seul et même réseau permet à n'importe qui d'avoir accès à n'importe quel savoir, il existe de nombreux moyens de se renseigner sur la cible en fonction du type de cible dont il s'agit ainsi que des informations que nous désirons récupérer.

2. Utilisation des moteurs de recherches :

Un des grands avantages des moteurs de recherches Internet est leurs énormes potentiels pour découvrir les plus obscurs des détails sur l'Internet.

L'un des plus grands risques pour la sécurité est aujourd'hui l'énorme potentiel des moteurs de recherche pour découvrir les détails sur l'Internet, il existe une variété de façons qu'un hacker peut exploiter en utilisant simplement les fonctionnalités avancées d'un service tel que Google.

Le ciblage des catégories suivant les résultats de recherche peuvent souvent fournir de riches détails sur la solution VoIP déployée par un organisme:

- Vendeur de produit VoIP, les communiqués de presse et des études de cas
- CV de l'administrateur ou liste de références des vendeurs
- Les forums

3. Utilisation des serveurs Whois :

«Whois» [17] (littéralement «Qui est ?») est un outil permettant d'interroger des bases d'informations (appelées registres) concernant les noms de domaines et adresses IP.

Les données contenues dans ces bases ne comportent aucune forme de garantie mais permettent généralement de retrouver le propriétaire d'un domaine ou d'une machine, notamment en cas de litige.

Le service Whois a ainsi deux principaux objectifs :

- Obtenir des informations sur le propriétaire d'un nom de domaine (contact administratif, technique et éventuellement de facturation) et sur les serveurs de noms associés au domaine.
- Obtenir des informations sur l'attribution des plages d'adresses IP.

4. Analyse de paquets avec Wireshark :

Wireshark [18] est l'analyseur réseau le plus populaire du monde, cet outil extrêmement puissant fournit des informations sur des protocoles réseaux et applicatifs à partir de données capturées sur un réseau,

comme un grand nombre de programmes, Wireshark utilise la librairie réseau pcap pour capturer les paquets. La force de Wireshark vient de:

- Sa facilité d'installation.
- Sa simplicité d'utilisation de son interface graphique.
- Son très grand nombre de fonctionnalités.

Wireshark analyse l'appel entre le client **sip 100** ayant et le client **sip 200**.De plus wireshark donne des informations précises sur les méthodes utilisées, les protocoles, l'expéditeur, le destinataire et même le softphone utilisé.

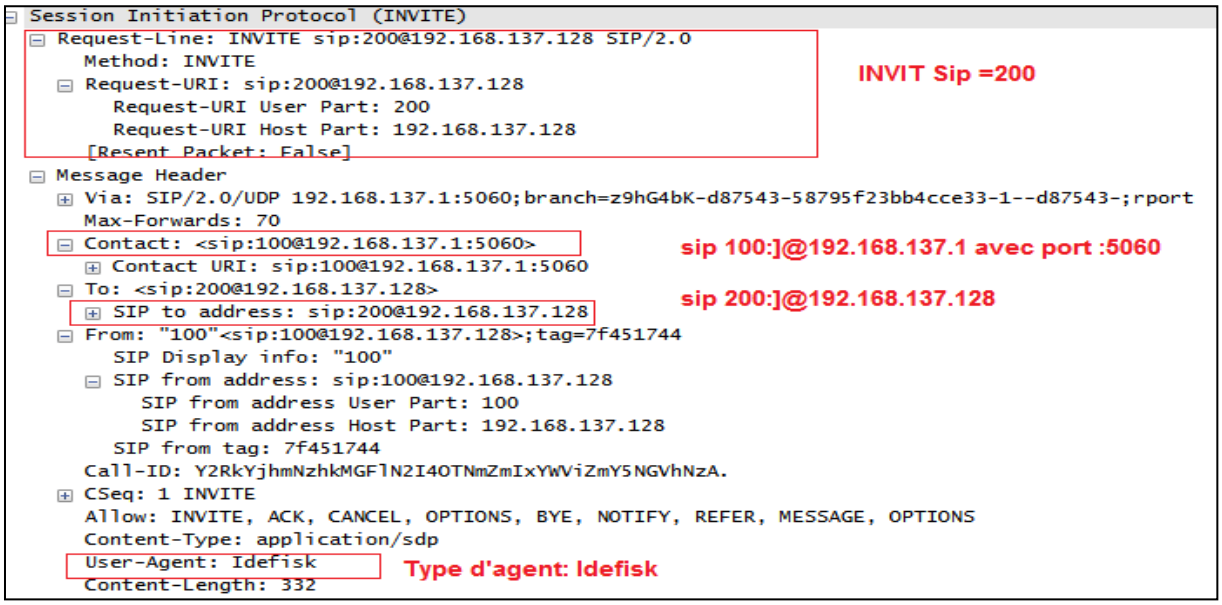


Figure 37:Exemple de paquet qui contient une requête INVITE

La figure 37 montre les paquets RTP interceptés par Wireshark, elle montre un résultat intéressant puisqu'il nous indique que nous sommes bien en RTP, que nous utilisons le codec G711, et même le champ SSRC qui correspond à l'identifiant de la conversation. Figure 38.

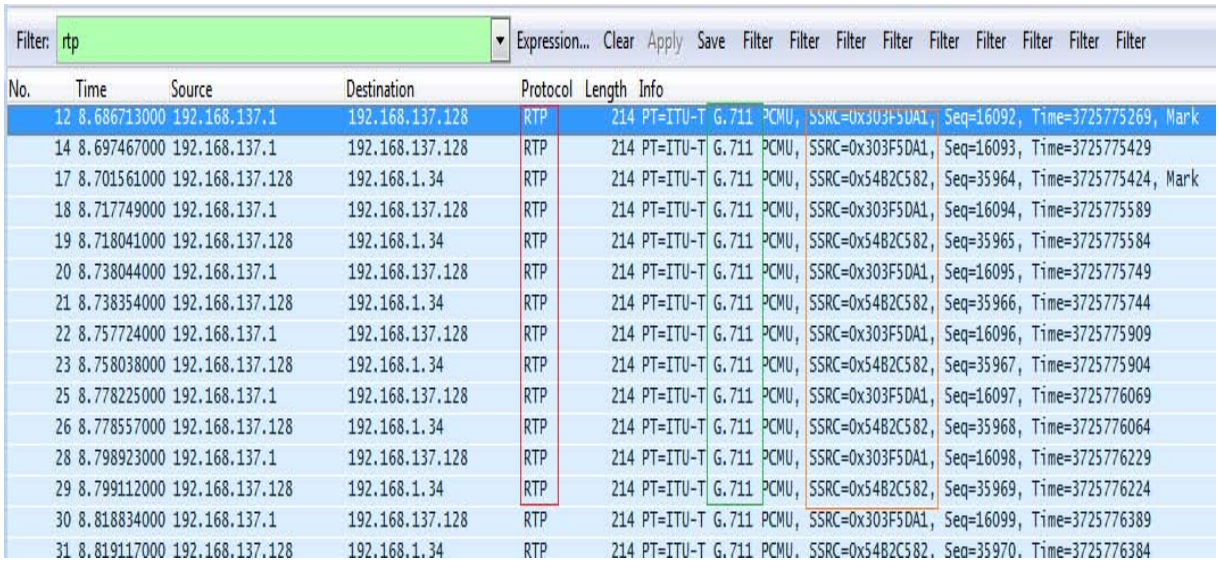


Figure 38:Les paquets RTP interceptés par Wireshark

5. Utilisation de Nmap :

Nmap[19] est un scanner de ports libre créé par Fyodor et distribué par Insecure.org. Il est conçu pour détecter les ports ouverts, identifier les services hébergés et obtenir des informations sur le système d'exploitation d'un ordinateur distant. Ce logiciel est devenu une référence pour les administrateurs réseaux car l'audit des résultats de Nmap fournit des indications sur la sécurité d'un réseau.

La collecte d'informations de notre système à attaquer peut se réaliser à l'aide de l'outil Nmap Cet outil permet de se renseigner sur les ports ouverts d'un système distant afin de savoir le type d'attaque qu'il est possible de lancer. Un scan intense nous permet de détecter tous les ports ouverts sur le réseau.

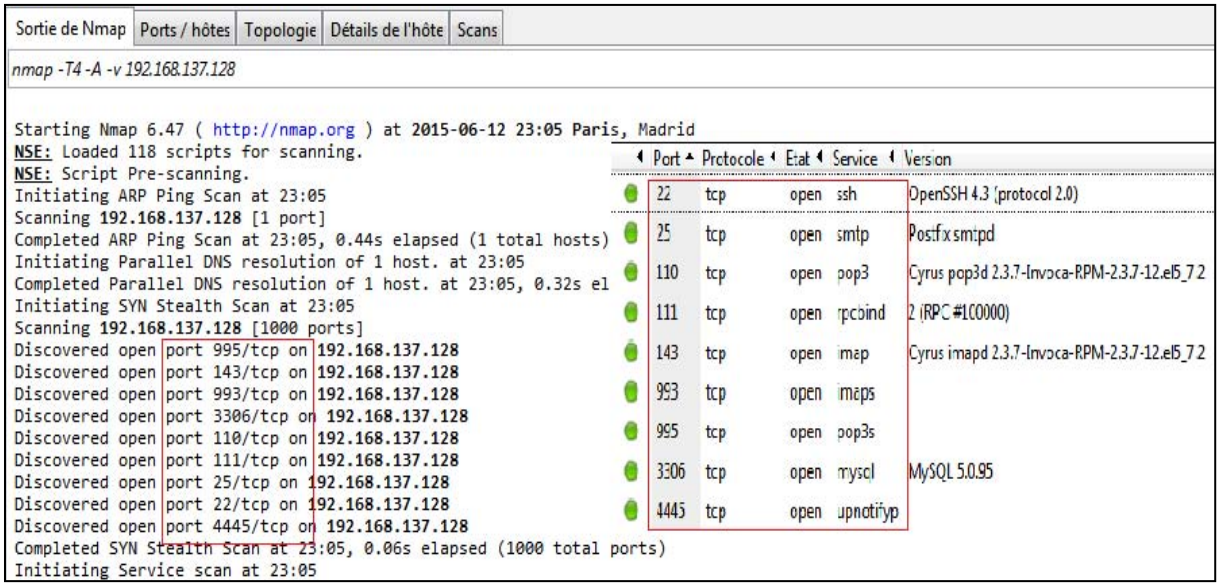


Figure 39:Scan intense de port via Nmap

On peut même scanner toute la plage d'adresses par exemple : 192.168.137.1– 255

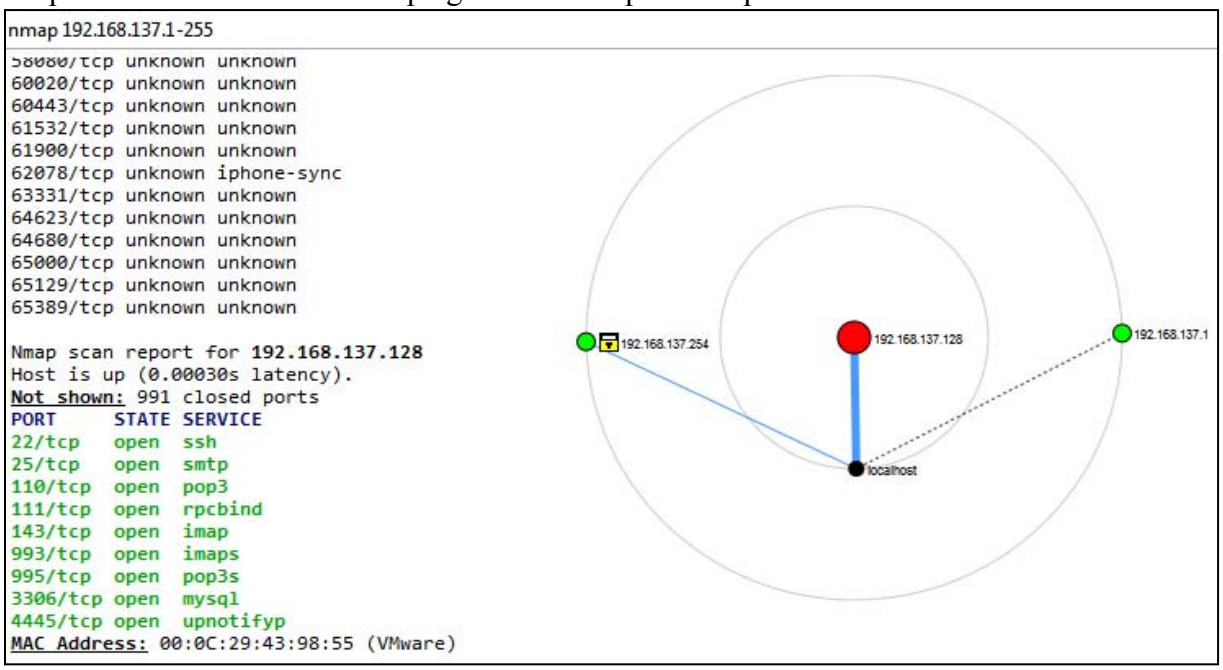


Figure 40:Scan d'une plage d'adresses avec Nmap

Nmap nous permet également de déterminer la version du système d'exploitation de la machine , si Nmap n'arrive pas à déterminer la version , on pourra lui demander de nous donner une liste des systèmes qui pourraient potentiellement correspondre :

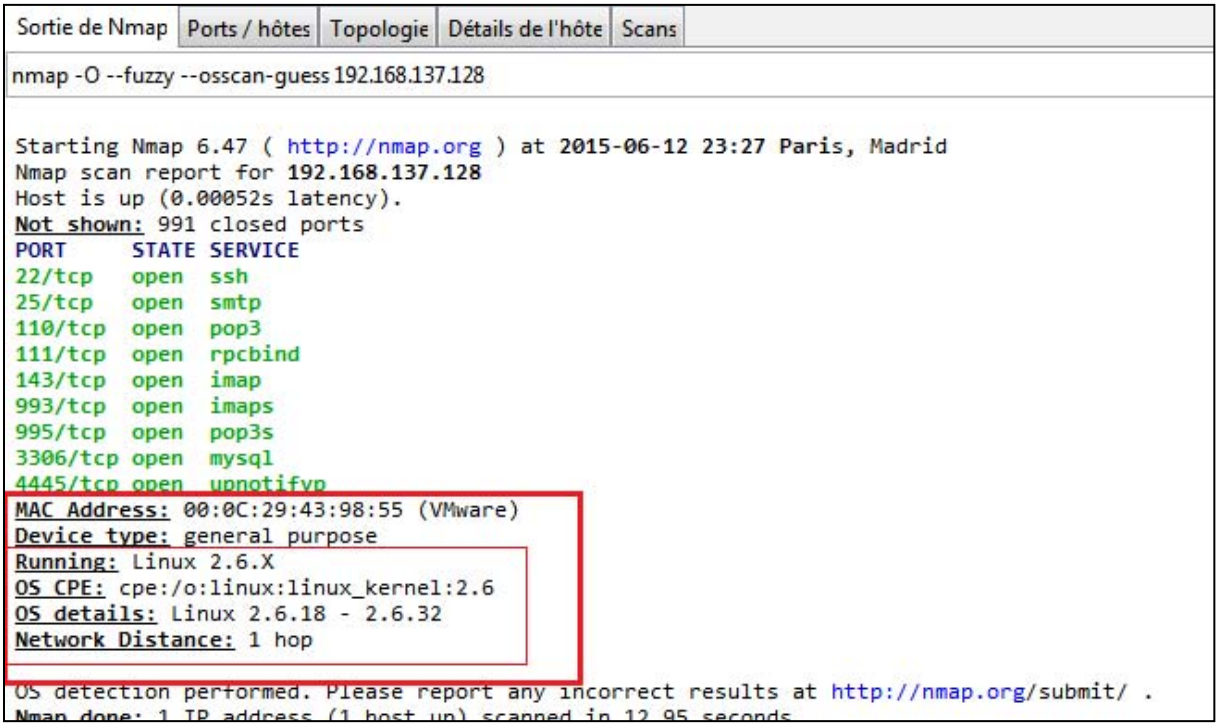


Figure 41:Scan de l'OS avec Nmap

Nmap est l'outil de référence pour scanner les ports ouverts d'une machine, je tiens à préciser que l'utilisation de Nmap peut réveiller un pare-feu, et avertir un utilisateur que sa machine a été victime d'un scan de port, il faut donc l'utiliser avec discrétion.

6. Espionnage des communications VIOP avec Wireshark :

L'écoute clandestine peut être effectuée avec plusieurs méthodes, la méthode la plus courante est l'écoute du réseau pour reconstituer ensuite la communication à partir de paquets RTP. Cette attaque a pour but d'écouter ou d'enregistrer une conversation en cours, l'attaquant gagne l'accès au réseau physique et utilise des outils pour espionner directement sur les câbles.

Wireshark est installé sur une troisième machine qui n'est pas autorisé à passer des appels à travers le serveur ELASTIK IPBX, il va sniffer tous le trafic circulant dans notre réseau local.

- **Ettercap :** Effectuer l'ARP Poisonnig, intercepter le trafic échangé sur le réseau, et réaliser les attaques MITM (Man In The Middle).

- **BackTrack** : Est une distribution basée sur Debian GNU / Linux distribution destinée au forensics et à l'utilisation des tests de pénétration. La version actuelle est BackTrack 5 R3. Elle est basée sur Ubuntu 10.04 (Lucid) LTS et appartient à la famille Debian.

1 ère étape : Lancement d'Ettercap afin d'effectuer l'ARP poisoning

On le lance en mode graphique grâce à la commande " Ettercap -G " et on choisit « Unified Sniffing »

Figure 42:Lancement Ettercap « Unified Sniffing »

2 éme étape : Scan du réseau et ajouts d'hôtes:

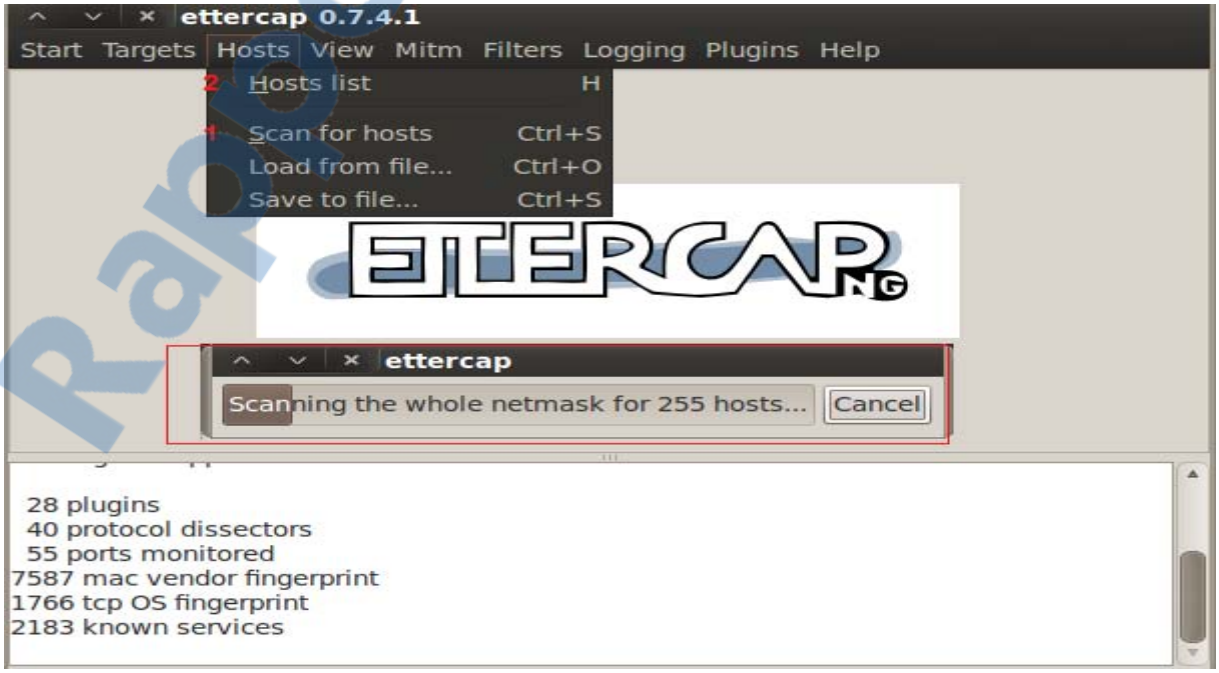


Figure 43:Scan le réseau et ajouts d'hôtes

Cette étape nous permet de visualiser les machines connectées sur ce réseau.

Le résultat de cette étape :

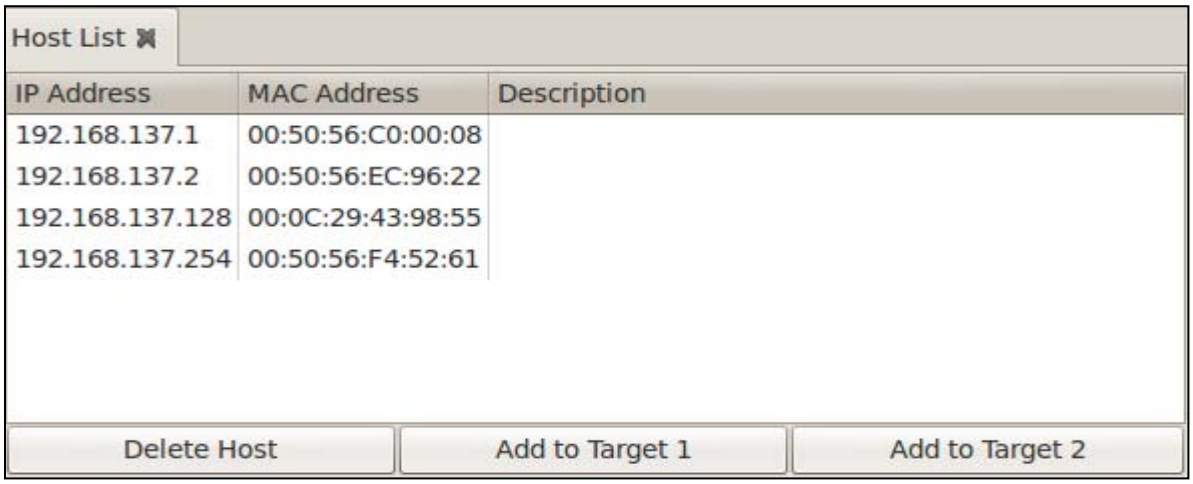


Figure 44:Résultat de Scan

3 éme étape : Choisir le type de l'attaque

Attaque man in the middle (« homme au milieu ») : Une des attaques man in the middle les plus célèbres consiste à exploiter une faiblesse du protocole ARP (Adresse Résolution Protocol) dont l'objectif est de permettre de retrouver .l'adresse IP d'une machine connaissant l'adresse physique (adresse MAC) de sa carte réseau. L'objectif de l'attaque consiste à s'interposer entre deux machines du réseau et de transmettre à chacune un paquet ARP falsifié indiquant que l'adresse ARP (adresse MAC) de l'autre machine a changé, l'adresse ARP fournie étant celle de l'attaquant. Les deux machines cibles vont ainsi mettre à jour leur table dynamique appelée Cache ARP. On parle ainsi de « ARP cache poisoning » (parfois « ARP spoofing » ou « ARP redirect ») pour désigner ce type d'attaque. De cette manière, à chaque fois qu'une des deux machines souhaitera communiquer avec la machine distante, les paquets

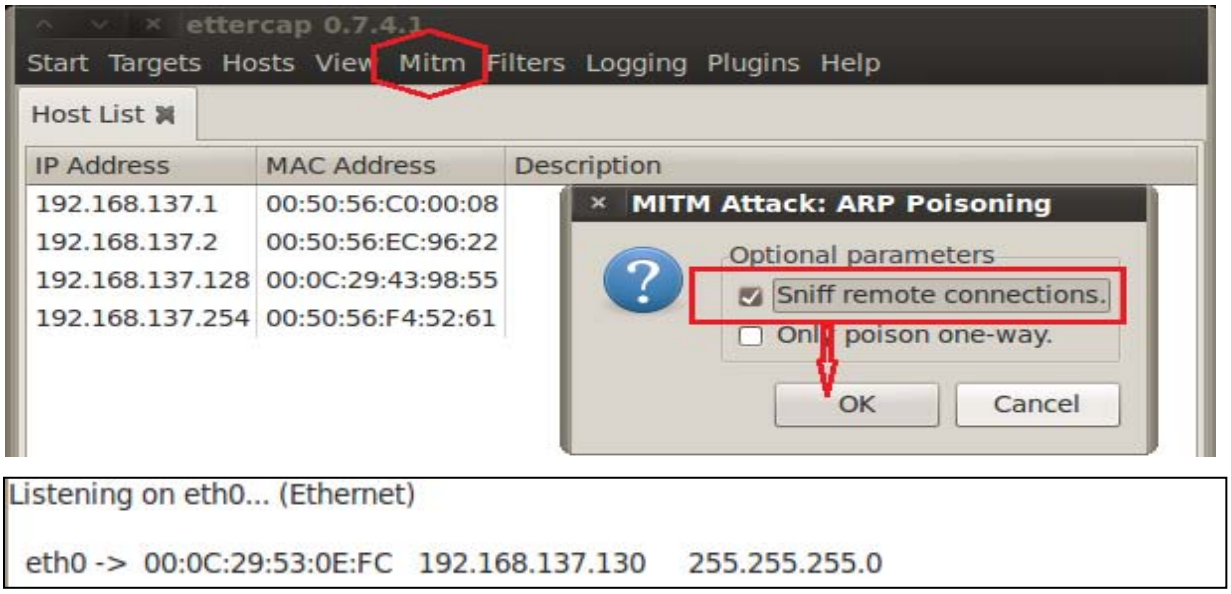


Figure 45:L'attaque Mitm ARP poisoning

L'attaquant émet une trame ARP en Broadcast (à tout le réseau) dans laquelle il fait correspondre son adresse MAC à l'adresse IP de la passerelle.

4 éme étape : Début du Sniffing

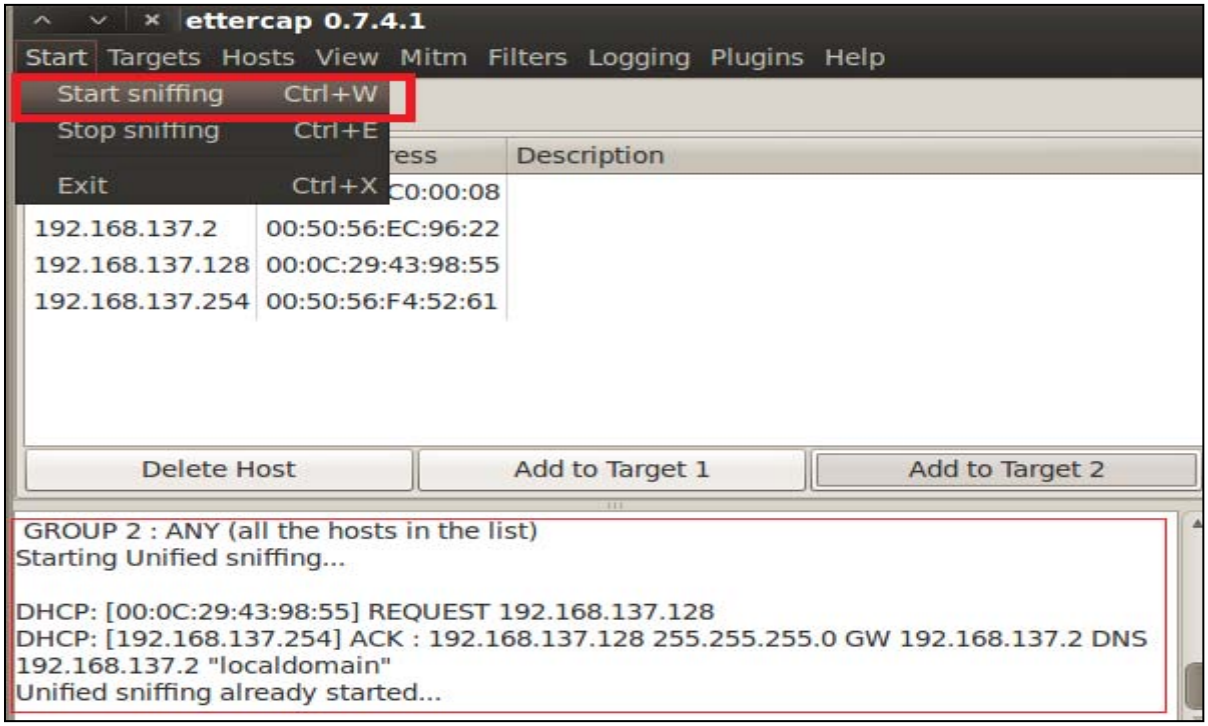


Figure 46:Début du Sniffing

Après avoir effectué cette étape l'architecture du réseau devient comme suit : L'attaque Man in the Middle est réalisée et les paquets transitent alors par le Hacker au lieu du routeur et ce dernier se charge de tout échange entre le client « victime » et le routeur !

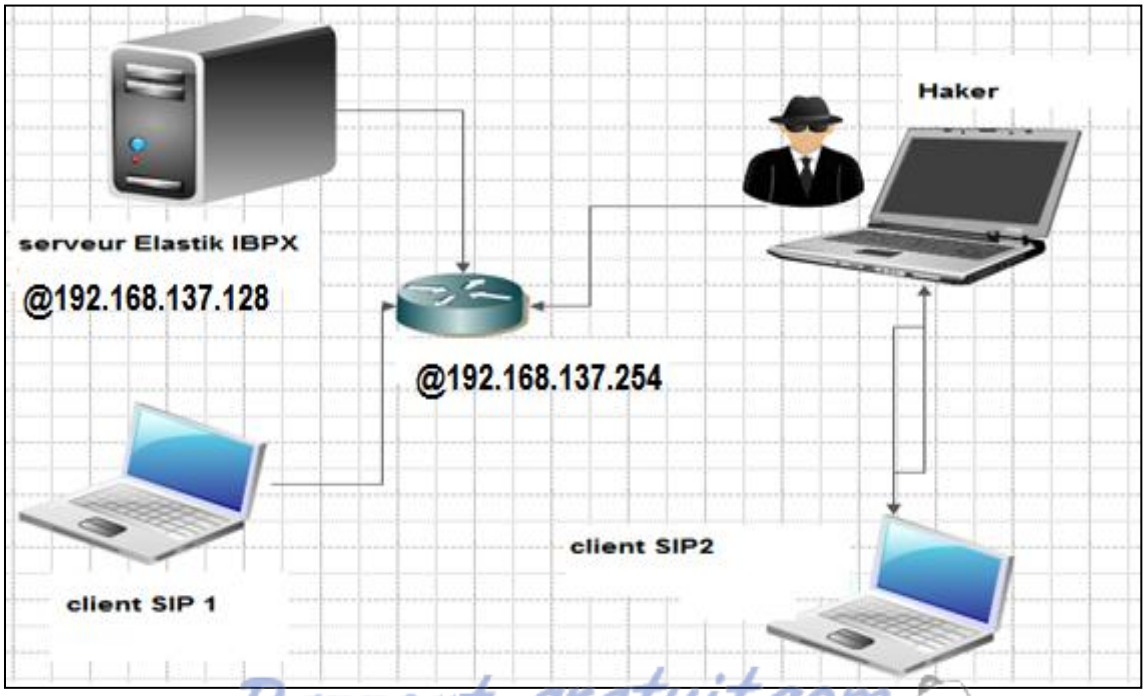


Figure 47:Architecture du réseau de l'attaque Mitm

5 éme étape : Lancer Wireshark

- **Wireshark :** analyseur de paquets, permettant la capture des paquets RTP échangés et l'enregistrement des conversations se déroulant sur le réseau.

Il suffit de taper dans le terminal de la machine pirate : **wireshark /root/sslstrip** :lancement graphique

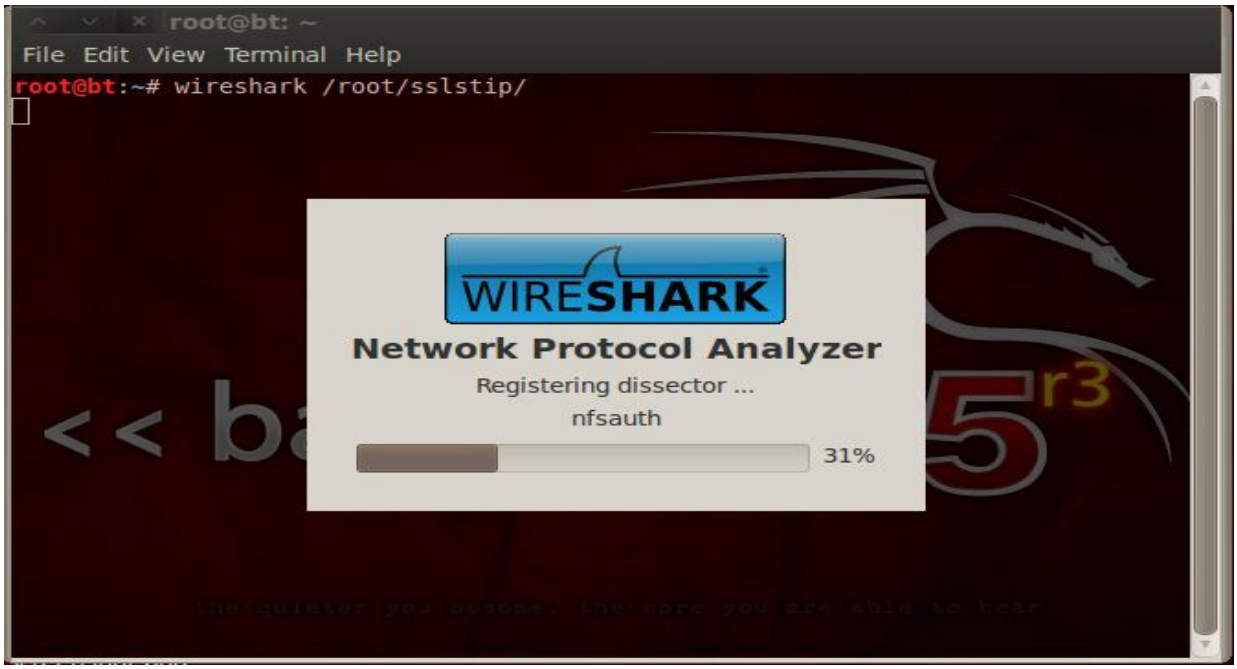


Figure 48: Lancement graphique de Wireshark de machine pirate

- Choix de l'interface réseau sur laquelle on va effectuer la capture des paquets échangés :

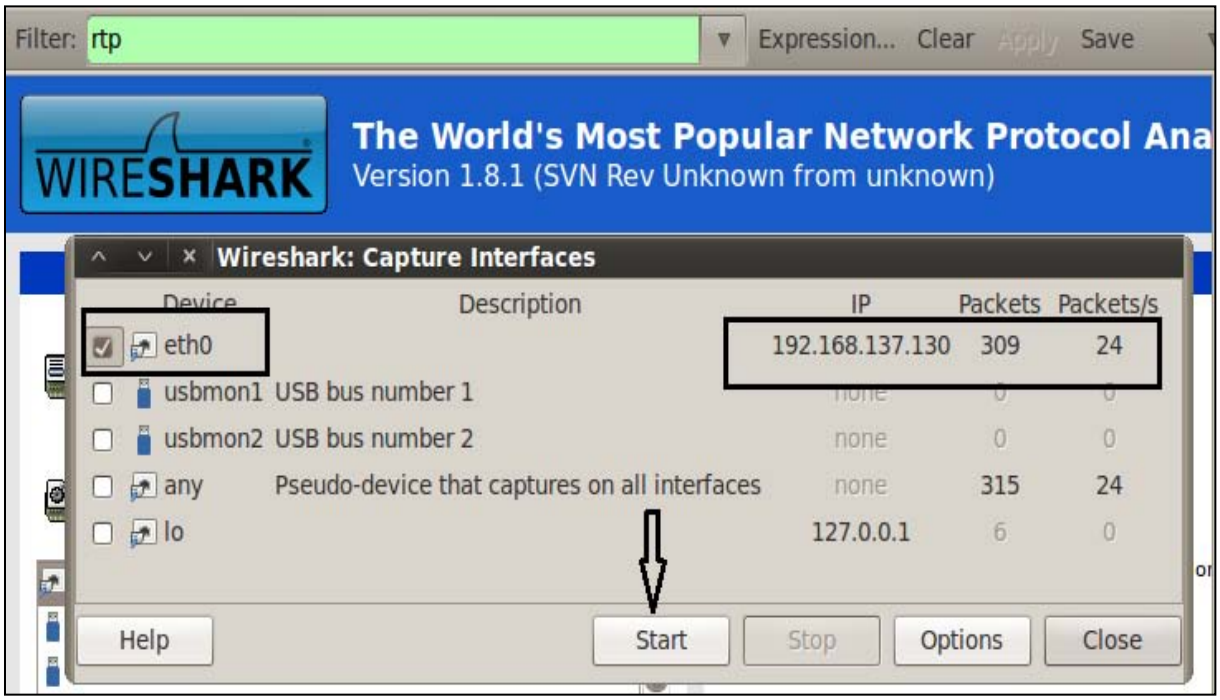


Figure 49:Choix d'interface eth0

- Filtrer les paquets à capturer et se limiter au protocole « RTP » :

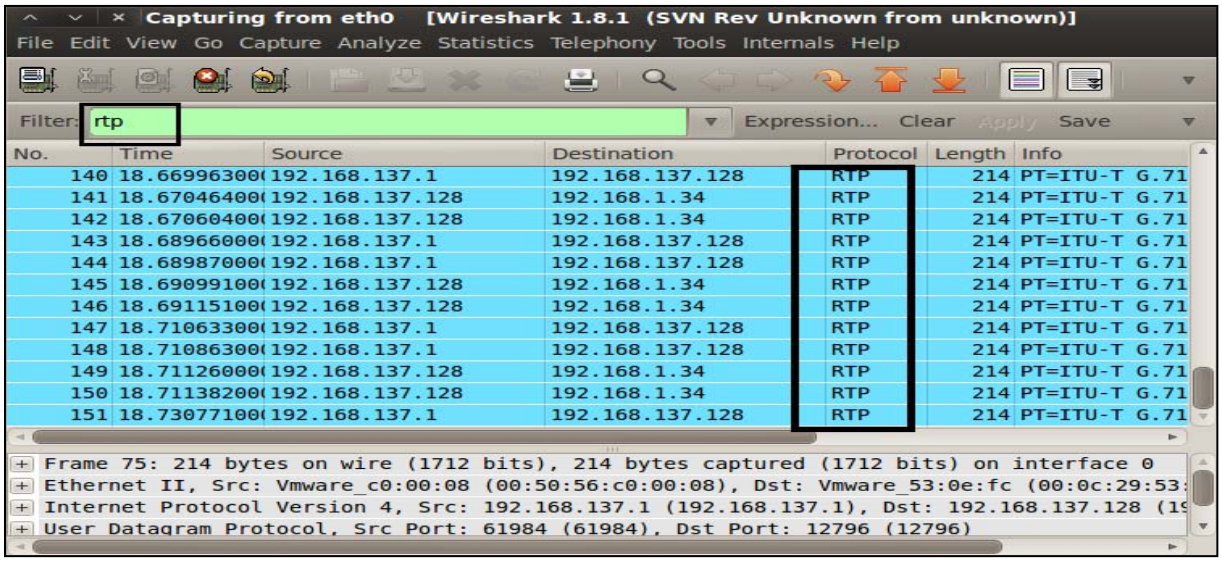


Figure 50:Filtrer les paquets à capturer se limite au protocole RTP

- Analyse des paquets capturés :

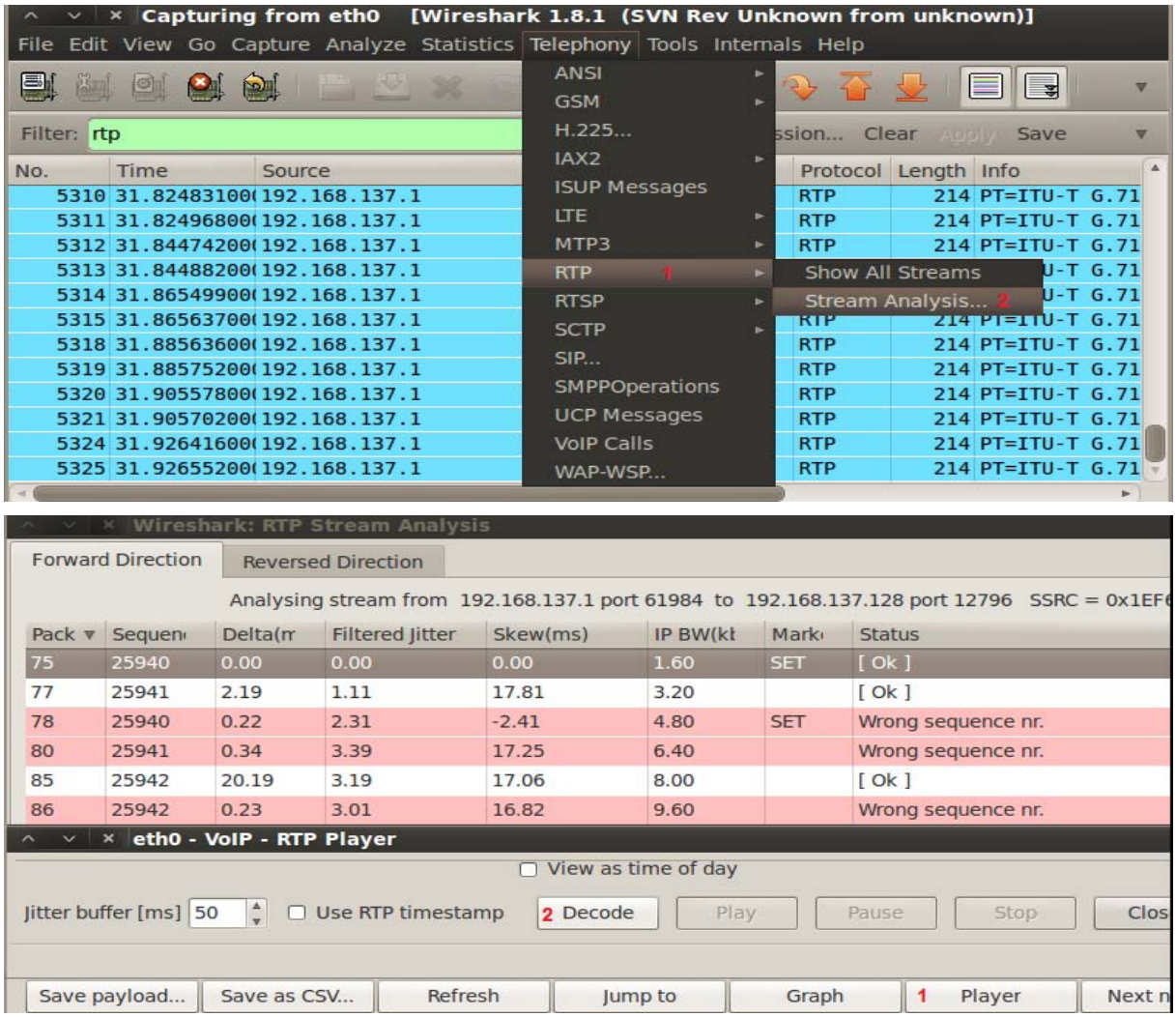


Figure 51:Analyse des paquets capturés RTP

- Ecoute des conversations enregistrées :

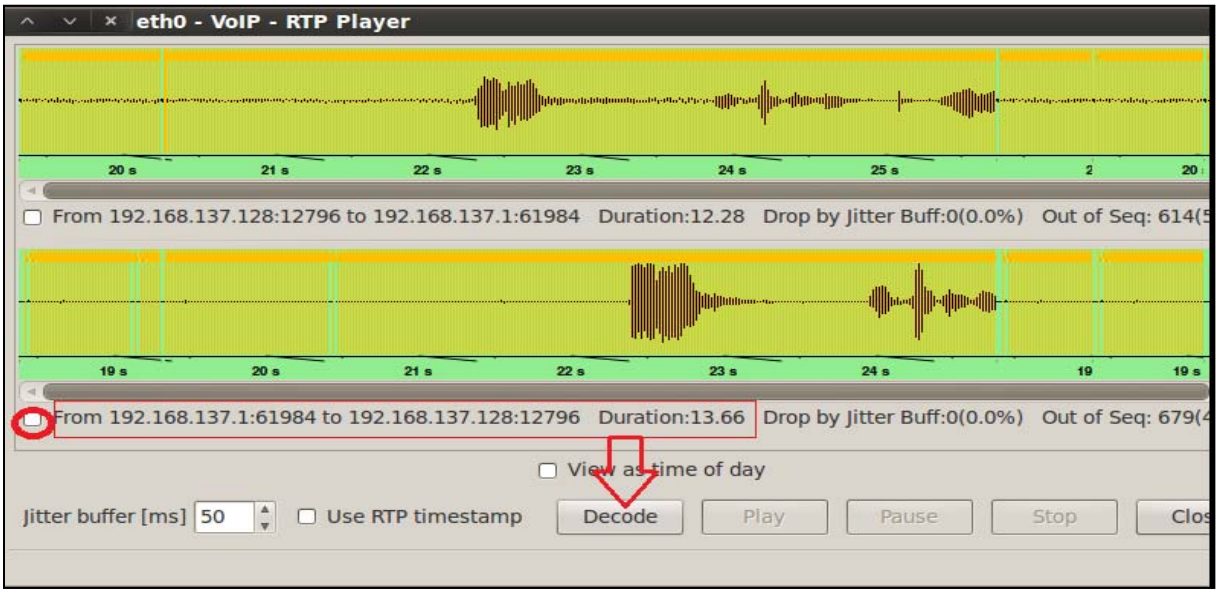


Figure 52:Ecoute des conversations enregistrées décoder

La communication décodée peut être sauvegardée dans un fichier audio (.au) et peut être même lu avec Windows Media Player ou Real Player.

7. Attaque par force brute avec Sipvicious :

Sipvicious est une suite d'outils qui permet de tester la sécurité des terminaux et autocommutateurs SIP.Elle est composée de quatre utilitaires : le premier, dénommé **Svmap,** permet de scanner une plage d'adresse IP à la recherche de dispositifs VoIP, le second **Svwar**, permet de déterminerla liste des extensions actives sur un autocommutateur (IPBX).**Svcrack** permet de cracker les mots de passes d'un PBX et **Svreport** gère les rapports générés par ces outils, qui peuvent être aux formats pdf, xml,html, csv ou txt.

On commence par un scan du serveur Elastix FPBX avec svmap, comme nous pouvons voir, sur la Figure 53 nous utilisons svmap.py pour scanner notre plage d'adresse IP pour trouver le serveur Elastix FPBX et le softphone Idefisk.

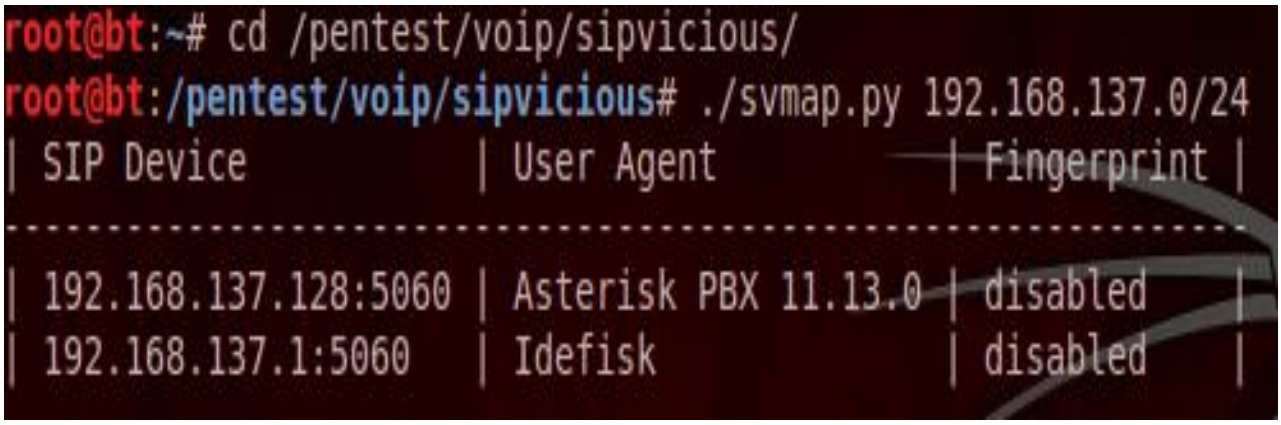


Figure 53:Scan du serveur FPBX avec svmap

Puis on détermine les extensions, on utilise ensuite svwar.py pour visualiser les extensions configurées :

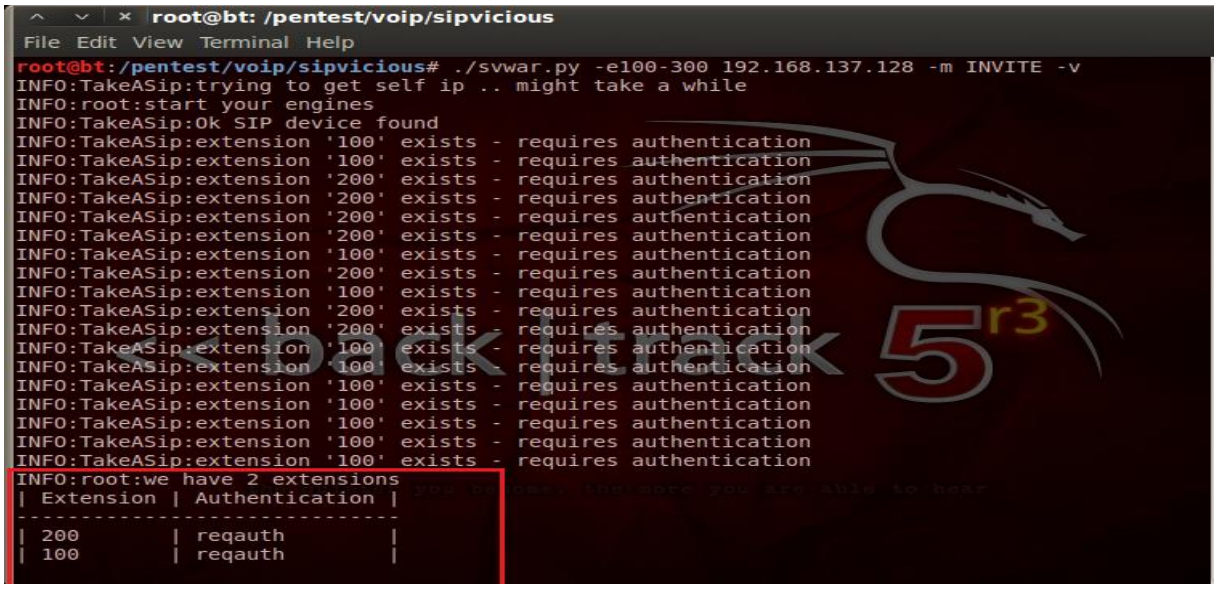


Figure 54:Capture déterminant les extensions configurées

On peut également cracker le mot de passe, avec la commande. /*svcrack –u 100 192.168.137.128*, on demande à Sipvicous de deviner le mot de passe de l'extension « 100 » détecté précédemment de notre serveur.

C'est l'attaque la plus dangereuse, car si un attaquant connaît votre mot de passe, alors il sera en mesure de s'authentifier sur le réseau en utilisant votre identité.

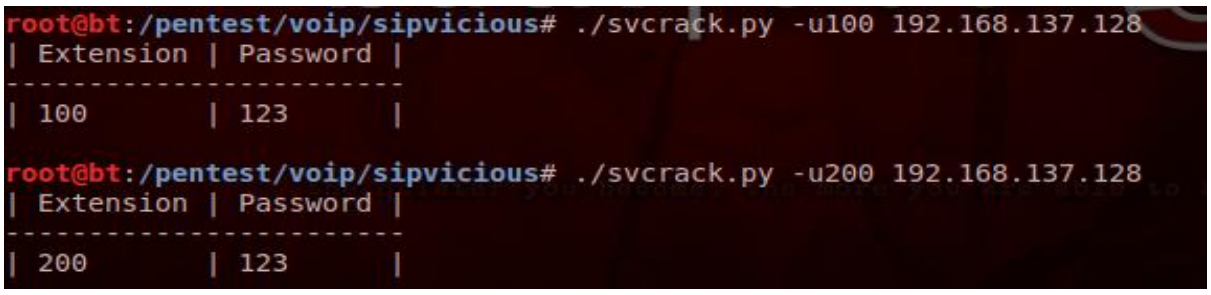
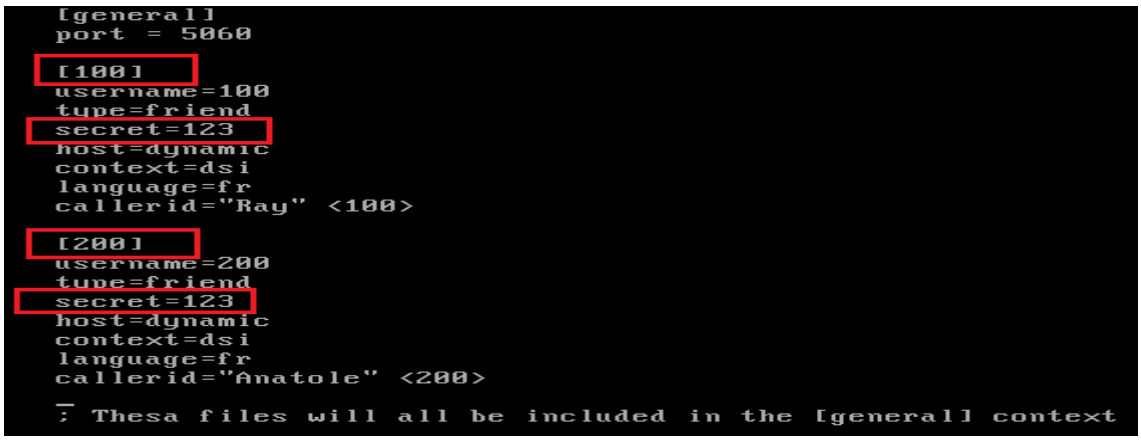


Figure 55:les mots de passe crackés avec Svcrack

Comparaison avec notre système :



Les noms des extensions et les mots de passe est juste

8. SIP crack:

Comme son nom l'indique, c'est une attaque qui vise à avoir toutes les informations nécessaires à propos de l'utilisateur, entre autre son identifiant et son mot de passe. Afin de réaliser cette opération, il suffit de télécharger le module sipcrack via la commande : **Apt-get install sipcrack.**

Ce module contient deux commandes primordiales pour la réalisation de l'SIPcrack : **sipdump** et **sipcrack**.

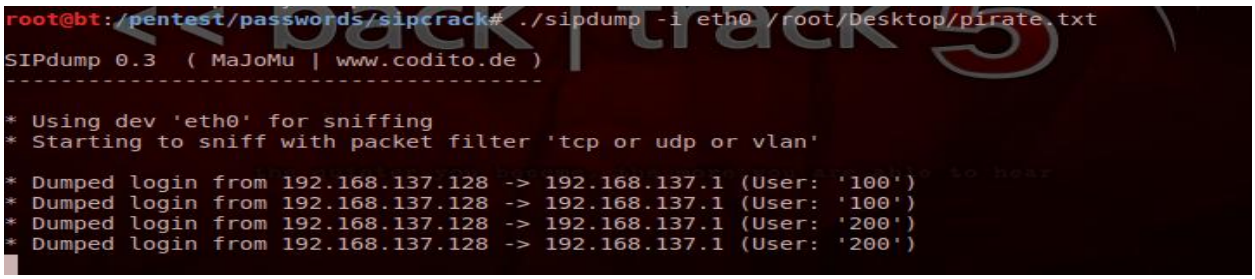


Figure 56:crack un sip à l'aide sipcrak

Sipdump : est une commande qui permet de déterminer les adresses des différents clients en associant leur caller ID. Le résultat sera stocké dans le fichier (dans notre cas :fichier)

Voici le résultat :

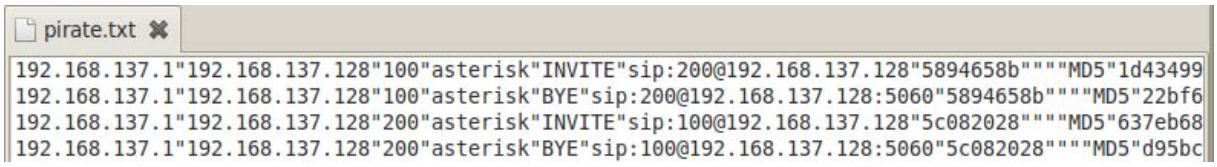


Figure 57:Résultat de crack de sip avec le caller ID

Par la suite on utilise la commande sipcrack en lui spécifiant un dictionnaire téléchargeable via le net et le fichier contenant le mot de passe crypté. Cela a pour but de décoder le mot de passe de l'utilisateur et de se connecter via X-lite avec son compte.

Voici un exemple :

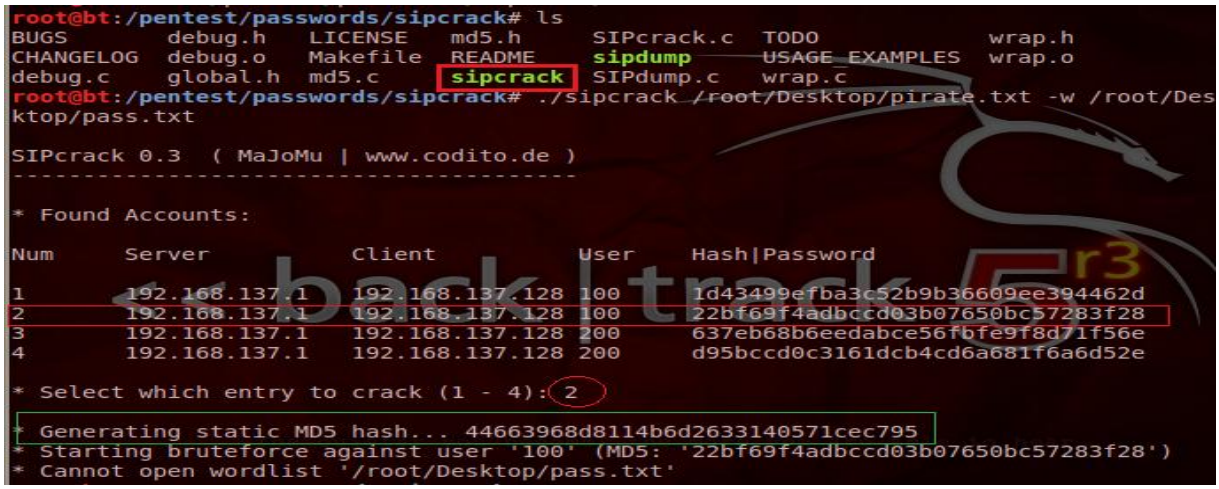


Figure 58:Mot de passe crypté à l'aide sipcrack

9. Invite flooding:

En informatique, le flood ou flooding est une action généralement malveillante qui consiste à envoyer une grande quantité de données inutiles dans un réseau afin de le rendre inutilisable, par exemple en saturant sa bande passante ou en provoquant le plantage des machines du réseau. C'est une forme de déni de service.

Inviteflood est un outil disponible sur Backtrack, utilisé pour lancer des attaques DOS contre toute extension (utilisateur) sur le réseau VoIP.Cette attaque s'effectue par le biais de la commande inviteflood sous le fichier **: /pentest/voip/inviteflood.**

- **SIP Flooding:**

Une attaque visant à renverser le serveur est possible (SIP flooding) avec la commande précédente; il suffit de remplacer le 1 qui représente le nombre des paquets envoyés par un nombre important visant à submerger le serveur avec des requêtes SIP.

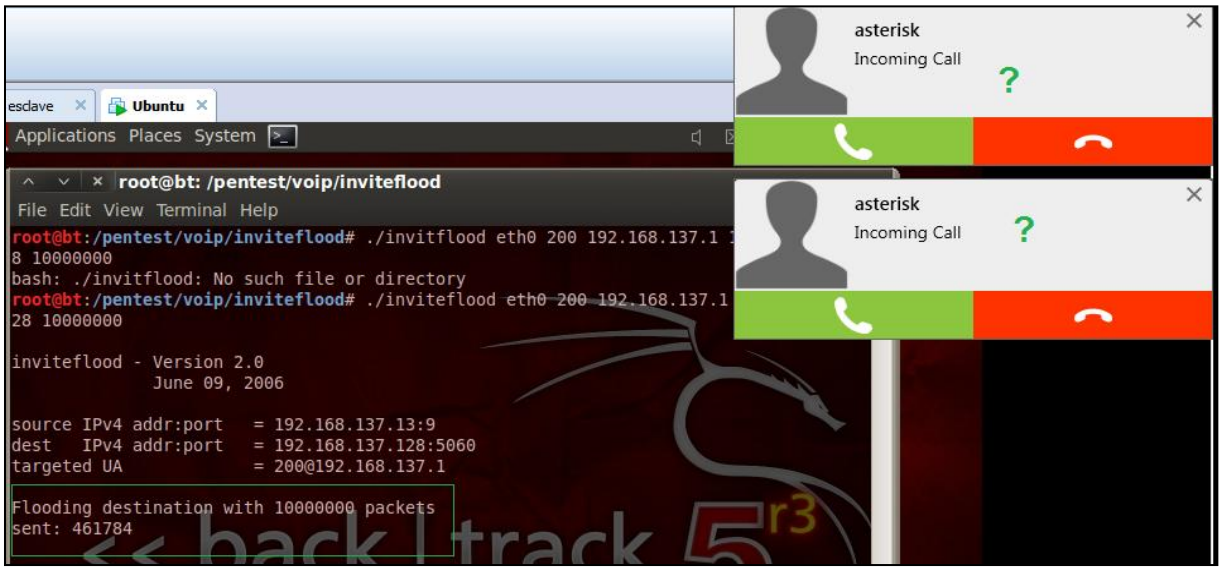


Figure 59:Attaque de type DOS avec inviteflood

Cet outil peut être utilisé pour inonder notre cible avec les requêtes de type INVITE. Nous avons envoyé 1000000 packets vers la cible (serveur voip) ayant l'adresse 192.168.137.128 et nous remarquons bel et bien que l'appel vers l'extension 200 a été interrompu. (La figure 57).

10. Caller ID spoofing:

Caller ID spoofing est une attaque qui permet de créer un scénario où un utilisateur inconnu peut usurper l'identité d'un utilisateur ayant le droit d'appeler les autres utilisateurs sur le réseau VoIP.

Il existe de nombreuses façons de concevoir une malformation des messages SIP INVITE (par exemple scapy, SIPp ...) pour la démonstration, nous allons utiliser le module auxiliaire de Metasploit nommé sip_invite_spoof.

Le caller ID spoofing est également appelé vishing ou voice phishing .Pour simuler cette attaque on utilisera deux méthodes une avec l'outil Inviteflood et l'autre avec Metasploit.

- **Inviteflood :**

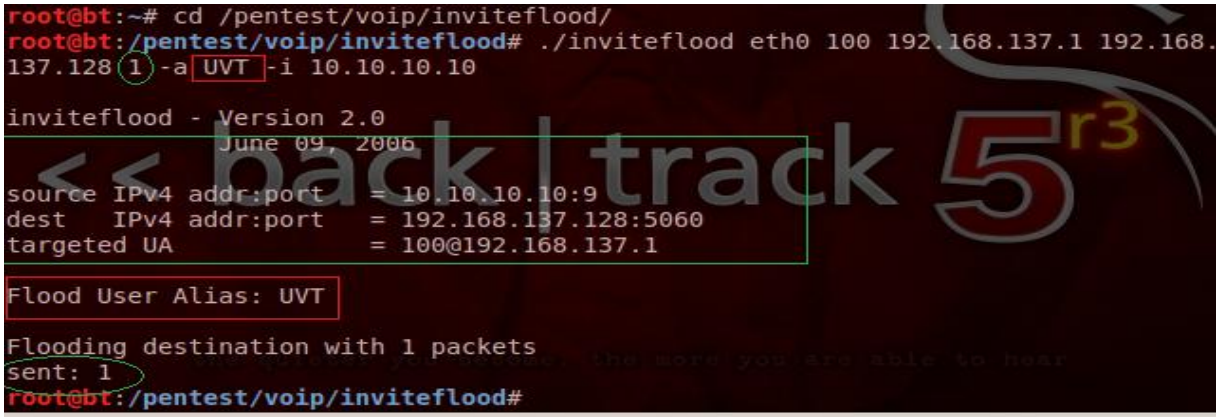


Figure 60:Attaque Caller IP spoofing via Inviteflood.

Cette commande signifie qu'un appel va être simulé à l'utilisateur dont l'identifiant est 1000. Pour ce faire, il faut préciser dans la commande d'abord l'adresse ip de la victime puis l'adresse ip du serveur. Le 0 représentent le nombre des paquets envoyés. Les options –a et –i permettent respectivement de spécifier le nom du destinataire (FakeName choisi par le pirate) et son adresse ip.

Nous allons exploiter un outil que nous avons déjà vu précédemment dans les attaques DOS.Il s'agit de « Inviteflood » qui peut être utilisé aussi pour envoyer une fausse requête de type INVITE pour appeler la cible en se faisant passer par un utilisateur légitime ayant le droit d'appeler les autres utilisateurs sur le réseau VoIP.

- **Metasploit :**

Metasploit est un projet (open-source à l'origine) sur la sécurité informatique qui fournit des informations sur des vulnérabilités, aide à la pénétration de systèmes informatisés et au développement de signatures pour les IDS, le plus connu des sous-projets est le Metasploit Framework, un outil pour le développement et l'exécution d'exploits (logiciel malveillant) contre une machine distante.

La première étape est de lancer le Métasploit et de charger le module auxiliaire **sip_invite_spoof**.

Figure 61:Lancement Métasploit et charger le module auxiliaire

Ensuite nous allons configurer le module auxiliaire pour l'exécuter, la prise d'écran ci dessous montre tous les réglages de configuration.

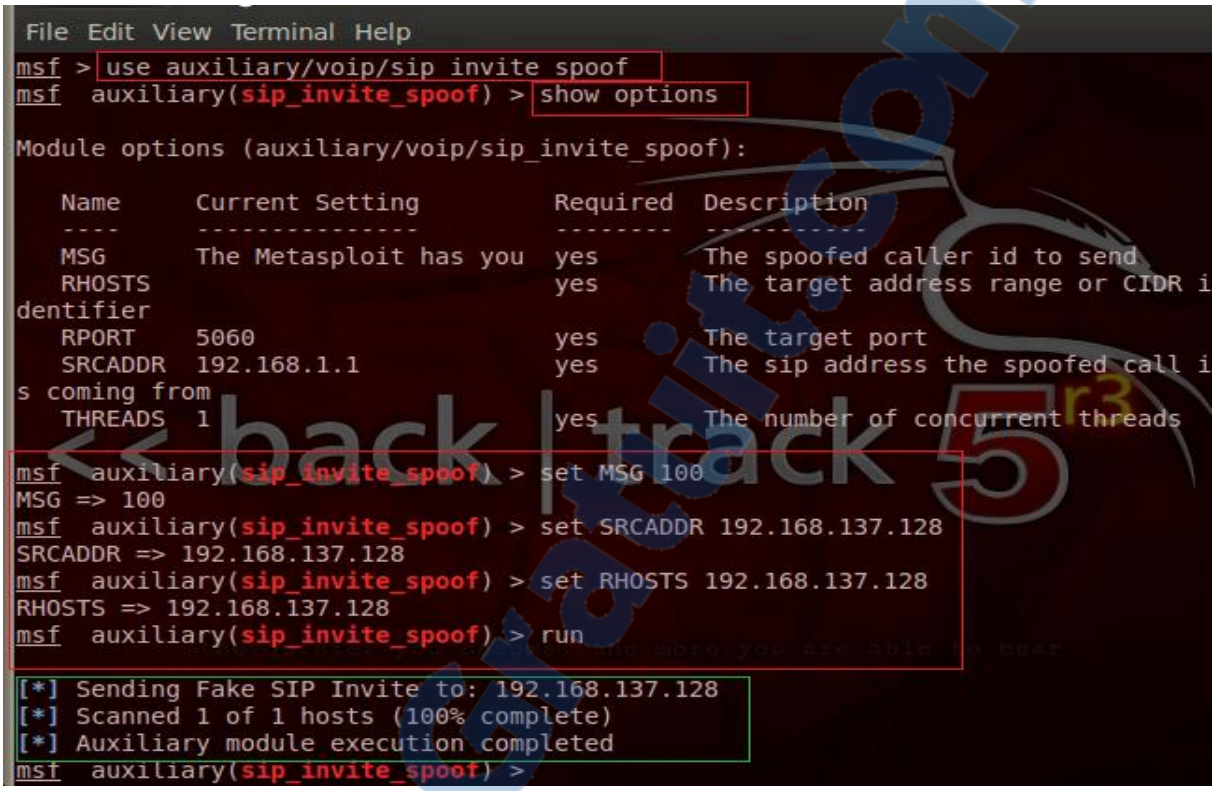


Figure 62:Réglages de configuration de sip-invite-spoof.

Le Module auxiliaire va envoyer une demande d'invitation usurpée à la victime (Client SIP 200), la victime répond à l'appel avec l'impression qu'il parle au client SIP 100 .

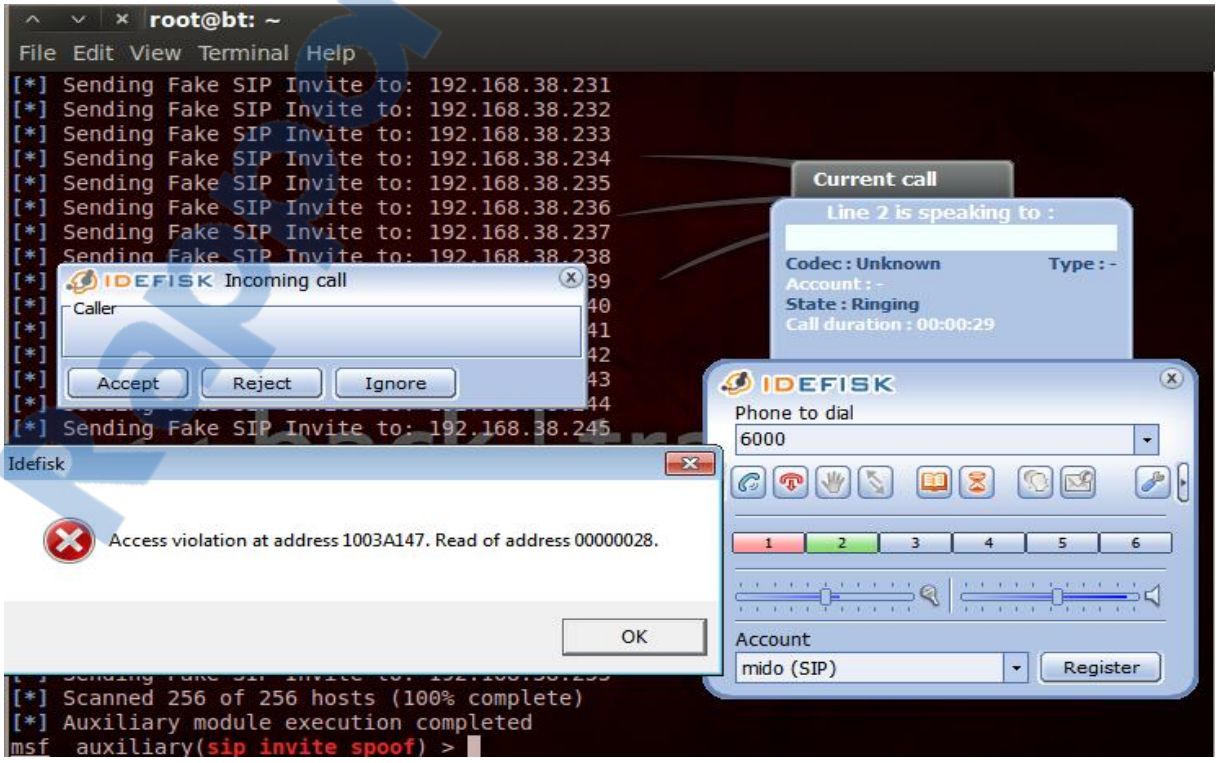


Figure 63:Démonstration de l'attaque caller ID spoofing avec Metasploit

V. Politiqe de Sécurité :

La ToIP/VoIP souffre encore d'une mauvaise image d'un point de vue sécurité, en effet les réseaux voix historiquement isolés, fusionnent de plus en plus avec les réseaux de données, ils sont donc plus sensibles aux attaques d'un piratage.

Les impacts peuvent être variables, confidentialité, dysfonctionnements, usurpations, écoute, changements des annonces de l'IPBX, accès aux messageries vocales, contournement de la politique de sécurité DATA, perte financière, alors qu'il existe un ensemble de solutions qui permettent de maitriser la sécurité de son système de téléphonie sur IP, nous commençons par sécuriser notre client ensuite on passe à la sécurité de notre serveur VoIP.

1. Sécurité du client :

➢ L'authentification 802 .1x :

L'une des méthodes les plus importantes pour anticiper une attaque sur un système de téléphonie est de déterminer clairement l'identité des périphériques ou des personnes participant à la conversation. On parlera d'authentification. 802.1x est un standard lié à la sécurité des réseaux informatiques. Il permet de contrôler l'accès aux équipements de l'infrastructure réseau.

Il s'appuie sur le protocole EAP, Extensible Autentication Protocol, pour les communications client/serveur, avec un serveur d'identification Radius.Ce dernier servira à authentifier les utilisateurs qui se connectent au réseau et à leur permettre ou non l'accès à certaines ressources de l'entreprise.

Le déploiement de l'IEEE 802.1X fournit une couche de sécurité pour l'utilisation des réseaux câblés et sans fil, et il est possible de contrôler l'accès à chacun des ports d'un équipement réseaux.

Un port peut avoir deux états différents :

- Contrôlé si l'identification au près du serveur Radius a fonctionné
- Non contrôlé si l'identification a échoué

L'architecture de notre projet se compose de deux téléphones VOIP, d'un serveur Elastix Asterisk et d'un serveur d'authentification FreeRadius.

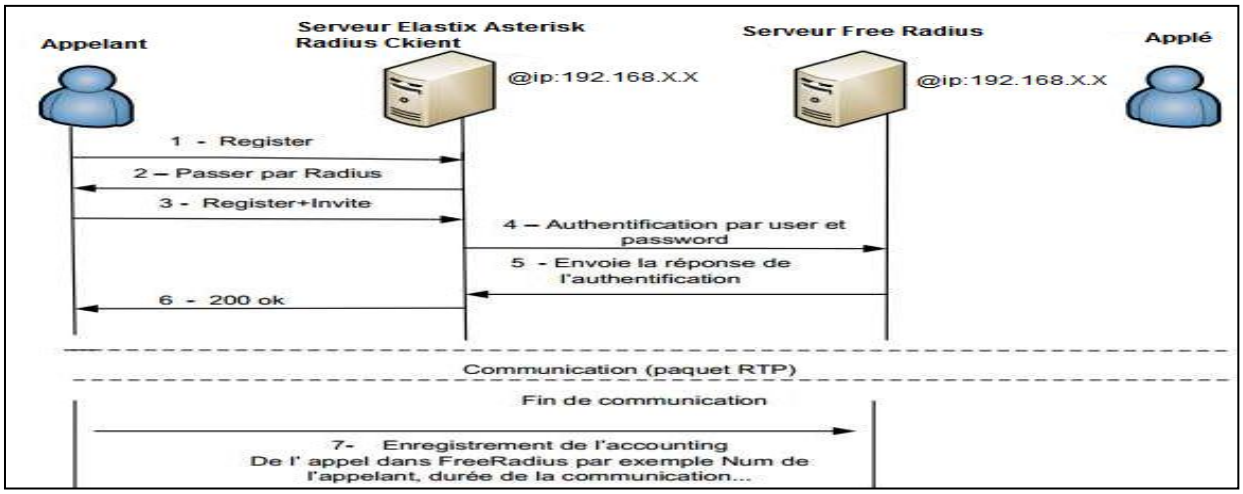


Figure 64: les étapes d'une communication VoIP en utilisant le serveur Raduis

1. L'user agent SIP va s'enregistrer dans Elastix Asterisk par son numéro de téléphone et un mot de passe.

2. Quand il essaye de composer le numéro de l'appelé, il reçoit un message qu'il doit passer par FreeRadius pour effectuer cet appel.

3. Il renvoie une autre demande de connexion à FreeRadius.

4. Le client radius se charge d'envoyer le nom d'utilisateur et son mot de passe pour s'identifier dans FreeRadius.

5. S'il reçoit une réponse positive donc l'utilisateur et le mot de passe sont corrects, si ce n'est pas le cas, on aura une réponse négative et l'appel ne peut pas être établi.

6. L'user agent reçoit un message qu'il a le droit d'effectuer cet appel donné par FreeRadius, et le téléphone sonnera chez le destinataire.

7. On envoie les données de l'accounting de cet appel dans FreeRadius.

- **Génération des mots de passe crypté :**

Il n'est pas possible de crypter les données transmises via le protocole IAX, seul l'authentification permet plusieurs types de mots de passes plus ou moins sécurisés.

Le protocole IAX permet trois types de mots de passe pour l'authentification des clients /serveurs à savoir :

Plain text :

Cette méthode est déconseillée, car les mots de passe sont écrits en clair dans les fichiers de Configuration.

MD5 :

Les mots de passe sont écrits cryptés à l'aide de la méthode MD5 dans les fichiers de configurations, donc difficilement décryptables (difficile mais pas impossible).

Nous utiliserons un compte SIP avec une authentification par md5.

Il suffit d'utiliser les commandes "echo" et "md5sum" pour encrypter un mot de passe en md5.

echo -n "<user>:<realm>:<secret>" | md5sum

<user> => le nom d'utilisateur

<realm> => asterisk

<secret> => le mots de passe en claire

```
[root@node1 ~]# cd  /var/lib/asterisk/keys
[root@node1 keys]# echo -n "210:asterisk:mido131265" | md5sum
897f9d6563686d912ca323fe18d20dd0  -
[root@node1 keys]#
```

Pour créer un mot de passe crypté en md5, on utilise les commandes « echo » et « md5sum » : Cette commande retourne le mot de passe crypté en md5, nous créons un utilisateur dans le fichier *sip.conf*.

RSA :

L'authentification RSA (Rivest Shamir Adleman) utilise deux clés partagées, une clé publique ainsi qu'une clé privée. Généralement, ces clefs ont une longueur entre 1024 et 2048 bits.

Génération de clés RSA **:**

Pour générer des clés de cryptage RSA, Asterisk nous fourni un utilitaire: astgenkey.

Les clés RSA doivent se trouver dans le répertoire **/var/lib/asterisk/keys**.

L'utilitaire "astgenkey" génère deux clés, une clé publique à mettre sur le(s) poste(s) client(s) et une clé privée à garder sur le serveur.

Note: Il est important que la clé privée ne soit accessible que par Asterisk, car si quelqu'un arrive à prendre cette clé il pourra décrypter la clé plus facilement.

Pour générer une clé il suffit de se déplacer dans le répertoire de stockage des clés d'Asterisk et de lancer l'application "astgenkey" .

```
cd  var/lib/asterisk/keys
```

Lorsque nous lançons astgenkey nous mettons le paramètres '-n' car par défaut "astgenkey" demande une "passphrase" à chaque démarrage d'Asterisk. Avec le paramètres '-n' il enregistre la clé sans "passphrase"

```
astgenkey –n
```

```
[root@node1 ~]# cd  /var/lib/asterisk/keys
[root@node1 keys]# ll
total 12
-rw-r--r-- 1 root root 887 juin 13 14:22 mido131265.key
-rw-r--r-- 1 root root 272 juin 13 14:22 mido131265.pub
-rw-r--r-- 1 root root 963 juin 13 14:40 -n.key
-rw-r--r-- 1 root root   0 juin 13 14:37 sip.conf
```

Figure 65:Création deux clés dans le serveur A

```
[root@node2 keys]# ll
total 8
-rw-r--r-- 1 root root 887 juin 13 14:53 mido131265.key
-rw-r--r-- 1 root root 272 juin 13 14:53 mido131265.pub
[root@node2 keys]# scp  root@192.168.137.128:/var/lib/asterisk/keys/mido131265_i
ax.pub  /var/lib/asterisk/keys/ mido131265__iax.pub
```

Figure 66:Création deux clés dans le serveur B

Nous avons créé deux clefs dans le serveur A:

- midotest_iax.pub qui est la clef publique.
- midotest_iax.key qui est la clef privée.

Maintenant, il faut transférer la clef publique dans l'autre serveur. Pour cela, nous allons nous positionner sur le serveur B et utiliser ssh avec la commande suivante :

- **scp user@IPserveur:/répertoire/nom_du_fichier /destination/nom_du_fichier**

serveur A :

- scp root@192.168.137.129:/var/lib/asterisk/keys/mido131265 _iax.pub /var/lib/asterisk/keys/ mido131265_iax.pub

serveur B :

- scp root@192.168.137.128:/var/lib/asterisk/keys/mido131265 _iax.pub /var/lib/asterisk/keys/ mido131265_iax.pub

Il faudra répéter l'opération dans l'autre sens afin de créer une interconnexion bidirectionnelle.

- Configuration des paramètres IAX sur chaque serveur

La configuration des paramètres IAX se fait dans le fichier *iax.conf* se trouvant dans le répertoire **/etc/asterisk/** .Sur chaque serveur nous allons configurer un utilisateur IAX qui servira à l'authentification avec le serveur opposé. [VOIP1] et [VOIP2] .

Configuration du fichier *iax.conf* pour le serveur A (serveur Maitre):

```
[VOIP2]
type=friend
host=192.168.137.128
auth=rsa
inkey=mido131265_iax
outkey=mido131265_iax2
context=FROM_VOIP2
qualify=yes
trunk=yes
```

Configuration du fichier *iax.conf* pour le serveur B (serveur Esclave) :

```
[VOIP1]

type=friend
host=192.168.137.129
auth=rsa
inkey=mido131265_iax2
outkey=mido131265_iax
context=FROM_VOIP1
qualify=yes
trunk=yes
```

- Définition du "dialplan"

Nous devons maintenant créer les contextes dans le fichier *extensions.conf* dans le serveur A.

```
[FROM_VOIP2]
include => VOIP1

[VOIP1]
exten => _1XX,1,Dial(IAX2/${EXTEN})
exten => _2XX,1,Dial(IAX2/VOIP2/${EXTEN})
```

Ce qui signifie que dans le contexte [FROM_VOIP2] est inclus le contexte [VOIP1] qui définit que pour les extensions commençant par 1, l'appel sera acheminé en interne et pour les appels commençant par 2, l'appel sera transmis au serveur B.

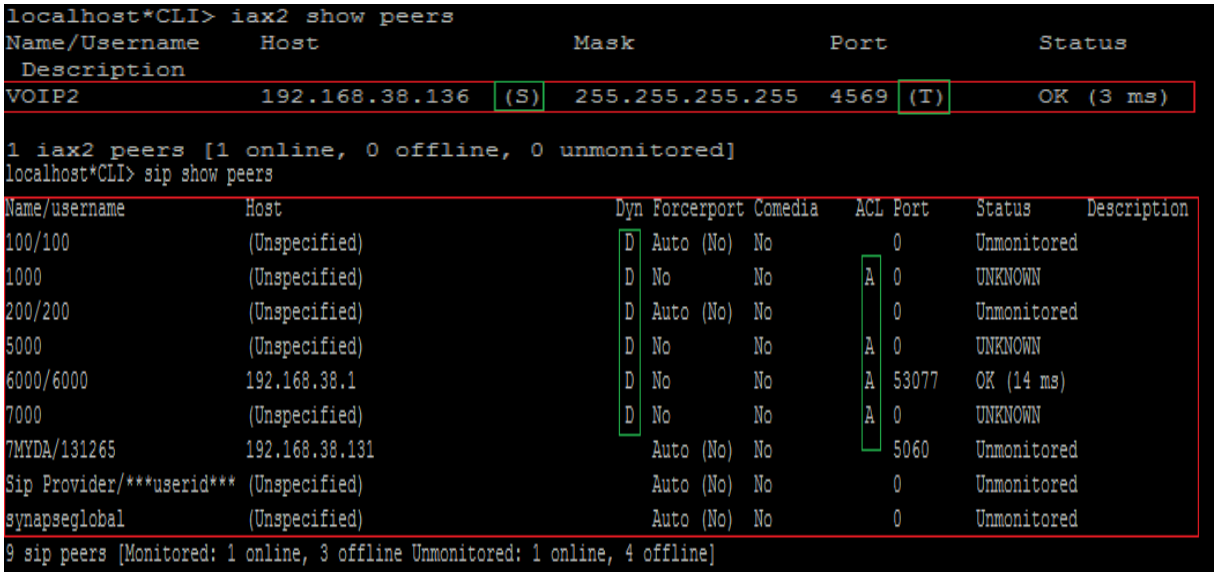
Nous faisons de même sur le serveur B.

```
[FROM_VOIP1]
include => VOIP2

[VOIP1]
exten => _2XX,1,Dial(IAX2/${EXTEN})
exten => _1XX,1,Dial(IAX2/VOIP1/${EXTEN})
```

- Vérification :

Nous lançons les 2 serveurs Elastix et nous tapons la commande suivante :



```
localhost*CLI> iax2 show peers
Name/Username     Host                 Mask              Port          Status
 Description
VOIP2             192.168.38.136  (S)  255.255.255.255   4569  (T)     OK (3 ms)

1 iax2 peers [1 online, 0 offline, 0 unmonitored]
localhost*CLI> sip show peers
Name/username           Host                 Dyn Forcerport Comedia    ACL Port     Status      Description
100/100                 (Unspecified)        D  Auto (No)  No             0        Unmonitored
1000                    (Unspecified)        D  No         No          A  0        UNKNOWN
200/200                 (Unspecified)        D  Auto (No)  No             0        Unmonitored
5000                    (Unspecified)        D  No         No          A  0        UNKNOWN
6000/6000               192.168.38.1         D  No         No          A  53077    OK (14 ms)
7000                    (Unspecified)        D  No         No          A  0        UNKNOWN
7MYDA/131265            192.168.38.131          Auto (No)  No             5060     Unmonitored
Sip Provider/***userid*** (Unspecified)         Auto (No)  No             0        Unmonitored
synapseglobal           (Unspecified)           Auto (No)  No             0        Unmonitored
9 sip peers [Monitored: 1 online, 3 offline Unmonitored: 1 online, 4 offline]
```

Explication des colonnes:

Name/Username: affiche le nom de la connexion

Host: affiche l'adresse IP de l'utilisateur

(S): affiche si l'adresse IP de l'utilisateur est statique

(D): affiche si l'adresse IP de l'utilisateur est dynamique

Mask: affiche le masque de sous réseau

Port: affiche le port IAX utilisé

(T): affiche si le lien est un "trunk"

Status: Affiche si le lien est OK avec les [ms] de lag

Affiche UNREACHABLE si le status du lien est mort

Affiche UNMONITORED si le status du lien n'est pas monitored ou inconnu

J'ai créé des comptes SIP : numéro 100 sur le serveur A et numéro 200 sur le serveur B.Le 200 a pu appeler le 100.

2. Redondance:

Pour la redondance, nous allons utiliser un cluster de haute disponibilité, c'est-à-dire utiliser 2 serveurs afin de garantir la disponibilité du service et des données. Pour cela, nous allons utiliser 2 logiciels open-source : DRBD et Heartbeat.

Les serveurs de bases de données peuvent travailler ensemble pour permettre à un second serveur de prendre rapidement la main si le serveur principal échoue (haute disponibilité, high availability), ou pour permettre à plusieurs serveurs de servir les mêmes données (répartition de charge load balancing). Idéalement, les serveurs de bases de données peuvent travailler ensemble sans jointure. Les serveurs web traitant des pages web statiques peuvent travailler ensemble assez facilement en répartissant la charge des requêtes web sur plusieurs machines. De même, les serveurs de bases de données en lecture seule peuvent aussi travailler ensemble assez facilement. Malheureusement, la plupart des serveurs de bases de données ont des requêtes de lecture/écriture et ce type de serveurs sont bien plus difficile à faire travailler ensemble. Ceci est dû au fait qu'il faut placer une seule fois sur chaque serveur les données en lecture seule et qu'une écriture sur un serveur doit être propagée à tous les serveurs pour que les futures lectures sur ces serveurs renvoient des résulats cohérents.

Ce problème de synchronisation est la difficulté fondamentale pour les serveurs travaillant ensemble. Comme il n'existe pas qu'une seule solution qui élimine l'impact du problème de synchronisation pour tous les cas pratiques, il existe plusieurs solutions. Chaque solution répond à ce problème d'une façon différente et minimise cet impact pour une charge spécifique.

Certaines solutions gèrent la synchronisation en autorisant les modifications des données sur un seul serveur. Les serveurs qui peuvent modifier les données sont appelés serveurs lecture/écriture ou serveurs maîtres. Les serveurs qui peuvent répondre aux requêtes en lecture seule sont appelés des serveurs esclaves. Les serveurs qui ne sont pas accessibles tant qu'ils ne se sont pas transformés en serveurs maîtres sont appelées des serveurs en attente (standby servers).

Certaines solutions de failover et de répartition de charge sont synchrones, signifiant qu'une transaction de modification de données n'est pas considérée validée tant que tous les serveurs n'ont pas validés la transaction. Ceci garantit qu'un failover ne perdra pas de données et que tous les serveurs en répartition de charge renverront des résultats cohérents quel que soit le serveur interrogé. En contraste, les solutions asynchrones autorisent un délai entre le moment de la validation et sa propagation aux autres serveurs, ceci qui comporte le risque que certaines transactions soient perdues dans le basculement à un serveur de sauvegarde et que les serveurs en répartition de charge pourraient renvoyer des données obsolètes. La communication asynchrone est utilisée quand la version synchrone est trop lente.

Les solutions peuvent aussi être catégorisées par leur granularité. Certaines solutions peuvent seulement gérer un serveur de bases entier alors que d'autres autorisent un contrôle par table ou par base.

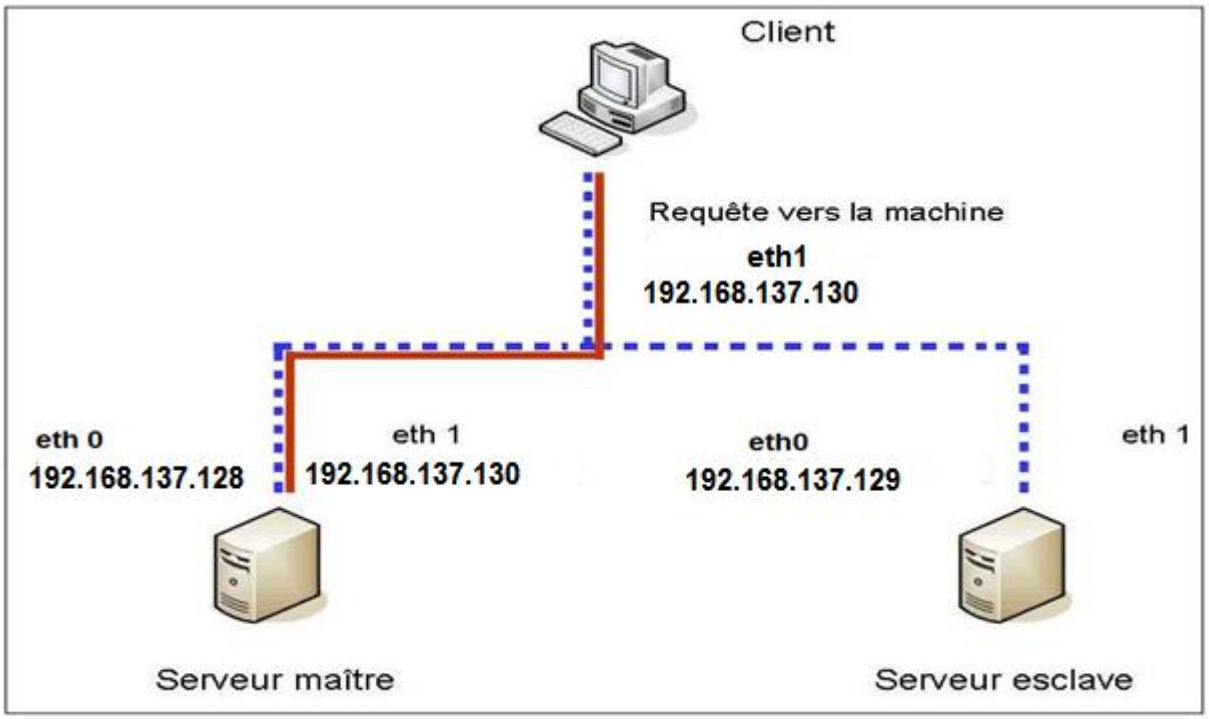
Les performances doivent être considérées dans tout choix d'une solution de failover ou de répartition de charges. Il y a généralement un compromis à trouver entre les fonctionnalités et les performances. Par exemple, une solution complètement synchrone sur un réseau lent pourrait diviser les performances par plus que deux alors qu'une solution asynchrone pourrait avoir un impact minimal sur les performances.

2.1 Le FailOver Services (FOS) :

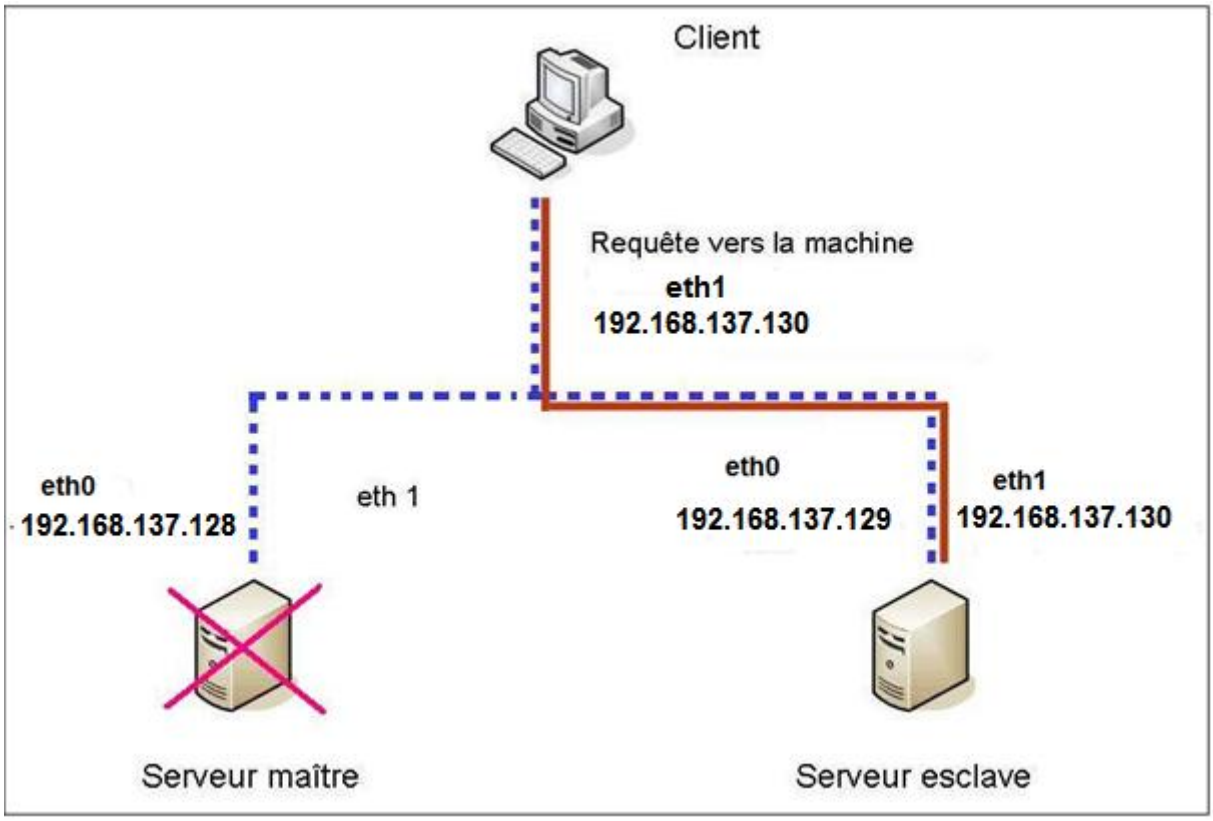
Le FailOver Services est utilisé pour la haute disponibilité des services et requiert 2 machines identiques : un serveur maître et un serveur esclave. Les deux serveurs se surveillent mutuellement par exemple en utilisant le réseau RJ45 (protocole TCP/IP) et un câble série branché sur les 2 machines. Le FailOver Services vérifie les services utilisant TCP/IP et peut commander l'arrêt ou le démarrage de scripts. Il contrôle aussi l'état réseau des machines.

FOS utilise l'IP Aliasing. L'IP Aliasing permet de définir une interface réseau avec plusieurs adresses IP différentes. Le serveur maître et le serveur esclave ont chacun une adresse IP sur le même sous-réseau (par exemple, 192.168.137.128) pour le maître et 192.168.137.129 pour l'esclave). Lorsque le client fait appel à un serveur, il interpelle un serveur avec une adresse IP aliasée, par exemple 192.168.137.130. Cette adresse IP ne sera pas définie comme IP principale mais comme IP Aliasing.

Lorsque le serveur maître tombe, l'adresse aliasée est redéfinie vers le serveur esclave. client fait appel à un serveur, il interpelle un serveur avec une adresse IP aliasée, par exemple 192.168.137.130. Cette adresse IP ne sera pas définie comme IP principale mais comme IP Aliasing. Lorsque le serveur maître tombe, l'adresse aliasée est redéfinie vers le serveur esclave.



Lorsque le serveur maître « tombe », le FailOver Services destitue l'IP Aliasé du serveur maître pour le réattribuer au serveur esclave : il désactive l'adresse IP sur l'un et active l'autre.



Lorsque le serveur maître peut de nouveau répondre aux requêtes, FailOver Services désactive l'IP Aliasé du serveur esclave et réactive celle du serveur maître.

- **How to clustering in CentOS 5&6**

La première étape est d'installer Heartbeat sur les deux serveurs VoIP, dans notre cas on va utiliser CentOS pour le faire :

Exigences pré-configuration :

Attribuer hostname *node01* à nœud principal avec l'adresse IP *192.168.137.128* à eth0, et attribuer hostname *node02* à asservir noeud avec l'adresse IP *192.168.137.129* Avec une adresse 192.168.137.130 est l'adresse IP virtuelle qui sera utilisé pour notre serveur web Apache (ie, Apache va écouter sur cette adresse).

Configuration:

Téléchargez et installez le paquet de pulsation. Dans notre cas, nous utilisons CentOS / RHEL nous allons donc installer battement de coeur avec la commande yum:

```
#yum install heartbeat
```

Il y a trois fichiers de configuration pour Heartbeat :

- *Authkeys*
- *ha.cf*
- *haresources*

Maintenant il faut copier les trois fichiers de configuration dans le répertoire */etc/ha.d* sur le serveur maitre et sur le serveur esclave.

```
#cp /usr/share/doc/heartbeat-2.1.2/authkeys /etc/ha.d/
#cp /usr/share/doc/heartbeat-2.1.2/ha.cf /etc/ha.d/
#cp /usr/share/doc/heartbeat-2.1.2/haresources /etc/ha.d/
```

- Configuration du fichier /etc/heartbeat/authkeys : ***vi /etc/ha.d/authkeys***

Le fichier *authkeys* permet aux différents serveurs Heartbeat de s'authentifier. Il y a plusieurs moyens de protéger (crc, md5 ou sha1) pour plus de sécurité, nous allons utiliser sha1, il ne faut pas oublier de changer la permission du fichier *autkheys*.

- Configuration du fichier /etc/heartbeat/ha.cf : ***vi /etc/ha.d/ha.cf***

Le fichier *ha.cf* est le fichier de configuration générale de Heartbeat, éditons le fichier et ajoutons les lignes suivantes :

```
logfile /var/log/ha-log
logfacility local0
keepalive 2
deadtime 30
initdead 120
bcast eth0
udpport 694
auto_failback on
node node01
node node02
```

- Configuration du fichier /etc/heartbeat/haressources : ***vi /etc/ha.d/haresources***

La dernière étape est de notre configuration consiste à éditer le fichier *haresources*, ce fichier contient les informations sur les ressources qui sont gérées par Heartbeat. Dans notre cas, nous voulons que le serveur Web (httpd) soit disponible, et ajoutons les lignes suivantes :

```
node01 192.168.137.130 httpd
```

Pour configurer notre serveur VoIP esclave, il suffit de copier les fichiers de configuration du premier serveur. On crée le fichier index .html dans les deux machines. Sur le serveur maitre :

On *node01*:

```
#echo "node01 heartbeat test server" > /var/www/html/index.html
```

On *node02*:

```
#echo "node02 heartbeat test server" > /var/www/html/index.html
```

Maintenant on lance le service Heartbeat à partir d'*init* sur les deux machines :

```
#/etc/init.d/heartbeat start
```

Ouvrons un navigateur Web et saisissons l'URL suivante: http://192.168.38.131 il affichera node01 heartbeat test server .

On stoppe le service Heartbeat dans le serveur maitre.

```
#/etc/init.d/heartbeat stop
```

Et on teste l'URL suivante : http://192.168.38.136 il affichera node02 heartbeat test server .

2.2 La réplication de données :

Une configuration de réplication maître/esclave envoie toutes les requêtes de modification de données au serveur maître. Ce serveur envoie les modifications de données de façon asynchrone au serveur esclave. L'esclave peut répondre aux requêtes en lecture seule alors que le serveur maître est en cours d'exécution. Le serveur esclave est idéal pour les requêtes vers un entrepôt de données.

Le logiciel DRDB (Distributed Replicated Block Device) effectue une réplication du disque primaire vers un autre disque via le réseau, en synchronisant des partitions.DRDB propose deux types de synchronisation : partielle ou totale. La synchronisation partielle n'effectue une mise à jour que dans les parties non synchronisées, au contraire de la synchronisation totale qui effectue une copie disque à disque complète.

Fonctionnement normal :

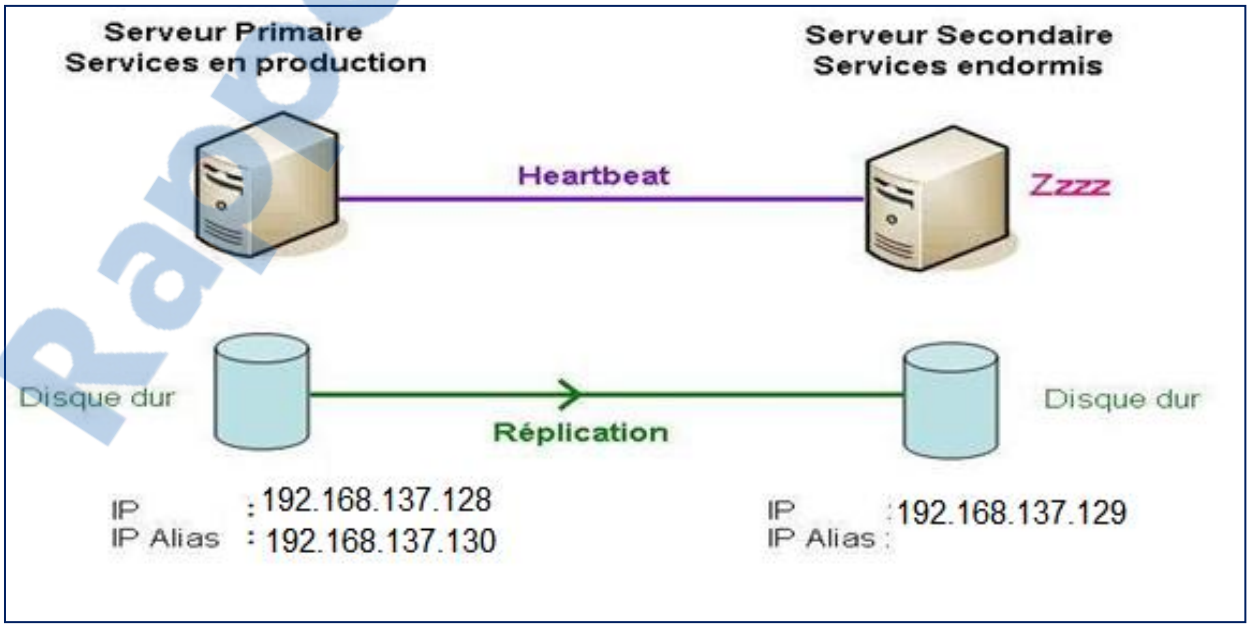


Figure 67:Fonctionnement normal de réplication de données

Fonctionnement anormal :

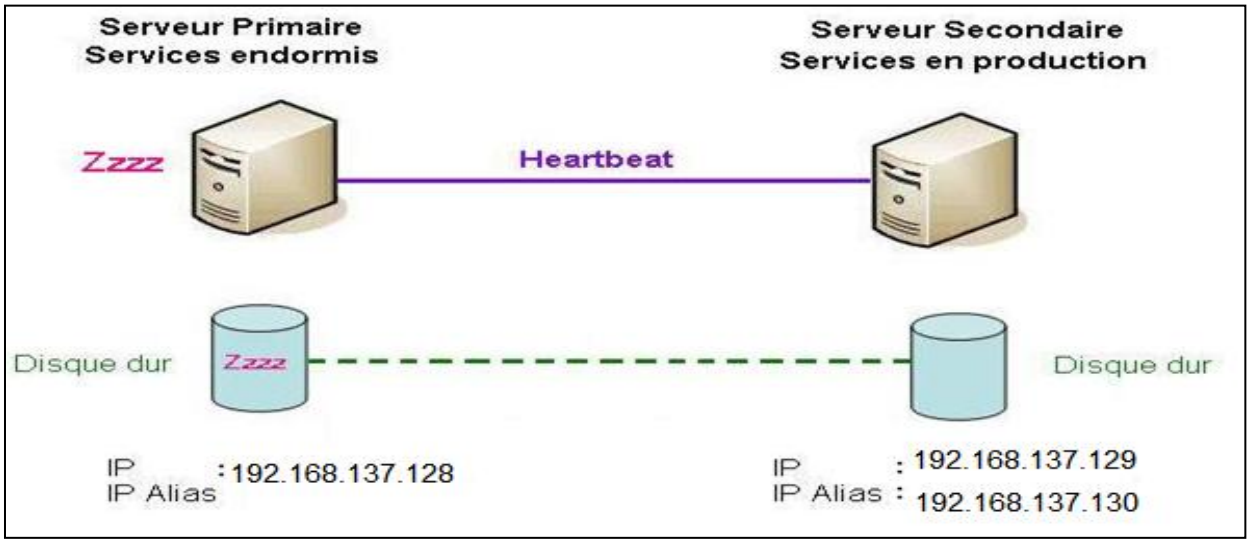


Figure 68:Fonctionnement anormal de réplication de données

DRBD va faire du Raid 1 sur les 2 serveurs. Heartbeat va vérifier la disponibilité des services et des disques. Si le serveur principal tombe, Heartbeat bascule le serveur secondaire en mode primaire. Dès que le serveur en panne revient, il devra resynchroniser son contenu avec le serveur primaire. Tout se passe sans interruption de service et en arrière-plan.

En conclusion, couplé avec Heartbeat, DRBD permet d'obtenir un cluster haut disponibilité.

3. Mise en place de la solution VPN :

Une des meilleures solutions pour crypter le trafic entre le client SIP et le serveur VoIP, est l'implémentation d'un VPN. Un VPN permet de véhiculer du trafic crypté grâce à des clés de cryptage ce qui rend leur déchiffrage presque impossible par une tierce partie. Un VPN permettra donc de contourner les attaques d'écoute clandestine. L'outil que nous avons choisi pour la mise en place d'un VPN est OpenVPN qui est un logiciel « open source » qui permet à des pairs de s'authentifier entre eux à l'aide d'une clé privée partagée à l'avance, de certificats ou de couples de noms d'utilisateur/mot de passe, il utilise la bibliothèque Open SSL ainsi que le protocole SSLv3/TLSv1.

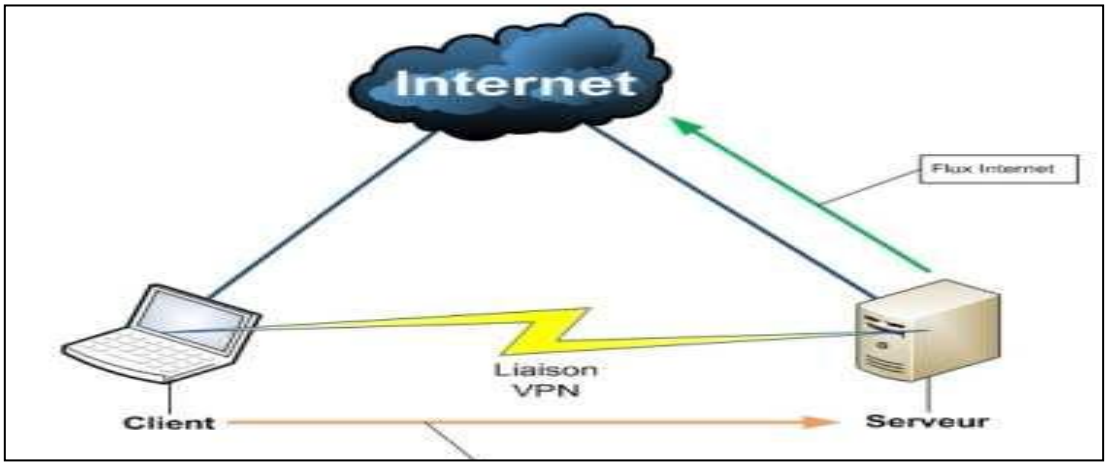


Figure 69: la liaison VPN entre le serveur VoIP et son Client

OpenVPN n'utilise pas de protocole de communication standard, il faut donc utiliser un client pour se connecter à un serveur OpenVPN.

Installation d'OpenVPN :

Tout d'abord il faut s'assurer que l'interface tun/tap est activé, pour vérifier cela on exécute la commande cat /dev/net/tun, si cette interface est bien installée on aura un message de ce type :« File descriptor in bad state ».Puis on ajoute les paquets EPEL, et on exécute la commande : *yum install OpenVPN* pour installer OpenVPN directement.

```
[root@localhost ~]#  wget http://download.fedoraproject.org/pub/epel/5/i386/epel
-release-5-4.noarch.rpm
--2015-06-04 18:09:08--  http://download.fedoraproject.org/pub/epel/5/i386/epel-
release-5-4.noarch.rpm
Résolution de download.fedoraproject.org... 85.236.55.6
Connexion vers download.fedoraproject.org|85.236.55.6|:80...connecté.
requête HTTP transmise, en attente de la réponse...302 Found
Emplacement: http://mirror.wbs.co.za/fedora-epel/5/i386/epel-release-5-4.noarch.
rpm [suivant]
--2015-06-04 18:09:09--  http://mirror.wbs.co.za/fedora-epel/5/i386/epel-release
-5-4.noarch.rpm
Résolution de mirror.wbs.co.za... 41.213.81.21
Connexion vers mirror.wbs.co.za|41.213.81.21|:80...connecté.
requête HTTP transmise, en attente de la réponse...200 OK
Longueur: 12232 (12K) [application/octet-stream]
Saving to: `epel-release-5-4.noarch.rpm'

100%[======================================>] 12 232      28,1K/s    in 0,4s
```

Tout d'abord on va dans le dossier *easy-rsa* et on édite le fichier *vars* pour modifier les valeurs des variables d'environnement afin de ne pas avoir à répéter les renseignements à fournir à la génération des clés comme indiqué dans la figure ci -dessous :

```
[root@localhost 2.0]# vi /etc/openvpn/easy-rsa/2.0/vars
export KEY_EXPIRE=3650

# These are the default values for fields
# which will be placed in the certificate.
# Don't leave any of these fields blank.
export KEY_COUNTRY="US"
export KEY_PROVINCE="CA"
export KEY_CITY="SanFrancisco"
export KEY_ORG="Fort-Funston"
export KEY_EMAIL="me@myhost.mydomain"
export KEY_OU="MyOrganizationalUnit"
```

Nous passons maintenant à la création des certificats, mais tout d'abord il faut commencer par la gestion de la clé privée de l'autorité de certification.

```
[root@localhost 2.0]# ./build-ca
Generating a 2048 bit RSA private key
.....................................................+++
.....................................................................
+++
writing new private key to 'ca.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [US]:
```

Ensuite on crée le certificat pour le serveur grâce à la commande suivante :

```
[root@localhost 2.0]# ./build-key-server server
Generating a 2048 bit RSA private key
..+++
.................+++
writing new private key to 'server.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
```

Maintenant il faut créer le certificat pour le client.

```
[root@localhost 2.0]# ./build-key vpnclient1
Generating a 2048 bit RSA private key
.........+++
.....................................................................
.....................................................+++
writing new private key to 'vpnclient1.key'
```

A présent, il reste à créer les paramètres Diffie-Hellman (D-H) qui est un algorithme permettant la génération de clés secrètes à travers des canaux non sécurisés. La commande de création est la suivantes :

```
[root@localhost 2.0]# ./build-dh
Generating DH parameters, 2048 bit long safe prime, generator 2
This is going to take a long time
.................+.....................+.................................
.....+.....................................................................
.....................................................................
.....................................................................
.................+.....................................................
.....................................++*++*
[root@localhost 2.0]#
```

La création des clés et certificats d'authentification est terminée, nous allons passer à la configuration du serveur et des clients. Afin de configurer au mieux le serveur et les clients, il est nécessaire de préparer le terrain. Il faut copier l'ensemble des informations vers le répertoire /etc/openvpn crée par défaut à l'installation d'OpenVPN.

```
[root@localhost 2.0]# cd /etc/openvpn
[root@localhost openvpn]# cp keys/* /etc/openvpn
```

Création d'un utilisateur OpenVPN

Maintenant on passe à la création d'un utilisateur ayant des droits restreints qui sera chargé de lancer le service de telle sorte que même si nous nous font pirater la machine, l'attaquant n'aura que les droits de cet utilisateur et pas avec les droits root. Il faut donc créer un groupe d'utilisateur.

```
[root@localhost 2.0]# cd /etc/openvpn
[root@localhost openvpn]#
```

Configuration du client :

Pour pouvoir se connecter à notre serveur VPN, il faut installer le client OpenVPN sur la machine ensuite il faut copier les fichiers qui se trouvent sous le répertoire /etc/openvpn du coté serveur (Ca.crt, Client.crt, Client.key, le fichier de configuration client.conf) .Voila maintenant le réseau VPN est prêt à être utiliser entre le serveur Asterisk et ces clients.

La mise en route du serveur entraine l'attribution automatique d'une adresse ip à l'interface tun0 du serveur. Contrairement au serveur vpn, il est possible de définir une plage d'ip disponibles pour l'attribution des ip clients, précisément chaque ip pour chaque client. Pour ce faire il faut modifier les paramètres suivants :

- Dev tun

Pour pouvoir utiliser OpenVPN en mode tunnel.

- Server 192.168.0.0 255.255.255.0 :80

Nous donnerons cette plage par défaut au serveur. A chaque fois qu'un client se connectera au vpn, le serveur lui attribuera une adresse IP contenue dans cette plage.

- User openvpn / group openvpn

Entrons ensuite le nom d'utilisateur et son groupe openvpn qu'on a crée pour lancer le serveur. Au final, le serveur est prêt à être utilisé, il faut maintenant passer à la configuration du coté du client.

4. Protection Asterisk avec fail2ban :

Fail2ban est un logiciel libre qui lit les logs de divers services (SSH, Apache, FTP, ...) à la recherche d'erreur d'authentification répétée où autres, et effectue des actions telles que l'ajout de règles pour bannir l'adresse IP de la source ou l'envoie de mail afin d'informer d'un mauvais fonctionnement du service.Nos serveurs se faisant constamment attaquer par des attaques de type brute force, nous avons décidé de mettre en place fail2ban pour le protocole SIP sur nos serveurs Asterisk, ceci pour des raisons évidentes de sécurité mais également pour la qualité de notre système. Développé en langage

Python, Fail2Ban est un logiciel libre permettant d'analyser des fichiers de logs et de déclencher des actions si certaines choses suspectes sont détectées.

La grande force de Fail2Ban est sa grande modularité que cela soit au niveau des mécanismes de détections basées sur les expressions régulières ou sur les actions à mener qui peuvent aller de l'expédition d'un mail à la mise en place de règles de Firewall. On commence par l'installation.

Fail2Ban sur son système, qui se fait grâce à la commande suivante :

```
[root@localhost ~]# yum install fai2ban
Loaded plugins: fastestmirror, kmod
Loading mirror speeds from cached hostfile
 * addons: mirror.crazynetwork.it
 * base: mirror.crazynetwork.it
 * commercial-addons: elastix.cjp.mx
 * elastix-base: elastix.cjp.mx
 * elastix-extras: elastix.cjp.mx
 * elastix-updates: elastix.cjp.mx
 * epel: mirrors.coreix.net
 * extras: mirror.crazynetwork.it
 * updates: mirror.crazynetwork.it
```

Ensuite il faut installer python iptables :

```
[root@localhost ~]# yum install phthon iptables
Loaded plugins: fastestmirror, kmod
Loading mirror speeds from cached hostfile
 * addons: mirror.crazynetwork.it
 * base: mirror.crazynetwork.it
 * commercial-addons: elastix.cjp.mx
 * elastix-base: elastix.cjp.mx
 * elastix-extras: elastix.cjp.mx
 * elastix-updates: elastix.cjp.mx
 * epel: mirrors.coreix.net
 * extras: mirror.crazynetwork.it
 * updates: mirror.crazynetwork.it
```

On crée le fichier : /etc/fail2ban/filter.d/asterisk.conf , et on y insére les définitions suivantes:

```
[root@localhost src]# nano /etc/fail2ban/filter.d/asterisk.conf
  GNU nano 1.3.12                          Fichier : /etc/fail2ban/filter.d/asterisk.conf

# Fail2Ban configuration file
#
#
# $Revision: 250 $
#
[INCLUDES]

# Read common prefixes. If any customizations available -- read them from
# common.local
#before = common.conf
[Definition]

#_daemon = asterisk

# Option: failregex
# Notes.: regex to match the password failures messages in the logfile.
The
# host must be matched by a group named « host ». The tag « <HOST> » can
# be used for standard IP/hostname matching and is only an alias for
# (?:::f{4,6}:)?(?P<host>\S+)
# Values: TEXT
#

failregex = SECURITY.* SecurityEvent= »FailedACL ».*RemoteAddress=
».+?/.+?/<HOST>/.+? ».*
SECURITY.* SecurityEvent= »InvalidAccountID ».*RemoteAddress=
».+?/.+?/<HOST>/.+? ».*
SECURITY.* SecurityEvent= »ChallengeResponseFailed ».*RemoteAddress=
».+?/.+?/<HOST>/.+? ».*
SECURITY.* SecurityEvent= »InvalidPassword ».*RemoteAddress=
».+?/.+?/<HOST>/.+? ».*

# Option: ignoreregex
# Notes.: regex to ignore. If this regex matches, the line is ignored.
# Values: TEXT
#
ignoreregex =
```

Éditons le fichier /etc/fail2ban/jail.conf et ajoutons ceci dans la liste des jails :

```
  GNU nano 1.3.12                                  Fichier : /etc/fail2ban/jail.con

[asterisk-iptables]
enabled = true
filter = asterisk
action = iptables-allports[name=ASTERISK, protocol=all]
sendmail-whois[name=ASTERISK, dest=root, sender=fail2ban@votredomen.org]
logpath = /var/log/asterisk/messages
maxretry = 2
findtime = 60000
bantime = 259200
```

Il est aussi important de configurer les paramètres suivants :

- maxretry : Le nombre de tentative authorisée avant de bloquer l'IP

-bantime : Le temps en seconde de la durée du banissement.

Maintenant on doit modifier la configuration du logger d'asterisk pour des raisons de compatibilité de format de date. Editons donc le fichier /etc/asterisk/logger.conf et décommentons la ligne date format comme ceci :

```
[general]
;
dateformat=%F %T ; ISO 8601 date format

#include logger_general_additional.conf
#include logger_general_custom.conf

[logfiles]
;debug => debug
security => security
console => notice,warning,error
messages => security,notice,warning,error
#include logger_logfiles_additional.conf
#include logger_logfiles_custom.conf
```

Puis on relance le logger asterisk via la commande shell suivante :

```
[root@localhost src]# asterisk -rx " logger reload"
[root@localhost src]#
```

Démarrons Fail2ban et iptables :

```
[root@localhost src]# /etc/init.d/iptables start
[root@localhost src]# /etc/init.d/fail2ban start
Starting fail2ban:                                         [  OK  ]
[root@localhost src]#
```

Une ip bannie par fail2ban est totalement bloquée sur tous les ports et on souhaite la libérer, on exécute cette commande :

iptables –D fail2ban-NOM_SERVICE–s -j DROP

Vérification :

```
[root@localhost src]# fail2ban-client status
Status
|- Number of jail:      1
`- Jail list:           ssh-iptables
```

fail2ban est un outil très puissant bien qu'il soit léger, une configuration assez rapide permet de protéger efficacement notre serveur VoIP en cas d'attaque brute force.

5. Implémentation d'un firewall Netfilter :

Netfilter est un module qui permet de filtrer et de manipuler les paquets réseau qui passent dans le système. Il fournit à Linux des fonctions de pare-feu et notamment le contrôle des machines qui peuvent se connecter, sur quels ports, de l'extérieur vers l'intérieur, ou de l'intérieur vers l'extérieur du réseau, de traduction d'adresse (NAT) pour partager une connexion internet (masquerading), masquer des machines du réseau local, ou rediriger des connexions, d'historisation du trafic réseau.

Dans le cadre de notre projet le firewall va nous permettre de minimiser le trafic entrant au serveur Asterisk est cela pour limiter les attaques de types DoS. En effet notre objectif est de n'autoriser que le trafic VoIP et plus exactement les paquets basés sur le protocole SIP et le protocole RTP, qui sont utilisés par notre serveur Asterisk pour le trafic VoIP. Dans la démonstration suivante nous avons configuré notre firewall pour qu'il puisse laisser passer seulement le trafic VoIP au niveau du serveur Asterisk et de bloquer tous le trafic restant.

```
[root@localhost ~]# iptables -A INPUT -p  udp -m udp --dport 5060 -j ACCEPT
[root@localhost ~]# iptables -A INPUT -p  udp -m udp --dport 10000:20000 -j ACCEPT
[root@localhost ~]# iptables -A INPUT -p  UDP -j DROP
[root@localhost ~]#
```

En ce qui concerne le trafic TCP on peut limiter la réception des requêtes de synchronisation à une requête par secondes, ainsi nous pouvons éviter les attaques de type SYN flood.

```
[root@localhost ~]# iptables -A INPUT -p  tcp --syn -m limit --limit 1/s -j ACCEPT
[root@localhost ~]#
```

VI. Conclusion :

Au long de ce chapitre, nous avons simulé plusieurs scenarios d'attaques contre notre maquette VoIP, et nous avons implémenté une panoplie d'outils permettant la sécurité de notre infrastructure. Pourtant il est important de savoir qu'il est impossible d'avoir une sécurité parfaite au niveau du réseau VoIP.

CONCLUSION GENERALE :

La sécurité de la VoIP est un problème capitale, bien que trop souvent délaissé pour diminuer les couts d'investissements, et qui pose des problèmes qui ne sont pas toujours simples à résoudre.

L'objectif de mon projet est la mise en place d'une solution open source sécurisée pour les services voix, pour cela, j'ai utilisé le logiciel Asterisk qui possède des fonctionnalités puissantes lui permettant de s'imposer dans l'avenir, j'ai étudié et pratiqué également une panoplie d' outils de sécurité tournant sous une plateforme Linux visant à mettre en œuvre la solution VOIP proposée .

J'ai entamé le sujet par une étude théorique ciblée et concise pour comprendre les protocoles, les architectures, et le fonctionnement de la technologie VoIP.

Puis, j'ai procédé à une étude comparative de différentes solutions open source disponibles sur le marché afin de choisir la solution la plus adaptée à High- Tech Service.

Ensuite, j'ai étudié les attaques qui peuvent compromettre le serveur VoIP et mis en œuvre les solutions de sécurité nécessaires remédiant à ces attaques.

L'intérêt de mon projet réside dans le fait que les entreprises, bénéficiant de cette solution, seront capables de mettre en place une plateforme de VoIP assez flexible, peu couteuse, et protégée contre les attaques de l'intérieur du réseau comme de l'extérieur.

Mon stage de fin d'études au sein de High-tech Service, qui a duré quatre mois était une expérience fructueuse, qui m'a permis d'acquérir de très bonnes connaissances technique (la VoIP et sa sécurité) et de me familiariser avec le milieu professionnel sans oublier une nette progression personnel.

LIMITATIONS ET PERSPECTIVES :

Limitations :

Notre projet nécessite plus de raffinement pour satisfaire aux mieux les attentes des entreprises.

Faute des moyens je ne suis pas arrivée à installer et configurer le serveur Asterisk Elastix pour fonctionner avec des téléphones analogiques et des Smartphones.

Perspectives :

Plusieurs extensions sont possibles, pour rendre notre solution plus efficace en termes de fonctionnalité et de sécurité.

En effet je propose l'utilisation d'un SDI tel que Snort pour détecter les intrusions visant le serveur Linux et le serveur VOIP.

Il serait très intéressant aussi d'utiliser les mécanismes d'équilibrage de charge et de restauration (Back-up) afin d'assurer la disponibilité et les performances adéquates pour notre solution VOIP.

BIBLIOGRAPHIE

REFERENCE :

- [1] G711 :. Page de l'ITU sur la norme G.711 https://fr.wikipedia.org/wiki/G.711
- [2] G722 : Page de l'ITU sur le G.722 : https://fr.wikipedia.org/wiki/G.722
- [3] G723.1 : VoiceAge Corporation (2007-10-14). "G.723.1 Licensing". Archived from the original on 2007-10-14. Retrieved 2009-09-17.https://en.wikipedia.org/?title=G.723.1
- [4] G729 : La recommandation G.729 sur le site de l'Union Internationale des Télécommunications https://fr.wikipedia.org/wiki/G.729
- [5] H323 : Davidson, Jonathan; James Peters; Jim Peters; Brian Gracely. "H.323". Voice over IP fundamentals. Cisco Press. pp. 229–230. ISBN 978-1-57870-168-1. https://en.wikipedia.org/wiki/H.323
- [6] RTP : Daniel Hardy (2002). *Network*. De Boeck Université.: https://en.wikipedia.org/wiki/Real-time_Transport_Protocol
- [7] RTCP : https://fr.wikipedia.org/wiki/Real-time_Transport_Control_Protocol
- [8] Gigue : Par Roger Hockaday* | Lundi 17 Mai 2004 Lundi 17 Mai 2004 http://www.zdnet.fr/actualites/voip-convergence-et-qualite-de-service-39153207.htm
- [9] DOS : About Demetrius Turner . http://www.websitepulse.com/blog/voip-ddos-attacks
- [10] IP flooding : M. Ali Akbar http://www.researchgate.net/publication/257482125_Securing_SIP
- [11] UDP flooding : CERT Advisory CA-1996-01 UDP Port Denial-of-Service Attack https://en.wikipedia.org/wiki/UDP_flood_attack
- [12] Dos type cancel : http://www.computerhope.com/breakhlp.htm
- [13] Dos type BYE : http://www.memoireonline.com/09/13/7361/m_Etude-dimplementation-dune-solution-VOIP-securisee-dans-un-reseau-informatique-dentrepr44.html
- [14] Sniffing : http://searchunifiedcommunications.techtarget.com/tip/How-to-get-a-Wireshark-VoIP-packet-capture
- [15] Intégrité : https://fr.wikipedia.org/wiki/Int%C3%A9grit%C3%A9
- [16] Authentification :*www.securite-informatique.gouv.fr* (consulté le 5 octobre 2010) https://fr.wikipedia.org/wiki/Authentification
- [17] whois : http://www.nirsoft.net/whois_servers_list.html
- [18] wireshark : Gordon Lyon / Nmap http://www.filehorse.com/download-nmap/
- [19] Nmap : Gordon Fyodor Lyon, Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning, Nmap Project,2009 https://fr.wikipedia.org/wiki/Nmap

BIBLIOGRAPHIE :

Les livres de référence :

Asterisk The Future of Telephony (O'Reilly)

TrixBox Made Easy (PACKT)

Hacking Exposed VoIP: David Endler et Mark Collier (McGraw-Hill/Osborne)

Les sites web de référence :

www.ietf.org/html.charters/sip-charter.html

www.sipforum.org

www.sipcenter.com

http://dumbme.voipeye.com.au/trixbox/

http://nerdvittles.com/

http://nerdvittles.com/

http://www.voip-info.org/wiki/

http://www.counterpath.com/

http://www.counterpath.com/

Les sites de référence sur SIP :

www.cs.columbia.edu/~hgs/sip/

www.ietf.org/html.charters/sip-charter.html

www.sipforum.org

www.sipcenter.com

Toute la documentation sur Asterisk

http://www.asterisk.org/

Manuel sur la VoIP

http://www.voip-info.org/wiki/

Manuel utilisation backtrack :

http://www.backtrack-linux.org/wiki/index.php/Pentesting_VOIP

Authentication Server: Setting up FreeRADIUS :

http://www.tldp.org/HOWTO/8021X-HOWTO/freeradius.html

http://www.it-connect.fr/autoriser-le-ssh-via-iptables/

http://people.via.ecp.fr/~alexis/asterisk/

http://fr.wikipedia.org/wiki/Asterisk_(logiciel)

http://www.journaldunet.com/expert/systemes-reseaux/38838/toip---voip---mythe-ou-realite-pour-les-pme.shtml

ANNEXE:

- **Configuration d'Asterisk :**

La configuration de base comporte au minimum les fichiers **asterisk.conf** et **extensions.conf**. Les sources sont dans différents fichiers en fonction de leur type: mgcp.conf, iax.conf, **sip.conf** (protocoles) .

asterisk.conf

Par défaut on positionne certains chemins de base au fonctionnement du moteur asterisk, la présence de ce fichier n'est pas obligatoire, mais voici un exemple de contenu:

astetcdir => /etc/asterisk
astmoddir => /usr/lib/asterisk/modules
astvarlibdir => /var/lib/asterisk
astagidir => /var/lib/asterisk/agi-bin
astspooldir => /var/spool/asterisk
astrundir => /var/run/asterisk
astlogdir => /var/log/asterisk

- **sip.conf**

Le fichier **sip.conf**, va définir l'ensemble de nos utilisateurs. Pour connaitre l'ensemble des fonctions utilisables, rendez-vous sur le site http://www.asteriskguru.com/tutorials/ et également sur le site http://www.voip-info.org/ Nous éditons le fichier sip.conf (avec Vi, par exemple). A la fin du fichier nous allons créer deux utilisateurs ainsi :

```
[general]
port = 5060

[100]
username=100
type=friend
secret=123
host=dynamic
context=dsi
language=fr
callerid="Ray" <100>

[200]
username=200
type=friend
secret=123
host=dynamic
context=dsi
language=fr
callerid="Anatole" <200>
```

Chaque client sera défini par un label, nous utilisons par défaut l'extension. Comme chaque fichier de configuration, une section initiale est globale, ensuite viennent toutes les sections variables.

- **extensions.conf**

Le fichier **extensions.conf** permet de définir les règles de routage c'est-à-dire les actions à faire lors d'un appel sur un numéro de téléphone.
Dans le contexte *dsi*, nous définissons comment joindre les différents postes. Chaque extension de notre plan de numérotation interne va être interprété et acheminé vers des liens physiques (IAX ou SIP dans notre cas).

```
[tsrite]
exten => 100,1,Dial(SIP/100)
exten => 200,1,Dial(SIP/200)
```

Les commandes utilisées pour la définition des extensions ont la forme suivante :

exten => <extension>,<priorité>,<application(paramètres)>

- extension : numéro composé pour contacter Asterisk. Ce paramètre peut également prendre la valeur d'une extension prédéfinie par Asterisk (a, i, s, t, etc.). Afin d'obtenir un complément d'information sur ces extensions prédéfinies veuillez consulter le site : www.voip-info.org/wiki-Asterisk+standard+extensions

- priorité : permet de définir l'ordre dans lequel plusieurs commandes pour une même extension vont être exécutées. La priorité la plus élevée est 1, puis on incrémente de 1 pour la priorité des commandes suivantes (1, 2, 3, etc.)

- application : permet de définir l'action à réaliser pour l'extension en cours. La totalité des commandes peuvent être consultées sur le site : www.voip-info.org/wiki-Asterisk+-+documentation+of+application+commands).

L'application Dial est utilisée pour l'acheminement de l'appel dans le contexte dsi, le premier argument passé est la ligne préfixée par son type (IAX2 ou SIP).

Démarrage du serveur

Pour démarrer automatiquement votre serveur Asterisk au démarrage de la machine, vous devez enregistrer la commande au démarrage de votre serveur (a l'aide de WebMin ?) :

```
/usr/sbin/safe_asterisk
```

Vous pouvez également démarrer depuis la console, en tapant la commande :

```
asterisk -vvvc
```

Une fois le serveur "démarré", vous pouvez vous connecter à la console en tapant la commande :

```
asterisk -r
```

Cette commande ne démarre pas le serveur, elle vous permet juste de vous reconnecter sur la console une fois le serveur déjà lancé !

Commandes du serveur

Pour connaître l'ensemble des commandes du serveur, vous pouvez taper : help, une fois connecté à la console Asterix

Ceci dit, voici quelques commandes utiles : A chaque modification du fichier sip.conf, vous devez exécuter la commande "sip reload" pour recharger le fichier

A chaque modification du fichier extensions.conf, vous devez exécuter la commande "extensions reload" pour recharger le fichier.

Pour recharger l'ensemble du serveur, tapez la commande : reload
Pour connaître l'ensemble des "peers" connectés (vos utilisateurs SIP), tapez : sip show peers

- **Commande utilisé :**

System	
setup	Permet d'effectuer les configurations primaires du système (Fuseau horaire, Type clavier, .etc.)
install-netconfig	Réinstallation de netconfig (Centos 5.1 enlève l'outil lors de l'installation)
netconfig	Configuration des interfaces réseau Ethernet
status	Donne une vue d'ensemble de l'état du système
install-key	Création de nouvelles clés d'encryptions pour le serveur
setup-mail	Configuration de sendmail
setup-tftp	Installation et configuration du serveur tftp
setup-samba	Mise en place de samba, partage de fichiers Windows sous Linux
Mise à jour	
update-source	Mise à jour d'Asterisk directement du site de Digium
update-scripts	Mise à jour des Scripts et des menus d'aide associés
update-fixes	Mise à jour de PIAF
yum -y update	Mise à jour des composants du système d'exploitation Centos.
Services & redémarrage	
amportal restart	Redémarrage de Freepbx à la suite de changement des configurations. Il est à noter que certains changements impliquent le redémarrage du système d'exploitation.
service asterisk restart	Redémarrage du service Asterisk.
service network restart	Redémarrage du service réseau.
shutdown now	Fermeture du système
shutdown –r now	Redémarrage du système
Sécurité	
passwd-master	Changement des mots de passe pour freepbx, webmin, maint, amp et meetme
passwd-maint	Changement du mot de passe pour maint, l'interface graphique web
passwd-wwwadmin	Changement du mot de passe pour wwwadmin
passwd-meetme	Changement du mot de passe pour l'interface graphique web MeetMe
passwd-webmin	Changement du mot de passe pour l'interface graphique web de webmin
passwd-ari	Changement du mot de passe d'administration ARI
passwd	Changement du mot de passe pour la session (root et autres utilisateurs)
enable-iptables	Activation de IPTABLES (doit être paramétrées)
disable-iptables	Désactivation de IPTABLES (pour certains problèmes avec Freepbx)
enable-fail2ban	Activation du moniteur de sécurité IP
disable-fail2ban	Désactivation du moniteur de sécurité IP
Asterisk	
asterisk –rvvvv	Donne accès à la console de ligne de commande d'Asterisk. (Command Line Interface = CLI).
sip reload	Recharge la configuration SIP à partir de la ligne de commande CLI d'Asterisk
Configuration dispositifs et interfaces Asterisk	

install-ZAPHFC	Install les interfaces pour ISDN/RDSI – QuadBRI DuoBRI & HFC Chipset
genzaptelconf	Reconfiguration des pilotes Zaptel
setup-aastra	Création de la configuration aastra.cfg dans le répertoire /tftpboot
setup-cisco	Création de la configuration SIPDefault.cnf dans le répertoire /tftpboot
setup-grandstream	Mise en place de l'auto configuration pour Grandstream
setup-linksys	Création de la configuration Linksys dans le répertoire /tftpboot
setup-polycom	Création de la configuration Polycom dans le répertoire /tftpboot
Installation composants Asterisk	
install-a2billing	Mise en place de A2Billing, une plate-forme de facturation
instal-munin	Installation des rapports munin

Tableau 8 : Commande utilisé :

Chiffrement RSA :

Le chiffrement RSA (nommé par les initiales de ses trois inventeurs) est un algorithme de cryptographie asymétrique, très utilisé dans le commerce électronique, et plus généralement pour échanger des données confidentielles sur Internet. Cet algorithme a été décrit en 1977 par Ronald Rivest, Adi Shamir et Leonard Adleman. RSA a été breveté1 par le Massachusetts Institute of Technology (MIT) en 1983 aux États-Unis. Le brevet a expiré le 21 septembre 2000.

Théorème des restes chinois:

Le théorème des restes chinois : est un résultat d'arithmétique modulaire traitant de résolution de systèmes de congruences. Ce résultat, établi initialement pour $\mathbb{Z}/n\mathbb{Z}$, se généralise en théorie des anneaux. Ce théorème est utilisé en théorie des nombres.

Méthode des éléments finis :La méthode des éléments finis fait partie des outils de mathématiques appliquées. Il s'agit de mettre en place, à l'aide des principes hérités de la formulation vibrationnelle ou formulation faible, un algorithme discret mathématique permettant de rechercher une solution approchée d'une équation aux dérivées partielles (ou ÉDP) sur un domaine compact avec conditions aux bords et/ou dans l'intérieur du compact. On parle couramment de conditions de type Dirichlet (valeurs aux bords) ou Neumann (gradients aux bords) ou de Robin (relation gradient/valeurs sur le bord).

Il s'agit donc avant tout de la résolution approchée d'un problème, où, grâce à la formulation vibrationnelle, les solutions du problème vérifient des conditions d'existence plus faibles que celles des solutions du problème de départ et où une discrétisation permet de trouver une solution approchée. Comme de nombreuses autres méthodes numériques, outre l'algorithme de résolution en soi, se posent les questions de qualité de la discrétisation :

existence de solutions,

unicité de la solution,

stabilité,

convergence,