الجـمهورية الجـزائرية الديمقراطـية الشـعبية
République Algérienne Démocratique et Populaire
وزارة التعليم العـالي و البحث العـلمي
Ministère de L'Enseignement Supérieur et de la Recherche Scientifique

UNIVERSITE BLIDA 1
Faculté de Technologie
Département d'Électronique

MEMOIRE DE MASTER
En Télécommunication

Spécialité : Réseaux & Télécommunications

THÈME :

Sécurisation d'une infrastructure VOIP basée sur Yate avec l'IDS Suricata

Réalisé par
Mr.OULD KHAOUA Riadh Imed Eddine
Mr.KHEGAR Abd El Hafidh

Encadré par
Mr.MEHDI Merouane
Mlle.BENACHOUR Lina

Juin 2024

Remerciement

*Louange à **Allah**, le Tout-Miséricordieux, le Très-Miséricordieux. C'est grâce à Sa bienveillance et à Sa guidance que nous avons pu achever ce modeste travail. Nous Lui adressons toute notre gratitude pour nous avoir doté de la faculté de raisonnement et nous avoir insufflé le désir d'acquérir le savoir.*

*En premier lieu, nous tenons à exprimer notre profonde reconnaissance à **nos chers parents.** Leur soutien indéfectible, leur amour inconditionnel et leurs sacrifices immenses ont été notre source de motivation tout au long de notre parcours académique. Nous leur sommes infiniment reconnaissants pour tout ce qu'ils ont fait pour nous permettre de réussir.*

*Nous adressons également nos sincères remerciements à notre encadreur, **M.MEHDI et L.Benachour**, pour leurs précieux conseils, leur orientation éclairée et leur aide constante tout au long de l'élaboration de notre projet de fin d'études. Leur patience, leur disponibilité et leur rigueur ont été d'une importance capitale pour la réussite de ce travail.*

*Nous sommes également reconnaissants envers **le président et les membres du jury** d'avoir accepté d'examiner et d'évaluer notre travail. Nous apprécions grandement le temps qu'ils nous ont accordé et les remarques constructives qu'ils nous ont faites.*

Nos remerciements s'étendent également à l'ensemble des professeurs et enseignants qui ont contribué à notre formation. Leurs cours, leurs conseils et leur encadrement ont été essentiels à notre développement intellectuel et à notre progression dans cette filière.

Enfin, nous ne saurions oublier toutes les personnes qui, de près ou de loin, ont contribué à la réalisation de ce projet. Nous leur exprimons notre gratitude la plus profonde pour leur soutien, leur encouragement et leur bienveillance.

Que ce travail soit un témoignage de notre reconnaissance et de notre attachement à tous ceux qui nous ont accompagnés sur le chemin de la connaissance.

ملخص

إن تأمين أنظمة نقل الصوت عبر بروتوكول الإنترنت في الشركات يمثل تحديا كبيرا بسبب التطور المستمر للتهديدات وأساليب الاختراق التي تستهدف اختراق هذه الأنظمة. في هذا السياق يندرج عملنا. لقد نشرنا بنية آمنة ضمن شبكة حاسوبية للشركة. من هذا المنظور، استخدمنا خادم يات وواجهة فري سنترال الرسومية وهواتف هواوي فيو بوينت ٠١٢٨ وعملاء برامج يات. قمنا بمحاكاة هجمات رفض الخدمة الموزعة والتنصت السري، وهجمات انتحال الهوية، من أجل استخراج توقيعاتها. تم تنفيذ هذه التوقيعات على نظام كشف التسلل سوريكاتا، للكشف عن هذه الهجمات.

الكلمات المفتاحية: سوريكاتا، فري سنترال، يات ، الصوت عبر بروتوكول الإنترنت

Abstract

Securing VoIP systems in enterprises represents a major challenge due to the constant evolution of threats and hacking methods aimed at compromising these systems. It is in this context that our work is situated. We have deployed a secure VoIP architecture within an enterprise computer network. In this perspective, we used the Yate server, the FreeSentral graphical interface, Huawei Viewpoint 8210 IP phones and Yate Client softphones. We simulated distributed denial of service (DDoS) attacks, ARP spoofing, eavesdropping, and identity theft attacks in order to extract their signatures. These were implemented on the Suricata IDS, allowing for the detection of attacks.

Keywords: VOIP, yate, FreeSentral, Suricata

Résumé

La sécurisation des systèmes VoIP dans les entreprises représente un défi majeur en raison de l'évolution constante des menaces et des méthodes de piratage informatique visant à compromettre ces systèmes. C'est dans ce contexte que s'inscrit notre travail. Nous avons déployé une architecture VoIP sécurisée au sein d'un réseau informatique d'entreprise. Dans cette optique, nous avons utilisé le serveur Yate, l'interface graphique FreeSentral, des clients IP phones Huawei Viewpoint 8210 et des clients softphones Yate Client. Nous avons simulé les attaques par déni de service distribué (DDoS), l'ARP spoofing, l'écoute clandestine et des attaques d'usurpation d'identité, afin d'extraire leurs signatures. Ces dernières ont été implémentées sur l'IDS Suricata, permettant de détecter les attaques.

Mots Clée : VOIP, Yate, FreeSentral, Suricata

Liste des Acronymes et Abréviations

ACK Accknowledgement

ARP Address Resolution Protocol

DECT Digital Enhanced Cordless Telecommunications

DDoS Distributed Denial of Service

DoS Denial of Service

DNS Domain Name System

DSP Digital Signal Processing

FTP File Transfert Protocol

GW Gateway

GK GateKeeper

HIDS Host-Based Intrusion Detection System

HIPS Host-Based Intrusion Prevention System

HTTP HyperText Transfer Protocol

HP Hewlett-Packard

IAX Inter-Asterisk Exchange

ICMP Internet Control Message Protocol

IDS Intrusion Detection System

IETF Internet Engineering Task Force

IP Internet Protocol

IPS Intrusion Prevention System

IPBX Internet Protocol Branch Exchange

LAN Local Area Network

MAC Media Access Control

MACOS Macintosh Operating System

MCU Multipoint Control Unit

MGW Media Gateway

MITM Man In The Middle

MSOFFICE Microsoft Office

NIDS Network Intrusion Detection System

NIPS Network Intrusion Prevention System

NSM Network Security Monitoring

PABX Private Automatic Branch Exchange

PDF Portable Document Format

PC Personal Computer

RTC Réseau Téléphonique Commuté

RTCP Real-time Transport Control Protocol

RTP Real-time Transport Protocol

RNIS Réseau Numérique à Intégration de Services

SIP Session Initiation Protocol

SMB Server Message Bloc

SRTP Secure Real-time Transport Protocol

SSL Secure Sockets Layer

SSRC Synchronization Source

TCP Transmission Control Protocol

TLS Transport Layer Security

UDP User Datagram Protocol

VOIP Voice Over IP

VPN Virtual Private Network

WIFI Wireless Fidelity

WIPS Wireless Intrusion Prevention System

YATE Yet Another Telephony Engine

Table des matières

Table des figures

Introduction Générale

L'essor d'Internet a révolutionné les télécommunications en propulsant la technologie IP au cœur de notre quotidien. Réservés initialement à un usage scientifique et militaire, les protocoles IP se sont désormais répandus dans tous les aspects de la vie, engendrant l'émergence de la voix sur IP (VOIP).

Contrairement à la téléphonie traditionnelle basée sur la commutation de circuits, la voip exploite la commutation par paquets et des logiciels dédiés pour transmettre la voix sur les réseaux informatiques. Cette révolution technologique ouvre de nouvelles perspectives de communications vocales entre ordinateurs ou téléphones ip, à moindre coût et avec une qualité de service améliorée.

Bien que l'adoption de la voip soit aujourd'hui une nécessité face à l'obsolescence des solutions analogiques et à l'essor du télétravail, son déploiement sur des réseaux IP non sécurisés l'expose à diverses menaces telles que les attaques DDoS, le spoofing, les attaques de l'homme du milieu ou encore l'écoute clandestine. À titre d'exemple, en 2015, des cybercriminels ont réussi à pirater le système voip de l'opérateur télécom belge Belgacom, leur permettant d'espionner les communications durant plusieurs années. La mise en place de mesures de sécurité robustes comme les pare-feu, ips et ids est donc cruciale pour protéger l'intégrité des communications vocales.

Notre projet vise à déployer une architecture voip sécurisée dans un environnement d'entreprise. Nous explorerons l'installation du serveur Yate, ainsi que son interface graphique FreeSentral. Cette infrastructure comprend deux clients Yate ainsi que deux téléphones ip Huawei ViewPoint. Après avoir validé le bon fonctionnement des appels, nous allons simuler plusieurs attaques depuis un ordinateur sous Kali Linux afin d'analyser les signatures propres à ces attaques. Ces signatures nous permettront d'élaborer nos propres règles de sécurité à implémenter dans suricata, un système de détection et de prévention d'intrusions (IDS/IPS).

Le but de cette étude est de mettre en place la sécurité de notre architecture voip en déployant nos propres règles de protection efficaces contre les attaques potentielles.

Le mémoire abordera dans Le premier chapitre présentation sur les généralités sur la technologie voip.

Le deuxième chapitre se focalise sur les principales menaces et attaques en proposant des solutions concrètes pour les contrer.

Le troisième chapitre guidera le lecteur dans l'installation et la configuration du serveur Yate, en incluant la mise en place de son interface graphique FreeSentral. Des tests d'appels seront réalisés pour valider la fonctionnalité du serveur.

Enfin, le quatrieme chapitre aborde la thématique de la sécurité de notre architecture voip, en détectant les menaces en utilisant nos propres régles de détection implémentées dans l'IDS Suricata.

Chapitre 1

Généralités sur la voix sur IP

1.1 Introduction

La voix sur IP, ou VOIP (Voice over IP), s'est imposée comme une technologie incontournable dans le paysage des télécommunications modernes. En acheminant les communications vocales directement sur les réseaux ip, la voip offre de nouvelles perspectives tant sur le plan technologique qu'économique, ouvrant la voie à des usages et services innovants.

D'un point de vue technologique, la voip repose sur des protocoles et codecs spécifiques qui encapsulent la voix dans des paquets IP et gèrent la signalisation et le transport de bout en bout. Les principaux protocoles utilisés sont H.323, RTP/RTCP et SIP. L'infrastructure nécessaire à la VOIP s'appuie sur des serveurs dédiés (PABX/IPBX), des passerelles de media (MGW) et des équipements réseau dimensionnés pour supporter le trafic voix et garantir sa qualité de service.

Sur le plan économique, la voip permet de faire transiter voix et données sur un réseau ip convergent, réduisant ainsi les coûts d'infrastructure. Son déploiement dans les entreprises génère des économies substantielles sur la facture télécom. De plus, la voip ouvre la porte à de nouveaux modèles économiques et usages pour les opérateurs [29].

1.2 VOIP

1.2.1 Définition

Le terme **"Voice Over Internet Protocol"**, ou plus simplement **"voip" (voix sur ip)**, désigne une technique permettant la communication vocale et multimédia (voix, vidéo et données) sur des réseaux compatibles avec le protocole internet (IP) [25].

La technologie voip permet d'acheminer le trafic vocal et multimédia sous forme de paquets de données numériques sur des infrastructures réseau ip, qu'elles soient publiques (comme internet) ou privées (réseaux d'entreprise ou opérateurs) [25].

La VOIP comprend les communications de PC à PC. Pour ce type de communication, chaque utilisateur doit disposer d'un logiciel approprié. Deuxième catégorie de voix sur ip, les communications de PC à téléphone (PC to Phone). Dans les deux cas, le PC communicant est appelé Softphone, terme qui insiste sur l'émulation du PC en téléphone grâce à un logiciel [22].

1.2.2 Principe de fonctionnement

La voip, comme son nom l'indique, permet de transporter des communications vocales sur un réseau ip (internet protocol), qui fonctionne en envoyant des données sous forme de paquets [23].

Avant d'être envoyée, la voix subit un traitement spécifique en plusieurs étapes :

1.Numérisation : Conversion du signal analogique en données numériques.

2.Compression : Réduction de la quantité de données.

3.Découpage en paquets : Division des données en petits paquets numérotés.

À la réception [23] :

1.Réassemblage des paquets : Reconstitution des données vocales dans l'ordre correct.

2.Décompression : Conversion des données compressées en leur format d'origine.

3.Conversion numérique-analogique : Transformation des données numériques en signal vocal audible.

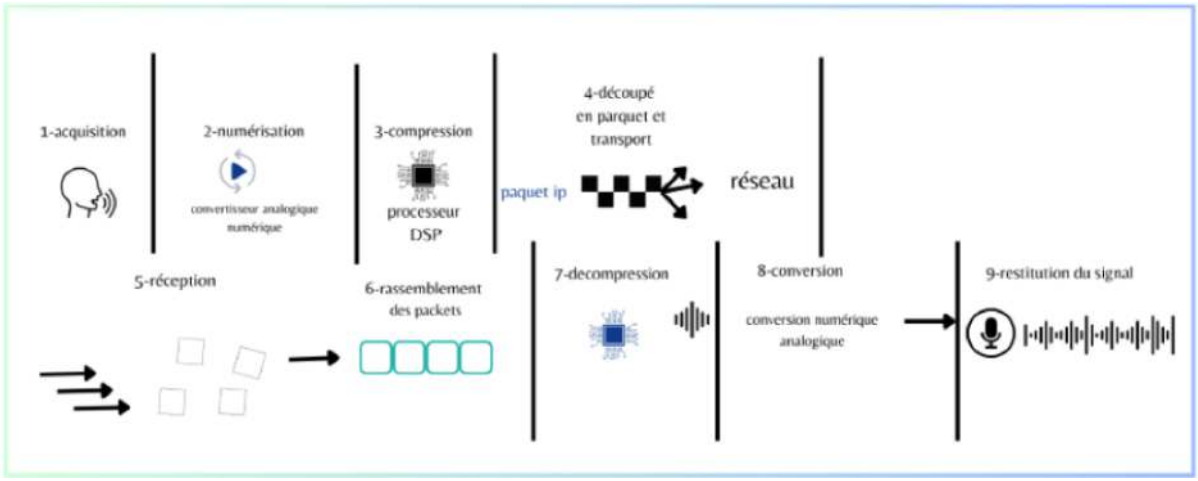


Figure 1.1 – Principe de Fonctionnement de voip [31]

1.2.3 Architecture de VOIP

On trouve dans l'architecture de voip les composants suivants :

•**Le routeur :** Est un équipement réseau essentiel qui assure l'acheminement des données à travers le réseau. Son rôle principal est de transférer les données entre différentes interfaces réseau [23].

•**La passerelle :** Quant à elle, fait office d'interface entre le réseau commuté traditionnel et le réseau IP. Elle assure la connexion et la communication entre ces deux types de réseaux [23].

•**Le switch :** Est un dispositif multiport qui relie plusieurs segments d'un même réseau informatique. Il agit comme un pont, permettant l'interconnexion et l'échange de données au sein du réseau.

•**PABX/IPBX :**

-PABX : Est un système de télécommunication principalement utilisé pour interconnecter les postes téléphoniques internes d'un établissement (lignes intérieures) avec le réseau téléphonique public extérieur (lignes externes) [20].

-IPBX : L'IPBX est un serveur de communication intégré qui utilise le protocole sip pour communiquer avec les postes téléphoniques clients. Il permet de converger le réseau téléphonique et le réseau informatique d'une petite ou moyenne entreprise en un seul réseau unifié gérable [13].

L'IPBX fonctionne avec différents types de téléphones IP (de bureau, WiFi, Bluetooth, DECT), des passerelles voip et des adaptateurs téléphoniques analogiques. Il achemine les

appels entre les téléphones ip clients, les téléphones analogiques traditionnels et le réseau téléphonique public commuté. Des fonctionnalités vocales avancées comme la téléconférence, le répondeur vocal et l'accueil automatique sont intégrées de manière transparente pour tous les postes [13].

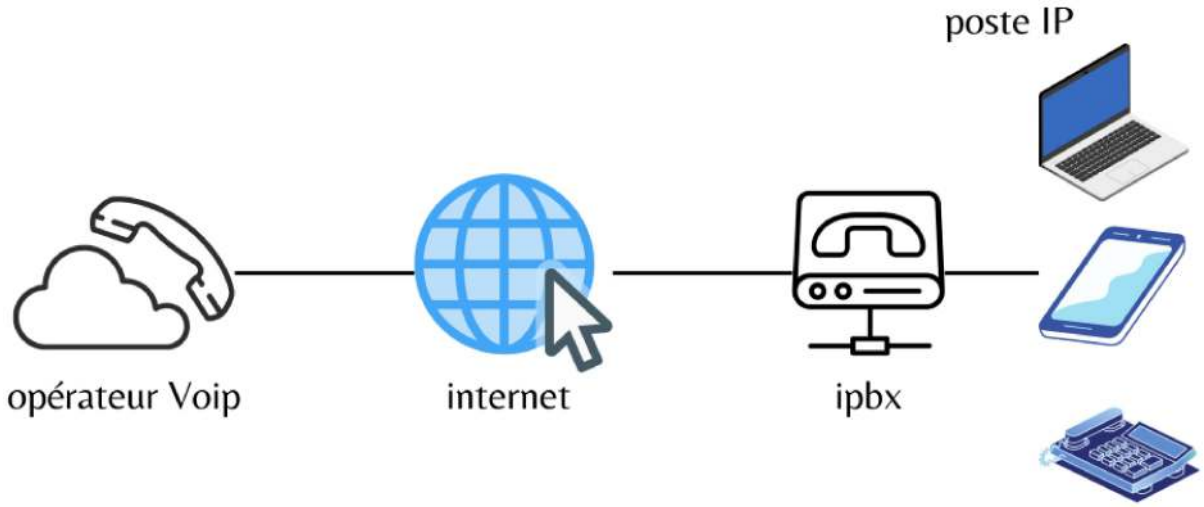


Figure 1.2 – IPBX [1]

•**Les terminaux :** Sont les périphériques situés à l'extrémité du réseau, utilisés par les utilisateurs finaux. Ils peuvent prendre la forme de logiciels téléphoniques installés sur les ordinateurs personnels ou d'interfaces audio comme des microphones et des haut-parleurs connectés à la carte son [23].

•**Le Gatekeeper :** Est un élément logiciel qui apporte une intelligence supplémentaire à la passerelle. Il agit comme un compagnon logiciel, offrant des fonctionnalités avancées à la passerelle pour une gestion optimisée des communications [23].

Ces différents composants forment l'infrastructure nécessaire pour permettre la communication vocale et la transmission de données sur un réseau ip, en assurant l'interopérabilité avec les réseaux traditionnels [23].

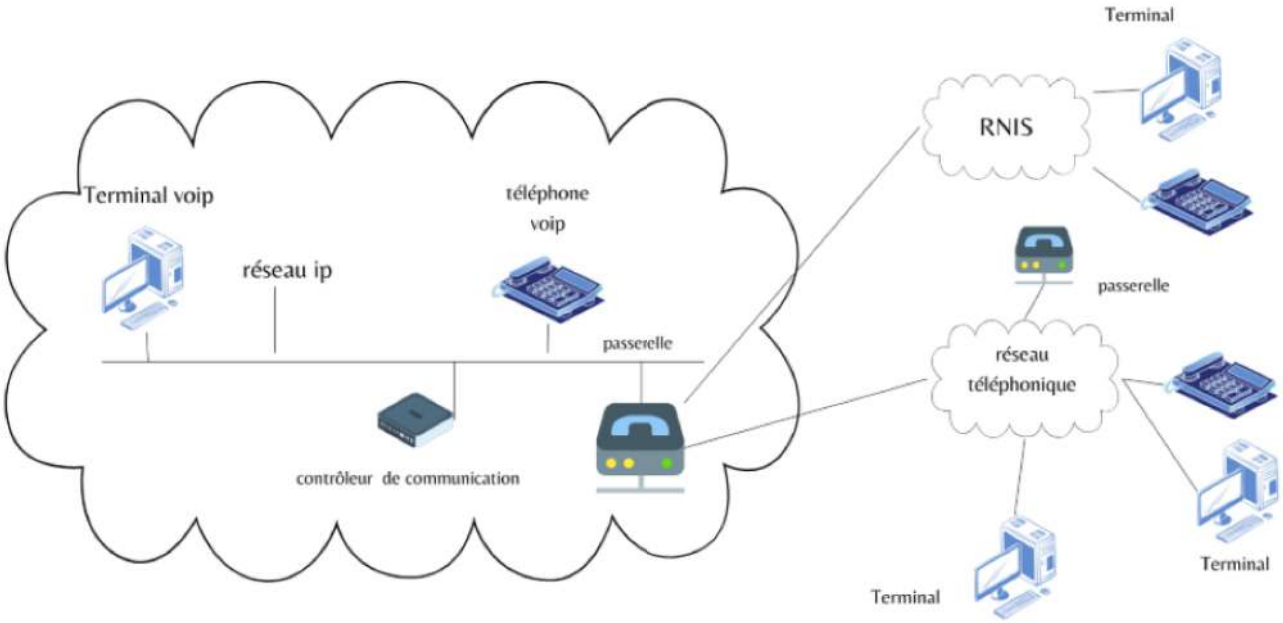


Figure 1.3 – Architecture VOIP [2]

1.3 Le Protocole H.323

1.3.1 Définition

H.323 est un protocole établie par l'Union Internationale des Télécommunications pour assurer la communication en temps réel sur des réseaux voip. Il définit l'un des protocoles de signalisation les plus connus et largement utilisés dans le domaine de la voip [18].

Le Protocole H.323 spécifie les règles et les procédures nécessaires pour établir, maintenir et terminer des sessions de communication multimédia, y compris les appels vocaux et vidéo sur des réseaux basés sur le protocole ip [18].

1.3.2 L'architecture de H.323

L'architecture de H.323 est généralement composée des quatre catégories d'entités suivantes [19] :

•**Terminal :** Un terminal H.323 est un équipement connecté à un réseau qui permet des échanges multimédias en temps réel avec un autre terminal. En fonction de ses capacités, un terminal peut prendre en charge la voix seulement, la voix et les données, la voix et la vidéo, ou la voix, les données et la vidéo simultanément.

•**Passerelle :** Une passerelle H.323 (GW) est un point d'extrémité sur le réseau qui permet

des communications en temps réel entre les terminaux H.323 sur le réseau à commutation de paquets et d'autres terminaux sur un réseau à commutation de circuits ou vers une autre passerelle H.323.

•**La Gatekeeper (GK) :** Est une entité H.323 sur le réseau qui fournit la traduction d'adresses et contrôle l'accès au réseau pour les terminaux, passerelles et unités de contrôle multipoint (MCU) H.323. La Gatekeeper peut également fournir d'autres services tels que la gestion de la bande passante et la localisation des passerelles.

•**Unité de contrôle multipoint (MCU) :** Est un point d'extrémité sur le réseau qui permet à trois terminaux ou plus ainsi qu'à des passerelles de participer à une conférence multipoint.

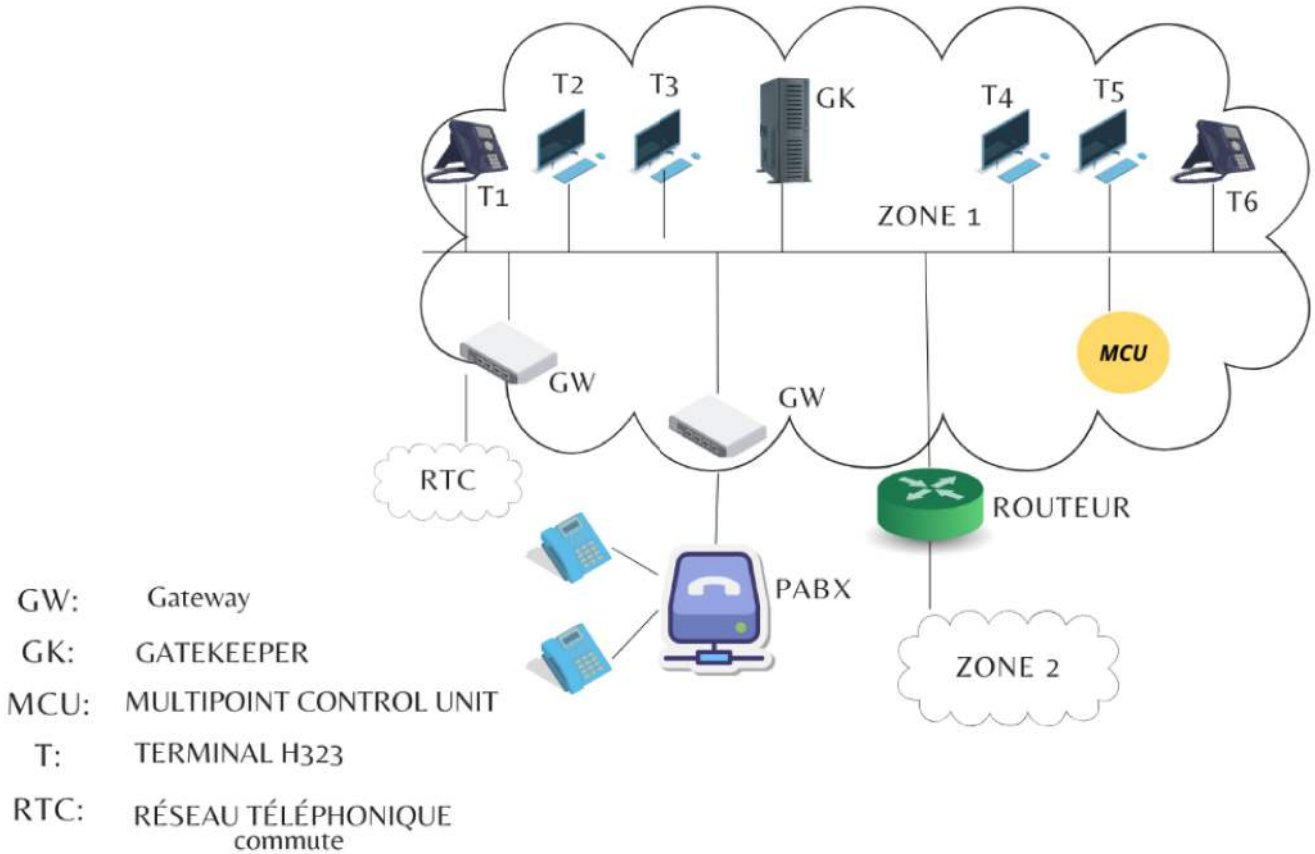


Figure 1.4 – L'Architecture du Protocole H.323 [31]

1.4 Les codecs

Les codecs (codeurs/décodeurs) sont des composants essentiels utilisés dans les protocoles de voix sur ip, y compris H.323, pour encoder et décoder les flux multimédias

transmis sur le réseau. Leur rôle est de définir le niveau de compression et les algorithmes de décompression à appliquer aux données audio et vidéo afin de les acheminer efficacement sur l'infrastructure réseau convergente [24].

1.5 Le protocole RTP

Le protocole RTP est conçu pour acheminer efficacement les flux multimédias en temps réel comme l'audio et la vidéo, via UDP, sur des réseaux uni ou multidiffusion. Bien qu'il ne garantisse pas une qualité de service, rtp apporte des fonctionnalités adaptées au transport en continu de ce type de données, notamment l'identification des sources, le séquençage des paquets et le marquage temporel. Il permet ainsi une transmission en temps réel optimisée sans les mécanismes lourds de fiabilisation complets [24].

1.6 Le protocole RTCP

RTCP est un protocole compagnon de RTP qui permet le contrôle et la supervision de la qualité de service lors de sessions multimédias sur des réseaux IP. Tous les participants échangent périodiquement des paquets RTCP contenant des statistiques sur la distribution des flux (taux de perte, délais, etc). Cela permet d'avoir une visibilité en temps réel sur l'état du réseau et d'ajuster dynamiquement les paramètres de transmission, dans le but d'optimiser la qualité d'expérience pour tous. Son rôle de monitoring et de contrôle compense le manque de fiabilité inhérent au protocole RTP [24].

1.7 Le Protocole SIP

SIP C'est un protocole de signalisation pour l'établissement des sessions de communication voip. Fonctionnant sur une architecture client-serveur similaire à HTTP. Il permet aux clients d'émettre des requêtes pour créer, modifier ou terminer des sessions multimédias impliquant un ou plusieurs participants [18].

1.8 Le Protocole IAX

Le protocole IAX est un protocole de signalisation pour les réseaux voip, tout comme sip et H.323. Contrairement à ces derniers, iax ne met pas en œuvre le protocole RTP pour le transport des données [18].

1.9 Étude des différents serveurs de VOIP (PABX)

1.9.1 YATE

YATE est un serveur de voip open source fonctionne sous Linux qui remplit les mêmes fonctions qu'un pabx, mais avec des performances et une flexibilité d'utilisation accrues [7].

1.9.2 Asterisk

Asterisk est un serveur voip pabx open source fonctionne sous Linux et d'autres systèmes Unix [7].

1.10 Types de téléphones VoIP

1.10.1 Softphones

Un softphone est une application logicielle qui s'installe sur votre ordinateur, tablette ou smartphone, et qui a la même fonction qu'un téléphone ip.

1.10.1.1 ZoiPer

Zoiper est une application de softphone qui vous permet de passer des appels vocaux sur ip. Zoiper fonctionne sur une multitude de plateformes différentes, peu importe que vous utilisiez Linux, Windows et MacOS [8].

1.10.1.2 Yate Client

Yate Client est un logiciel de téléphonie basé sur le serveur Yate. Il est compatible avec plusieurs plateformes : Windows, MacOS et Linux [9].

1.10.2 Hardphones

Le hardphone est un téléphone ip physique, un appareil matériel dédié conçu spécifiquement pour les communications voix sur ip. Ils se connectent directement à un réseau IP et permettent les appels voix sur ip.

Les hardphones offrent souvent plus de fonctionnalités avancées adaptées aux environnements professionnels que les softphones.

1.10.2.1 ViewPoint 8210

ViewPoint 8210 est un nouveau vidéophone de génération permettant des communications en face à face sur les réseaux à large bande. Portable et compact, il convient aussi bien aux applications personnelles qu'aux entreprises. Son apparence moderne et ses fonctionnalités conviviales permettent aux utilisateurs de bénéficier de communications vidéo et audio de qualité. Compatible avec les systèmes H.323 ou sip. ViewPoint 8210 peut interopérer avec divers terminaux, tels que les vidéophones, téléphones ip, terminaux vidéo de groupe, téléphones mobiles 3G (via une passerelle 3G) et téléphones RTC (via une passerelle voip) [10].

1.11 Les interfaces Graphiques

En plus des IPBX vus précédemment, il existe des interfaces de contrôle et de gestion, parmi lesquelles FreePBX et FreeSentral.

1.11.1 FreePBX

FreePBX est une interface utilisateur graphique web open-source qui administre le système Asterisk PBX, une solution de communications unifiées. Publié pour Linux en novembre 2004, FreePBX est maintenu par une communauté de développeurs et contributeurs bénévoles. Leur objectif est de simplifier l'utilisation de ce système PBX complexe [11].

1.11.2 FreeSentral

FreeSentral est un IPBX complet , constitué d'une distribution Linux, d'un ipbx et d'une interface utilisateur graphique web pour une configuration facile [12].

1.12 Conclusion

La Voix sur IP représente une révolution dans les télécommunications, offrant flexibilité, convivialité, coûts réduits et nouveaux services par rapport à la téléphonie traditionnelle. Les entreprises l'adoptent massivement pour rester compétitives. La voip vise à libérer l'utilisateur des contraintes du téléphone physique. Les protocoles sip, H.323, RTP et RTCP constituent les bases techniques de cette technologie permettant de transmettre la voix sur des réseaux ip.

Avec les nouvelles technologies, les aspects défensifs et offensifs de la sécurité des systèmes de téléphonie ip font face à de nouveaux défis. Bien qu'il soit plus difficile d'intercepter les communications voip par rapport aux réseaux traditionnels, cela reste possible avec les connaissances et équipements adéquats.

Le prochain chapitre se concentrera sur les menaces et les attaques contre les réseaux voip, en détaillant les attaques connues, puis fournira une description sur les meilleures pratiques pour sécuriser les communications voip.

Chapitre 2

Les vulnérabilités de la VoIP et mesures de sécurité

2.1 Introduction

L'adoption de la voix sur ip par les entreprises a permis de bénéficier de nouveaux services comme la vidéoconférence et le transfert de données, réduction de couts. Cette convergence de la voix et des données sur une infrastructure IP unique nécessite en effet de renforcer les mesures de sécurité [31].

Parmi les menaces pesant sur la sécurité des systèmes voip, on peut citer les attaques par déni de service, les attaques de l'homme du milieu, Les écoutes clandestines interceptant les communications voix, Les attaques par usurpation d'identité (spam vocal, phishing vocal, etc.) visant à tromper les utilisateurs, etc [31].

Ces vulnérabilités doivent être soigneusement analysées afin de mettre en place une protection efficace. Pour contrer ces attaques, différentes méthodes de sécurisation sont appliquées, telles que les pare-feux, les systèmes de prévention d'intrusion (IPS), les proxies et les antivirus [31].

2.2 Les attaques contre la VoIP

La voip est devenue la technologie prédominante permettant aux personnes de communiquer, représentant la majorité des systèmes et des appareils dans les entreprises. Elle est également largement utilisée par les fournisseurs de services et les consommateurs [17].

Cependant, la voip présente de nombreux défis en matière de sécurité. Avec l'adoption croissante de la voip sur les réseaux publics, qui deviennent de plus en plus hostiles, il est

crucial d'identifier et de traiter ces menaces et attaques significatives liées à la voip. La sécurité de la VoIP est une priorité essentielle pour garantir des communications vocales fiables et sécurisées dans les entreprises et auprès des consommateurs [17].

Il existe deux principales classes des attaques contre un environnement voip :

•**Les attaques sur les protocoles de communication VOIP :** Ciblent les protocoles sous-jacents utilisés par la technologie. Puisque les protocoles voip utilisent tcp et udp comme moyens de transport, ils sont également vulnérables aux attaques visant ces protocoles. Par exemple, les attaques de L'empoisonnement ARP et d'usurpation d'identité peuvent être utilisées pour compromettre les communications VoIP [14].

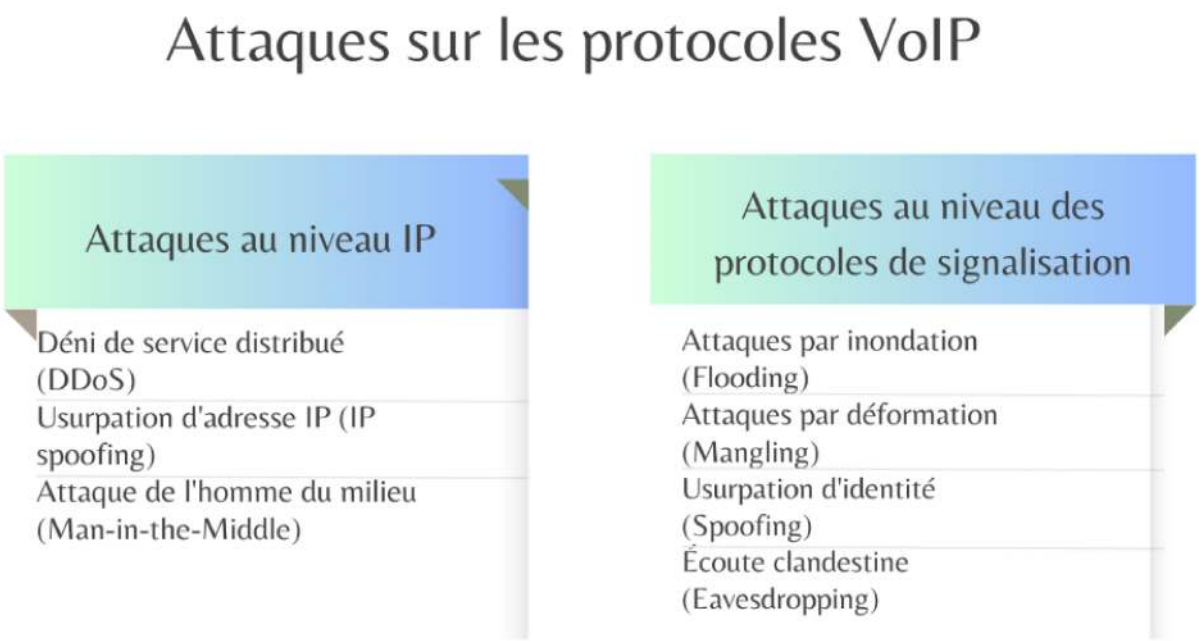


Figure 2.1 – Les attaques sur les protocoles de communication VoIP [30]

•**Les attaques concerne les vulnérabilités présentes dans l'infrastructure sur laquelle les éléments VoIP sont déployés :** L'infrastructure voip comprend divers composants tels que les téléphones ip, les passerelles, les serveurs (proxy, registre, etc.). Ces systèmes peuvent présenter des failles de sécurité qui permettraient à un attaquant de compromettre les communications voip. Par exemple, des vulnérabilités dans le micrologiciel ou le système d'exploitation des téléphones ip pourraient être exploitées pour accéder illégalement à l'appareil. De même, des faiblesses dans la configuration ou le code des serveurs voip crucials comme les proxys ou les registres pourraient conduire à des violations de sécurité [14].

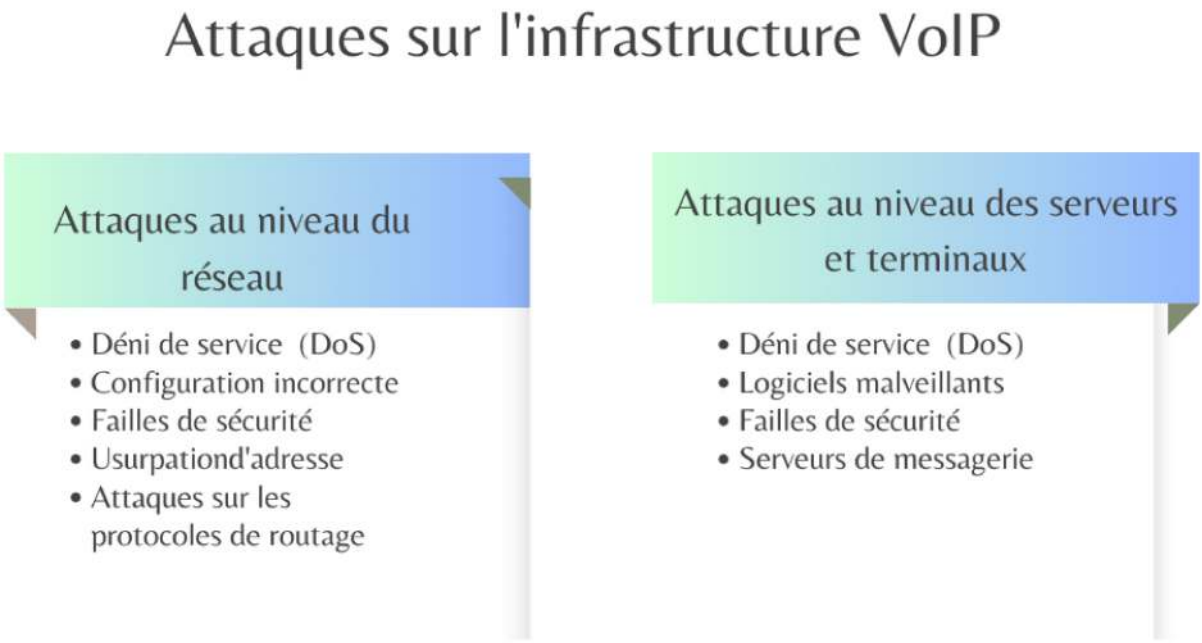


Figure 2.2 – Les Attaques sur l'infrastructure VoIP [30]

2.3 Les attaques sur les protocoles de communication VoIP

2.3.1 Attaque usurpation d'identité

Dans le domaine informatique, l'usurpation d'identité fait référence au vol d'identité, où une personne se fait passer pour une autre personne, une organisation ou une entreprise dans le but d'accéder à des informations personnelles sensibles. Cela inclut les noms d'utilisateurs, les mots de passe, les informations bancaires et les numéros de cartes de crédit [28].

Il existe plusieurs méthodes pour réaliser une attaque usurpation d'identité, en voici quelques-unes :

•**Svmap :** C'est un scanner sip, il liste les périphériques SIP trouvés sur une plage ip [31].

•**Nmap :** Nmap est un outil de découverte de réseaux et d'audit de sécurité. Il est couramment utilisé par les administrateurs réseau et les professionnels de la sécurité pour détecter les ports ouverts sur des systèmes cibles,ce qui peut être utile pour adapter les tests de sécurité [21].

•**Metasploit :** Est un logiciel utilisé pour exploiter les failles de sécurité sur une machine cible dans le but de la compromettre et d'obtenir un accès [31].

2.3.2 ARP Spoofing

L'ARP spoofing consiste à envoyer des messages ARP contrefaits sur un réseau, dans le but d'associer l'adresse MAC de l'attaquant à l'adresse ip d'un autre périphérique présent sur ce réseau. Cela permet à l'attaquant d'intercepter les données destinées au périphérique légitime. Une fois cette interception établie, l'attaquant a la possibilité d'espionner le trafic réseau, de modifier les données échangées, ou encore de mener une attaque par déni de service en provoquant la perte totale ou partielle des paquets circulant sur le réseau [14].

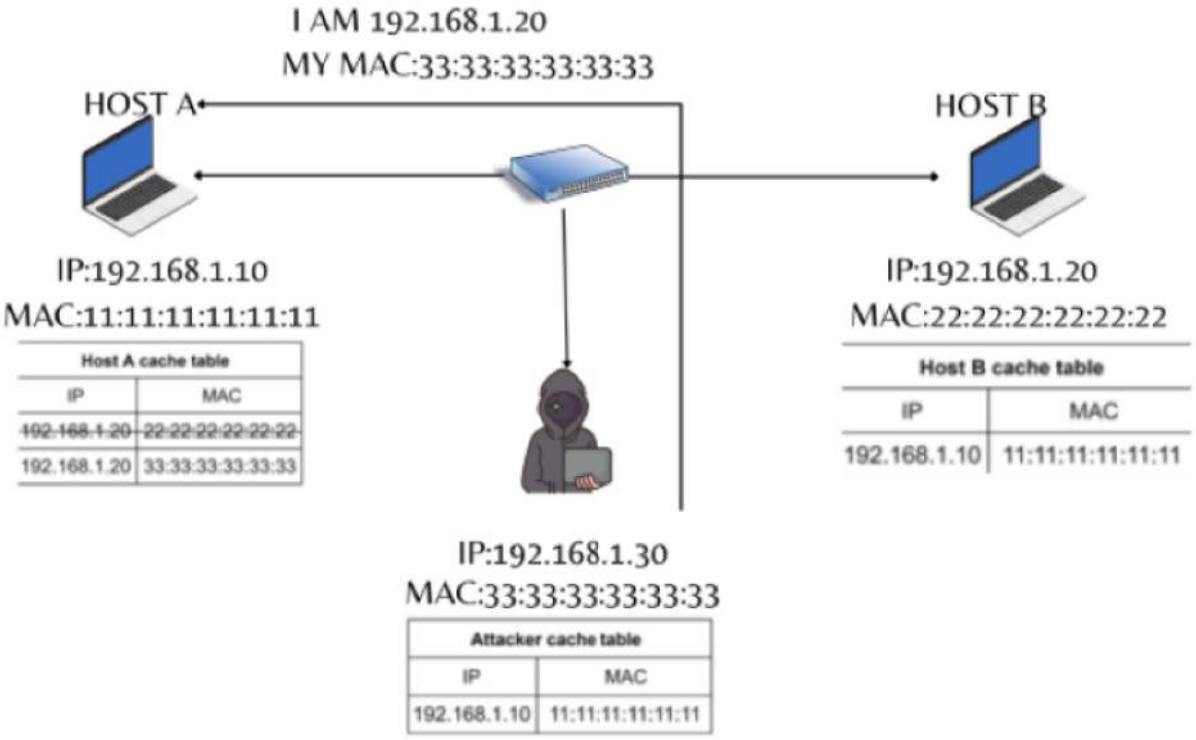


Figure 2.3 – L'attaque ARP Spoofing [26]

2.3.3 Écoute clandestine (Eavesdropping)

L'Eavesdropping consiste à intercepter illégalement une conversation téléphonique. Dans un environnement voip, un attaquant ayant accès au réseau peut capturer le trafic de données et déchiffrer le contenu vocal de la communication afin d'écouter la conversation de manière clandestine [31].

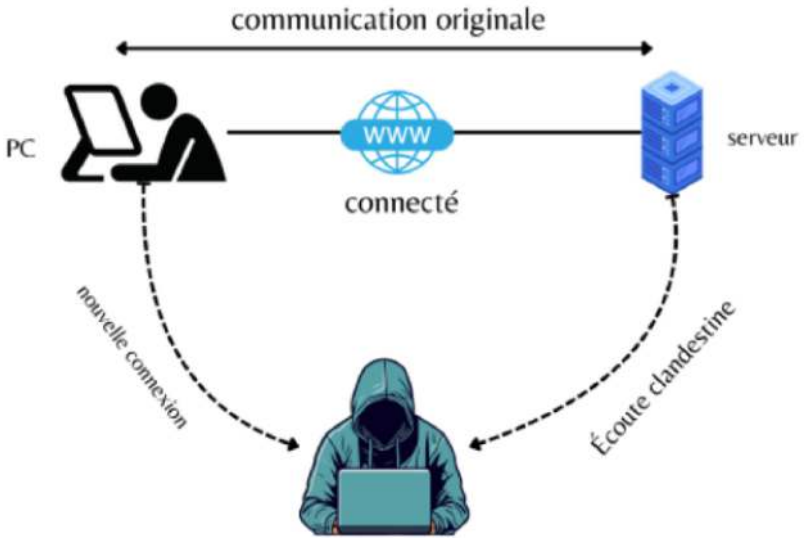


Figure 2.4 – Eavesdropping [3]

Pour réaliser cette attaque, nous utiliserons les outils **Ettercap** pour tester l'attaque l'homme du milieu et **Wireshark** pour objet d'écouter le réseau.

1-Ettercap : Est un outil logiciel open source d'analyse et d'audit de réseaux informatiques, disponible dans la distribution Kali Linux. Il dispose de fonctionnalités permettant de mener diverses attaques sur les protocoles de VoIP [31].

2-L'attaque l'homme du milieu : Les attaques par **MITM** sont un type d'attaque de cybersécurité qui permet aux attaquants d'espionner les communications entre deux cibles [14].

3-L'attaque ARP Poisining : L'empoisonnement ARP est une technique de cyberattaque qui exploite le protocole arp pour intercepter, rediriger ou espionner le trafic réseau [14].

4-Wireshark : Est un logiciel open source d'analyse de trafic réseau, largement utilisé pour le dépannage, l'analyse, le développement de protocoles, la formation et également à des fins malveillantes comme le piratage [31].

2.3.4 Le déni de service distribué

Une attaque de **DoS** vise à surcharger un serveur voip avec un grand nombre de requêtes jusqu'à ce qu'il ne puisse plus répondre et s'arrête. Cela permet potentiellement de saturer les réseaux des entreprises utilisant la voip, bloquant ainsi les communications internes, externes, ainsi que le système d'information [21].

Cependant, l'approche privilégiée par les attaquants s'est tournée vers le déni de service

distribué **(DDoS)**. Une attaque DDoS repose sur des attaques DoS simultanées menées par plusieurs systèmes contre une seule cible. Cela réduit le temps nécessaire pour l'attaque et amplifie ses effets dévastateurs [21].

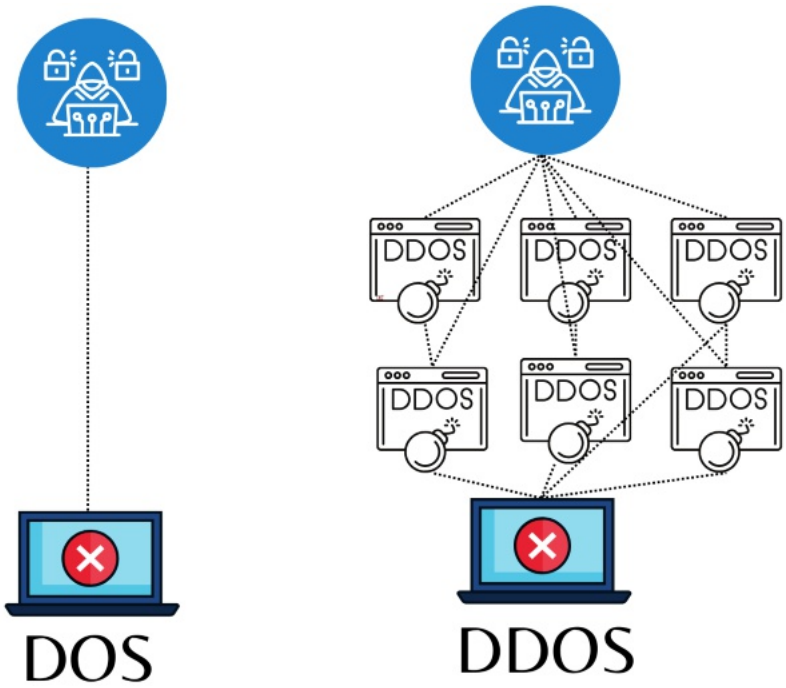


Figure 2.5 – DoS/DDoS [15]

Il existe plusieurs méthodes pour réaliser une attaque DOS, en voici quelques-unes [14] :

•**Hping3 :** Permet d'envoyer des paquets TCP/IP modifiés et de contrôler la taille, le nombre et la fragmentation des paquets dans le but de surcharger la cible et de contourner ou attaquer les pare-feux.

•**Inondation par invites (Invite-flooding) :** Cette méthode consiste à envoyer une grande quantité de données inutiles sur un réseau pour le rendre inutilisable en épuisant ses ressources.

2.4 Les attaques sur l'infrastructure VOIP

2.4.1 Faiblesses dans la configuration des dispositifs de la voip

De nombreux équipements voip, avec leur configuration par défaut, peuvent avoir divers ports tcp et udp ouverts. Les services fonctionnant sur ces ports peuvent présenter des vulnérabilités aux attaques par déni de service (dos) ou des attaques ddos. Si les

services accessibles ne sont pas configurés avec des mots de passe suffisamment robustes, un attaquant pourrait obtenir un accès non autorisé à ces dispositifs [14].

2.4.2 Les téléphones IP

Un pirate peut compromettre un dispositif de téléphonie IP comme un téléphone ip, un softphone ou d'autres logiciels/matériels clients. En général, il obtient des privilèges lui permettant de contrôler complètement les fonctionnalités du dispositif. Cette compromission peut se faire à distance ou par un accès physique [14].

Les softphones sont plus vulnérables que les téléphones ip car ils cumulent les failles du système d'exploitation, des applications, des services, virus/vers, etc [11].

2.4.3 Les serveurs

Un pirate peut également viser les serveurs fournissant les services du réseau de téléphonie ip. Compromettre un tel serveur met généralement en péril l'ensemble du réseau voip dont il fait partie. Par exemple, si un serveur de signalisation sip est compromis, un attaquant peut prendre le contrôle total des échanges de signalisation pour les différents appels passant par ce serveur [14].

2.4.4 Les vulnérabilités du système d'exploitation

De nombreuses vulnérabilités affectant les systèmes d'exploitation et firmwares sont relatives à des manquements de sécurité dès la phase initiale de développement, et ne sont découvertes qu'après la mise en production [14].

2.5 Sécurisation des systèmes VOIP

Nous avons déjà vu que des vulnérabilités existent au niveau du protocole et au niveau du l'infrastructure. Pour cela, la sécurité a été divisée en deux niveaux : la sécurité du protocole et la sécurité de l'infrastructure [14].

2.5.1 La sécurité du protocole

2.5.1.1 Pare-feu

Un pare-feu (firewall en anglais) est un système de protection du réseau qui surveille le trafic entrant et sortant, et décide d'autoriser ou de bloquer une partie de ce trafic

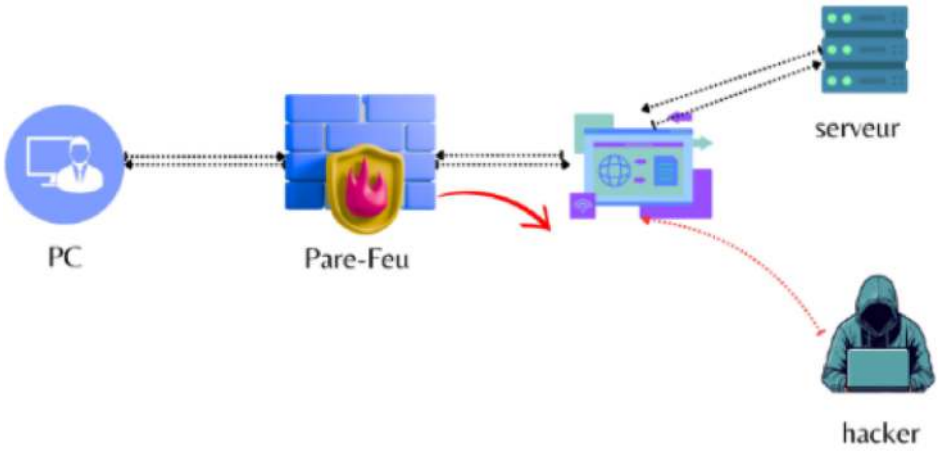


Figure 2.6 – Pare-Feu [4]

en fonction d'un ensemble de règles de sécurité prédéfinies [21].

Il est possible d'implémenter un pare-feu sur n'importe quelle machine suffisamment puissante pour traiter le trafic. Exemples de bons pare-feux pour les systèmes Linux : UFW (Pare-feu simple), IPCop, Vuurmuur, pfSense, IPFire, etc [21].

2.5.1.2 VPN VoIP

La VoIP VPN combine la voix sur ip et la technologie de réseau privé virtuel pour fournir une méthode sécurisée de transmission de la voix. Puisque la voip transmet la voix numérisée sous forme de flux de données, la solution voip vpn est particulièrement adaptée car elle crypte ces données grâce à des mécanismes de chiffrement, garantissant ainsi l'intégrité des paquets voip [31].

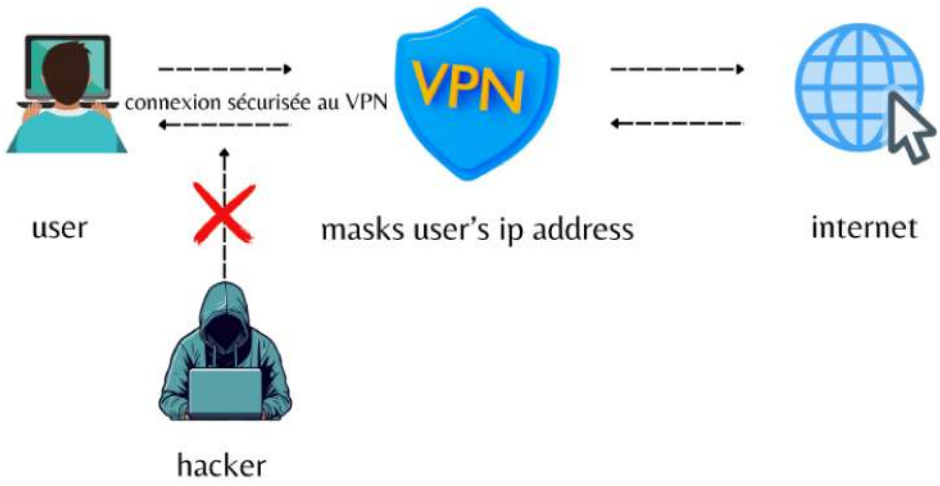


Figure 2.7 – VPN [27]

2.5.1.3 Protocole TLS

Le protocole TLS est utilisé pour sécuriser les échanges au niveau de la couche de transport. Anciennement connu sous le nom de **SSL**. TLS est un protocole standard conçu pour chiffrer et authentifier les communications sur Internet [14].

2.5.1.4 Secure RTP ou SRTP

SRTP est basé sur **RTP**, est conçu pour sécuriser les échanges multimédias en temps réel sur les réseaux ip. Il permet de protèger les communications voip, les vidéoconférences et de minimiser les risques d'attaques telles que celles par déni de service [14].

2.5.1.5 Système de détection d'intrusion (IDS)

Un IDS est un mécanisme qui sert à détecter des activités anormales ou suspectes sur une cible analysée, qui peut être un réseau ou un hôte. Le but est donc de réduire les attaques en mettant en place des règles afin de limiter l'impact d'une éventuelle attaque [27].

Il existe trois grandes familles d'IDS [14] :

1-Les HIDS (IDS hôte) : Qui surveillent l'état de la sécurité au niveau des hôtes

. **2-Les NIDS (IDS réseau) :** Qui surveillent l'état de la sécurité au niveau du réseau.

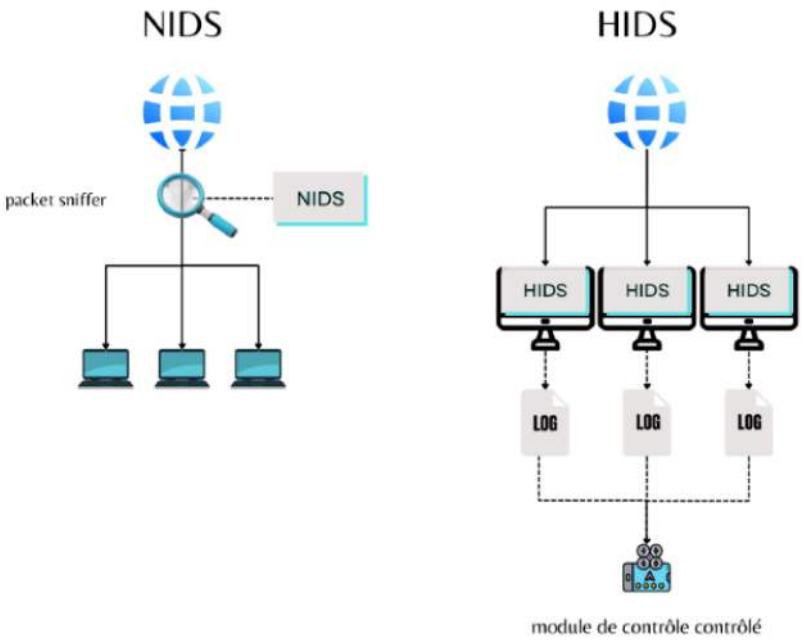


Figure 2.8 – Différence entre NIDS et HIDS [5]

3-Les IDS hybrides : Qui utilisent les NIDS et HIDS pour fournir des alertes plus pertinentes.

Voici une figure illustrant quelques outils IDS open source populaires :

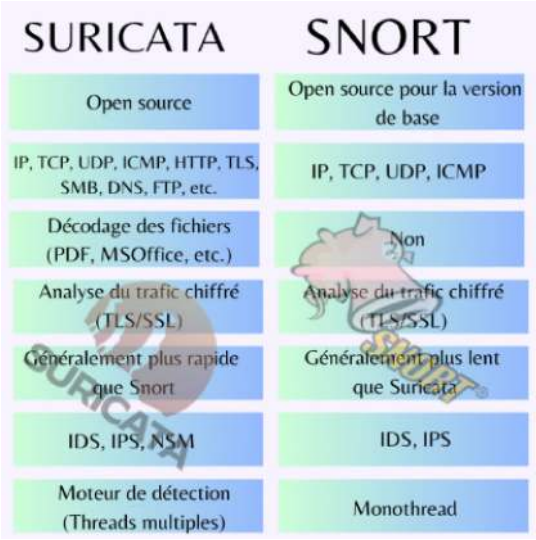


Figure 2.9 – Les Outils IDS open source les plus populaires [6]

Pour notre projet, le choix s'est porté sur l'IDS **Suricata.**

Suricata est un outil de détection d'intrusion réseau qui utilise un ensemble de règles simples, légères, flexibles et puissantes pour détecter les violations de politique et les comportements malveillants [27].

Exemple d'une régle [27] :

block icmp $HOME_NET any -> $EXTERNAL_NET any (msg :"PING BLOCKED" ;)

Ces règles sont divisées en deux sections principales : [27]

1-L'en-tête de la règle : Cette section contient les informations suivantes :

•**L'action :** Spécifie l'action à entreprendre lorsque Suricata détecte un paquet correspondant aux critères de la règle. Les actions courantes sont "alert" (alerter), "pass" (laisser passer), "drop" (bloquer) et "reject" (rejeter).

•**Le protocole :** Définit le protocole de communication auquel la règle s'applique comme IP, TCP, UDP ou ICMP.

•**Les adresses IP source et destination :** Spécifie les adresses IP source**($HOME_NET)** et destination**($EXTERNAL_NET)** concernées par la règle.

•**Les ports source et destination :** Précise les ports source et destination concernés par la règle. Exemple le port 80 pour HTTP ou any pour tous les ports.

2-Les options de la règle : Ces options contiennent des informations supplémentaires sur les critères de correspondance et les actions à entreprendre. Voici quelques-unes des options couramment utilisées [27] :

•**Msg (Message) :** Définit le message d'alerte qui sera affiché et enregistré dans les journaux lorsqu'un paquet correspond à la règle.

•**Sid (Signature Identifier) :** Attribue un identifiant unique à la règle. Cet identifiant permet à Suricata de comparer l'analyse des paquets avec une base de données de signatures connues. Si une correspondance est trouvée, une alerte sera générée.

•**Rev (Révision) :** Indique la version de la signature de la règle. Cette information est utile pour suivre les mises à jour et les modifications apportées à la règle au fil du temps.

Le système ids peut être utiliser avec un autre système, appelé **IPS (Intrusions Prevention System)**.

2.5.1.6 Système de prévention d'intrusion (IPS)

Les systèmes IPS opèrent au même niveau que les pare-feux dans le réseau. Cependant, contrairement aux pare-feux qui se contentent de filtrer le trafic selon des règles prédéfinies, les ips vont plus loin en analysant activement le contenu des paquets réseau [16].

Lorsqu'un paquet est analysé et qu'il ne correspond pas aux critères de sécurité définis dans les profils, l'ips prend des mesures proactives pour le rejeter ou le bloquer. Cela peut se faire en supprimant le paquet malveillant, en réinitialisant la connexion réseau ou en appliquant d'autres actions de protection [16].

Il se classifié en trois importantes classes : [16]

1-HIPS (IPS hôte) : Les HIPS sont des logiciels installés directement sur un ordinateur ou un serveur pour le protéger contre les intrusions et les activités malveillantes.

2-NIPS (IPS réseau) : Surveille le trafic réseau à la recherche d'activités malveillantes ou de trafic suspect en analysant l'activité des protocoles. Une fois qu'une intrusion est détectée, le NIPS peut prendre diverses mesures pour la bloquer.

3-WIPS (IPS sans fil) : Est un dispositif réseau qui empêche l'accès non autorisé aux réseaux locaux et autres ressources informatiques par des périphériques sans fil.

2.5.2 La sécurité d'infrastructure

Il est crucial de sécuriser le système d'exploitation sous-jacent, car si celui-ci est compromis, l'attaque peut se propager à l'application serveur de voip. Pour renforcer la sécurité du système, plusieurs mesures doivent être mises en place [31] :

1-Utiliser un système d'exploitation stable.

2-Mettre régulièrement à jour le système d'exploitation en installant les derniers correctifs de sécurité recommandés par le fournisseur.

3-Ne pas se contenter de la configuration par défaut en désactivant les services et fonctionnalités non nécessaires.

4-Éviter d'installer des applications clientes sur le serveur de voip.

2.6 Conclusion

Avec la croissance de l'utilisation de la voix sur ip, cette technologie est devenue une cible de plus en plus prisée par les pirates informatiques. Il est donc impératif de mettre en place une stratégie de sécurité robuste et fiable afin de mieux protéger les réseaux voip des menaces potentielles.

Dans ce chapitre, nous avons exploré les principales attaques susceptibles de compromettre la sécurité d'un serveur voip, telles que le déni de service, l'écoute clandestine, le vol d'identité, etc. Nous avons également examiné différentes solutions et mesures de sécurité pour remédier à ces risques.

Dans le prochain chapitre, nous nous concentrerons sur la mise en œuvre de notre architecture voip basée sur le serveur yate sous le système d'exploitation Linux et son interface graphique FreeSentral, en utilisant les hardphones et les softphones comme des clients.

Chapitre 3

Mise en place de l'architecture VOIP

3.1 Introduction

Après avoir abordé les concepts de base de la voix sur ip, ses vulnérabilités et les attaques associées, nous allons présenter dans ce chapitre une architecture voip permettant d'assurer la transmission de la voix sur les réseaux ip basée sur le serveur Yate.

Nous détaillerons les étapes nécessaires pour établir cette architecture sous le système d'exploitation Linux, ainsi que l'utilisation du Yate Client comme softphone et l'utilisation des hardphones IP.

3.2 Architecture du travail

Afin de réaliser une architecture voip sécurisée, nous avons opté pour le serveur Pbx « Yate » qui sera géré par son interface graphique « FreeSentral ». Pour la partie client, nous avons choisi deux Hardphones de la marque Huawei de type ViewPoint 8210 et nous avons utilisé « Yate Client » comme softphone.

Ensuite, nous avons utilisé Kali Linux pour simuler quelques attaques potentielles :

•Usurpation d'identité

•ARP Spoofing

•Écoute clandestine (Eavesdropping)

•Déni de service distribué (DDoS)

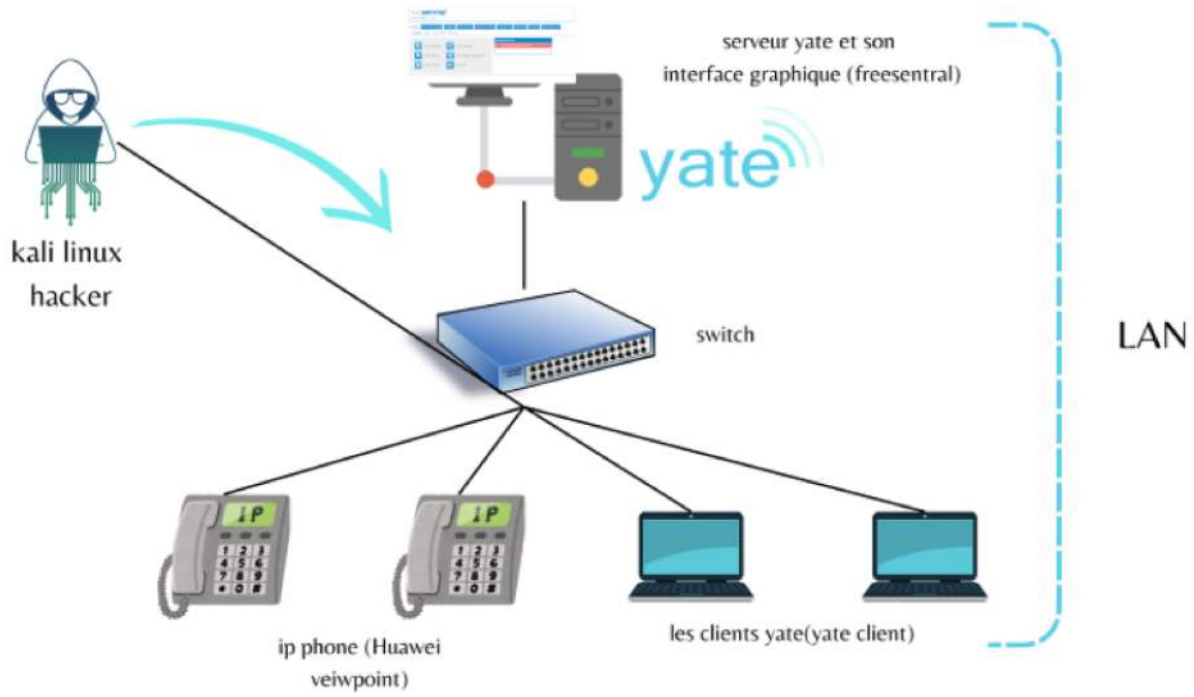


Figure 3.1 – L'architecture d'attaque de notre travail

3.3 Environnement du travail

3.3.1 Environnement matériel

Pour la réalisation de ce projet, nous avons utilisé le matériel suivant :

1-Pour le Serveur : Nous avons utilisé un pc de bureau jouant le rôle de serveur, ses caractéristiques sont données dans la figure suivante :

PC	CONDOR
processeurs	Intel core i3-3220 CPU @ 3.30GHZ
RAM	8GO
disque dur	500 GO
TYPE de système	64 Bits
Système d'exploitation	UBUNTU 14.04 trusty

Figure 3.2 – Les caractéristiques du PC serveur

2-Pour les clients :

1-Nous avons utilisé deux IPphones, avec les caractéristiques suivantes :

TELEPHONE IP	HUAWEI VIEWPOINT 8210
TYPE	viewpoint 8210
software VERSION	4. 05. 2 2005. 11. 23
BIOS VERSION	1.00
hardware VERSION	2.1.3
software ID	00111 (H323)

Figure 3.3 – Les caractéristiques des IPphones

2-Nous avons utilisé deux modèles d'ordinateurs portables "HP" comme des clients softphones, avec les caractéristiques suivantes :

PC	HP	HP
processeurs	Intel(R) core(TM) i5-8265 CPU @ 1.60GHZ 1.80GHZ	Intel(R) core(TM) i5-7200 CPU @ 2.50GHZ
RAM	16GO	8GO
disque dur	500 GO	256 GO
TYPE de système	64 Bits	64 BITS
Système d'exploitation	windows 10 Pro	windows 10 Pro

Figure 3.4 – Les caractéristiques des PC clients

3-Pour l'attaquant : Nous avons utilisé un pc de bureau jouant le rôle de l'attaquant, ses caractéristiques sont données dans la figure suivante :

PC	CONDOR
processeurs	Intel core i3-3220 CPU @ 3.30GHZ
RAM	4GO
disque dur	500 GO
TYPE de système	64 Bits
Système d'exploitation	Kali Gnu/Linux 2024.1 kali-rolling

Figure 3.5 – Les caractéristiques du PC Attaquant

3.3.2 L'environnement logiciel

Concernant la partie logicielle, nous avons travaillé avec différents systèmes d'exploitation comme Windows, Linux, sur lesquels nous avons installé les outils nécessaires pour

effectuer le travail.

Sur les pc Windows "les clients" : nous avons installé Yate client.

3.3.3 Les étapes suivies

Ci-dessous, on trouve les étapes qui sont à suivre :

-La préparation de l'environnement de travail avec les équipements essentiels.

-Installation et configuration du serveur Yate sous Ubuntu.

-L'activation des fonctionnalités de gestion du Protocole H.323 en lançant GnuGk.

-Installation et configuration de l'interface graphique FreeSentral sous Ubuntu.

-La Configuration des hardphones.

-Installation et configuration du softphone Yate Client sur les ordinateurs portables "HP".

-Installation de kali linux et lancement de plusieurs attaques vers le serveur et les clients.

-Installation et configuration du suricata sous Ubuntu.

3.4 Mise en place d'un serveur Yate

Dès sa conception, YATE a été développé pour être compatible avec les hardphones et les softphones. Il supporte tous les protocoles de VOIP.

3.4.1 Configuration du serveur yate.

Après avoir installé yate, il est nécessaire de lancer le serveur yate de cette manière afin de vérifier que l'installation s'est déroulée correctement.

```
yate@yate-desktop:~$ sudo su
[sudo] password for yate:
root@yate-desktop:/home/yate# yate -vv
Yate (2462) is starting Sun May 26 09:53:54 2024
```

Figure 3.6 – Yate est en cours de démarrage

yate : C'est le fichier exécutable qui lance le serveur Yate.

-v : Cette option signifie "verbeux" et indique à Yate d'afficher plus d'informations pendant son fonctionnement.

-vv : Utiliser deux fois l'option -v augmente encore le niveau de verbosité, ce qui amène Yate à afficher des informations plus détaillées, ce qui peut être utile pour le débogage ou le dépannage.

Par la suite, on lance **GnuGk**, le logiciel de gestion des communications H.323.

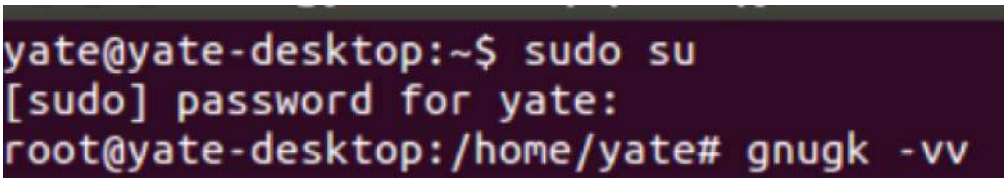


Figure 3.7 – La commande pour démarrer GnuGk

gnugk -vv : Exécutez le logiciel GnuGK avec un niveau de verbosité élevé, ce qui signifie que le système affichera des informations détaillées sur l'exécution de la commande.

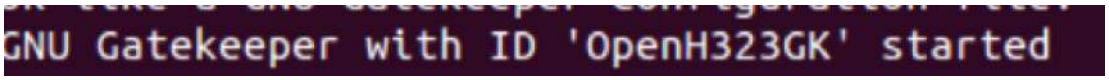


Figure 3.8 – GnuGk en Fonctionnement

3.5 Mise en place du FreeSentral

FreeSental est un outil de configuration graphique convivial et la seule solution officiellement prise en charge pour gérer le serveur Yate. Il permet aux administrateurs de gérer la plateforme.

3.5.1 Configuration du FreeSentral

Pour configurer Freesentral, veuillez suivre les étapes suivantes :

1-Pour commencer, connectons-nous à FreeSental en utilisant notre navigateur web. Maintenant que tout a été mis à jour, nous pouvons ouvrir le navigateur web et entrer "localhost/freesentral" dans la barre d'adresse.

Une fenêtre d'accés va apparaître, où vous pouvez entrer le nom d'utilisateur "admin" et le mot de passe "admin" fournis par l'administrateur.

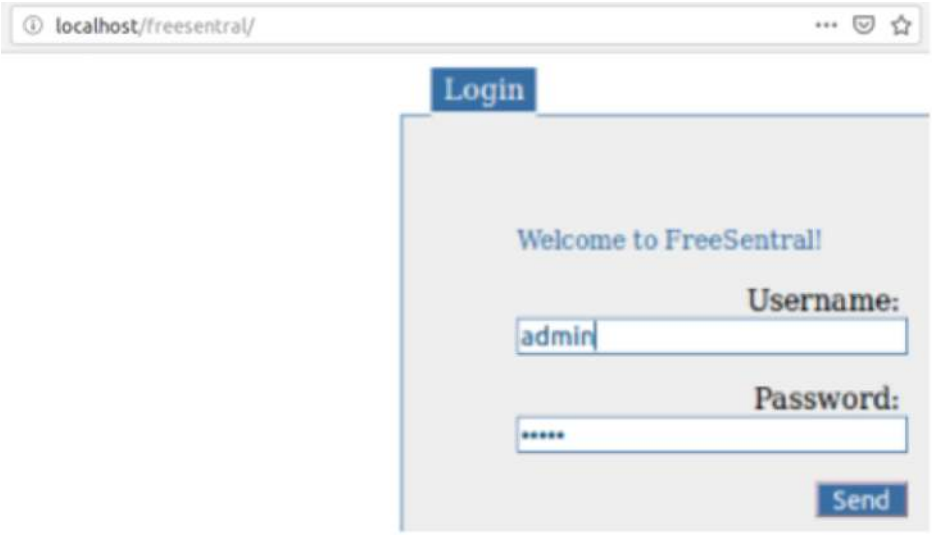


Figure 3.9 – La fenêtre d'accès à FreeSentral

2-Dans le menu principal, On clique sur Outbound > Add Gateway, pour créer une nouvelle passerelle. On sélectionne "H323" comme type de passerelle.

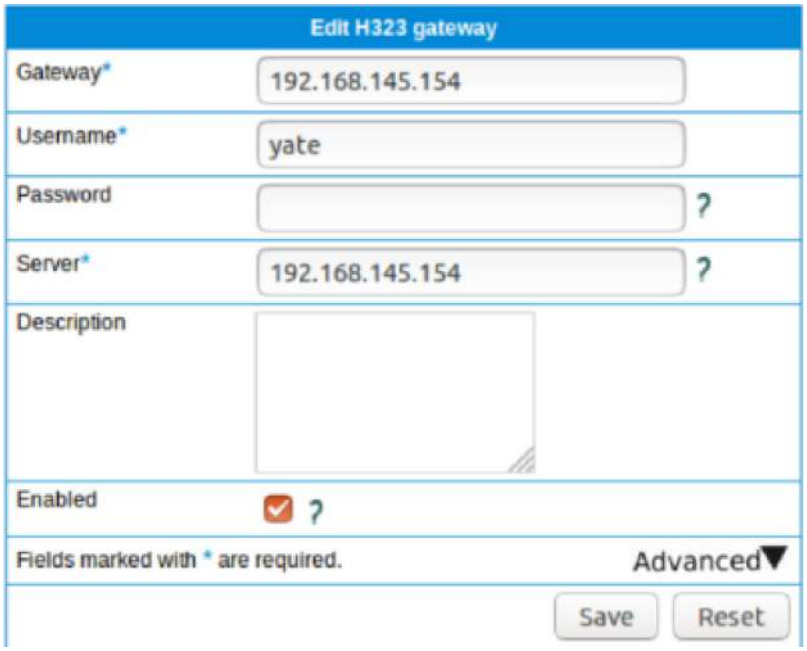


Figure 3.10 – Ajouter une passerelle H323

On modifie les paramètres suivants et on clique sur « Save ».

1.Gateway : On spécifié l'adresse du serveur.

2.Username : Il s'agit de notre nom d'utilisateur yate.

3.Password : Il s'agit du mot de passe.

4.Server : On spécifié l'adresse du serveur.

3-Dans le menu principal, On clique sur DIDs > Add group, pour créer un groupe.

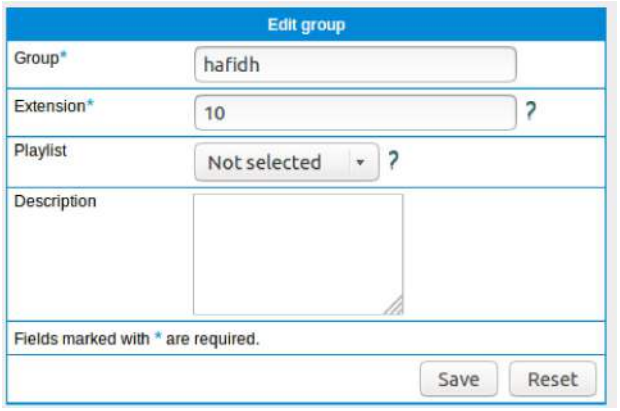


Figure 3.11 – Ajouter un groupe

On modifie les paramètres suivants et on clique sur « Save ».

1.Group : On spécifié le nom du groupe hafidh.

2.Extension : Il s'agit le nombre des extensions dans le groupe.

4-Dans le menu principal, cliquez sur Extensions > Add Extension pour créer des extensions pour les clients associés.

On modifie les paramètres suivants et on clique sur « Save ».

1.Extension : Il s'agit le numéro de l'extension.

2.Password : Il s'agit le mot de passe de l'extension.

3.Firstname/Lastname : Correspond au prénom et nom de l'extension.

4.Address : Spécifier l'adresse du client.

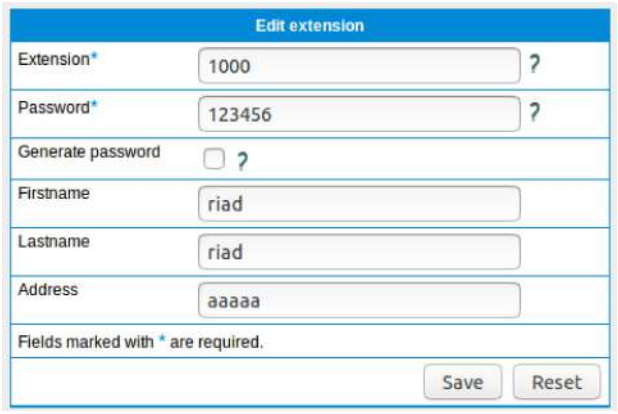


FIGURE 3.12 – Ajouter Une extension

De la même manière, créer les autres extensions.

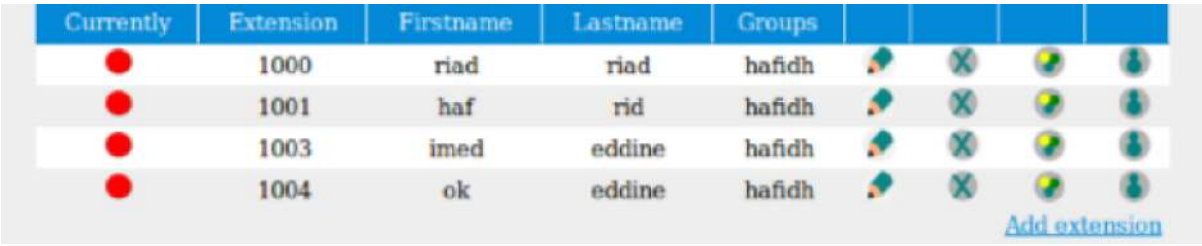


FIGURE 3.13 – La liste des extensions créées

3.6 Mise en place des IPphones

Nous avons choisi les IP phones Huawei ViewPoint 8210 pour les tester, pour les appels vocaux et vidéo.

3.6.1 Configuration des IPphones

La configuration se fait dans les deux ipphones comme suit :

1-Dans le menu principal, On clique sur Setting > User et On modifie les paramètres suivants et aprés on clique sur « Save ».

1.Register server : On choisit ip, puis on tape l'adresse IP du serveur Yate : 192.168.145.154.

2.Number : Il s'agit du numéro de l'extension créée dans FreeSentral.

3.Password : Il s'agit du mot de passe de l'extension créée dans FreeSentral.

4.Address : Il s'agit d'une option ou d'un paramètre pour la commande Register server, qui spécifie un surnom ou un nom court pour le serveur.

Figure 3.14 – Configuration de l'utilisateur 1000

De la même manière, configurer l'utilisateur 1001.

2-Dans le menu principal, On clique sur Setting > Network et On modifie les paramètres suivants et aprés on clique sur « Save ».

1.Net mode : LAN (adresse IP fixe) Cela indique que l'appareil est connecté à un réseau local et dispose d'une adresse IP fixe.

2.IP : Il s'agit de l'adresse IP de l'appareil.

3.Subnet mask : Un masque de sous-réseau est utilisé pour diviser une adresse ip en deux parties, l'une pour identifier le réseau et l'autre pour identifier l'appareil sur le réseau.

4.Gateway IP : C'est l'adresse ip du passerelle 192.168. 145. 154.

5.DNS IP : DNS signifie Système de noms de domaine, qui est utilisé pour traduire les noms de domaine en adresses IP.

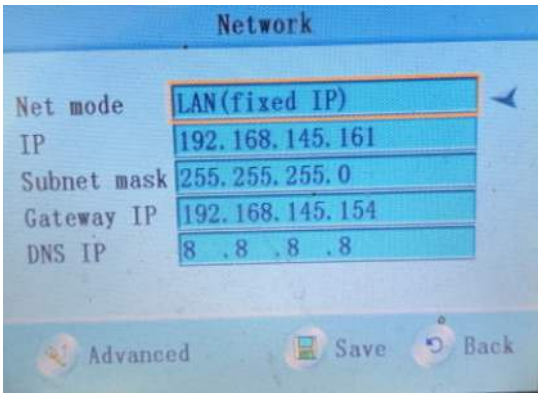


Figure 3.15 – Configuration du réseau de l'utilisateur 1000

De la même manière, configurer le réseau pour l'utilisateur 1001.

3.7 Mise en place du Yate Client

Yate client est la seule solution de softphone officielle pour le serveur Yate qui prend en charge les appels vocaux.

3.7.1 Configuration du Yate Client

La configuration se fait dans les deux pc HP de cette manière :

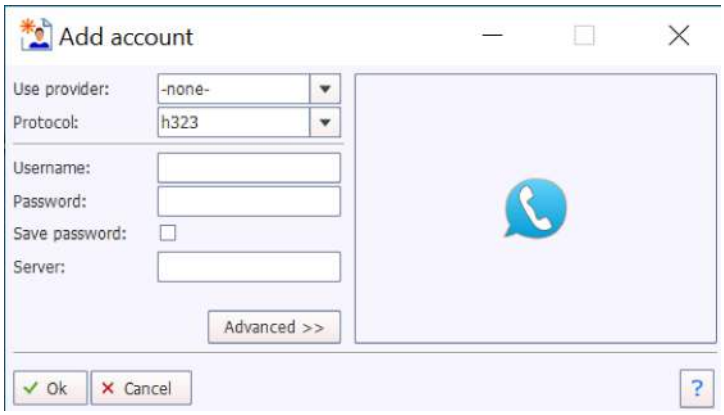


Figure 3.16 – Ajout de compte

On ouvre le Yate Client et sélectionne dans le menu la barre "Yate" > "Add Account" et on modifie les paramètres suivants :

1.Protocol : On sélectionne le protocole H323.

2.Username : On utilise l'une des extensions créées, 1004 pour l'ordinateur portable HP de Riadh et 1003 pour l'ordinateur portable HP de Hafidh.

3.Password : On saisit le mot de passe des extensions et on clique sur "save password".

4.Server : On tape l'adresse du serveur 192.168.145.154.

3.8 Tests d'appels

Après avoir terminé l'installation et la configuration du serveur Yate, les hardphones et les softphones Yate client, nous avons testé le réseau VoIP déployé en effectuant des appels.

Test d'appel de IPphone 1000 vers IPphone 1001 :

Figure 3.17 – Test d'appel de 1000 vers 1001

Test d'appel de 1004 de HP de Riadh vers 1003 de HP de Hafidh :

Figure 3.18 – Test d'appel de 1004 vers 1003

3.9 Conclusion

Ce chapitre a détaillé l'environnement matériel utilisé dans ce travail, ainsi que les différentes solutions logicielles open source adoptées et leurs configurations pour mettre en place des services de voip.

Dans le chapitre prochain, nous simulerons différents types d'attaques à partir de Kali Linux. L'analyse approfondie des signatures spécifiques générées par ces attaques nous permettra alors d'élaborer nos règles de sécurité personnalisées à implémenter dans le système de détection d'intrusion Suricata.

Chapitre 4

Simulation, Analyse et Détection des attaques

4.1 Introduction

Après avoir validé le bon fonctionnement des appels VoIP, nous procéderons à la simulation de plusieurs types d'attaques depuis un ordinateur exécutant le système d'exploitation Kali Linux. L'objectif est d'analyser les signatures spécifiques associées à ces attaques. L'identification de ces signatures nous permettra ensuite d'élaborer nos propres règles de sécurité personnalisées à implémenter dans le système de détection d'intrusion Suricata, afin de renforcer la sécurité de notre architecture voip.

4.2 Simulation

4.2.1 Kali Linux

Kali Linux (anciennement connu sous le nom de BackTrack Linux) est une distribution Linux open-source, basée sur Debian, visant les tests d'intrusion avancés et l'audit de sécurité. Elle le fait en fournissant des outils, configurations et automatisations courants qui permettent à l'utilisateur de se concentrer sur la tâche à accomplir, et non sur l'activité environnante.

Kali Linux contient des modifications spécifiques à l'industrie ainsi que plusieurs centaines d'outils ciblés vers diverses tâches de sécurité de l'information, telles que la sécurité réseau, le testing d'intrusion et la cryptographie.

Parmi les outils qui nous avons utilisé :

o Netdiscover : utilisé pour détecter les hôtes en ligne, les adresses ip, les adresses MAC et les vendeurs mac.

o Svmap : utilisé pour trouver les périphériques SIP sur une plage ip.

o Nmap : conçu pour détecter les ports ouverts sur le système d'exploitation d'un ordinateur distant.

o Metasploit : utilisé pour l'exploitation d'une faille de sécurité sur la machine cible. Elle contient plusieurs modules auxiliaires « scanner/scanner/h323 »,...

o ARPspoof : utilisé pour intercepter des paquets sur un LAN commuté. Il fonctionne en envoyant de faux messages ARP à la machine victime, ce qui la pousse à envoyer son trafic à la machine de l'attaquant ou à une autre passerelle sur le réseau.

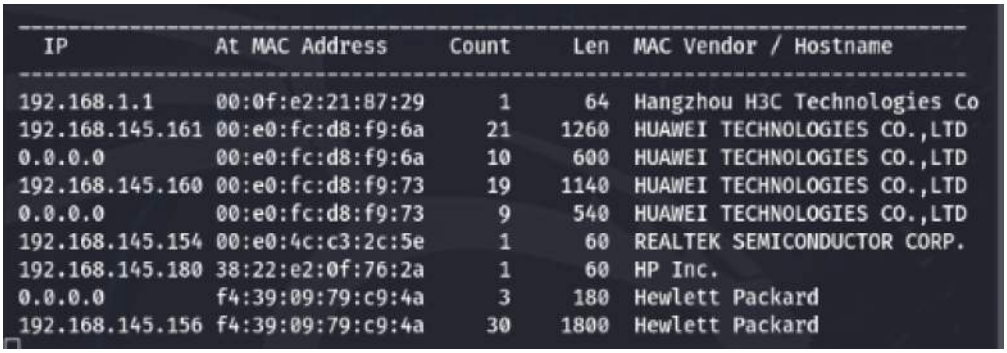
o Ettercap : Permet d'effectuer des attaques sur le protocole arp pour faire changer l'adresse mac de la victime.

o Wireshark : Permet d'écouter le réseau et d'analyser les paquets.

o Hping3 : Permet de générer des paquets tcp, ICMP et offre une grande variété d'options.

4.2.2 Simulation

Avant de lancer des attaques, l'attaquant commence par l'utilisation de l'outil **«netdiscover»** afin de détecter la plage d'adresses ip du réseau ciblé.



IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.1.1	00:0f:e2:21:87:29	1	64	Hangzhou H3C Technologies Co
192.168.145.161	00:e0:fc:d8:f9:6a	21	1260	HUAWEI TECHNOLOGIES CO.,LTD
0.0.0.0	00:e0:fc:d8:f9:6a	10	600	HUAWEI TECHNOLOGIES CO.,LTD
192.168.145.160	00:e0:fc:d8:f9:73	19	1140	HUAWEI TECHNOLOGIES CO.,LTD
0.0.0.0	00:e0:fc:d8:f9:73	9	540	HUAWEI TECHNOLOGIES CO.,LTD
192.168.145.154	00:e0:4c:c3:2c:5e	1	60	REALTEK SEMICONDUCTOR CORP.
192.168.145.180	38:22:e2:0f:76:2a	1	60	HP Inc.
0.0.0.0	f4:39:09:79:c9:4a	3	180	Hewlett Packard
192.168.145.156	f4:39:09:79:c9:4a	30	1800	Hewlett Packard

FIGURE 4.1 – La plage d'IP détectée

4.2.2.1 Attaque usurpation d'identité

Pour ce type d'attaque, le pirate va utiliser les outils «Svmap», «Nmap» et «Metasploit» en suivant ces étapes :

•Il commence par un scan de chaque adresse ip dans la plage IP avec « **svmap** » pour trouver les dispositifs VOIP.

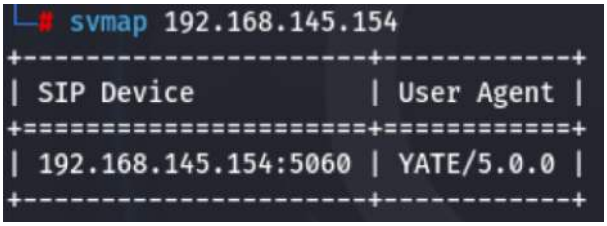


Figure 4.2 – scan de l'adresse IP 192.168.145.154 avec svmap

Le pirate a détecté la présence d'un serveur Yate sur l'adresse IP 192.168.145.154.

•Ensuite, il utilise « **nmap** » pour détecter les ports ouverts sur la plage d'adresse ip.

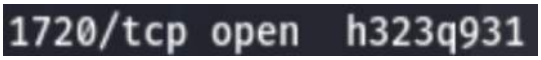


Figure 4.3 – Détection des ports avec nmap

Le résultat **1720/tcp open h323q931** obtenu avec Nmap indique que le système cible a un service en cours d'exécution sur le port tcp 1720, et ce service est identifié comme h323q931.

H323 est un Protocole pour la communication multimédia sur les réseaux ip, et h323q931 est un protocole spécifique utilisé pour le signalement d'appel dans H323.

•Il termine l'attaque en utilisant l'outil «**Metasploit**» pour scanner la plage d'adresses ip afin de trouver les clients de ce système cible.

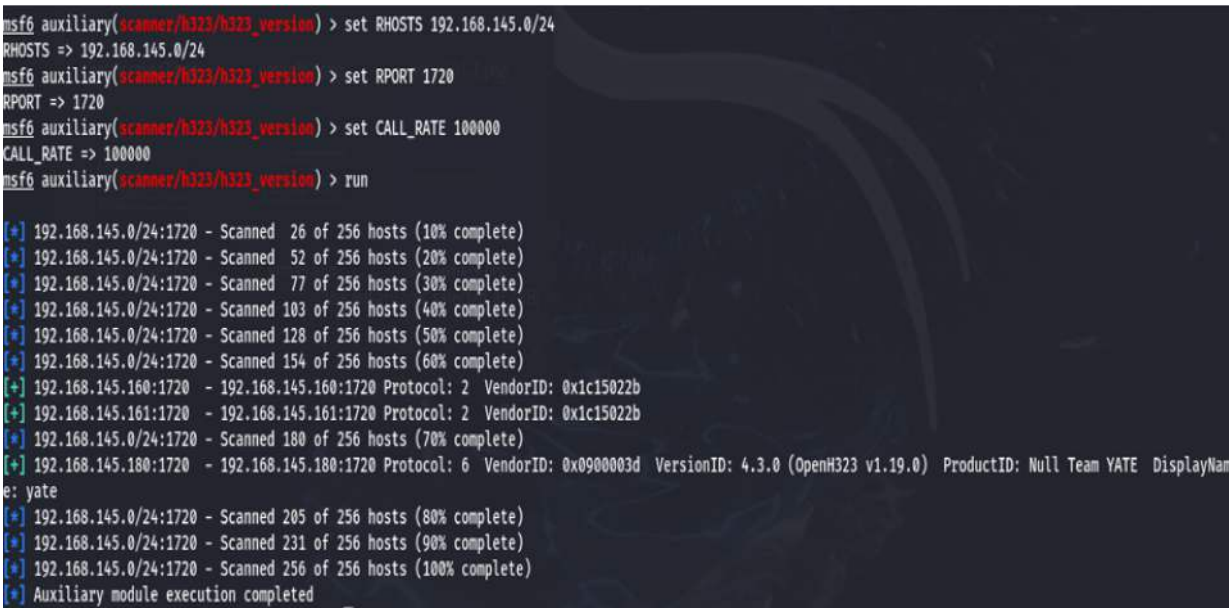


Figure 4.4 – Scan la plage d'adresse IP du réseau avec Metasploit

Les commandes utiliser dans Metasploit :

msf6 > use auxiliary/scanner/h323/h323_version : Cette ligne indique que l'on a sélectionné l'auxiliaire Metasploit h323_version pour scanner les versions H323.

set RHOSTS 192.168.145.0/24 : Cette ligne indique que l'on a défini l'adresse IP cible pour le scan.

set RPORT 1720 : Cette ligne indique que l'on a défini le port cible pour le scan sur le port H323 standard, qui est le port 1720.

set CALL_RATE 10000 : Le taux d'appels est fixé à 10000, ce qui signifie que Metasploit enverra jusqu'à 10000 appels par seconde aux adresses ip cibles.

run : Cette ligne indique que l'on a lancé le scan.

4.2.2.2 L'Attaque ARP Spoofing

Pour ce type d'attaque, le pirate va utiliser l'outil **«arpspoof»**.

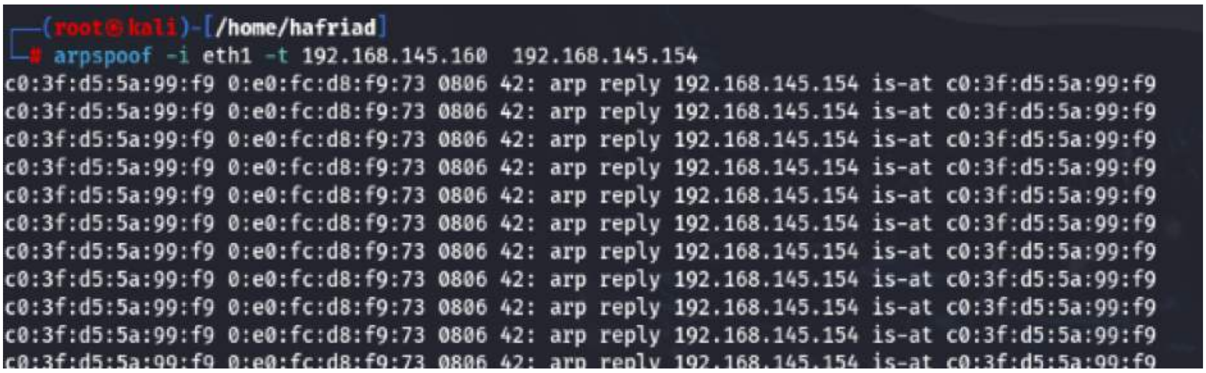


Figure 4.5 – L'Attaque ARP Spoofing avec arpspoof

La commande **arpspoof -i eth1 -t 192.168.145.160 192.168.145.154** :

-i eth1 : spécifie l'interface réseau à utiliser (dans ce cas, eth1).

-t 192.168.145.160 : spécifie l'adresse IP cible à usurper.

192.168.145.154 : spécifie l'adresse IP associée à l'adresse MAC usurpée.

4.2.2.3 Attaque Eavesdropping

Pour réaliser cette attaque, le pirate va utiliser les outils Ettercap et Wireshark.

1ère Étape : Lancement d'Ettercap.

Figure 4.6 – Lancement d'Ettercap.

2ème Étape : Scan du réseau et ajouts d'hôtes pour visualiser les machines connectées sur ce réseau.

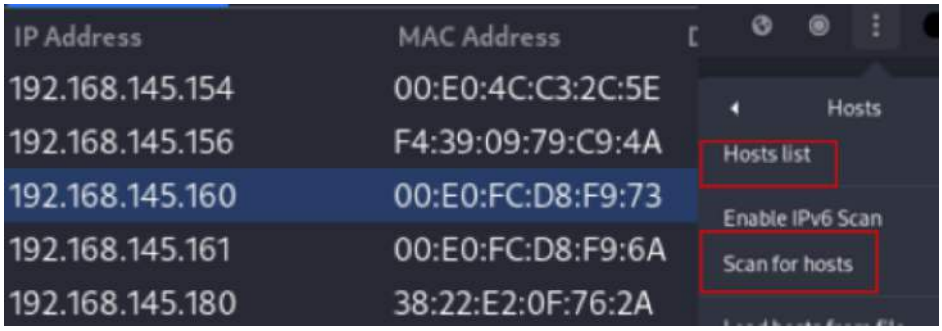


Figure 4.7 – Scan du réseau et ajouts d'hôtes

3ème Étape : Choix du type d'attaque.

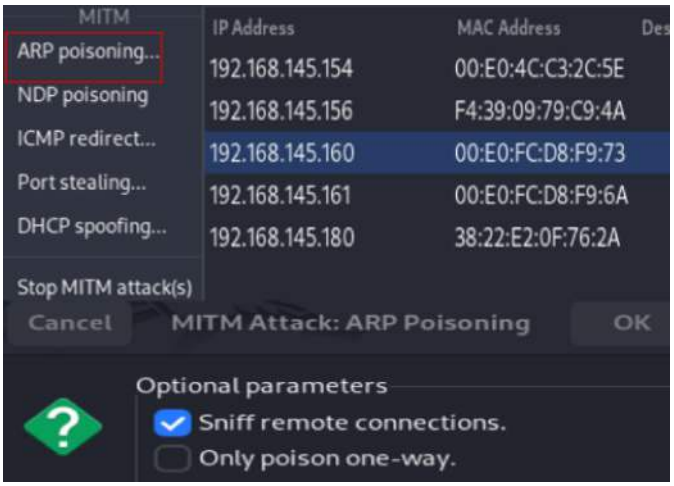


Figure 4.8 – Choix du type d'attaque Mitm ARP poisoning

Sniff remote connections : Cette attaque permet d'intercepter le trafic sortant et entrant en direction de la victime. Par contre l'attaque **only poison One-way** permet d'intercepter le trafic sortant de la victime vers d'autres appareils du réseau, mais pas le trafic entrant en direction de la victime.

L'attaque **MITM** est mise en place de telle sorte que la machine de l'attaquant, ayant l'adresse ip 192.168.145.200, se positionne entre le serveur et les clients. Dans ce scénario, le serveur Yate a l'adresse IP 192.168.145.154, tandis que les machines clientes ont des adresses IP dans la plage 192.168.145.0/24.

Dans cette attaque, l'attaquant a choisi l'adresse 192.168.145.161.

Comme vous pouvez le voir dans la figure ci-dessous, l'adresse mac du client 192.168.145.161 de la table mac du l'attaquant avant et après l'attaque ARP Poisoning.

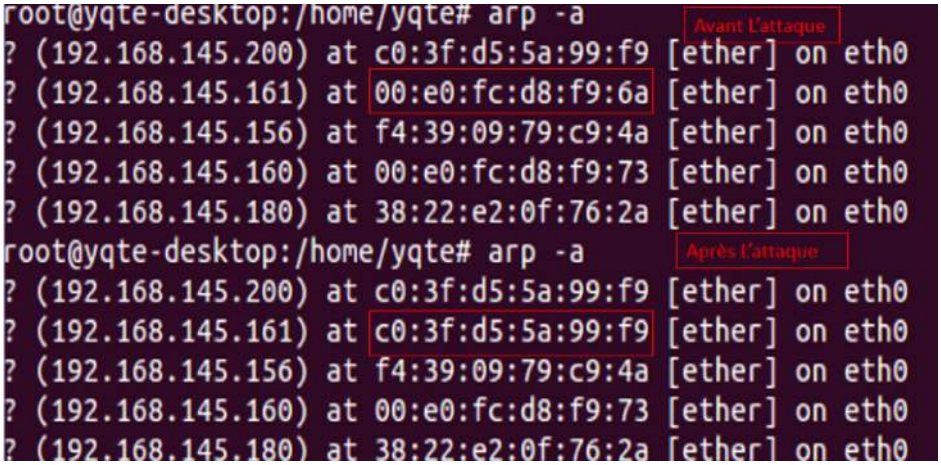


Figure 4.9 – Piratage de la table MAC d'une victime

Figure 4.10 – Conflit d'adresse IP du hardphone IP

4ème Étape : Lancement du Wireshark. Après lancement de Wireshark, le pirate choisis l'interface réseau sur laquelle il va effectuer la capture des paquets échangés.

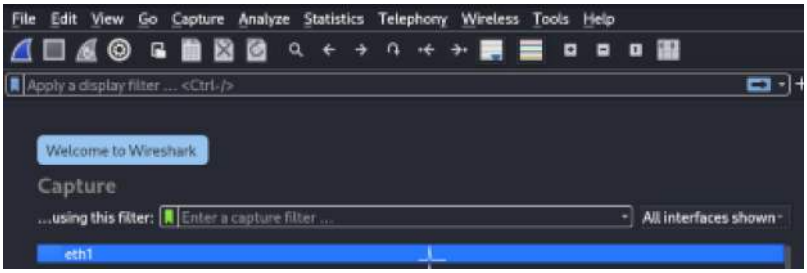


Figure 4.11 – Lancement de Wireshark et choix de l'interface.

5ème Étape : Filtrage des paquets capturés en se limitant au protocole « **RTP** ».

1060	743.076968257	192.168.145.180	192.168.145.161	RTP
1069	743.087669967	192.168.145.161	192.168.145.180	RTP
1070	743.088078189	192.168.145.180	192.168.145.161	RTP
1073	743.094496533	192.168.145.161	192.168.145.180	RTP
1074	743.094810540	192.168.145.180	192.168.145.161	RTP
1075	743.103388027	192.168.145.180	192.168.145.161	RTP
1076	743.108545666	192.168.145.161	192.168.145.180	RTP
1077	743.108969952	192.168.145.180	192.168.145.161	RTP

Figure 4.12 – Filtrage des paquets

Après avoir filtré les paquets capturés, vous pouvez aller dans le menu Telephony > RTP, puis cliquer sur RTP Play pour écouter les conversations RTP enregistrées.

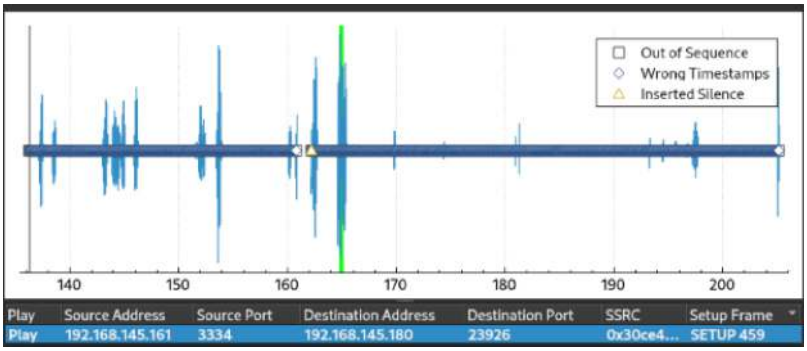


Figure 4.13 – Écoute de conversations enregistrées

SSRC : Est un identifiant unique utilisé dans les sessions multimédias pour identifier la source des paquets RTP.

Setup frame : Est une trame utilisée pour une négociation entre les ports du commutateur.

4.2.2.4 Attaque DDOS

Le pirate utilise l'outil **«Hping3 »** pour simuler une attaque ddos, la commande de simulation est : **hping3 -S -p 1720 –flood 192.168.145.161 –rand-source**

hping3 : Est un outil utilisé pour dos/ddos attaque.

-S : Pour envoyer des paquets SYN.

-p : 1720 spécifie le numéro de port.

–flood : Active le mode d'inondation, qui envoie les paquets aussi vite que possible.

192.168.145.161 : Est l'adresse ip cible.

–rand-source : Randomiser l'adresse ip source des paquets.

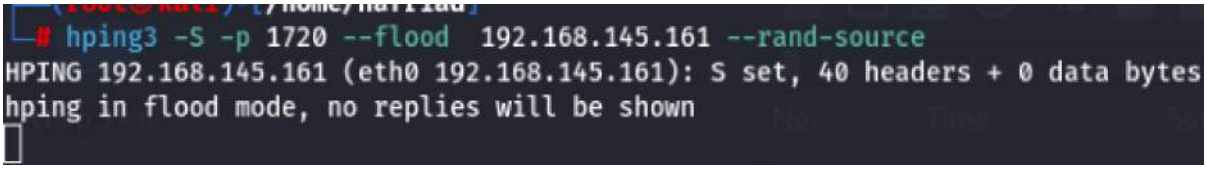


Figure 4.14 – Attaque DDOS avec Hping3

Cet outil est utilisé pour inonder notre cible avec des requêtes de type SYN. Une fois l'attaque lancée, on remarque une perturbation de la cible qui sera déconnectée complètement du réseau.

4.3 L'analyse des attaques

On utilise l'outil wireshark pour analyser les attaques.

L'ATTAQUE	LES PROTOCOLES VISÉS	L'IMPACT DE L'ATTAQUE	SIGNATURE (WIRESHARK)
Usurpation d'identité	TCP/H225	Découvrir le serveur Yate et ses clients sonnent en effet de l'utilisation de Metasploit.	30.712498S 192.168.145.200 192.168.145.180 H.225.0/H.245 1050 CS: setup Open Logical Channel terminal Capability Set master Slave Determination
ARP Spoofing	ARP	Modification de l'adresse MAC de la cible afin d'empêcher la cible d'établir des connexions.	4.536371S HP_0f:76:2a RealtekS_c3:2c:5e ARP 42 Who has 192.168.145.154? Tell 192.168.145.180
Eavesdropping	ARP/RTP	Modification de l'adresse MAC de la cible et L'écoute des conversations enregistées entre la cible et les autres clients.	26.297764S Elitegro_5a:99:f9 HP_0f:76:2a ARP 60 192.168.145.161 is at c0:3f:d5:5a:99:f9
DOS/DDOS	TCP	Perturbation de la cible attaquée qui sera déconnectée complètement du réseau.	49.482196S 161.246.225.89 192.168.145.180 TCP 60 9664 → 1720 [SYN] Seq=0 Win=512 Len=0

Figure 4.15 – L'analyse des attaques

4.4 Détection des attaques

4.4.1 Implémentation du l'IDS Suricata

Aprés l'installation de Suricata au niveau du serveur yate, nous avons configuré suricata dans le fichier de configuration suricata.yaml afin de lancer l'IDS suricata comme suit :

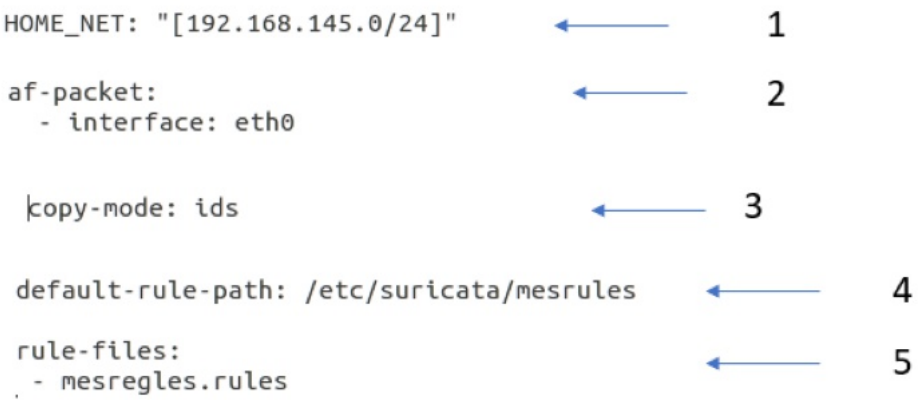


Figure 4.16 – Configuration de Suricata

1 : La Configuration de notre réseau de travail en tant que Home_NET.

2 : Dans la section af-packet, on spécifie notre interface de travail eth0.

3 : Dans la section af-packet, on spécifie le mode IDS.

4 : Dans la section default-rule-path, nous créons un nouveau répertoire **/etc/suricata/mesrules.**

5 : Dans répertoire /etc/suricata/mesrules, nous créons un nouveau fichier **mesregles.rules** pour ajouter nos règles afin de détecter les attaques.

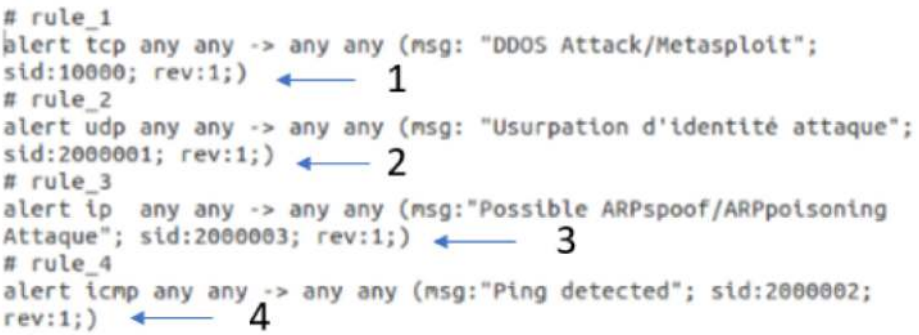


Figure 4.17 – Nos règles IDS

1 : Cette règle détecte les tentatives d'attaques par DDoS ou Metasploit.

2 : Cette règle détecte les tentatives d'attaques d'usurpation d'identité.

3 : Cette règle détecte les tentatives d'attaques ARPspoofing/ARPpoisoning.

4 : Cette règle détecte les tentatives d'attaques utilisant le protocole ICMP.

4.4.2 Détection des attaques

Aprés la configuration de suricata, nous allons lancer l'IDS Suricata.

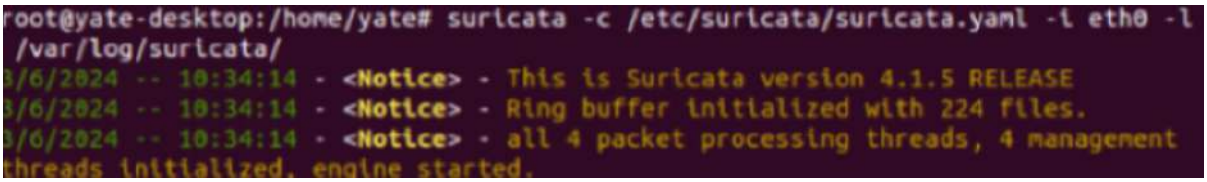


Figure 4.18 – Lancement de l'IDS Suricata

1.suricata : Le nom exécutable du système Suricata.

2. -c /etc/suricata/suricata.yaml : Spécifie le fichier de configuration utiliser par Suricata.

3. -i eth0 : Indique à suricata de détecter les paquets entrants sur l'interface eth0.

4. -l /var/log/suricata : Spécifie le répertoire où Suricata doit enregistrer ses logs.

Ensuite, nous vérifions les logs de suricata pour voir si l'IDS Suricata fonctionnent bien avec la commande **« tail -f /var/log/suricata/fast.log »**

Figure 4.19 – Détection des attaques par l'IDS suricata

Par conséquent, après avoir lancé l'IDS suricata, nous avons détecté les attaques suivantes :

1 : Détection d'une attaque d'usurpation.

2 : Détection d'une attaque ARPspoofing.

3 : Détection d'une attaque ARPpoisoning.

4 : Détection d'une attaque DDoS.

4.5 Conclusion

Dans ce chapitre, nous avons simulé diverses attaques à partir d'un ordinateur équipé du système d'exploitation Kali Linux, reconnu pour ses outils dédiés à la cybersécurité. Nous avons analysé les signatures spécifiques générées par ces attaques. Ces signatures nous a permis de présenter notre solution de sécurité en élaborant et implémentant nos règles de détection d'attaques dans l'ids Suricata.

Nous pouvons désormais détecter efficacement les tentatives d'attaques visant notre architecture voip, telles que les attaques d'usurpation d'identité, les attaques ARPspoofing, ARP poisoning et les attaques DDoS.

Notre solution de sécurité renforce considérablement la sécurité de notre système voip, en offrant une surveillance en temps réel.

Conclusion Générale

La technologie VoIP est une innovation majeure qui a révolutionné les moyens de communication existants depuis son apparition. En effet, les nombreux bénéfices qu'elle procure ont poussé de nombreuses entreprises à vouloir tirer parti de cette technologie évolutive.

Ce projet a porté sur la mise en place d'une solution VoIP sécurisée. Pour cela, nous avons installé et configuré une solution VoIP utilisant un PBX **Yate** comme serveur géré par son interface graphique **FreeSentral**. Comme client, nous avons utilisé des clients **IP phones Huawei Viewpoint 8210** et des clients softphones **Yate Client**.

Ensuite, en utilisant un pc Kali Linux nous avons simulé quelques attaques notamment des attaques par déni de service distribuée (DDoS), du ARP spoofing et des attaques d'usurpation d'identité.

Pour assurer la protection de notre architecture voip, nous avons élaboré et implémenté nos propres règles de sécurité sur un système de détection suricata.

Ce projet a démontré qu'il est possible de mettre en place une solution voip sécurisée. L'utilisation de suricata a permis de détecter efficacement les attaques contre l'infrastructure voip. Ce projet a également mis en évidence l'importance de la sécurité dans les environnements voip et la nécessité de mettre en place des mesures de sécurité adéquates pour protéger les réseaux contre les attaques.

Ce projet peut être étendu de plusieurs façons. Une future étude pourrait se concentrer sur l'implémentation d'un système de prévention des intrusions (IPS) pour bloquer les attaques détectées par Suricata.

Bibliographie

[1] Consultez le 28 mars 2024. URL : https://ami-gestion.fr/ipbx/.

[2] Consultez le 28 mars 2024. URL : https://wikimemoires.net/2011/03/architecture-de-voip-voice-over-internet-protocol/.

[3] Consultez le 14 avril 2024. URL : https://networksimulationtools.com/eavesdropping-attack-network-projects/.

[4] Consultez le 15 avril 2024. URL : https://networkinterview.com/secure-real-time-transport-protocol/.

[5] Consultez le 15 avril 2024. URL : https://bunny.net/academy/security/what-is-network-intrusion-detectionnids/.

[6] Consultez le 16 avril 2024. URL : https://www.netgate.com/blog/suricata-vs-snort.

[7] Consultez le 5 avril 2024. URL : https://wikimemoires.net/2011/03/logiciels-de-telephonie.

[8] Consultez le 5 avril 2024. URL : https://www.zoiper.com/.

[9] Consultez le 5 avril 2024. URL : https://www.yate.ro/.

[10] Consultez le 5 avril 2024. URL : huaweicatalog,ViewPoint8000Datasheetpdf.279897124.

[11] Consultez le 5 avril 2024. URL : https://www.freepbx.org/.

[12] Consultez le 5 avril 2024. URL : https://www.freesentral.com/.

[13] *IP pbx telephony system user guide*. Smc networks, Inc. 20 mason irvine, CA 92618, Printed in Taiwan, 2007. Consultez le 28 mars 2024.

[14] Hakim Agdour Anis Amziane. *Mémoire de fin d'Etude de master academique*. Mise en place et sécurisation d'une plateforme VoIP basée sur la solution open source Asterisk. Université Mouloud Mammeri de Tizi-Ouzou, 17 juillet 2016. Consultez le 6 avril 2024.

[15] Rashmi Bhardwaj. Dos vs ddos : Detailed comparison. Consultez le 14 avril 2024.

[16] Manu Bijone. A survey on secure network : Intrusion detection prevention approaches. *American journal of information systems,2016, Vol. 4, No. 3, 69-88.* Consultez le 16 avril 2024.

[17] Mark Collier David Endler. Hacking exposedtm :unified communications voip security secrets solutions, second edition, December 2013. Consultez le 6 avril 2024.

[18] Sinclair J Flannagan, M. E. *Livre, configuring cisco voice over ip.* 2002. Consultez le 30 mars 2024.

[19] UIT-T Rec. H.323. *Packet-based multimedia communications systems.* 03/2022. Consultez le 30 mars 2024.

[20] Theodore-Wallingford James-Guerin. *Switching to VoIP.* Edition o'Reilly media., 2005. Consultez le 26 mars 2024.

[21] George Kurtz Joel Scambray, Stuart Mcclure. *Hacking exposed :network security secrets solutions second editions.* Osborne/McGraw-Hill, October 11, 2000. Consultez le 7 avril 2024.

[22] Philippe-Attelin José-Dordoigne. *Réseau informatique.* Edition eni, novembre 2009. Consultez le 22 mars 2024.

[23] Moo Wan Kim and Fumikazu Iseki. *VoIP System for enterprise network.* Tokyo university of information sciences japan, December 2015. Consultez le 22 mars 2024.

[24] G. Pujolle L. Ouakil. *Téléphonie sur IP.* 2ème édition, eyrolles, paris, 2008. Consultez le 5 avril 2024.

[25] M. Labidi. *Etude et mise en place d'une solution voix sur ip sécurisée*, volume mémoire de fin d'étude, Institut national des sciences appliquées et de technologie, Tunis. 2013. Consultez le 20 mars 2024.

[26] Sabah M. Morsey and Dalia Nashat. D-arp : An efficient scheme to detect and prevent arp spoofing. *Ieee Access*, May 3, 2022. Consultez le 8 avril 2024.

[27] développeur auteur Nicolas Tourrete, ingénieur sécurité et qualité des réseaux. Mise en place d'un ids. *www.nicolas-t.ovh*, Le 31 janvier 2020. Consultez le 15 avril 2024.

[28] Pecb. *La sécurité des réseaux et les attaques d'usurpation d'identité.* Consultez le 6 avril 2024. URL : www.pecb.com.

[29] L. Ouakil. G. Pujolle. *Téléphonie sur ip*, volume 1ère édition. Eyrolles. Paris. 2007. Consultez le 20 mars 2024.

[30] Guide sur la sécurité des communications VoIP par promelit. Consultez le 6 avril 2024.

[31] Mezhoudi yazid. *Mémoire de master.* Voix sur ip sécurisée. Université de Biskra, jeudi 26 avril 2018. Consultez le 26 mars 2024.