

الجمهورية الجزائرية الديمقراطية الشعبية

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

وزارة التعليم العالي والبحث العلمي

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

جامعة أبي بكر بلقايد - تلمسان

Université Aboubakr Belkaïd – Tlemcen –

Faculté de TECHNOLOGIE



MEMOIRE

Présenté pour l'obtention du **diplôme de MASTER**

En : Télécommunications

Spécialité : Réseaux Mobiles et Services de Télécommunications

Par : BENDELHOUM Selma Lila

Sujet

Développement d'un serveur SIP pour la Voix sur IP

Soutenu publiquement, le 13 / 06 / 2017, devant le jury composé de :

M. BOUABDALLAH Réda	MAA	Univ. Tlemcen	Président
M. MERAD BOUDIA Omar Rafik	MCB	Univ. d'Oran	Directeur de mémoire
M. FEHAM Mohammed	Prof.	Univ. Tlemcen	Co-directeur de mémoire
M. BEMMOUSSAT Chemseddine	MCB	Centre Univ. Temouchent	Examinateur

Dédicaces

Je dédie ce mémoire à :

Mes parents :

Ma mère, qui s'est consacré pour ma réussite, de par son amour, son soutien, tous les sacrifices consentis et ses précieux conseils, pour toute son assistance et sa présence au cours de ma vie, doit recevoir à travers ce travail aussi modeste soit-il, l'expression de mes sentiments de reconnaissance et de mon éternelle gratitude.

Mon père, qui peut être fier et trouver ici le résultat de longues années de sacrifices et de privations pour m'aider à avancer dans la vie. Puisse Dieu faire en sorte que ce travail porte son fruit ; Merci pour les valeurs nobles, l'éducation et le soutien permanent et la confiance reçus de lui.

Mes frères et sœurs qui n'ont cessé d'être à mes côtés.

Mes ami(e)s de la promotion RMS7 2016-2017

Mes professeurs de l'Université Aboubakar BELKAD de Tlemcen qui doivent trouver dans ce travail l'accomplissement d'avoir transmis un savoir bien acquis.

Remerciements

Ce travail n'aurait pas connu son accomplissement sans l'apport de certaines personnes. Je ne pouvais m'empêcher d'exprimer ma reconnaissance aux :
Président et membres du jury, pour leur disponibilité, malgré leurs multiples occupations.

Monsieur FEHAM.

Monsieur MERAD BOUDIA Omar Rafik

Mes chers parents.

Mes frères et sœurs.

Mes chers amis.

Je voudrais aussi transmettre mes remerciements les plus sincères à :

Messieurs M.FEHAM et O.R. MERAD BOUDIA mes tuteurs de projet pour leurs précieuse contribution pédagogique qui a favorisé le couronnement de ce travail.

Mes vifs remerciements également à l'égard de toute ma famille et à ceux qui, de près ou de loin, m'ont soutenu à travers leurs contributions multiformes dans l'élaboration et la rédaction de ce projet.

J'adresse enfin, mes remerciements à tous mes collègues de classe, à tous ceux de ma promotion pour leur franche collaboration durant ces trois années.

TABLE DES MATIÈRES

Introduction général.....	1
Chapitre I : étude générale de la voix sur IP	
I.1 Introduction	3
I.2 Présentation de la Voix sur IP (VoIP)	3
I.2.1 Définition	3
I.2.1.1 Internet Protocol (IP).....	3
I.2.1.2 La voix sur IP (VoIP).....	3
I.2.1.3 PABX.....	4
I.2.2 Fonctionnement.....	5
I.2.2.1 Acquisition du signal.....	6
I.2.2.2 Numérisation	6
I.2.2.3 Compression	6
I.2.2.4 Habillage des en-têtes	6
I.2.2.5 Emission et transport.....	6
I.2.2.6 Réception.....	6
I.2.2.7 Conversion numérique analogique	6
I.2.2.8 Restitution.....	6
I.2.3 Avantages.....	6
I.2.4 Inconvénients.....	7
I.3 Protocoles de la Voix sur IP.....	8
I.3.1 Le protocole SIP.....	8
I.3.1.1 Serveur Registrar.....	9
I.3.1.2 Location Serveur.....	9
I.3.1.3 Serveur Proxy.....	9
I.3.1.4 Serveur Redirect	10
I.3.1.5 Fixation d'un compte SIP	10
I.3.2 Le protocole H323.....	11
I.3.2.1 Pile protocolaire	11
I.3.2.2 Application de l'H323	11
I.3.2.3 Comparaison entre H.323 et SIP.....	12
I.3.3 Les protocoles de transport	13
I.3.3.1 Le protocole RTP	13
I.3.3.2 Le protocole RTCP	13
I.3.3.3 Le protocole ICMP	14
I.3.3.4 Le protocole UDP.....	14
I.3.3.5 Le protocole SRTP	14
I.4 Asterisk	15
I.4.1 Définition	15
I.4.2 Fonctionnalités	15
I.4.3 Le protocole IAX	16
I.5 Conclusion	18

Chapitre II : Installation et configuration d'une solution de VoIP basée sur l'outil Asterisk

II.1 Introduction	20
II.2 Installation d'Asterisk	20
II.3 Configuration d'Asterisk et création des comptes utilisateurs	21
II.3.1 Configuration des comptes users	21
II.3.2 Configuration du Dialplan	23
II.4 Installation et configuration de Zoiper	24
II.5 Conclusion	27

Chapitre III : Vulnérabilités contre la VOIP et quelques moyens de Sécurisation

III.1 Introduction	29
III.2 Les attaques protocolaires	29
III.2.1 Spam	29
III.2.1.1 Call Spam	29
III.2.1.2 IM (Instant Message) Spam	29
III.2.1.3 Présence Spam	29
III.2.2 Suivie des appels	29
III.2.3 Voice phishing (phishing via VoIP)	30
III.2.4 Le sniffing	30
III.2.5 Déni de service	30
III.2.6 Compromission de serveurs	30
III.2.7 Les interceptions illégales d'appels	31
III.3 Les attaques sur les couches basses	31
III.3.1 ARP spoofing	31
III.3.2 MITM : Man-In-The-Middle : écoute passive ou modification de flux	31
III.4 Les vulnérabilités de l'infrastructure	32
III.4.1 Les téléphones IP	32
III.4.2 Vulnérabilités de la confidentialité et l'intégrité de la VOIP	33
III.4.3 Vulnérabilités de disponibilité de la VOIP	33
III.4.4 Vulnérabilités des navigateurs	33
III.5 Sécuriser le SIP d'un serveur Asterisk	33
III.6 Sécurisation du système et de l'application	35
III.6.1 Sécurisation d'application	35
III.6.2 Le Firewall	35
III.6.3 La Protection d'Intrusion	35
III.6.4 IPTABLE	35
III.6.5 L'authentification des clients	36
III.6.6 IDS systems	36
III.6.7 Rate limiting	36

III.6.8 Bloquer les attaques courantes	36
III.6.9 Protection contre les attaques ARP	37
III.7 Conclusion	38

Chapitre IV : Sécurisation de la VoIP

IV.1 Introduction	40
IV.2 Systèmes de détection d'intrusions	40
IV.2.1 Les serveurs Whois	40
IV.2.2 Aspirateur de site HTTrack	41
IV.3 logiciels de tests d'intrusion	41
IV.3.1 Wireshark	41
IV.3.1.1 Téléchargement de Wireshark	41
IV.3.1.2 Lancement du wireshark	42
IV.3.2 John The Ripper	45
IV.3.2.1 Installation de john	45
IV.3.2.2 Configuration de john	46
IV.4 solutions pour sécuriser le serveur	47
IV.4.1 Crypter le mot de passe avec MD5	47
IV.4.2 IPsec.....	49
IV.4.2.1 Installer les outils	49
IV.4.2.2 Configuration pour une authentification par clé partagée.....	49
IV.4.2.3 Cacher le fichier conf au public.....	51
IV.4.2.4 Lancer la mise à jour	51
IV.4.2.5 Vérifier les modifications	51
IV.4.3 Fail2Ban	53
IV.4.3.1 Installation de fail2ban	53
IV.4.3.2 Autorisation de l'IP de la machine	53
IV.4.3.3 Modification du logger d'asterisk	53
IV.4.3.4 Création du fichier filtre	53
IV.4.3.5 Création de la prison (jail)	54
IV.4.3.6 Lancement de Fail2Ban	55
IV.5 Conclusion	56
Conclusion général.....	57

Introduction générale

Depuis quelques années, la technologie VoIP commence à intéresser les entreprises, surtout celles de service comme les centres d'appels. La migration des entreprises vers ce genre de technologie n'est pas pour rien. Le but est principalement de minimiser le coût des communications, utiliser le même réseau pour offrir des services de données, de voix, et d'images.

Cette approche facilite l'adoption du téléphone IP surtout dans les grandes sociétés possédant une plateforme classique et voulant bénéficier de la voix sur IP. Mais elle ne permet pas de bénéficier de tous les services et la bonne intégration vers le monde des données.

Certaines attaques sur les réseaux VoIP, comme les attaques de déni de service, et les vols d'identités, peuvent causer des pertes catastrophiques et énormes pour les entreprises. Pour cela la sécurité du réseau VoIP n'est pas seulement une nécessité mais plutôt une obligation, avec laquelle on peut réduire au maximum le risque d'attaques sur les réseaux VoIP.

Ce travail entre dans le cadre d'un Projet National de Recherche (PNR) dont l'objectif est de sécuriser les communications mobiles (Data et Voix) sur la VoIP. Le projet est divisé en deux parties, une partie concerne le serveur dont fait l'objet ce mémoire et une autre partie client dont fait l'objet un autre projet de fin d'études.

La partie dont fait l'objet ce mémoire consiste en la création et la sécurisation d'un serveur SIP pour la voix sur IP en utilisant Asterisk. Un serveur qui se charge de relayer les messages SIP pour établir, contrôler et terminer la session entre les clients SIP distants. Nous allons aussi identifier les problèmes de sécurité de la VoIP en général et d'un serveur SIP en particulier et enfin proposer des solutions.

Ce mémoire est structuré comme suit : Dans le premier chapitre, nous présentons des généralités autour de la technologie de la VOIP. Le second chapitre détaille les étapes à suivre pour l'installation et la configuration d'un serveur SIP sous Asterisk. Le troisième chapitre concerne la thématique de sécurité au niveau de la VOIP et enfin nous présentons des solutions de sécurité dans le quatrième chapitre.

Chapitre I

Etude générale de la voix sur

IP

I.1 Introduction

La VoIP n'est pas réellement une nouvelle technologie ; des documents et brevets portant sur le sujet sont datés de plusieurs décennies et les premiers logiciels de VoIP étaient déjà disponibles en 1991. Actuellement, la VoIP est l'un des services de télécommunications les plus performants et les plus dynamiques basés sur une suite de protocoles Internet. La VoIP permet aux utilisateurs d'utiliser Internet comme moyen de transmission pour la communication vocale. L'objectif de ce chapitre est de présenter des généralités autour de cette technologie. Nous commencerons par définir la VoIP et présenter son principe de fonctionnement. Ensuite, nous présentons des protocoles VoIP de signalisation et de transport ainsi que leurs principes de fonctionnement et de leurs principaux avantages et inconvénients.

I.2 Présentation de la Voix sur IP (VoIP)

I.2.1 Définitions

I.2.1.1 Internet Protocol (IP)

Internet Protocol (abrégé en IP) introduit par Vint Cerf et Bob Kahn en 1974, est une famille de protocoles de communication de réseaux informatiques conçus pour être utilisé sur Internet. Les protocoles IP sont au niveau 3 dans le modèle OSI comme le montre la figure I.1. Les protocoles IP s'intègrent dans la suite des protocoles Internet et permettent un service d'adressage unique pour l'ensemble des terminaux connectés [1].

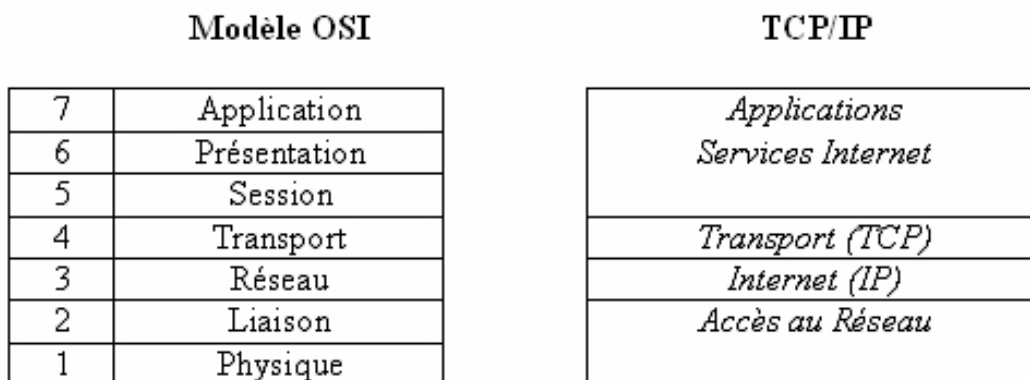


Figure I.1 Le modèle OSI et TCP/IP [1]

I.2.1.2 La Voix sur IP (VoIP)

La VoIP, raccourci de voix par le protocole internet, est aussi connue sous le terme de VoIP est la technologie qui permet aux gens d'utiliser Internet comme moyen de transmission pour les communications vocales. Le protocole Internet (IP) a été conçu à l'origine pour la gestion

de réseaux de données puis après son succès, le protocole a été adapté à la gestion de la voix en transformant et transmettant l'information en paquet de données IP. Depuis sa création, des progrès énormes ont été réalisés et maintenant VoIP bénéficie d'une popularité répandue en tant que solution de rechange à la téléphonie traditionnelle dans les maisons et les entreprises. La VoIP est à présent disponible sur de nombreux smartphones, ordinateurs et tablettes [2]. Cette technologie est complémentaire de la téléphonie sur IP (« ToIP » pour Telephony over Internet Protocol). La ToIP concerne les fonctions réalisées par un commutateur téléphonique PABX.



Figure I.2 Equipements nécessaires pour utiliser la VoIP [3]

I.2.1.3 PABX

PABX ou PBX sont l'acronyme de **P**riate **A**utomatic **B**ranch **E**Xchange, ce qui correspond à un commutateur téléphonique privé utilisé dans les entreprises. Les utilisateurs d'un système téléphonique basé sur un PABX partagent un nombre de lignes externes pour effectuer des appels téléphoniques vers l'extérieur de l'entreprise Figure I.2.

Un PABX connecte les postes internes d'une entreprise mais il les connecte aussi au réseau public téléphonique commuté (RTC), voir Figure I.3. Une des dernières tendances dans le développement de PABX est le PBX-VoIP, appelé également IPBX, qui utilise le protocole Internet pour transmettre les appels [3].

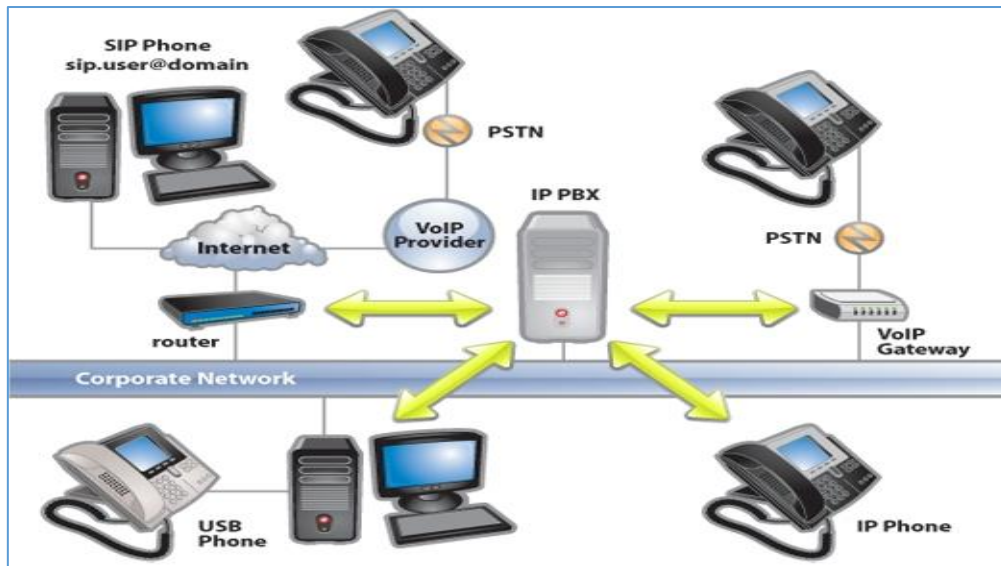


Figure I.3 le fonctionnement d'un PABX [3]

IPBX ou IP PABX est un système téléphonique PBX logiciel qui accomplit certaines tâches et offre des services qu'il peut être difficile et onéreux de mettre en œuvre en utilisant un PBX traditionnel de marque propriétaire. Le 3CX Phone System pour Windows est un bon exemple de IPBX .

I.2.2 Fonctionnement

Le principe est la numérisation de la voix, c'est-à-dire le passage d'un signal analogique à un signal numérique, voir Figure I.4. Les étapes sont comme suit [4] :

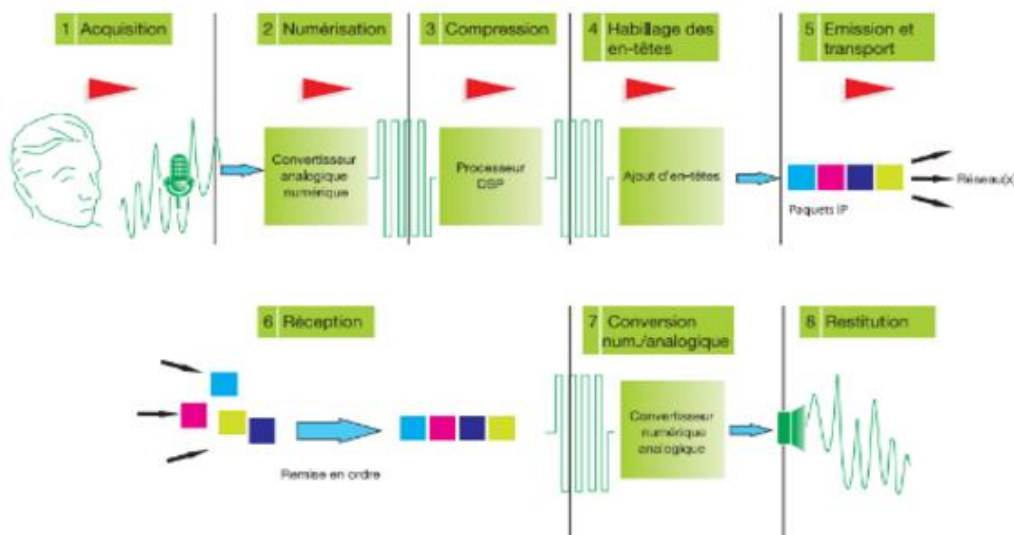


Figure I.4 Les étapes de la VoIP [4]

I.2.2.1 Acquisition du signal

La première étape consiste naturellement à capter la voix à l'aide d'un micro, qu'il s'agisse de celui d'un téléphone ou d'un micro-casque.

I.2.2.2 Numérisation

La voix passe alors dans un convertisseur analogique numérique qui réalise deux tâches distinctes :

- Echantillonnage du signal sonore : un prélèvement périodique de ce signal
- Quantification : qui consiste à affecter une valeur numérique à chaque échantillon.

Plus les échantillons sont codés sur un nombre de bits importants, meilleure sera la qualité.

I.2.2.3 Compression

Le signal une fois numérisé peut être traité par un DSP (Digital Signal Processor) qui va le compresser, c'est-à-dire réduire la quantité d'informations nécessaires pour l'exprimer.

L'avantage de la compression est de réduire la bande passante nécessaire pour transmettre le signal.

I.2.2.4 Habillage des en-têtes

Les données doivent encore être enrichies en informations avant d'être converties en paquets de données à expédier sur le réseau.

I.2.2.5 Emission et transport

Les paquets sont acheminés depuis le point d'émission pour atteindre le point de réception sans qu'un chemin précis soit réservé pour leur transport.

I.2.2.6 Réception

Lorsque les paquets arrivent à 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.

I.2.2.7 Conversion numérique analogique

La conversion numérique analogique est l'étape réciproque de l'étape 2.

I.2.2.8 Restitution

Dès lors, la voix peut être retranscrite par le haut-parleur du casque, du combiné téléphonique ou de l'ordinateur.

I.2.3 Avantages

La voix sur IP a un grand nombre de prestations et avantages.

- **Docilité** : l'acheminement de l'aboutissement actuel vers la téléphonie sur IP peut donc être pratiqué en douceur. L'afflux facilite l'intégration avec le système d'information et simplifie l'infrastructure.
- **Coûts plus bas** : Les services VoIP sont moins chers que les services téléphoniques standards et dans de nombreux cas ils sont gratuits. Cela est particulièrement utile pour les appels interurbains internationaux. D'un autre côté, la mise en place de la

téléphonie IP permet de limiter et même d'éliminer les coûts et la complexité associés aux utilisateurs ayant à se déplacer, car ceux-ci adhèrent à tous les services du réseau partout où ils peuvent s'y connecter.

- **Portabilité :** VoIP peut être consulté partout où vous pouvez accéder à Internet. Idéal pour les utilisateurs à mobilité élevée. Ce qui accorde de maximiser les ressources et mieux les manier afin de réaliser des économies substantielles sur l'administration et l'infrastructure.
- **De nombreuses fonctionnalités :** VoIP offre de nombreuses fonctionnalités qui ne sont pas couramment retrouvées dans le téléphone traditionnel : appel à plusieurs parties, appel en attente / transfert, identification de l'appelant et blocage de l'ID de l'appelant, pour n'en nommer que quelques-uns. Egalement aussi la gestion des trois réseaux (voix, données et vidéo) par l'unique transport IP.

I.2.4 Inconvénients

Malgré ses nombreux avantages, la VoIP n'est pas exempte de certains inconvénients dont il est important d'avoir connaissance avant de s'engager auprès d'un FAI (un fournisseur d'accès à Internet).

- **Qualité de service :** Le service VoIP est sensible à la gigue, aux retards, à l'écho et à d'autres retards de qualité causés par de nombreux facteurs, du matériel, de la connexion Internet à la destination de l'appel.
- **La sécurité :** Les téléphones VoIP sont sensibles aux attaques virales, comme tout autre dispositif Internet, les vols d'identité, le spamming ou encore les attaques phishing sont autant d'inconvénients qui peuvent également nuire à leur fonctionnement.
- **Dépendance énergétique :** contrairement aux lignes téléphoniques traditionnelles, le modem, le routeur, le PC et tout autre matériel VoIP dépendent d'une alimentation électrique. Sans électricité, aucun des susmentionnés ne pourrait travailler.

Les inconvénients liés à la technologie VOIP sont donc limités et peuvent trouver des solutions visant à les amoindrir voir à les faire disparaître.

I.3 Protocoles de la Voix sur IP (VoIP)

I.3.1 Le protocole SIP

Le protocole SIP (Session Initiation Protocol) est, comme son nom l'indique un protocole d'initialisation de sessions multimédias voir Figure I.5 [5]. C'est un protocole jeune mais qui a le "vent en poupe" car soutenu par bon nombre d'industriels qui travaillent à son élaboration et

à son développement. C'est le protocole qui devrait être retenu pour l'établissement des communications types visioconférence sur UMTS (mobiles de troisième génération).

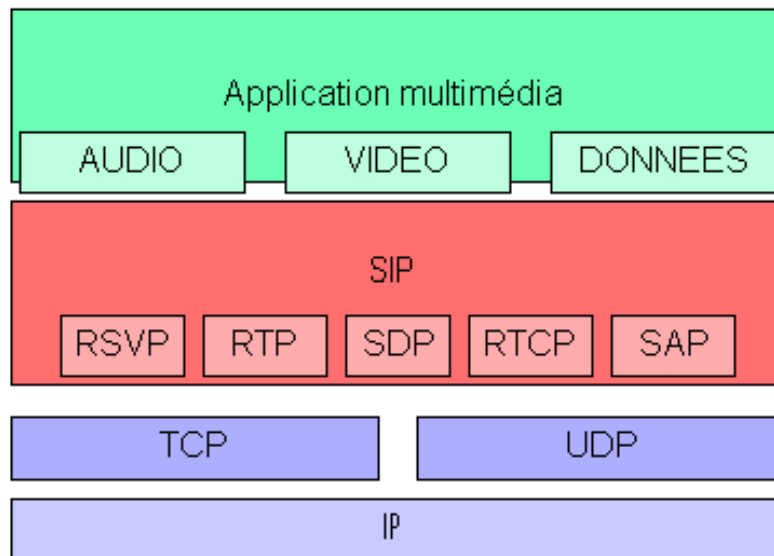


Figure I.5 Protocole de la couche Application du modèle OSI [5]

SIP est un protocole de signalisation appartenant à la couche application du modèle OSI. Son rôle est d'ouvrir, modifier et libérer les sessions ou appels ouverts entre un ou plusieurs utilisateurs. Il se charge de l'authentification et de la localisation des multiples participants mais 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 données et de protocoles peut être utilisé pour cet échange. Cependant, le protocole RTP (Real-time Transport Protocol) assure le plus souvent les sessions audio et vidéo.

Il faut savoir que le protocole SIP est pour l'instant moins utilisé que le protocole H.323 car il est beaucoup plus récent. Mais il se développe très rapidement et sa simplicité de mise en œuvre lui confère un réel avantage. La plupart des grands constructeurs travaillent maintenant sur ce protocole. Le fait de travailler sur ce protocole a aussi été une des raisons de notre choix de projet car c'est un protocole prometteur qui s'insère parfaitement dans le mouvement émergent de convergence des réseaux téléphonique vers les réseaux IP.

I.3.1.1 Serveur Registrar

Afin de pouvoir joindre une personne à partir de son adresse SIP, une entité dans le réseau doit maintenir une correspondance (mapping) entre les adresses IP et les adresses SIP : c'est le rôle du serveur Registrar. Un utilisateur peut donc changer d'adresse, il lui suffit de s'inscrire auprès du Registrar en lui indiquant son adresse SIP et son adresse de machine sur le réseau.

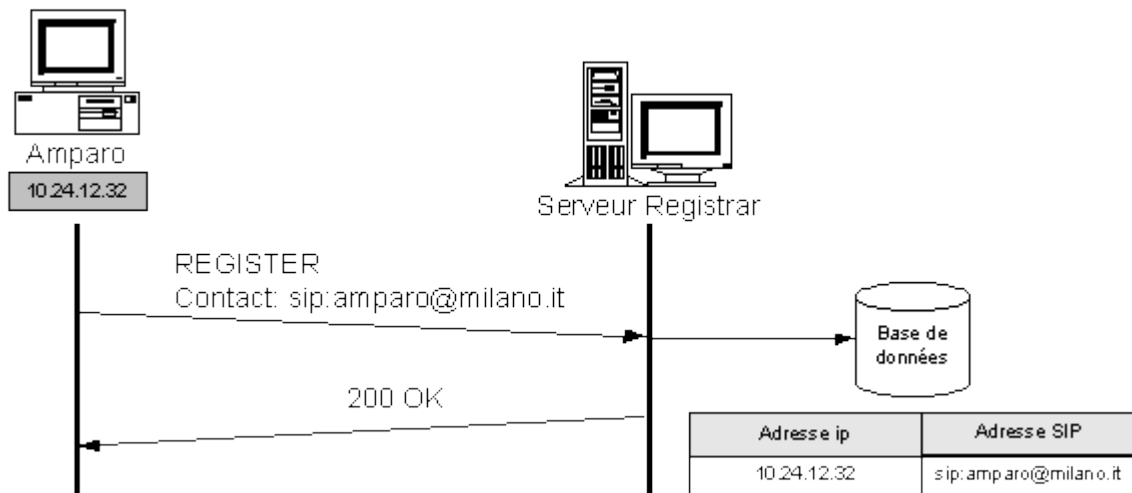


Figure I.6 Exemple d'enregistrement SIP [5]

La Figure I.6 montre l'enregistrement du terminal d'Amparo sur un serveur Registrar. A la réception du message REGISTER, le serveur Registrar a accès à l'adresse IP de la source, Amparo, dans l'en-tête IP du message. Il enregistre alors la correspondance entre cette adresse IP et l'adresse SIP donnée dans le champ « Contact : », soit ici « sip:amparo@milano.it ».

I.3.1.2 Location Serveur

Lorsqu'une entité SIP souhaite joindre un correspondant à partir de son adresse SIP, elle est renseignée par le Location server qui accède à la base d'information renseignée et tenue à jour par le Serveur Registrar [5].

I.3.1.3 Serveur Proxy

Un serveur proxy a la charge de router les messages SIP. Il a uniquement un rôle dans la signalisation et il ne gère pas de medias. Il n'est en général à l'origine d'aucune requête excepté la requête CANCEL utilisée pour libérer une session pendante [5].

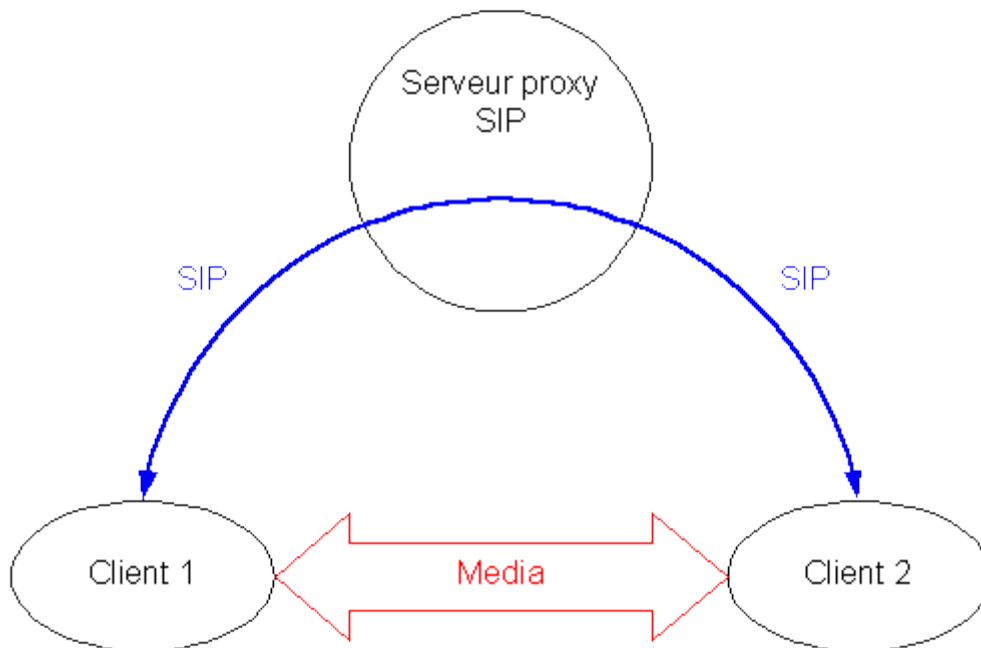


Figure I.7 Représentation schématique des flux SIP et des flux media lors de l'utilisation d'un serveur proxy [5]

Cette figure schématise, dans le cas de l'établissement d'une session grâce à un serveur proxy, la séparation de la partie signalisation et de la partie flux media. Le proxy peut se contenter de router les messages SIP vers l'opérateur sélectionné. Le « dialogue » SIP fournira aux deux terminaux (celui du client1 et celui du client2) les données nécessaires à l'établissement d'une session de media entre eux. Ces données sont entre autres leurs adresses IP respectives, les ports et les formats de codages utilisés. Les deux terminaux peuvent alors s'envoyer des flux média sans passer par le serveur proxy ce qui en allège la charge.

I.3.1.4 Serveur Redirect

Les serveurs Redirect aident à localiser les User Agent SIP en fournissant une adresse alternative à laquelle l'utilisateur appelé peut-être joint.

Lorsqu'une requête lui parvient, il retourne une réponse de redirection contenant la ou les prochaines adresses à contacter pour joindre le destinataire final [5].

I.3.1.5 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 un utilisateur d'un service de voix sur IP dispose d'un compte SIP et que chaque fois qu'il redémarre son ordinateur, son adresse IP change, il doit cependant toujours être joignable. Son compte SIP doit donc être associé à un serveur SIP (proxy SIP) dont l'adresse IP est fixe. Ce serveur lui allouera un compte et il permettra d'effectuer ou de recevoir des

appels quelques soit son emplacement. Ce compte sera identifiable via son nom (ou pseudo).

I.3.2 Le protocole H323

Il est devenu nécessaire de créer des protocoles capables de supporter l'arrivée des technologies du multimédia sur les réseaux, tel que la visioconférence : l'envoi de son et de vidéo avec un souci de données temps réel. Le protocole H.323 en fait donc partie. Il permet entre autres de faire de la visioconférence sur des réseaux IP.

H.323 regroupe un ensemble de protocoles Figure I.8 pour le transport et la configuration de la voix, de l'image et de data sur IP. C'est un protocole dérivé du protocole H.320 utilisé sur RNIS [6].

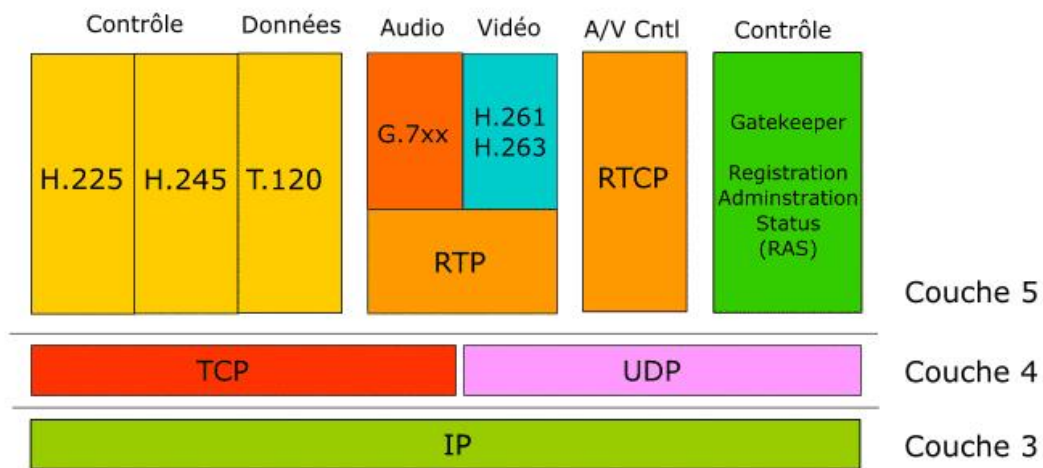


Figure I.8 le protocole H.323 [6]

I.3.2.1 Pile protocolaire

H.323 est un regroupement de plusieurs protocoles qui concernent trois catégories distinctes : la signalisation, la négociation de codecs et le transport de l'information.

Le transport de l'information s'appuie sur le protocole RTP 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.

I.3.2.2 Application de l'H323

L'H.323 est un standard fournissant une base pour la communication utilisant de l'audio, de la vidéo, et des données à travers les réseaux IP. Il permet de faire inter opérer des applications multimédia entre elles sans souci de compatibilité. H.323 est utilisé dans tous types d'applications destinés aux particuliers et aux entreprises. Il est utilisé par un grand nombre

d'opérateurs qui proposent du triple-play qui s'impose très largement sur le marché des télécommunications avec le passage sur la VoIP des systèmes téléphoniques depuis la téléphonie classique (sur lien RTC) et RNIS (Numéris).

I.3.2.3 Comparaison entre H.323 et SIP

Une comparaison entre SIP et H.323 de quelques caractéristiques de chacun d'eux est présentée dans le tableau 1.1.

	H.323	SIP
Philosophie	<p>La norme H.323, développé par l'IUT-T, est utilisée pour l'interactivité en temps réel (échange audio, vidéo, données, contrôle et signalisation).</p> <p>C'est la norme la plus utilisée concernant la VoIP. Elle hérite de la norme H320 utilisée pour la voix sur RNIS. Comme toute norme, elle est constituée d'un ensemble de protocoles réalisant les différentes fonctions nécessaires à la communication.</p>	<p>Contrairement à la norme H323, SIP (Session Initiation Protocol) est un protocole unique de type requête/réponse très proches des protocoles HTTP et SMTP. Il commence à prendre le pas sur la norme H323. SIP est normalisé par l'IETF (RFC 3261).</p> <p>Il permet de créer et gérer des sessions entre participants pour échanger des données indépendamment de leur nature et du protocole de transport.</p>
Inspiration	Téléphonie	HTTP
Nombres d'échanges pour établir la connexion	6 à 7 aller-retour	1 à 5 aller-retour
Complexité	Elevée	Faible
Adapté à Internet	Non	Oui
Protocoles de transport	TCP	TCP ou UDP
Avantages	<ul style="list-style-type: none"> - Maturité du protocole (Version 4) - Beaucoup de constructeurs utilisent H323 	<ul style="list-style-type: none"> - Interopérabilité très bonne - Bonne gestion de la mobilité

Inconvénients	<ul style="list-style-type: none"> - Manque d'interopérabilité entre les différentes implémentations - Difficultés avec les FireWall - Support des fonctions avancées de la téléphonie très complexe 	<ul style="list-style-type: none"> - En pleine maturation - Problème avec la translation d'adresses
----------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------

Tableau 1.1. Comparaison entre SIP et H.323 [7].

I.3.3 Les protocoles de transport

I.3.3.1 Le protocole RTP :

Le but de RTP (Real-time Transfert Protocol) est de fournir un moyen uniforme de transmettre sur IP des données soumises à des contraintes de temps réel (audio, vidéo, ...). Le rôle principal de RTP consiste à mettre en œuvre des numéros de séquence de paquets IP pour reconstituer les informations de voix ou vidéo même si le réseau sous-jacent change l'ordre des paquets. Plus généralement, RTP permet d'identifier le type de l'information transportée, d'ajouter des marqueurs temporels et des numéros de séquence l'information transportée et de contrôler l'arrivée à destination des paquets. De plus, RTP peut être véhiculé par des paquets multicast afin d'acheminer des conversations vers des destinataires multiples [8].

I.3.3.2 Le protocole RTCP :

Le protocole RTCP (Real-time Transfert Control Protocol) est basé sur des transmissions périodiques de paquets de contrôle par tous les participants dans la session. C'est un protocole de contrôle des flux RTP, permettant de véhiculer des informations basiques sur les participants d'une session, et sur la qualité de service.

Le protocole RTCP demande aux participants de la session d'envoyer périodiquement les informations citées ci-dessus. La périodicité est calculée en fonction du nombre de participants de l'application. On peut dire que les paquets RTP ne transportent que les données des utilisateurs. Tandis que les paquets RTCP ne transportent en temps réel, que de la supervision [8].

Parmi les principales fonctions qu'offre le protocole RTCP sont les suivants :

- Une synchronisation supplémentaire entre les médias : les applications multimédias sont souvent transportées par des flots distincts.
- L'identification des participants à une session : en effet, les paquets RTCP contiennent des informations d'adresses, comme l'adresse d'un message électronique, un numéro de téléphone ou le nom d'un participant à une conférence téléphonique.

- Le contrôle de la session : en effet le protocole RTCP permet aux participants d'indiquer leur départ d'une conférence téléphonique.

- On peut détailler les paquets de supervision en 5 types :

SR (Sender Report) : ce rapport regroupe des statistiques concernant la transmission (pourcentage de perte, nombre cumulé de paquets perdus, variation de délai (gigue), etc.). Ces rapports sont issus d'émetteurs actifs d'une session.

RR (Receiver Report) : ensemble de statistiques portant sur la communication entre les participants. Ces rapports sont issus des récepteurs d'une session.

SDES (Source Description) : Carte de visite de la source (nom, e-mail, localisation).

BYE : Message de fin de participation à une session.

APP : Fonctions spécifiques à une application

I.3.3.3 Le protocole ICMP :

Le protocole ICMP (Internet Control Message Protocol) est un protocole qui permet de gérer les informations relatives aux erreurs aux machines connectées. Etant donné le peu de contrôles que le protocole IP réalise, il permet non pas de corriger ces erreurs mais de faire part de ces erreurs aux protocoles des couches voisines. Ainsi, le protocole ICMP est utilisé par tous les routeurs, qui l'utilisent pour signaler une erreur (appelé Delivery Problem).

I.3.3.4 Le protocole UDP

Le protocole UDP (User Datagram Protocol) est un protocole non orienté connexion de la couche transport du modèle TCP/IP. Ce protocole est très simple étant donné qu'il ne fournit pas de contrôle d'erreurs (il n'est pas orienté connexion...).

Il ne sert qu'à « emballer » les paquets de contenus, en leur apportant les numéros de ports, voies logiques qui serviront à les orienter au sein de l'application [9].

I.3.3.5 Le protocole SRTP :

On peut se retrouver avec un réseau VoIP qui fonctionne correctement mais qui risque des problèmes de sécurité, comme par exemple : Deny of Service (DoS), écoute et analyse du trafic, usurpation d'identité et parodie, fraude. Donc pour ça on doit prendre nos précautions en utilisant des protocoles qui peuvent éliminer toute sorte de menace.

SRTP (Secure Realtime Transport Protocol) définit un profil de RTP (Real-time Transport Protocol), qui a pour but d'apporter la **confidentialité** (chiffrement : protection contre le replay de données RTP en unicast et multicast), l'**authentification** et l'**intégrité** des messages. SRTP a été conçu par une équipe d'experts d'IP et de la cryptographie travaillant pour Cisco et Ericsson.

Les protocoles SRTP et SRTCP (la version sécurisée de l'RTCP) peuvent être utilisés à la place de RTP et RTCP, l'utilisation des fonctions fournies, telles que le cryptage et l'authentification, restent optionnels. Elles peuvent être activées séparément, à l'exception de la fonction "message d'authentification" qui est indispensable avec SRTCP [8].

I.4 Asterisk

I.4.1 Définition

Asterisk est un projet démarré en 1999 par Mark Spencer [10]. Son objectif était alors de fournir à Linux un commutateur téléphonique complet et totalement libre. La VoIP sur Asterisk passe entre autre par la prise en charge d'un protocole standard, ouvert et très largement utilisé, le SIP (Session Initiation Protocol). SIP qui est un protocole très proche d'HTTP qui n'est pas limité à la voix seulement mais qui prend aussi en charge la vidéo et la messagerie instantanée d'un point de vue de fonctionnalité.

I.4.2 Fonctionnalités

Asterisk comprend un nombre très élevé de fonctions permettant l'intégration complète pour répondre à la majorité des besoins en téléphonie. Il permet de remplacer totalement, par le biais de cartes FXO/FXS, un PABX propriétaire, et d'y adjoindre des fonctionnalités de VoIP pour le transformer en PBX IP. Il permet également de fonctionner totalement en VoIP, par le biais de téléphones SIP ou IAX du marché. Enfin, des fonctionnalités de routage d'appel, menu vocal et boîtes vocales entre autres le placent au niveau des PBX les plus complexes. Au sein des grandes installations d'Asterisk, il est courant de déployer les fonctionnalités sur plusieurs serveurs [11].

Asterisk permet tout ce que l'on peut attendre d'un PABX moderne : La gestion des postes téléphonique sur IP locaux. Il peut s'agir de téléphones physiques mais aussi logiciels (ou Softphone) comme Ekiga ou Zoiper.

Asterisk implémente les protocoles H.323 et SIP .Figure I.9



Figure I.9 les interconnexions avec Asterisk [11]

I.4.3 Le protocole IAX

Le projet Asterisk a donné naissance à un second projet, appelé IAX (Inter Asterisk eXchange) Voir figure I.10. Celui-ci définit un protocole permettant l'interconnexion entre serveurs Asterisk, mais également la communication entre un client et un serveur Asterisk [12].

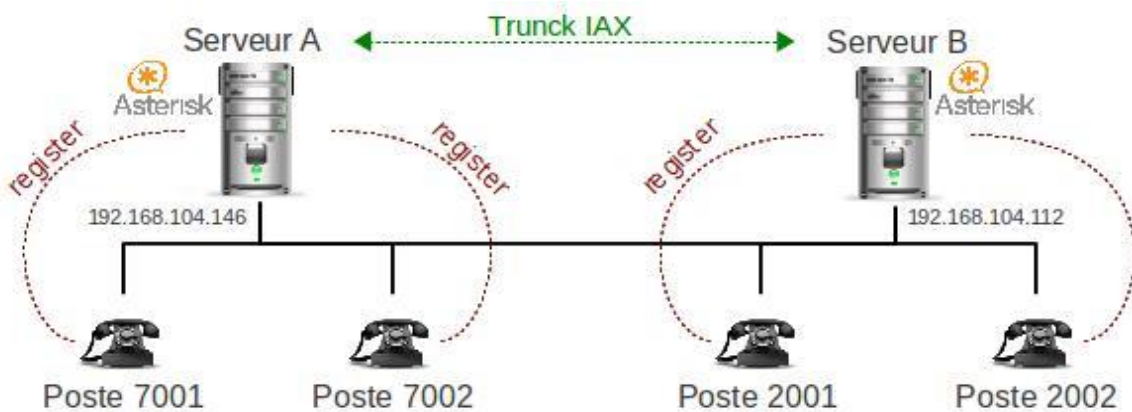


Figure I.10 le protocole IAX [13]

Initialement, le protocole IAX a été développé par le concepteur d'Asterisk Mark Spencer de la société Digium. Il est aujourd'hui maintenu par la société Digium et est disponible dans sa deuxième version IAX2, laquelle fait l'objet d'une proposition de normalisation à l'IETF.

Pour être convaincante dans un contexte où la concurrence entre les protocoles H.323 et SIP est déjà importante, la philosophie proposée par IAX diffère sur deux points importants :

Traversée transparente des passerelles NAT et des pare-feu. Contrairement aux protocoles SIP et H.323, qui n'assurent que la fonction de signalisation et se combinent généralement à RTP pour la fonctionnalité de transport des flux, le protocole IAX est à la fois un protocole de transport et un protocole de signalisation. Cela lui permet plus facilement de traverser les pare-feu et de supporter les translations d'adresses IP (NAT) dans un réseau. Ses flux n'utilisent qu'un port fixe et unique et peuvent de la sorte être aisément identifiés.

En général, IAX a été conçu spécifiquement pour le problème du transport et de la signalisation de la voix, en écartant les considérations plus générales des applications multimédias. Le protocole IAX répond ainsi à des objectifs simples et bien délimités. Bien qu'il n'exclue pas a priori le traitement de flux vidéo, il s'intéresse avant tout aux flux audio et optimise les paramètres des flux en tenant compte des contraintes et des spécificités de ces flux audio.

IAX est un protocole puissant, qui propose des solutions efficaces aux problèmes importants rencontrés par H.323 et SIP et permet les communications entre serveurs Asterisk. Il souffre toutefois de l'inconvénient de ne pas être normalisé. De plus, il n'optimise que le traitement des flux téléphoniques, alors que H.323 comme SIP sont plus généralistes et peuvent s'appliquer au transfert de la vidéo.

I.5 Conclusion

En analysant après l'étude de ce chapitre que, la VoIP est la solution la plus avantageuse pour effectuer des conversations. A présent il est évident que la VoIP va continuer à se mouvoir. La téléphonie IP est une bonne solution en matière d'intégration, fiabilité et de coût. Nous avons vu que la voix sur IP n'a pas encore de standard unique. Chaque standard possède ses propres caractéristiques pour garantir une fiabilité du service. Effectivement, le respect des empêchements temporels est le facteur le plus important lors du transport de la voix.

Dans le chapitre suivant, nous allons présenter en détail les étapes nécessaires à la création d'un serveur pour la VoIP en utilisant l'outil Asterisk.

Chapitre II

Installation et configuration d'une solution de VoIP basée sur l'outil Asterisk

II.1 Introduction

Aujourd'hui **Asterisk** est un PABX (Private Automatic Branch eXchange) qui est une entité logique, presque toujours gérée par un équipement matériel physique dont la fonction est au moins triple : router les appels au sein d'un réseau privé, interconnecter les réseaux et gérer les services de téléphonie. D'une rare puissance et souplesse, capable de gérer la téléphonie analogique, mais surtout, et c'est ce qui nous intéresse, la voix sur IP. Dans ce chapitre, nous allons créer un serveur SIP sous Asterisk pour la VoIP.

II.2 Installation d'Asterisk

Asterisk est un serveur de téléphonie open source permettant de disposer sur un simple PC les fonctions réservées aux PABX professionnel.

Les étapes pour l'installation sont comme suit :

-Mettre à jour notre distribution Linux et installer les dépendances nécessaires à la compilation d'**Asterisk**.

```
Sudo apt-get update &&apt-get upgrade
```

- Procédons ensuite à l'installation des dépendances

```
Sudo apt-getinstall build-essential libxml2-dev libncurses5-dev linux-headers-`uname -r`  
libsqlite3-dev libssl-dev
```

- Créer un dossier où nous allons placer les sources d'Asterisk

```
Sudo mkdir /usr/src/asterisk  
cd /usr/src/asterisk
```

- Télécharger la dernière version d'**Asterisk** et l'installer (Asterisk-13.14.0) via la commande
wget

```
Sudo wget http://downloads.asterisk.org/pub/telephony/asterisk/releases/asterisk-  
13.14.0tar.gz
```

- On aura besoin d'extraire les archives compressées qui contiennent le code source avec la commande tar

```
Sudo tar xvzf asterisk-13.14.0.tar.gz  
cd asterisk-13.14.0  
Sudo ./configure  
Sudo make menuselect
```

La commande **make menuselect** va nous permettre de personnaliser notre installation d'Asterisk

```
*****
Asterisk Module and Build Option Selection
*****

Press 'h' for help.

--> Add-ons (See README-addons.txt)
Applications
Bridging Modules
Call Detail Recording
Channel Event Logging
Channel Drivers
Codec Translators
Format Interpreters
Dialplan Functions
PBX Modules
Resource Modules
Test Modules
Compiler Flags
Voicemail Build Options
Utilities
AGI Samples
Module Embedding
Core Sound Packages
Music On Hold File Packages
Extras Sound Packages
```

Figure II.1 Menu du select

- Pour terminer l'installation :

```
Sudo make
```

```
Sudo make install
```

```
Sudo make samples
```

```
Sudo make config
```

Ainsi Asterisk est installé il suffit maintenant de lancer le serveur et de se connecter à la console CLI (Command Line Interface) via la commande :

```
Sudo /etc/init.d/asterisk start
```

```
Sudo Asterisk -cvvvvvvvvvvr
```

II.3 Configuration et création des comptes utilisateurs

II.3.1 Configuration des comptes users

- Pour la configuration des utilisateurs :

```
Sudo nano /etc/asterisk/sip.conf
```

Voici un exemple du fichier sip.conf avec deux utilisateurs **Rym BOUKARI** et **Rym BENDELHOUM** avec comme numéro SIP le **6001** et le **6002**.

```
[general]
hasvoicemail = yes
hassip = yes
hasiax = yes
callwaiting = yes
threewaycalling = yes
callwaitingcallerid = yes
transfer = yes
canpark = yes
cancallforward = yes
callreturn = yes
callgroup = 1
pickupgroup = 1
nat = yes
videosupport=yes
```

Figure II.2 la rubrique générale

```
[6001]
type=friend
host=dynamic
dtmfmode=rfc2833
disallow=all
allow=ulaw
fullname =Rym BOUKARI
username = rymbou
secret=secret
context = work
allow=h263p
allow=h264
allow=vp8
videosupport=yes
```

Figure II.3 Utilisateur 6001

```
[6002]
type=friend
host=dynamic
dtmfmode=rfc2833
disallow=all
allow=ulaw
fullname =Rym BENDELHOUM
username = rymben
secret=secret
context = work
allow=h263p
allow=h264
allow=vp8
videosupport=yes
```

Figure II.4 Utilisateur 6002

Explication :

[6001] , [6002] → Numéro SIP

type=friend → type d'objet SIP, friend = utilisateur

host=dynamic → Vous pouvez vous connecter à ce compte SIP à partir de n'importe quelle adresse IP

dtmfmode=rfc2833 → type de rfc utilisé

disallow=all → Désactivation de tous les codecs

allow=ulaw → Activation du codec µlaw

fullname = Rym BOUKARI , Rym BENDELHOUM → Prénom et NOM de l'utilisateur (ce qui sera affiché sur le téléphone lors d'un appel)

username = rymbou, rymben → Nom d'utilisateur

secret=secret → Mot de passe du compte SIP

context = work → Contexte (exploité par le fichier extensions.conf)

videosupport=yes, allow=h263p, allow=h264, allow=vp8 → autoriser la vidéo à fonctionner régulièrement.

II.3.2 Configuration du Dialplan

Sudo nano /etc/asterisk/extensions.conf : pour la configuration du **Dialplan**

```
[work]
exten => 6001,1,Dial(SIP/6001,20)
exten => 6002,1,Dial(SIP/6002,20)
exten => 6001,2,Hangup()
exten => 6002,2,Hangup()
```

Figure II.5 la rubrique extension

[Work] est le contexte, c'est une sorte de conteneur dans lequel les utilisateurs faisant partie de ce contexte pourront communiquer entre eux.

Lors de la création de nos deux utilisateurs nous avons spécifié le contexte work.

Exten : déclare l'extension (on peut aussi simplement dire numéros)

6001,6002 : Prend les extensions (ou numéros) 6001 et 6002

1 : Ordre de l'extension

Dial : application qui va être utilisée

SIP: Protocol qui va être utilisé

20: temps d'attente avant de passer à l'étape suivante.

Donc la ligne **exten => 6001(ou 6002), 1,Dial(SIP/6001(ou 6002),20)** se traduit par :

Quand on compose le numéro (par exemple) 6001, on appelle le numéro 6001 et si au bout de 20 secondes il n'y a pas de réponse on passe à la ligne du dessous.

La seconde ligne : **exten => 6001(ou 6002),2,Hangup()** permet de raccrocher si l n'y a pas de réponse au bout de 20 secondes.

Dans le cas général :

```
[work]
```

```
exten => _6XXX,1,Dial(SIP/${EXTEN},20)
```

```
exten => _6XXX,2,Hangup()
```

Après avoir configuré le contexte « Work » nous allons pouvoir effectuer un appel entre les deux utilisateurs sous Linux. Pour cela, nous avons utilisé Zoiper.

II.4 Installation et configuration de Zoiper

Zoiper est un Softphone, anciennement connu sous le nom Idefisk. Zoiper est un logiciel de téléphonie combinant une haute qualité de téléphonie et de vidéo intégrant les fax, les messages instantanés et une liste de contact intuitive.

L'installation sur Linux se fait comme suit :

- On télécharge Zoiper, puis on ouvre le Zoiper installé .tar.gz .

```
cd current-working-directory
```

- On choisit la version d'après notre machine

```
cd /home/slav/Downloads/Zoiper_3.2_Linux_Free_32Bit_64Bit
```

```
sudo ./Zoiper_3.2_Linux_Free_32Bit.run
```

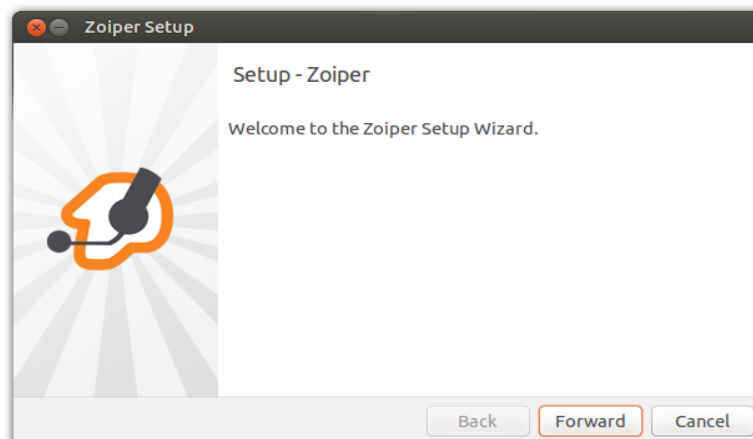


Figure II.6 configuration de Zoiper

Et pour la configuration on choisit les options qui nous conviennent jusqu'à avoir ceci :

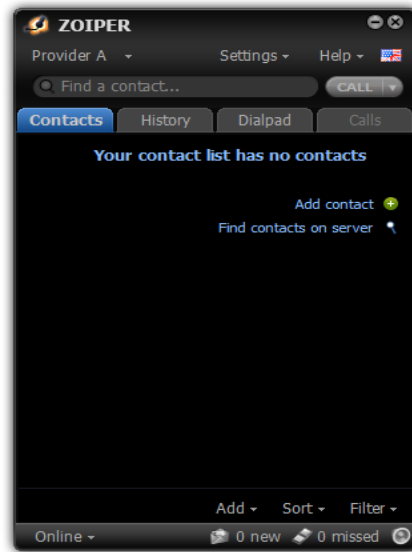


Figure II.7 l'Interface de Zoiper

- Pour tester la fonctionnalité, on doit créer des comptes SIP

Et chaque compte doit contenir :

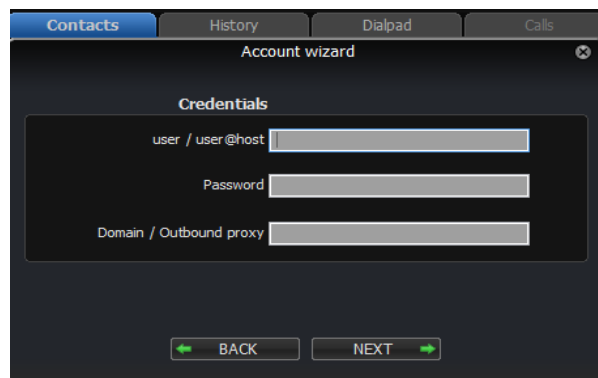


Figure II.8 les champs de chaque compte SIP

Exemple :

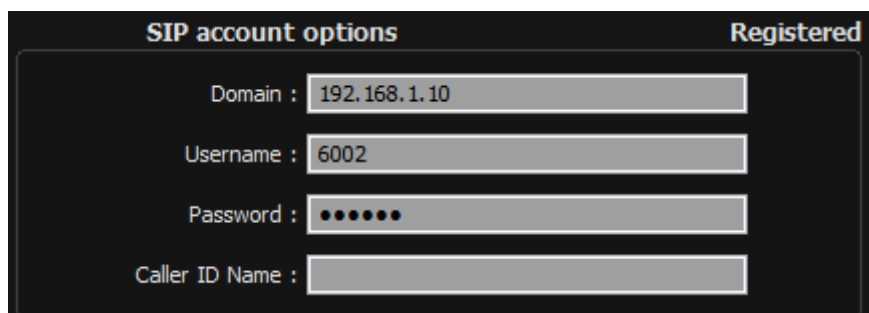


Figure II.9 Configuration du compte du client « 6002 »

Afin que l'authentification soit possible, ces valeurs doivent être conformes à celles saisies dans le fichier sip.conf du serveur Asterisk.

Et pour faire passer l'appel on doit écrire le SIP comme le montre la figure II.10 (on appelle 6002 depuis le 6001).



Figure II.10 Test d'appel entre 2 pc

Comme l'objectif de ce mémoire est de créer un serveur SIP pour la VoIP dédiée à la communication mobile, nous avons suivi les mêmes étapes de configuration citées précédemment et puis nous avons testé un appel entre deux smartphones comme le montre la figure suivante :

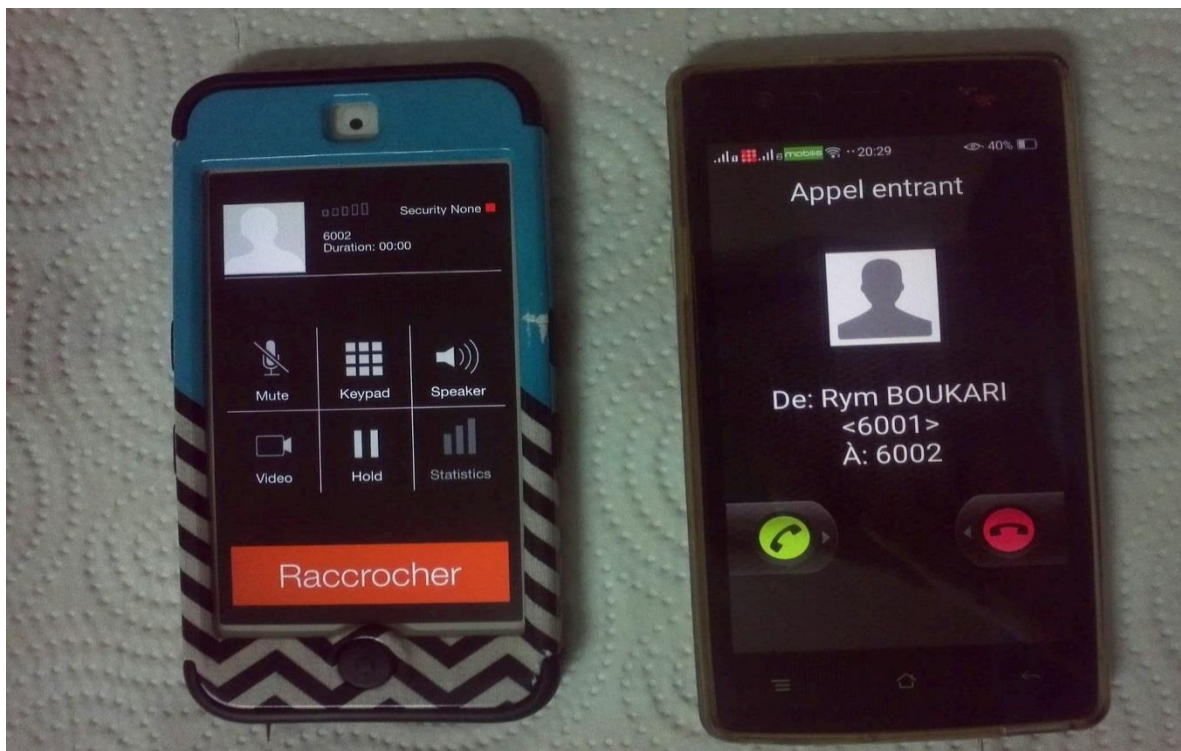


Figure II.11 test d'appel entre deux Smartphones

II.5 Conclusion

Cette partie du projet nous a permis d'appréhender et de bien comprendre le fonctionnement de la VoIP, le protocole SIP et aussi les principaux éléments de configuration d'un central de téléphonie aussi complet que peut l'être Asterisk. Asterisk a pour avantage qu'il est Open-source, gratuit et simple d'utilisation. Le projet est extrêmement puissant et ouvre des possibilités infinies à qui sait les exploiter. Cependant, en matière de sécurité, il y a plusieurs types d'attaques contre ce type de serveur, que le créateur ou le développeur doit prendre en considération. Dans le chapitre suivant, nous allons présenter les principaux problèmes de sécurité liés à la VoIP.

Chapitre III

Vulnérabilités contre la VOIP et quelques moyens de Sécurisation

III.1 Introduction

La téléphonie sur IP est une évolution majeure récente dans le monde des télécommunications. Cette technologie consiste à utiliser le protocole de transfert de données IP pour acheminer des communications téléphoniques numérisées sur des réseaux privés ou publics. L'intégration de ces services dans une seule plateforme nécessite plus de sécurité.

Dans ce chapitre, nous présentons les principales attaques qui menacent la VoIP. Il existe deux principales classes de vulnérabilités sur un environnement VoIP. La première dépend des protocoles utilisés (SIP, H.323...) et la deuxième est reliée aux systèmes sur lesquels les éléments VoIP sont implémentés. Chaque protocole ou service a ses propres incertitudes.

III.2 Les attaques protocolaires

Les lignes VoIP sont exposées aux mêmes attaques que votre connexion Internet et que votre messagerie. Les cybercriminels sont entrain de mettre au point de nouvelles attaques visant spécifiquement la téléphonie sur IP. Il est important de connaître ces risques potentiels [14].

III.2.1 Spam

Les lignes VoIP sont la cible d'actions marketing indésirables qui leur sont propres, plus connues sous le nom de "SPIT" (Spam over Internet Telephony). Et il existe trois types de SPAM [14].

III.2.1.1 Call Spam : ce type de spam est défini comme une masse de tentatives d'initiation de session (des requêtes INVITE) non sollicitées.

III.2.1.2 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 spam sont pour la plupart envoyés sous forme de requête SIP.

III.2.1.3 Présence Spam : ce type de spam est semblable à l'IM spam. Il est défini comme une masse de requêtes de présence non sollicitées. L'attaquant fait ceci dans le but d'appartenir à la "white list" d'un utilisateur afin de lui envoyer des messages instantanés ou d'initier avec lui d'autres formes de communication.

III.2.2 Suivi des appels

Appelé aussi Call tracking, cette attaque se fait au niveau du réseau LAN/VPN et cible les terminaux (soft/hard phone). Elle a pour but de connaître qui est entrain de communiquer et quelle est la période de la communication.

Pour réaliser cette attaque, L'attaquant doit être capable d'écouter le réseau et récupérer les messages INVITE et BYE.

III.2.3 Voice phishing (phishing via VoIP)

Egalement appelée "vishing", cette méthode d'attaque consiste pour le pirate à vous appeler sur votre ligne VoIP et à vous amener par la ruse à lui communiquer des informations confidentielles comme vos numéros de carte de crédit et de compte bancaire.

III.2.4 Le sniffing

Le Sniffing ou reniflement de trafics constitue l'une des méthodes couramment utilisées par les pirates informatiques pour espionner le trafic sur le réseau. Dans la pratique, les hackers ont généralement recours à ce procédé pour détecter tous les messages circulant sur le réseau en récupérant des mots de passe et des données sensibles.

III.2.5 Déni de service

L'attaque par déni de service consiste à surcharger le serveur Web de requêtes jusqu'à ce qu'il ne puisse plus suivre et s'arrête. Il est envisageable de saturer les réseaux des sociétés équipées en voix sur IP, bloquant ainsi les communications internes, externes mais aussi le système d'information.

Les attaques par déni de service se retrouvent sous plusieurs formes. Les plus classiques sont celles qui visent à utiliser toute la bande passante disponible ou abuser de problèmes intrinsèques à TCP/IP, bloquant ainsi les tentatives de communication. Dans le cadre d'une solution VoIP bien des éléments peuvent être attaqués comme le téléphone, le réseau, le système d'exploitation, l'application, ... etc.

III.2.6 Compromission de serveurs

Les serveurs jouent un rôle important dans une solution de voix sur IP, et même s'il n'est pas forcément possible d'intercepter un appel si un serveur est compromis, il est souvent possible de récupérer des CDRs (Call Detail Records) qui contiennent toutes les traces des appels effectués. En revanche la compromission d'une passerelle entre le réseau VoIP et le réseau téléphonique classique permet d'écouter de manière transparente les appels, même s'ils sont chiffrés du côté VoIP (SRTP).

III.2.7 Les interceptions illégales d'appels

Avec la VoIP, tous les postes téléphoniques deviennent en quelque sorte des serveurs puisqu'ils sont désormais accessibles de l'extérieur de l'entreprise. Si aucune mesure n'est prise, cela revient à supprimer l'intérêt du Firewall d'entreprise. Ce risque devient d'autant plus dangereux que si aujourd'hui peu de personnes sont capables de pirater un réseau téléphonique classique, avec la VoIP, cela devient possible pour n'importe quel informaticien.

III.3 Les attaques sur les couches basses

III.3.1 ARP spoofing

L'ARP est un protocole qui de par sa conception expose les réseaux informatiques, et leurs composants à des vulnérabilités et des dangers qui sont faciles à exploiter lorsque l'on connaît bien son fonctionnement. Cette attaque, appelée aussi ARP Redirect, redirige le trafic réseau d'une ou plusieurs machines vers la machine du pirate.

Elle consiste à s'attribuer l'adresse IP de la machine cible, c'est-à-dire à faire correspondre son adresse IP à l'adresse MAC de la machine pirate dans les tables ARP des machines du réseau. Pour cela il suffit en fait d'envoyer régulièrement des paquets ARP_reply en broadcast, contenant l'adresse IP cible et la fausse adresse MAC. Cela a pour effet de modifier les tables dynamiques de toutes les machines du réseau. Celles-ci enverront donc leurs trames Ethernet à la machine pirate tout en croyant communiquer avec la cible, et ce de façon transparente pour les switches. De son côté, la machine pirate stocke le trafic et le renvoie à la vraie machine en forgeant des trames Ethernet comportant la vraie adresse MAC.

Cette technique est très puissante puisqu'elle opère au niveau Ethernet, permettant ainsi de spoofer le trafic IP.

III.3.2 MITM : Man-In-The-Middle : écoute passive ou modification de flux

Man-in-the-Middle signifie l'homme du milieu. Cette attaque fait intervenir trois protagonistes : le client, le serveur et l'attaquant. Le but de l'attaquant est de se faire passer pour le client auprès du serveur et se faire passer pour le serveur auprès du client. Il devient ainsi l'homme du milieu. Cela permet de surveiller tout le trafic réseau entre le client et le serveur, et de le modifier à sa guise pour l'obtention d'informations (mots de passe, accès système, etc.). Voir Figure III.1.

La plupart du temps, l'attaquant utilise les techniques de détournement de flux pour rediriger les flux du client et du serveur vers lui [15].

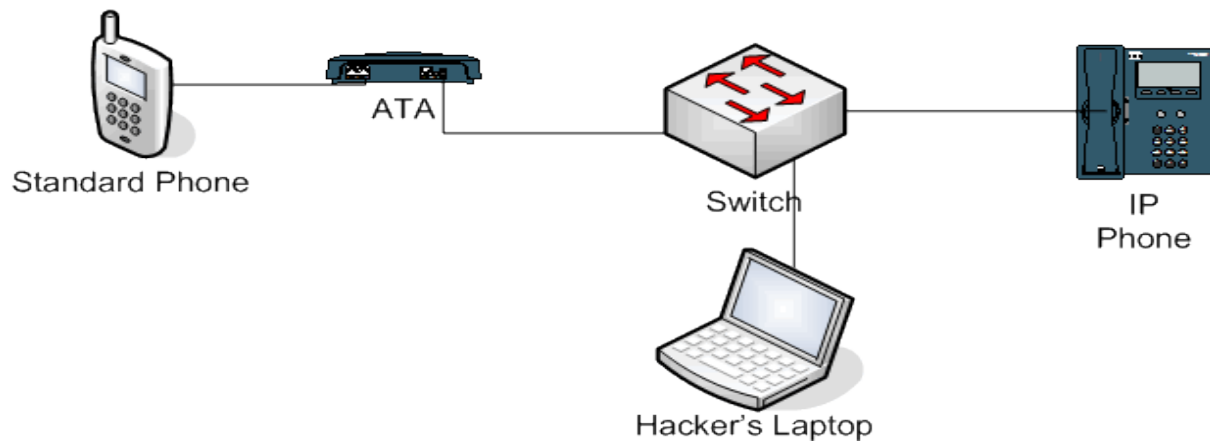


Figure III.1 Représentation d'une attaque MITM [15]

III.4 Les vulnérabilités de l'infrastructure

Les infrastructures critiques sont constituées de l'ensemble des grands réseaux indispensables au bon fonctionnement d'une société. Leur sécurisation est donc, par nature, un enjeu majeur pour cette dernière. Ces réseaux sont d'une importance majeure pour les autres infrastructures critiques. Cet accroissement des dépendances entre les infrastructures amène à l'apparition de nouvelles vulnérabilités qu'il s'agit d'identifier.

III.4.1 Les téléphones IP

Un pirate peut enfoncez un dispositif de téléphonie sur 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.

D'autres conséquences possibles sont :

- Des backdoors (une porte dérobée qui donne un accès secret au logiciel.) pourront être installés.
- L'acquisition d'un accès non autorisé sur un dispositif de téléphonie IP peut être le résultat d'un autre élément compromis sur le réseau IP, ou de l'information récoltée sur le réseau.
- Les téléphones IP exécutent quant à eux leurs propres systèmes d'exploitation avec un nombre limité de services supportés et possèdent donc moins de vulnérabilités.

III.4.2 Vulnérabilités de la confidentialité et l'intégrité de la VOIP

Pour la confidentialité de la communication, les données doivent être chiffrées. Le chiffrement s'effectue généralement par une clé symétrique, qui offre une grande rapidité du chiffrement et du déchiffrement.

La difficulté réside dans la distribution sécurisée de la clé entre les deux extrémités communicantes. Une clé asymétrique peut être utilisée pour le transport de la clé symétrique utilisée pour établir le tunnel chiffré transportant la VOIP.

L'intégrité est obtenue par une signature électronique. La signature électronique s'effectue à partir d'un hash (Un hash cryptographique est une série de chiffres et lettres générées par une fonction de hachage) chiffré de l'information à transmettre. Après déchiffrement, le destinataire doit obtenir la même valeur du hash.

III.4.3 Vulnérabilités de disponibilité de la VOIP

La disponibilité désigne le temps pendant lequel un système est en état de marche ou, ce qui revient au même, le temps pendant lequel le système n'est pas en état de marche. La téléphonie classique présente une disponibilité dite aux 5 « neuf », c'est-à-dire que le système est en état de marche 99,999 % du temps, ce qui représente cinq minutes de panne au total sur l'année. Un bon FAI (Fournisseur d'Accès Internet) travaille aux 3 « neuf », c'est-à-dire que son réseau est disponible 99,9 % du temps, ce qui équivaut à 8,8 heures de panne par an.

III.5 Sécuriser le SIP d'un serveur Asterisk

Du point de vue SIP, Asterisk est un B2BUA. Un B2BUA (back-to-back user agent) est un élément logique du réseau dans les applications SIP. Il intervient entre les deux terminaisons d'un appel et divise la communication en deux appels indépendants. Tous les messages de control passent par le B2BUA, ce qui lui permet d'intervenir lors de l'appel afin de lancer si nécessaire des applications comme l'interception, l'enregistrement, la diffusion de messages. Par contre Asterisk n'est pas un proxy SIP. Il intègre quelques-unes des fonctions (routage des appels, serveur registrar), mais gère de manière incomplète l'ensemble des messages SIP [15].

On peut distinguer les niveaux de sécurité de VOIP suivants :

- Limitation d'accès physique dans le réseau VOIP et sur le serveur VOIP (DOD : Accès réseau)
- Configuration fiable des équipements de réseau et la surveillance permanent de topologie et des propriétés de réseau (DOD : Transport et Internet)
- Configuration fiable de Linux et d'Asterisk

Voici quelques moyens de protéger un réseau VOIP et le serveur Asterisk :

- **Limitation d'accès physique**

L'accès aux équipements réseau tel que switches ou serveurs ne doit pouvoir être fait que par les personnes autorisées (administrateurs ou techniciens). Il est aussi important que les

employés ne puissent pas brancher ou débrancher des équipements sur le réseau de l'entreprise.

- **Séparation des flux data/voip via 2 vlans différents**

Les communications entre les VLAN doivent être rigoureusement filtrées de manière à n'autoriser que les flux nécessaires. Seuls les flux définis sont autorisés.

On a trois possibilités : Création de VLAN par ports (couche n°1 de modèle OSI), par adresse MAC (couche n°2 de modèle OSI) et par adresse IP (couche n°3 de modèle OSI).

Par exemple, les IP Phones n'ont pas besoin d'envoyer un flux média (ex : RTP) aux serveurs VoIP. Donc, au lieu d'autoriser toutes communications entre les VLAN VOIP Hardphones /Softphones et le VLAN VoIP Servers, seul le trafic concernant le protocole de signalisation (ex : SIP) devraient être autorisé.

- **Authentification forte**

Une authentification sur tous les équipements de réseau et des serveurs.

- **Changement des ports par défaut**

Pour **SIP** la modification peut être faite dans le fichier sip.conf dans la section « general ».

- **Intégration de VPN**

Intégrer des réseaux privés virtuels pour des utilisateurs nomades.

- **L'Interdiction d'accès à Asterisk sans authentification**

allowguest=yes autorise n'importe quel appel entrant SIP sans authentification ou autre restriction, et le passe au contexte déclaré par défaut pour les appels SIP.

L'option allowguest ne devrait jamais être mise sur yes.

- **Limiter le nombre des appels simultanés.**

Dans la configuration de clients SIP il faut établir le paramètre call-limit=1.

- **Différenciez vos noms d'utilisateurs de vos extensions SIP.**

Il est conseillé de choisir un nom d'utilisateur SIP différent de l'extension.

III.6 Sécurisation du système et de l'application

Une application Client/Serveur était hiérarchique et centralisée : les clients étaient connus, qui accédaient tous à un serveur spécifique via le réseau LAN et WAN.

Mais les données du problème ont changé. L'utilisation des technologies web, notamment l'utilisation d'un navigateur Internet standard pour accéder à l'application, fait que le logiciel n'est plus maîtrisable.

De même, les nouvelles générations d'applications, comme la Téléphonie sur IP, ou la messagerie instantanée remettent ce modèle en cause. En effet, le modèle n'est plus hiérarchique et centralisé (des clients qui convergent tous vers un serveur), mais distribué et non prédictif (tout le monde doit pouvoir parler à tout le monde, sans savoir ni quand ni combien de temps).

Le modèle de sécurisation des applications vole donc en éclats : on en peut plus sécuriser d'application centrale, il faut distribuer cette sécurisation partout, dans chaque élément traversé [16].

Les technologies spécifiques permettant de sécuriser les Applications :

III.6.1 Sécurisation d'application

Sécurisez les autres applications (ssh, http, etc.), en appliquant les meilleures pratiques pour chaque application, et en les tenants à jour.

III.6.2 Le Firewall

Le Firewall (en français Pare-Feu) contrôle qui accède à l'application et l'usage qui va en être fait, basé sur des politiques définies à l'avance.

III.6.3 La Protection d'Intrusion

Cette protection se fait en vérifiant que le flux qui se présente est bien conforme à ce qu'il doit être, et donc le confronter à une base de signatures d'attaques connues, attaques en " exploitation de vulnérabilité " (activité IDS classique) ou attaques virales (activité anti-virus classique). En fonction des cas et des endroits où il va intervenir ces technologies deviennent indispensables [17].

III.6.4 IPTABLE

Dans tous les cas, et surtout si le serveur Asterisk est accessible depuis l'extérieur, mettre en place des règles IPTABLES (est un logiciel libre de l'espace utilisateur Linux grâce auquel l'administrateur système peut configurer les chaînes et règles dans le pare-feu en espace noyau (et qui est composé par des modules Netfilter)).

III.6.5 L'authentification des clients

allowguest autorise un client sans user ni mot de passe à passer des appels => TRES DANGEREUX

alwaysreject permet de renvoyer la même erreur, que ce soit le username ou le password qui soit incorrect. Cela complique les attaques de force brute.

III.6.6 IDS systems

Ces systèmes surveillent les fichiers journaux à la recherche de comportements suspects, comme un certain nombre de mots de passe mal entrés dans un court laps de temps.

Les règles par défaut permettent également un certain nombre de tentatives, si les attaques peuvent être chronométrés de ne pas déclencher l'IDS ou dès que l'adresse IP est bloquée, le pirate peut reprendre la tentative d'une autre adresse IP.

III.6.7 Rate limiting

Utilisation d'iptables pour limiter la vitesse à laquelle les messages SIP peuvent être envoyés à partir d'un seul appareil, ce qui donne moins de temps pour l'attaquant de faire des attaques de force brute, et arrête la charge étant reportée à votre système IDS.

III.6.8 Bloquer les attaques courantes

La plupart des attaques sont des logiciels librement et largement disponibles, et comprennent le nom du logiciel dans le message SIP, autant de pirates amateurs ne se soucient pas de changer cela. La reconnaissance et le blocage des noms les plus populaires permettront de réduire le nombre d'attaques.

Des exemples de noms d'outils de hacking SIP populaire présents comprennent :

- Facile à scanner
- VaxSIPUserAgent
- sundayddr
- sipsak
- sipvicious
- iWar
- SIP-scan
- sipcli

III.6.9 Protection contre les attaques ARP

Cette méthode consiste à empêcher la connexion du pirate sur le réseau

- Sécuriser l'accès physique du réseau pour un réseau filaire.
- En Wi-Fi, tous les paquets sont rejetés si le pirate ne connaît pas la clé secrète.
- Installer un pare feu.
- Implémenter les tables ARP statiques.
- Analyser les historiques.

III.7 Conclusion

Un système téléphonique d'entreprise est avant tout un système informatique (serveur linux, Windows ou dérivé d'Unix) disposant des failles de sécurité qui doit entrer dans les processus de sécurité informatique : gestion des accès externes rigoureux, politique de gestion des mots de passe, surveillance, etc. Dans le chapitre suivant nous allons présenter quelques solutions que nous avons mises en œuvre et qui sont nécessaires pour la sécurisation de notre serveur SIP.

Chapitre IV

Sécurisation du serveur

IV.1 Introduction

Dans le chapitre précédent nous avons étudié quelques vulnérabilités qu'on pourra croiser en utilisant la VoIP et les bonnes solutions afin de sécuriser le serveur Asterisk. La VoIP est souvent déployée dans un environnement ouvert ; par conséquent, il est soumis à un nombre important de menaces. Donc pour lutter contre toutes ces menaces, le développeur doit prendre ses précautions en considérant les services de sécurité qu'on verra dans ce chapitre.

IV.2 Le « profiling » de la cible

Avant d'exécuter son attaque sur la machine cible, le pirate commence par une étape très importante, à savoir, établir le profil de la cible, connu sous le nom « profiling » ou encore « foot printing ». Une empreinte englobe les informations sur la cible qui déploie le serveur VoIP et ces paramètres de sécurité. Il existe plusieurs méthodes pour la collecte des informations, des méthodes que le développeur pourra aussi utiliser pour connaître les informations qui sont divulgués (sur son serveur) pour éventuellement les sécuriser. En voici quelques-unes des plus utilisées :

IV.2.1 Les serveurs Whois

Le terme 'WHOIS' vient de l'anglais 'who is' Appliqué à l'univers des noms de domaine, un WHOIS est un annuaire qui permet de répertorier les informations techniques et légales d'un nom de domaine. Avec ces informations, il est possible de déterminer le propriétaire du nom de domaine, la personne à contacter en cas de problème, ainsi que le contact technique qui administre le nom de domaine [18]. Les champs affichés, lors de la consultation WHOIS, sont propres aux registres de noms de domaines, mais reprennent les éléments suivants :

- le nom du domaine consulté ;
- les noms, adresse, numéro de téléphone, fax (éventuellement), email du propriétaire du nom de domaine ;
- les identifiants NIC du propriétaire, du contact technique, et du contact de facturation ;
- les adresses (ou IP) des serveurs DNS ;
- Les dates de création, modification et d'expiration du nom de domaine consulté lors du WHOIS

IV.2.2 Aspirateur de site HTTrack

HTTrack est un aspirateur de sites web facile d'utilisation et libre (GPL, logiciel libre). Il permet de télécharger un site web d'Internet vers un disque dur, en construisant récursivement tous les répertoires, récupérant html, images et fichiers du serveur vers votre ordinateur. HTTrack réorganise la structure des liens en relatif. Ouvrez simplement une page du site "aspiré" dans votre navigateur, et vous pourrez naviguer librement à l'intérieur, comme si vous étiez connecté. HTTrack peut aussi mettre à jour un site existant, ou continuer un téléchargement interrompu. Le robot est entièrement configurable, avec un système d'aide intégré [19].

IV.3 logiciels de tests d'intrusion

IV.3.1 Wireshark

Autrefois connu sous le nom d'Ethereal, Wireshark est un "sniffer" ou analyseur de protocoles réseau et applicatif. C'est-à-dire qu'il va capturer des paquets IP transitant sur un réseau de manière transparente pour qu'ils soient ensuite analysés. Des filtres de capture peuvent être appliqués afin de recueillir des paquets correspondants à des besoins particuliers. Distribué sous licence GNU GPL, Wireshark est utilisé par les administrateurs réseau et les experts en sécurité lors de tests d'intrusion, notamment pour des scénarios d'attaque man-in-the-middle [20].

IV.3.1.1 Téléchargement de Wireshark

On pourra l'effectuer grâce à la commande suivante :

```
Sudo apt-get install wireshark
```

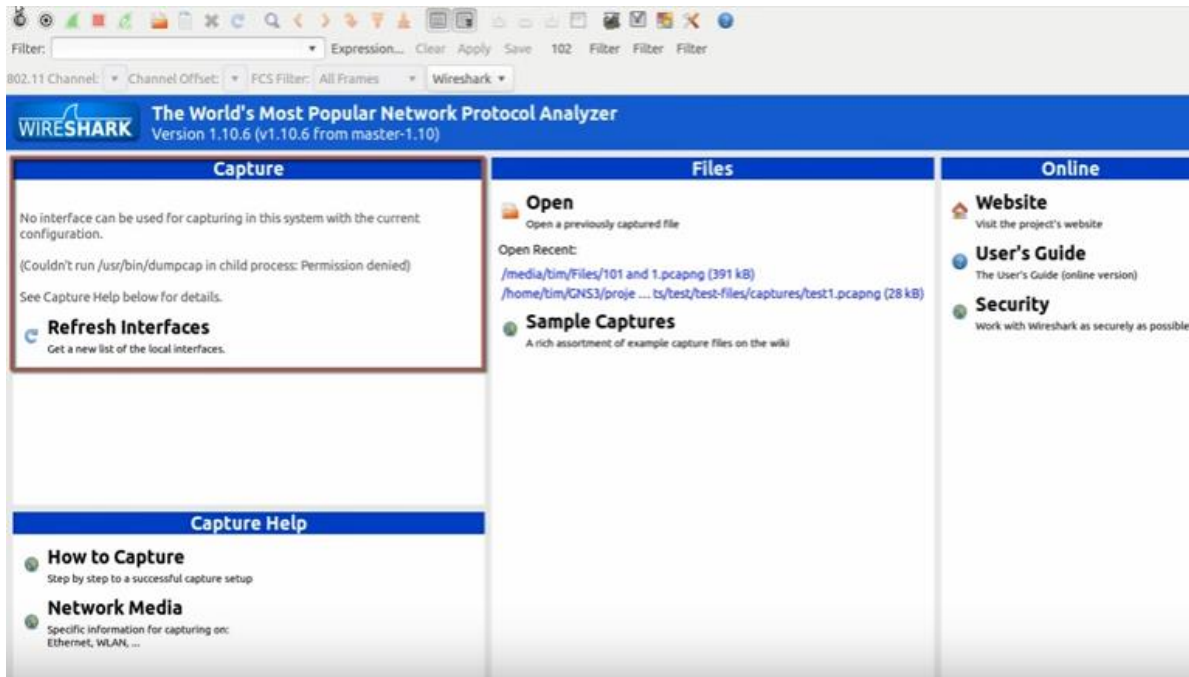


Figure IV.1 la page de wireshark

Ensuite pour pouvoir capturer on intègre les commandes suivantes :

`Sudo dpkg-reconfigure wireshark- common`

`Sudo adduser $USER wireshark`

IV.3.1.2 Lancement du wireshark

Le résultat est le suivant pour pouvoir faire des captures

Il suffit de taper dans le terminal de la machine : Wireshark

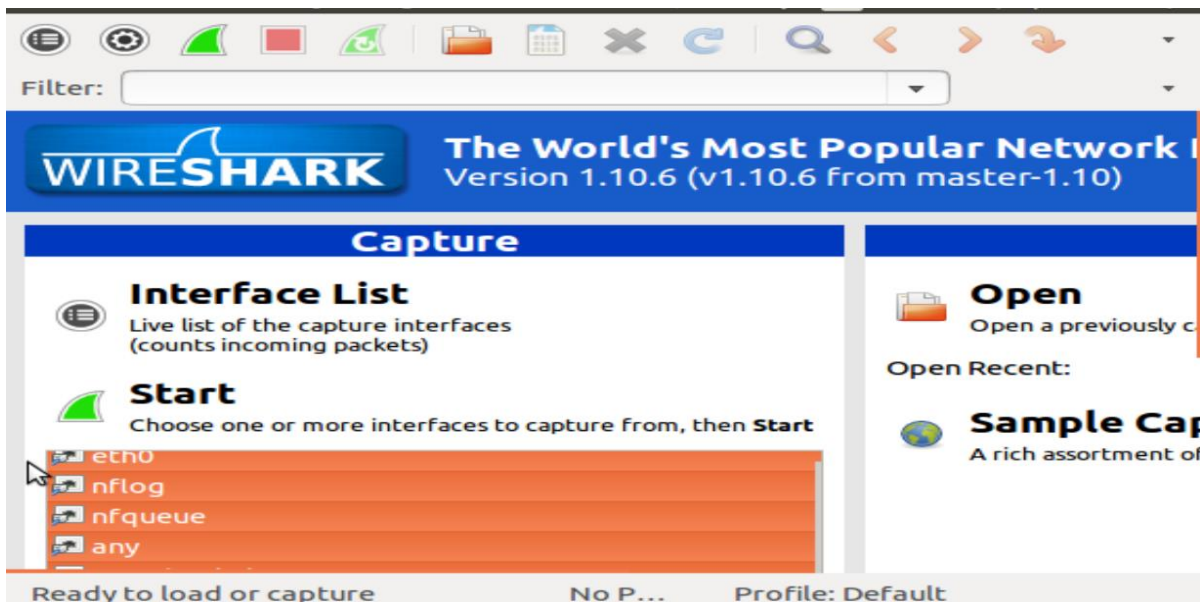


Figure IV.2 Lancement de l’outil WireShark sur la passerelle eth0

Maintenant, nous allons commencer la capture d'une partie du trafic. Pour sniffer le trafic, lorsque le client 6001 appelle le client 6002.

No.	Time	Source	Destination	Protocol	Length	Info
464	21.062497000	192.168.1.11	192.168.1.10	SIP	485	Request:
465	21.105543000	192.168.1.11	192.168.1.10	RTP	214	PT=ITU-T
466	21.124059000	192.168.1.11	192.168.1.10	RTP	214	PT=ITU-T
467	21.143591000	192.168.1.11	192.168.1.10	RTP	214	PT=ITU-T
468	21.155216000	192.168.1.2	255.255.255.255	UDP	150	Source p
469	21.163624000	192.168.1.11	192.168.1.10	RTP	214	PT=ITU-T
470	20.993553000	192.168.1.10	192.168.1.11	RTP	62	PT=Unass
471	21.050159000	192.168.1.10	192.168.1.11	SIP/SDP	758	Status:
472	21.050444000	192.168.1.11	192.168.1.10	SIP	487	Request:
473	21.050828000	127.0.0.1	127.0.0.1	SIP/SDP	888	Status:
474	21.051285000	192.168.1.11	192.168.1.10	SIP/SDP	885	Request:
475	21.062209000	192.168.1.10	192.168.1.11	SIP/SDP	758	Status:
476	21.062497000	192.168.1.11	192.168.1.10	SIP	487	Request:
477	21.063428000	127.0.0.1	127.0.0.1	SIP	644	Request:
478	21.063534000	127.0.0.1	127.0.0.1	SIP/SDP	899	Request:
479	21.078795000	127.0.0.1	127.0.0.1	SIP/SDP	946	Status:
480	21.079060000	127.0.0.1	127.0.0.1	SIP	451	Request:

Figure IV.3 L'analyse des paquets récupérés

On analyse les appels VoIP détectés :

No.	Time	Source	Destination	Protocol	Length	Info
464	21.062497	192.168.1.11	192.168.1.10	SIP	485	Request:
465	21.105543	192.168.1.11	192.168.1.10	RTP	214	PT=ITU-T
466	21.124059	192.168.1.11	192.168.1.10	RTP	214	PT=ITU-T
467	21.143591	192.168.1.11	192.168.1.10	RTP	214	PT=ITU-T
468	21.155216	192.168.1.2	255.255.255.255	UDP	150	Source p
469	21.163624	192.168.1.11	192.168.1.10	RTP	214	PT=ITU-T
470	20.993553	192.168.1.10	192.168.1.11	RTP	62	PT=Unass
471	21.050159	192.168.1.10	192.168.1.11	SIP/SDP	758	Status:
472	21.050444	192.168.1.11	192.168.1.10	SIP	487	Request:
473	21.050828	127.0.0.1	127.0.0.1	SIP/SDP	888	Status:
474	21.051285	192.168.1.11	192.168.1.10	SIP/SDP	885	Request:
475	21.062209	192.168.1.10	192.168.1.11	SIP/SDP	758	Status:
476	21.062497	192.168.1.11	192.168.1.10	SIP	487	Request:
477	21.063428	127.0.0.1	127.0.0.1	SIP	644	Request:
478	21.063534	127.0.0.1	127.0.0.1	SIP/SDP	899	Request:
479	21.078795	127.0.0.1	127.0.0.1	SIP/SDP	946	Status:
480	21.079060	127.0.0.1	127.0.0.1	SIP	451	Request:

Figure IV.4 l'analyse des appels VoIP

On clique sur le bouton player

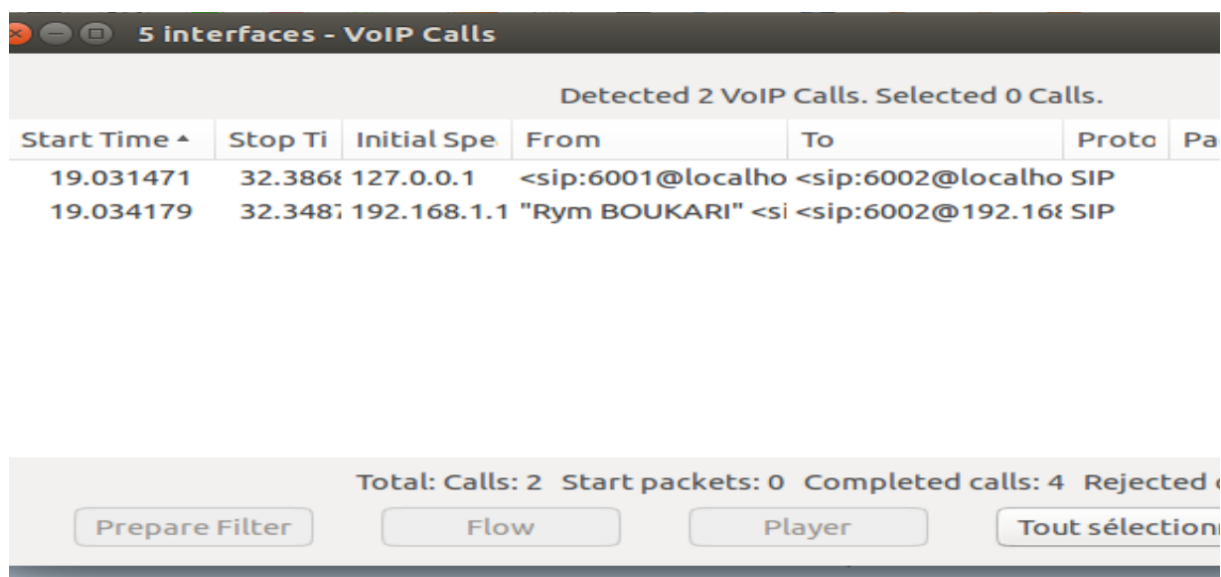


Figure IV.5 appels Voip détectés

Ensuite, on clique sur le bouton Décode et on obtient :

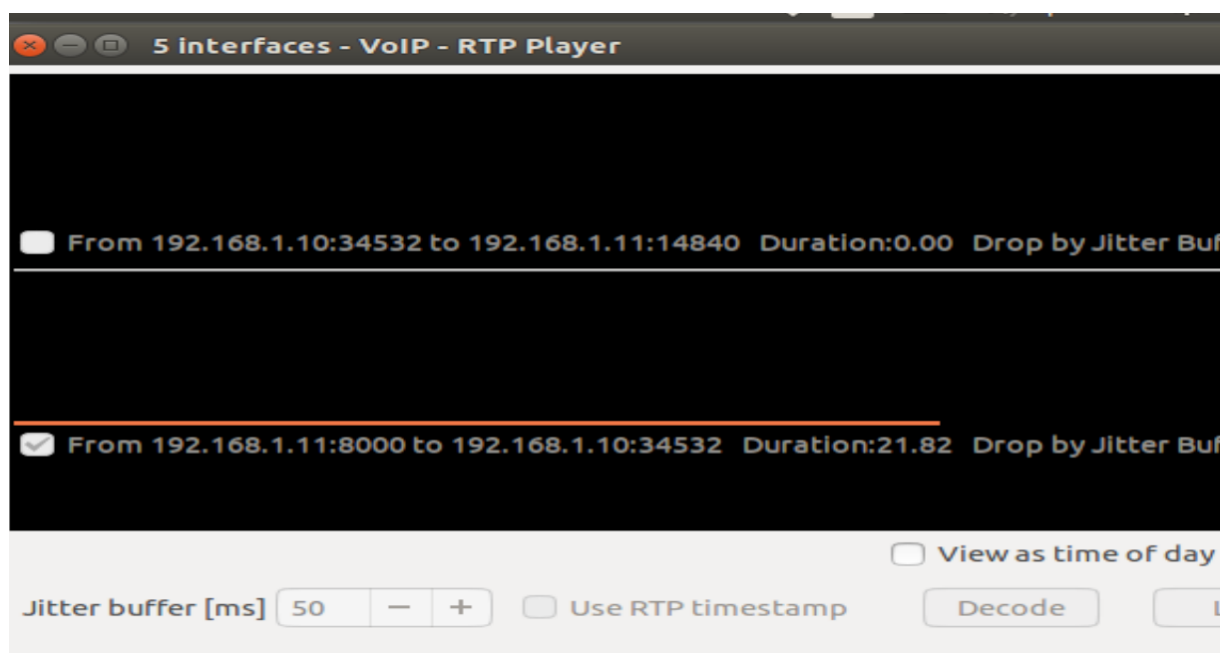


Figure IV.6 conversations décodés

Dans cette capture, on constate qu'une conversation entre les clients 6001 et 6002 a été décodée. Pour l'écouter, il suffit de cliquer sur le bouton Player.

IV.3.2 John The Ripper

John the Ripper (ou JTR, ou John) est un logiciel libre de cassage de mot de passe, utilisé notamment pour tester la sécurité d'un mot de passe (audit, crack). D'abord développé pour

tourner sous les systèmes dérivés d'UNIX, le programme fonctionne aujourd'hui sous une cinquantaine de plates-formes différentes, telles que BeOS, BSD et ses dérivés, DOS, Linux, OpenVMS, Win32....

John est l'un des craqueurs de mots de passe les plus populaires, car il inclut l'auto-détection des tables de hachage utilisées par les mots de passe, l'implémentation d'un grand nombre d'algorithmes de cassage, par le fait qu'il soit très facilement modifiable, et aussi qu'il soit possible de reprendre une attaque après une pause (arrêt de la machine). John The Ripper supporte en natif de multiples protocoles de chiffrement dont Kerberos / AFS, Blowfish, MD5 ou LM hash. John ou certaines de ses extensions permettent aussi d'évaluer la robustesse des mots de passe de diverses applications, dont Office, ou encore Microsoft SQL Server, MySQL, et certains serveurs LDAP [21].

IV.3.2.1 Installation de john

Sudo apt-get install john

```

root@bendelhoum-VirtualBox: /test
2017-05-02 00:14:40 (4.68 KB/s) - Fermeture de la connexion à l'octet 120308610. Nouvel essai.

--2017-05-02 00:14:42-- (essai : 3) http://scrapmaker.com/data/wordlists/dictionaries/rockyou.txt
Connexion à scrapmaker.com (scrapmaker.com)|192.254.232.166|:80
... connecté.
requête HTTP transmise, en attente de la réponse... 206 Partial Content
Taille : 139921497 (133M), 19612887 (19M) restant [text/plain]
Enregistre : «rockyou.txt.2»

100%[+++++++=====] 139,921,497 32.3KB/s ds 2m 15s

2017-05-02 00:16:58 (142 KB/s) - «rockyou.txt.2» enregistré [139921497/139921497]

```

Figure IV.7 installation de john

IV.3.2.2 Configuration de john

On passe à l'étape du changement de la fonction de hachage cryptographique sha512 à MD5

Sudo nano /etc/pam.d/common-password

Puis on crée un dossier pour les tests

Sudo mkdir /test

On fait passer tout le dossier test en chmod777

Sudo chmod -R 777 /test

Pour casser des hashes, il est important d'avoir des dictionnaires diversifiés, complets et réalistes. Donc nous avons choisis le rockyou.

`Sudo wget http://scrapmaker.com/data/wordlists/dictionaries/rockyou.txt`

`Sudo adduser kitten` (Kittene le nom du nouvel utilisateur)

On ajoute un nouvel utilisateur qui a toutes les informations demandées y compris le mot de passe qu'on doit craquer par la suite et qui est caché au début.

```

root@bendelhoum-VirtualBox: /test
Paramétrage de python-sip-dev (4.15.5-1build1) ...
Traitement des actions différées (« triggers ») pour libc-bin (
2.19-0ubuntu6.5) ...
root@bendelhoum-VirtualBox:/test# sudo adduser kitten
Ajout de l'utilisateur « kitten » ...
Ajout du nouveau groupe « kitten » (1001) ...
Ajout du nouvel utilisateur « kitten » (1001) avec le groupe «
kitten » ...
Création du répertoire personnel « /home/kitten »...
Copie des fichiers depuis « /etc/skel »...
Entrez le nouveau mot de passe UNIX :
Retapez le nouveau mot de passe UNIX :
passwd : le mot de passe a été mis à jour avec succès
Modification des informations relatives à l'utilisateur kitten
Entrez la nouvelle valeur ou « Entrée » pour conserver la valeur
proposée
  Nom complet []:
  N° de bureau []:
  Téléphone professionnel []:
  Téléphone personnel []:
  Autre []:
Ces informations sont-elles correctes ? [O/n] o
root@bendelhoum-VirtualBox:/test#
  
```

Figure IV.8 configuration de john

Pour pouvoir craquer les mots de passe y compris celui de l'utilisateur créé :

`Sudo john -w:/test/rockyou.txt /etc/shadow`

```

azerty          (kitten)
1g 0:00:01:04 0% 0.01547g/s 80.21p/s 121.8c/s 121.8C/s caleb1..
honeybunch
1g 0:00:01:11 0% 0.01392g/s 80.21p/s 117.6c/s 117.6C/s mirella.
.tractor
1g 0:00:01:13 0% 0.01369g/s 80.18p/s 116.9c/s 116.9C/s thumper1
..precioso
1g 0:00:01:16 0% 0.01304g/s 80.17p/s 115.2c/s 115.2C/s honeybea
r..Joshua
1g 0:00:01:19 0% 0.01265g/s 80.18p/s 114.1c/s 114.1C/s holmes..
jordan2
1g 0:00:01:25 0% 0.01176g/s 80.18p/s 111.8c/s 111.8C/s thebest1
..bethan
1g 0:00:01:26 0% 0.01159g/s 80.17p/s 111.3c/s 111.3C/s bball23.
.bizkit
1g 0:00:01:29 0% 0.01113g/s 80.17p/s 110.1c/s 110.1C/s danika..
sheree
1g 0:00:01:33 0% 0.01070g/s 80.17p/s 108.9c/s 108.9C/s 212223..
confused1
  
```

Figure IV.9 les mots de passe craqués

La liste des mots de passe que j'ai utilisé est de :

<http://scrapmaker.com/data/wordlists/dictionaries/rockyou.txt>

IV.4 solutions pour sécuriser le serveur

IV.4.1 Crypter le mot de passe avec MD5

Une meilleure pratique pour mieux assurer la sécurité du serveur Asterisk est de crypter le mot de passe du client à l'aide de la méthode MD5 [22]. Grâce au cryptage, le mot de passe du client devient illisible dans le cas où une personne malveillante accède au fichier sip.conf. Et cela est effectué grâce à la commande suivante appliquée sur chaque client :

```
echo -n "utilisateur:Asterisk:motdepasse" | md5sum
```

```
root@bendelhoum-VirtualBox:/usr/src/asterisk/asterisk-13.14.0# sudo echo -n "6001:asterisk:secret" | md5sum
7b2a40087e63a67107c3aa72b11fa7f5 -
root@bendelhoum-VirtualBox:/usr/src/asterisk/asterisk-13.14.0# sudo echo -n "6002:asterisk:secret" | md5sum
a7a3746ba901bd0f9fcda398034697ce -
root@bendelhoum-VirtualBox:/usr/src/asterisk/asterisk-13.14.0#
```

Figure IV.10 cryptage des mots de passe

Après on remarque qu'en effectuant cette étape on reçoit un code pour chaque client qui va appliquer le hachage voulu.

Des modifications seront nécessaires dans sip.conf pour que la configuration soit fonctionnelle. Dans notre cas on a crypté les deux clients 6001 & 6002, donc on change la ligne secret par md5secret.

Md5sercet = le code reçu

Avant les changements on avait :

```
bendelhoum-VirtualBox*CLI> sip show users
```

Username	Secret	Accountcode	Def.Context	ACL	Forcerport
6002	secret		work	No	Yes
6001	secret		work	No	Yes

Figure IV.11 avant l'application de MD5

Les mots de passe étaient visibles

Et après l'application on a obtenu des mots de passe invisibles pour les deux clients :

```
bendelhoum-VirtualBox*CLI> sip show users
```

Username	Secret	Accountcode	Def.Context	ACL	Forcerport
6002			work	No	Yes
6001			work	No	Yes

Figure IV.12 après l'application de MD5

En utilisant John the ripper, impossible de craquer les mots de passe des utilisateurs comme on l'a fait auparavant avant la sécurisation en utilisant MD5.

```
bendelhoum@bendelhoum-VirtualBox:~$ sudo john --show /etc/shadow
root:azerty:17301:0:99999:7:::
kittene:azerty:17301:0:99999:7:::

2 password hashes cracked, 1 left
bendelhoum@bendelhoum-VirtualBox:~$ sudo john /etc/shadow
Warning: only loading hashes of type "md5crypt", but also saw type "crypt"
Use the "--format=crypt" option to force loading hashes of that type instead
Loaded 2 password hashes with 2 different salts (md5crypt [MD5 32/32])
No password hashes left to crack (see FAQ)
bendelhoum@bendelhoum-VirtualBox:~$ █
```

Figure IV.13 Test de john après sécurisation

IV.4.2 IPsec

IPsec (*Internet Protocol Security*), défini par l'IETF comme un cadre de standards ouverts pour assurer des communications privées et protégées sur des réseaux IP, par l'utilisation des services de sécurité cryptographiques, est un ensemble de protocoles utilisant des algorithmes permettant le transport de données sécurisées sur un réseau IP [23].

IV.4.2.1 Installer les outils

```
sudo apt-get install ipsec-tools
```

IV.4.2.2 Configuration pour une authentification par clé partagée

Les deux clients ayant les adresses IP 192.168.1.12 et 192.168.1.9 communiquent à l'aide d'IPsec.

Modifiez le fichier `/etc/ipsec-tools.conf`

```
Sudo nano /etc/ipsec-tools.conf
```

Flush ;

Spdflush ;


```

add 192.168.1.12 192.168.1.9 ah 0x200 -A hmac-md5
    0xc0291ff014dccdd03874d9e8e4cdf3e6;
add 192.168.1.9 192.168.1.12 ah 0x300 -A hmac-md5
    0x96358c90783bbfa3d7b196ceabe0536b;

add 192.168.1.12 192.168.1.9 esp 0x201 -E 3des-cbc
    0x7aeaca3f87d060a12f4a4487d5a5c3355920fae69a96c831;
add 192.168.1.9 192.168.1.12 esp 0x301 -E 3des-cbc
    0xf6ddb555acfd9d77b03ea3843f2653255afe8eb5573965df;

spdadd 192.168.1.12 192.168.1.9 any -P out ipsec
    esp/transport//require
    ah/transport//require;

spdadd 192.168.1.9 192.168.1.12 any -P in ipsec
    esp/transport//require
    ah/transport//require;

```

Figure IV.14 configuration des outils

AH SAs using 128 bit long keys

```

add 192.168.1.12 192.168.1.9 ah 0x200 -A hmac-md5
    0xc0291ff014dccdd03874d9e8e4cdf3e6;
add 192.168.1.9 192.168.1.12 ah 0x300 -A hmac-md5
    0x96358c90783bbfa3d7b196ceabe0536b;

```

Cette section répertorie les clés de 128 bits pour la connexion 192.168.1.12 et 192.168.1.9. Chaque paire IP comporte 2 touches - une pour chaque direction (entrée et sortie). Chaque paire de machines doit connaître cette information. Donc, cela signifie que, pour chaque paire d'IP, vous devez générer une nouvelle clé.

De même pour :

ESP SAs using 192 bit long keys (168 + 24 parity)

```

add 192.168.1.12 192.168.1.9 esp 0x201 -E 3des-cbc
    0x7aeaca3f87d060a12f4a4487d5a5c3355920fae69a96c831;
add 192.168.1.9 192.168.1.12 esp 0x301 -E 3des-cbc
    0xf6ddb555acfd9d77b03ea3843f2653255afe8eb5573965df;

```

Donc, ses deux premières sections devraient énumérer les clés pour toutes les adresses IP dont la machine se préoccupe. Ces sections ne changent pas lors du déplacement du fichier entre les machines de chaque côté d'une connexion. Cela nous amène à la prochaine section :

```
# Security policies
```

```
spdadd 192.168.1.12 192.168.1.9 any -P out ipsec
```

```
    esp/transport//require
```

```
    ah/transport//require;
```

```
spdadd 192.168.1.9 192.168.1.12 any -P in ipsec
```

```
    esp/transport//require
```

```
    ah/transport//require;
```

Cela définit les politiques d'entrée et de sortie des communications. Ainsi, la version ci-dessus fonctionnera pour 192.168.1.12, car toute communication sortante vers 192.168.1.9 et toutes les communications entrantes de 192.168.1.9 seront chiffrées. Pour l'utiliser sur l'autre machine (192.168.1.9), basculez les directives d'entrée et de sortie, comme suit :

```
# Security policies
```

```
spdadd 192.168.1.12 192.168.1.9 any -P out ipsec
```

```
    esp/transport//require
```

```
    ah/transport//require;
```

```
spdadd 192.168.1.9 192.168.1.12 any -P in ipsec
```

```
    esp/transport//require
```

```
    ah/transport//require;
```

IV.4.2.3 cacher le fichier Conf au public :

```
sudo chmod 750 ipsec-tools.conf
```

Maintenant ça devient facile. Il sera lancé au démarrage par défaut sur les systèmes. Le démarrage ne nuirait pas non plus.

```
Sudo /etc/init.d/setkey start
```

IV.4.2.4 Lancer la mise à jour

```
setkey -f /etc/racoon/setkey.conf
```

IV.4.2.5 Vérifier les modifications

```
Sudo setkey -D
```

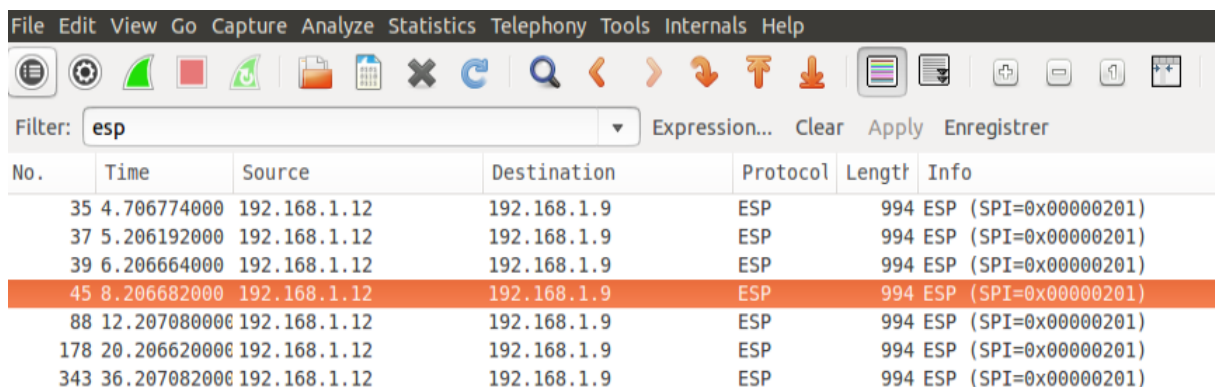
```

allocated: 0   hard: 0 soft: 0
sadb_seq=1 pid=12468 refcnt=0
192.168.1.12 192.168.1.9
esp mode=transport spi=513(0x00000201) reqid=0(0x00000000)
E: 3des-cbc 7aeaca3f 87d060a1 2f4a4487 d5a5c335 5920fae6 9a96c831
seq=0x00000000 replay=0 flags=0x00000000 state=mature
created: Jun  6 16:36:42 2017   current: Jun  6 16:57:26 2017
diff: 1244(s)   hard: 0(s)       soft: 0(s)
last: Jun  6 16:37:43 2017     hard: 0(s)       soft: 0(s)
current: 6377(bytes)   hard: 0(bytes)   soft: 0(bytes)
allocated: 7   hard: 0 soft: 0
sadb_seq=2 pid=12468 refcnt=0
192.168.1.9 192.168.1.12
ah mode=transport spi=768(0x00000300) reqid=0(0x00000000)
A: hmac-md5 96358c90 783bbfa3 d7b196ce abe0536b
seq=0x00000000 replay=0 flags=0x00000000 state=mature
created: Jun  6 16:36:42 2017   current: Jun  6 16:57:26 2017
diff: 1244(s)   hard: 0(s)       soft: 0(s)
last: Jun  6 16:37:43 2017     hard: 0(s)       soft: 0(s)
current: 0(bytes)   hard: 0(bytes)   soft: 0(bytes)
allocated: 0   hard: 0 soft: 0
sadb_seq=3 pid=12468 refcnt=0
192.168.1.12 192.168.1.9
ah mode=transport spi=512(0x00000200) reqid=0(0x00000000)
A: hmac-md5 c0291ff0 14dccdd0 3874d9e8 e4cdf3e6
seq=0x00000000 replay=0 flags=0x00000000 state=mature
created: Jun  6 16:36:42 2017   current: Jun  6 16:57:26 2017
diff: 1244(s)   hard: 0(s)       soft: 0(s)
last: Jun  6 16:37:43 2017     hard: 0(s)       soft: 0(s)
current: 6552(bytes)   hard: 0(bytes)   soft: 0(bytes)
allocated: 7   hard: 0 soft: 0
sadb_seq=0 pid=12468 refcnt=0
root@bendelhoum-VirtualBox:~#

```

Figure IV.15 vérification des modifications

Et pour confirmer que le tunnel à bien été mis en place on a fait le test avec wireshark comme le montre la figure suivante :



No.	Time	Source	Destination	Protocol	Length	Info
35	4.706774000	192.168.1.12	192.168.1.9	ESP	994	ESP (SPI=0x00000201)
37	5.206192000	192.168.1.12	192.168.1.9	ESP	994	ESP (SPI=0x00000201)
39	6.206664000	192.168.1.12	192.168.1.9	ESP	994	ESP (SPI=0x00000201)
45	8.206682000	192.168.1.12	192.168.1.9	ESP	994	ESP (SPI=0x00000201)
88	12.207080000	192.168.1.12	192.168.1.9	ESP	994	ESP (SPI=0x00000201)
178	20.206620000	192.168.1.12	192.168.1.9	ESP	994	ESP (SPI=0x00000201)
343	36.207082000	192.168.1.12	192.168.1.9	ESP	994	ESP (SPI=0x00000201)

Figure IV.16 analyse wireshark

Encapsulating Security Payload (ou *ESP*), est un protocole appartenant à la suite IPsec, permettant de combiner plusieurs services de sécurité : confidentialité, authentification et intégrité.

IV.4.3 Fail2Ban

Le but de fail2ban est d'empêcher une attaque qui, par force brute, trouve un identifiant/mot de passe permettant l'accès à un service. Les postes serveurs ne dormant jamais, ils sont la cible d'attaques automatiques en provenance de partout. Et sans un tel outil, qui sanctionne les tentatives, plus un serveur est rapide à répondre, plus il est menacé [24].

Pour la sécurisation du serveur SIP grâce au Fail2Ban on doit suivre les étapes suivantes :

IV.4.3.1 Installation de fail2ban

Tout d'abord, il faut installer Fail2Ban. Pour cela, entrer la commande suivante :

```
apt-get install fail2ban
```

IV.4.3.2 Autorisation de l'IP de la machine

Afin de ne pas nous bloquer nous-même, nous pouvons mettre notre @ IP (ou une autre) en liste blanche.

Pour cela, éditer le fichier **jail.conf**, et ajouter votre IP dans **ignoreip**.

Dans `sudo nano /etc/fail2ban/jail.conf`

```
[DEFAULT]
```

```
ignoreip = 127.0.0.1 192.168.1.12
```

IV.4.3.3 Modification du logger d'asterisk

Nous devons modifier la configuration du logger d'asterisk pour des raisons de compatibilité de format de date, éditez le fichier `sudo nano /etc/asterisk/logger.conf` et dé-commentons la ligne dateformat comme ceci :

```
[general]
```

```
dateformat=%F %T
```

Asterisk utilisera le format suivant pour les logs : yyyy-mm-dd HH:MM:SS*

Relancez le logger asterisk via la commande shell suivante :

```
Asterisk -rv
```

```
logger reload
```

IV.4.3.4 Création du fichier filtre

Nous devons créer le fichier `sudo nano /etc/fail2ban/filter.d/asterisk.conf` et le remplir avec ceci :

```
[INCLUDES]
```

```
[Definition]
```

```
failregex = NOTICE.* .*: Registration from '.*' failed for '<HOST>:.*' - Wrong password
```

```
NOTICE.* .*: Registration from '.*' failed for '<HOST>:.*' - No matching peer found
```


NOTICE.* .*: Registration from '.*' failed for '<HOST>.*' - No matching peer found

NOTICE.* .*: Registration from '.*' failed for '<HOST>.*' - Username/auth name mismatch

NOTICE.* .*: Registration from '.*' failed for '<HOST>.*' - Device does not match ACL

NOTICE.* .*: Registration from '.*' failed for '<HOST>.*' - Peer is not supposed to register

NOTICE.* .*: Registration from '.*' failed for '<HOST>.*' - ACL error (permit/deny)

NOTICE.* .*: Registration from '.*' failed for '<HOST>.*' - Device does not match ACL

NOTICE.* .*: Registration from \".*\".*' failed for '<HOST>.*' - No matching peer found

NOTICE.* .*: Registration from \".*\".*' failed for '<HOST>.*' - Wrong password

NOTICE.* <HOST> failed to authenticate as '.*\$

NOTICE.* .*: No registration for peer '.*' \\\(from <HOST>\\)

NOTICE.* .*: Host <HOST> failed MD5 authentication for '.*' (.*)

NOTICE.* .*: Failed to authenticate user .*@<HOST>.*

NOTICE.* .*: <HOST> failed to authenticate as '.*'

NOTICE.* .*: <HOST> tried to authenticate with nonexistent user '.*'

VERBOSE.*SIP/<HOST>.*Received incoming SIP connection from unknown peer
ignoreregex =

IV.4.3.5 Création de la prison (jail)

Celle-ci a pour but de faire le lien entre le filtre et le fichier de log. C'est aussi elle qui définit les paramètres du blocage.

Dans le fichier `sudo nano /etc/fail2ban/jail.conf`, ajouter la section suivante :

```
[asterisk-iptables]
```

```
enabled = true
```

```
filter = asterisk
```

```
action = iptables-allports[name=ASTERISK, protocol=all]
```

```
logpath = /var/log/asterisk/messages
```

```
maxretry = 5
```

```
bantime = 3600
```

```
findtime = 120
```

Cette prison définit un maximum de 5 tentatives manquées dans l'espace de 2 minutes. Au-delà, l'utilisateur est bloqué pour 1 heure.

Ces paramètres sont modifiables.

IV.4.3.6 Lancement de Fail2Ban

Redémarrez fail2ban :

```
Sudo /etc/init.d/fail2ban start
```

```
bendelhoum@bendelhoum-VirtualBox:~$ sudo /etc/init.d/fail2ban start
* Starting authentication failure monitor fail2ban [ OK ]
bendelhoum@bendelhoum-VirtualBox:~$
```

Figure IV.16 lancement de Fail2ban

Pour tester Fail2Ban sur Asterisk, entrer la commande suivante :

```
Sudo fail2ban-regex /var/log/asterisk/messages /etc/fail2ban/filter.d/asterisk.conf
```

Cela va demander à Fail2Ban d'analyser le fichier de log, pour voir si le filtre détecte des erreurs d'authentification

En faisant le test avec un faux mot de passe pour nous connecter aucune intrusion n'a eu lieu grâce à la sécurisation.

```
g/asterisk/messages /etc/fail2ban/filter.d/asterisk.conf
Running tests
=====
Use failregex file : /etc/fail2ban/filter.d/asterisk.conf
Use log file : /var/log/asterisk/messages

Results
=====
Failregex: 3 total
|- #) [# of hits] regular expression
| 4) [3] NOTICE.* .*: Registration from '.*' failed for '<HOS
T>:.*' - Username/auth name mismatch
|
Ignoreregex: 0 total

Date template hits:
|- [# of hits] date format
| [2750] MONTH Day Hour:Minute:Second
| [15] Year-Month-Day Hour:Minute:Second
|
Lines: 2766 lines, 0 ignored, 3 matched, 2763 missed
Missed line(s):: too many to print. Use --print-all-missed to
print all 2763 lines
bendelhoum@bendelhoum-VirtualBox:~$
```

Figure IV.17 test de Fail2ban

IV.5 Conclusion

Dans ce chapitre, nous avons présenté quelques solutions pour sécuriser notre serveur SIP pour la VoIP. Nous avons vu qu'il existe un nombre important d'outils (Whois, Wireshark, etc.) que le développeur doit connaître pour éviter les failles de sécurité. Les solutions que nous avons présentées et appliquées à notre serveur dans ce chapitre sont primordiales pour la sécurisation des comptes et aussi les messages SIP.

Conclusion générale et perspectives

L'objectif principal de ce projet consiste à protéger les services dans les infrastructures VoIP. Après avoir étudié les différentes étapes pour l'établir, nous avons étendu une solution de gestion de risques à ses infrastructures qui s'appuient sur le protocole SIP.

En premier, nous avons vu l'étude générale de la voix sur IP et son fonctionnement avec ses différents protocoles. En second, nous avons installé et configuré une solution basée sur l'outil Asterisk, et la création des deux clients SIP configurés avec Zoiper. Troisièmement nous nous sommes intéressés aux vulnérabilités qui peuvent toucher la VoIP et quelques moyens de sécurisation. Et enfin nous avons choisi des outils de récupération d'informations, des logiciels de détection d'intrusion et des solutions pour sécuriser le serveur.

Comme perspective, nous envisageons de considérer d'autres solutions de sécurité pour sécuriser encore plus notre serveur, et aussi de prendre en compte la technologie IAX qui permet l'interconnexion entre serveurs Asterisk.

Références

- [1] CERF, Vinton G. et ICAHN, Robert E. A protocol for packet network intercommunication. *ACM SIGCOMM Computer Communication Review*, 2005, vol. 35, no 2, p. 71-82.
- [2] KARAPANTAZIS, Stylianos et PAVLIDOU, Fotini-Niovi. VoIP: A comprehensive survey on a promising technology. *Computer Networks*, 2009, vol. 53, no 12, p. 2050-2090.
- [3] « Qu'est ce qu'un PABX ? ». Disponible sur le lien : <https://www.3cx.fr/voip-sip/systeme-telephonique-pabx/>
- [4] Etude et mise au point d'un systeme de communication VOIP : application sur un PABX-IP open source "cas de l'agence en douane Getrak" par Yannick YANI KALOMBA, 2009 Université protestante de Lubumbashi
- [5] Loic Debourdeau : « Le protocole SIP ». Disponible sur le lien : <http://www-igm.univ-mlv.fr/~dr/XPOSE2002/DEBOURDEAU/>
- [6] « Introduction à H323 ». Disponible sur le lien : <https://wapiti.telecom-lille.fr/commun/ens/peda/options/st/rio/pub/exposes/exposesser2010-ttnfa2011/barisaux-gourong/H323.html>
- [7] Romain DELETRE & Aurélien MECHIN. Comparaison des technologies de téléphonie sur IP. Enic Telecom Lille1 - Mars 2006
- [8] Nico VanHaute, Julien Barascud et Jean-Roland Conca. « Les protocoles RTP/RTCP ». Disponible sur le lien : <http://www.commentcamarche.net/contents/535-les-protocoles-rtp-rtcp>
- [9] « Les protocoles UDP et TCP ». Tristan DEBEAUPUIS. Disponible sur le lien : http://www.gipsa-lab.grenoble-inp.fr/~christian.bulfone/MIASS/PDF/3-Les_protocoles_UDP_TCP.pdf
- [10] SPENCER, Mark, ALLISON, Mack, et RHODES, Christopher. The asterisk handbook. *Asterisk Documentation Team*, 2003.
- [11] VAN MEGGELEN, Jim, MADSEN, Leif, et SMITH, Jared. *Asterisk: the future of telephony*. " O'Reilly Media, Inc.", 2007.
- [12] SPENCER, Mark, CAPOUCH, Brian, GUY, Ed, et al. Iax: Inter-asterisk exchange version 2. 2010.
- [13] « Echange entre deux serveurs Asterisk ». Disponible sur le lien: http://wiki.ncad.fr/index.php?title=Fichier:ASTERISK_IAX.JPG#filehistory
- [14] Dantu, Ram, et al. "Issues and challenges in securing VoIP." *computers & security* 28.8 (2009): 743-753.

- [15] « Sécurité Asterisk ou quelques moyens de protéger votre serveur VoIP ». TSRIT. Disponible sur le lien : <https://tsrit.com/2013/11/15/securite-asterisk-ou-quelques-moyennes-de-protger-votre-server-voip/>
- [16] « Sécurisation des applications ». CISCO. Disponible sur le lien : http://www.cisco.com/c/fr_fr/solutions/security/implementation/application-security.html
- [17] « sécuritié d'Asterisk ». Disponible sur le lien : <http://www.star2billing.com/securing-asterisk/>
- [18] Qu'est ce que le WHOIS? ». Disponible sur le lien : <https://www.namebay.com/whois/Whols.aspx>
- [19] L'outil HTTrack. Disponible sur le lien : <http://www.httrack.com/page/1/fr>
- [20] L'outil Wireshark. Disponible sur le lien : <http://www.wireshark.org>
- [21] L'outil John the Ripper. Disponible sur le lien : <http://www.openwall.com/john/>
- [22] Redha Bouzaida. Etude et mise en plase d'une solution VoIP securisée. *Mémoire de Master Proffessionnel*. Université virtuelle de Tunis.
- [23] « IPsec ». Briec Jeunhomme. Disponible sur le lien : <http://www.frameip.com/ipsec/>
- [24] La solution Fail2Ban. Disponible sur le lien : <http://www.fail2ban.org>

❖ Résumé

La VoIP permet aux gens d'utiliser Internet comme moyen de transmission pour les communications vocales. Plusieurs protocoles peuvent être envisagés pour cette technologie (SIP, H323, etc.). Asterisk est un outil qui permet de fournir à Linux un commutateur téléphonique complet et totalement libre. Dans ce mémoire, nous avons développé un serveur SIP pour la VoIP sous Asterisk tout en présentant toute les étapes de création et aussi en considérant les problèmes de sécurité. En effet, le nombre d'attaques possibles sur ce type de serveur est considérable. Sécuriser le serveur n'est pas seulement une nécessité mais plutôt une obligation. Nous avons présenté les principales solutions qui permettent de sécuriser le serveur (sécurisation des comptes SIP, sécurisation de la communication entre les clients, etc.). Nous avons aussi utilisé des outils pour montrer que notre serveur pour la VoIP est sécurisé.

❖ Abstract

VoIP allows people to use the Internet as a means of transmission for voice communications. Several protocols can be considered for this technology (SIP, H323, etc.). Asterisk is a tool that provides solutions to Linux with a complete and completely free phone switch. In this work, we have developed a SIP server for VoIP under Asterisk while presenting all the stages of the creation and also considering the security problems. Indeed, the number of possible attacks on this type of server is considerable. Securing the server is not only necessary but an obligation. We have proposed the main solutions that make it possible to secure the server (securing SIP accounts, securing communication between clients, etc.). We also used tools to show that our server for VoIP is secure.

❖ ملخص

الصوت عبر بروتوكول الإنترنت تسمح للناس لاستخدام شبكة الإنترنت باعتبارها وسيلة انتقال للاتصالات الصوتية. يمكن اعتبار عدة بروتوكولات لهذه التكنولوجيا (SIP, H323). Asterisk هو أداة لتوفير حلول للينوكس لتبديل الهاتف و ذلك مجانا. في هذا العمل، انشئنا سيرفر لنقل الصوت عن طريق Asterisk في حين عرض جميع المراحل وأيضا النظر في قضايا السلامة. والواقع أن عددا كبيرا من هجمات محتملة على هذا النوع من السيرفرات. تأمين السيرفر ليس فقط التزاما بل هو واجب. اقترحنا الحلول الرئيسية لتأمين السيرفر (تأمين حسابات SIP، تأمين الاتصال بين العملاء، وما إلى ذلك). كما استخدمنا أدوات لإظهار أن السيرفر لنقل الصوت آمن.