RÉPUBLIQUE DU BÉNIN
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR
ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITÉ D'ABOMEY-CALAVI

INSTITUT DE FORMATION ET DE RECHERCHE EN INFORMATIQUE

BP 526 Cotonou Tel : +229 21 14 19 88
https://www.ifri-uac.bj Courriel : contact@ifri-uac.bj

MÉMOIRE

pour l'obtention du

Diplôme de Licence en Informatique

Option : Sécurité Informatique

Présenté par :
OUMAR Hissein Hassan

Mise en place d'un système de détection d'intrusion pour la sécurité des réseaux et service VoIP: Cas de la société Doctor Computer

Sous la supervision de :
Mr. Mawuenan Hervé Guy **AKAKPO**
Ingénieur Réseaux et Systèmes d'Information

Membres du jury :

DEGUENONVO Roland	Docteur	Réseaux Informatiques et télécommunications	Président
DJOSSOU Frederic	Ingénieur	Réseaux et Systèmes d'Information	Examinateur
AKPAKPO Hervé	Ingénieur	Réseaux et Systèmes d'Information	Rapporteur

Année Académique : **2019-2020**

Sommaire

Remerciements ii

Table des figures iii

Liste des tableaux v

Liste des acronymes vi

Introduction 1

1 Etude générale sur la VoIP 3

2 Les systèmes de détection d'intrusion 15

3 Implémentation de la solution 25

Bibliographie 39

Webographie 40

Table des matières 42

Remerciements

Je tiens à remercier toutes les personnes qui ont contribué au succès de mon stage et qui m'ont aidé lors de la rédaction de ce mémoire.

Je voudrais dans un premier temps remercier, mon maître de mémoire **M. Mawuenan Hervé Guy AKAKPO D.** Ingénieur Réseaux et Systèmes d'Information, pour sa patience, sa disponibilité et surtout ses judicieux conseils, qui ont contribué à alimenter ma réflexion.

Je remercie également toute l'équipe pédagogique de l'Institut de Formation et de Recherche en Informatique de l'Université d'Abomey Calavi et les intervenants professionnels responsables de ma formation.

Je remercie mes très chers parents, **AMINA Hissein** et **HISSEIN Hassan**, qui ont toujours été là pour moi. Je remercie mes sœurs **Amouna** et **Khadidja**, et mes frères **Abdelsalam**, **Mahamat**, **Abdelrazakh** et **Moussa** pour leurs encouragements.

Enfin, je remercie mes amis qui ont toujours été là pour moi. Leur soutien inconditionnel et leurs encouragements ont été d'une grande aide.

Table des figures

1.1 Architecture de la VoIP 4
1.2 Principe de fonctionnement de la VoIP 5
1.3 Requêtes et réponses SIP 8

2.1 Choix d'emplacement d'un système de détection d'intrusion 16
2.2 Positionnement Nids 16
2.3 Positionnement Hids 17
2.4 L'approche centralisée 18
2.5 L'approche hiérarchique 19
2.6 L'approche distribuée 19

3.1 Environnement de travail 25
3.2 Architecture du réseau d'étude 26
3.3 Installation et configuration du serveur Asterisk dans l'environnement de travail . . . 27
3.4 Lancement du serveur Asterisk 28
3.5 Configuration des comptes utilisateurs 28
3.6 Lancement d'appel 29
3.7 Lancement d'appel 29
3.8 Réception d'appel 30
3.9 Installation de Kali Linux dans l'environnement de travail 30
3.10 Capture des paquets 31
3.11 Verification d'existance d'un serveur SIP 31
3.12 Simulation d'attaque SIP DoS 32
3.13 Réaction du serveur Asterisk 32
3.14 Simulation d'attaque SYN Flood 32
3.15 Installation et configuration de Snort dans l'environnement du travail 33
3.16 Installation et configurasion de Snort 34
3.17 Lancement de configuration de Snort 34
3.18 Choix du mode de lancement de Snort 34
3.19 Redémarage du service Snort 35
3.20 Ouverture de fichiers d'ajout des régles de Snort 35
3.21 Fichier locale.rules 36
3.22 Ajout au niveau de la section include 36
3.23 Lancement de Snort 36
3.24 Détection de ping 37
3.25 Interface de supervision du réseau 37
3.26 Détection d'attaque SIP Dos 37

3.27 Fichier local.rules 38
3.28 Détection d'attaque SYN Flood 38

Liste des tableaux

1.1 Requêtes du protocole SIP 8
1.2 Reponses du protocole SIP 9

2.1 Comparaison des différents types de IDS 21

Liste des abréviations

CAN : Convertisseur Analogique-Numérique

CIDS : Collaborative Intrusion Detection System

DIDS : Distributed Intrusion Detection System

DOS : Deny Of Service

HIDS : Host-based Intrusion Detection System

HIPS : Host-based intrusion Prevention System

IDS : Intrusion detection System

IETF : Internet Engineering Task Force

MEGACO : Media Gateway Control Protocol

NIDS : Network Intrusion Detection System 23,

NIPS : Network Intrusion Prevention System

PABX : Private Automatic Branch Exchange

PC : Personal Computer

PCM : Pulse Code Modulation

RTP : Realtime Transport Protocol

SIEM : Security Event Information Management

SIP : Session Initiation Protocol

SPIT : Spam via Internet Telephony

SPOF : Point Of Failure

SRTP : Secure Realtime Transport Protocol

TCP : Transmission Control Protocol

VoIP : Voice over Internet Protocol

VPN : Virtual Private Network

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 a principalement pour but de minimiser le coût des communications ; utiliser le même réseau pour offrir des services de données, de voix, d'images et simplifier les coûts de configuration et d'assistance. La forte croissance que connaît actuellement la téléphonie IP (VoIP) représente en même temps son principal danger. Elle devient en effet une cible attrayante pour les pirates et les agresseurs de réseaux. Nous constatons que les réseaux de données sont depuis des années déjà en train de se protéger contre les attaques nuisibles. Il devient impératif de mettre en place des mesures de sécurité adéquates pour protéger les systèmes VoIP. En dehors de la mise en place de pare-feu et des systèmes d'authentification de plus en plus sécurisé, il est nécessaire d'avoir des outils de surveillance pour auditer le système d'information et détecter d'éventuelles intrusions[10]. Dans ce même contexte se situe le présent travail dont le but est de mettre en place un système de détection d'intrusion évolué destiné à la VoIP, basé sur les vulnérabilités du protocole de signalisation SIP(Session Initiation Protocol).

1. Problematique

La Voix sur IP présente plusieurs avantages mais il faut plus d'efforts pour innover et essayer de réduire les failles et les inconvénients qui y existent. Face à la complexité croissante des réseaux qui sont devenus de plus en plus gigantesques et étendues, nous nous retrouvons devant le défi de contribuer à la recherche des solutions répondant à la question suivante : **Comment protéger un réseau et un service voix sur IP contre les pirates et les attaques nuisibles ?**

2. Contexte du projet

Il s'agit de mettre en place un système de détection d'intrusion, permettant la surveillance des réseaux et voix sur internet.
Ce système consiste à :

- analyser les informations collectées.
- repérer les activités anormales ou suspectes sur le réseau ou sur un hôte.

3. Objectifs

L'objectif général de notre étude est de mettre en place un IDS évolué capable d'analyser les paquets potentiellement malicieux et de recevoir des nouvelles règles de contrôles pour assurer la sécurité des réseaux VoIP.
Les objectifs spécifiques sont :

- D'étudier le fonctionnement de base de la VoIP et montrer son importance en entreprise.
- D'étudier les vulnérabilités et les attaques de sécurité sur les composants d'une architecture VoIP dans un réseau.
- De détecter, d'enregistrer les évènements, d'analyser les informations , de générer des alertes et amorcer les usages anormaux des ressources (machines, données, services, équipement).

4. Organisation du mémoire

Ce rapport comprend trois (03) chapitres : dans le premier chapitre nous présentons une étude générale sur la VoIP et le protocole d'initiation de session SIP où nous avons décrit de manière brève ce protocole et la signalisation des appels. Le deuxième chapitre concerne les systèmes IDS où nous avons décrit de manière brève les fonctionnalités de bases de ces systèmes et nous avons présenté un aperçu sur les principes de fonctionnement de ces systèmes de sécurité. Le troisième chapitre est dédié à la réalisation de notre solution(implémentation), nous avons décrit l'environnement de travail ainsi que des captures d'écran de l'exécution de programme, nous avons présenté les tests réalisés.

Chapitre 1

Etude générale sur la VoIP

Introduction

La **Voix sur IP** constitue actuellement l'une des évolutions la plus importante du domaine des Télécommunications. Avant 1970, la transmission de la voix s'effectuait de façon analogique sur des réseaux dédiés à la téléphonie. La technologie utilisée était la technologie électromécanique (Crossbar). Dans les années 1980, une première évolution majeure a été le passage à la transmission numérique (TDM). La transmission de la voix sur les réseaux informatiques à commutation de paquets IP constitue aujourd'hui une nouvelle évolution majeure comparable aux précédentes[4].
L'objectif de ce chapitre est l'étude de cette technologie et de ses différents aspects. On parlera en détail de l'architecture de la VoIP, ses éléments et son principe de fonctionnement. On détaillera aussi le protocole de signalisation SIP et son principe de fonctionnement ainsi que les attaques contre la VoIP.

1.1 Présentation de la VoIP

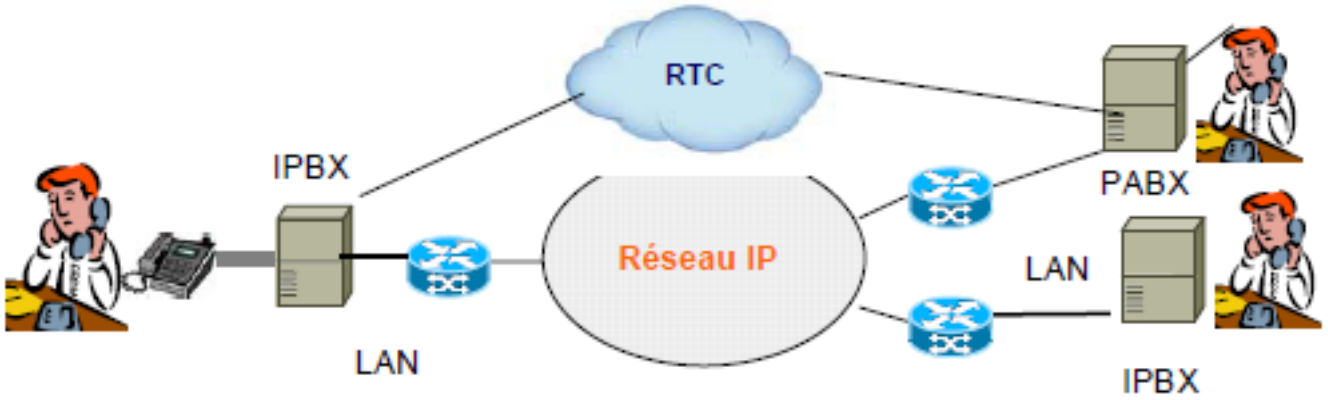
1.1.1 Définition

VoIP signifie Voice over Internet Protocol ou Voix sur IP. Comme son nom l'indique, elle permet de transmettre des sons (en particulier la voix) dans des paquets IP circulant sur Internet. La VoIP peut utiliser du matériel d'accélération pour réaliser ce but et peut aussi être utilisée en environnement de PC[5].

1.1.2 Architecture

La VoIP étant une nouvelle technologie de communication, elle n'a pas encore de standard unique. Les trois principaux protocoles sont : H323, SIP et MEGACO. Il existe donc plusieurs approches pour offrir des services de la téléphonie et de la visiophonie sur des réseaux IP. Certaines approches placent l'intelligence dans le réseau alors que d'autres préfèrent une approche égale à égale avec l'intelligence répartie à la périphérie. Chacune ayant ses avantages et ses inconvénients. La **figure 1.1** décrit, de façon générale l'architecture VoIP, elle comprend toujours des terminaux, un serveur de

communication et une passerelle vers les autres réseaux[4]. Nous pouvons identifier sur ce schéma que le RTC et le réseau IP coexiste et qu'ils sont reliés par une passerelle permettant la conversion des appels analogiques en numérique et inversement.



00000

FIGURE 1.1 – Architecture de la VoIP
Source : http://monge.univ-mlv.fr

Nous pouvons identifier en haut à droite un PABX connecté à un routeur. Cela est possible grâce à une carte spécifique que nous ajoutons sur le routeur. Cette carte se nomme FXS (Foreign eXchange Subscriber). Elle permet de connecter le PABX au routeur, ainsi que de fournir la tonalité, le courant de charge et le voltage de la sonnerie. Un routeur muni d'une carte FXS est alors appelé une Gateway FXS.
L'équipement de gauche est quant à lui un IPBX. C'est un serveur et nous pouvons donc le voir comme une PABX logiciel. Il offre les mêmes fonctionnalités qu'un PABX et même plus encore grâce aux modules qui peuvent être développés et lui être ajouté. Pour connecté un téléphone analogique à cet IPBX il faut utiliser, comme ci-dessus, une carte FXS. Ensuite un simple cable réseau RJ45 permet de relier l'IPBX et leehrigtyhtyky routeur[6]. Cependant, nous pouvons également voir que l'IPBX est connecté au RTC. Cela est possible grâce à une carte spécifique que nous ajoutons sur l'IPBX. Cette carte se nomme FXO (Foeign eXchange Office). Elle permet de founir l'information d'état décroché ou raccroché
Description des equipements de l'architecture VoIP :

- **Routeur :** permet d'aiguiller les données et le routage des paquets entre deux réseaux. Certains routeurs permettent de simuler un Gatekeeper grâce à l'ajout de cartes spécialisées supportant les protocoles VoIP.
- **Passerelle :** permet d'interfacer le réseau commuté et le réseau IP.
- **PABX :** est le commutateur du réseau téléphonique classique. Il permet de faire le lien entre la passerelle ou le routeur, et le réseau téléphonique commuté (RTC). Toutefois, si tout le réseau devient IP, ce matériel devient obsolète.
- **Terminaux :** sont généralement de type logiciel (software phone) ou matériel (Hardphone), le Softphone est installé dans le PC de l'utilisateur. L'interface audio peut être un microphone et des haut-parleurs branchés sur la carte son, même si un casque est recommandé. Pour une meilleure clarté, un téléphone USB ou Bluetooth peut être utilisé.

Le Hardphone est un téléphone IP qui utilise la technologie de la Voix sur IP pour permettre des appels téléphoniques sur un réseau IP tel que l'Internet au lieu de l'ordinaire système PSTN. Les appels peuvent parcourir par le réseau internet comme par un réseau privé. Un terminal utilise des protocoles comme le SIP ou l'un des protocoles propriétaire tel que celui utilisée par Skype[4].

1.1.3 Le Processus du traitement de la voix IP

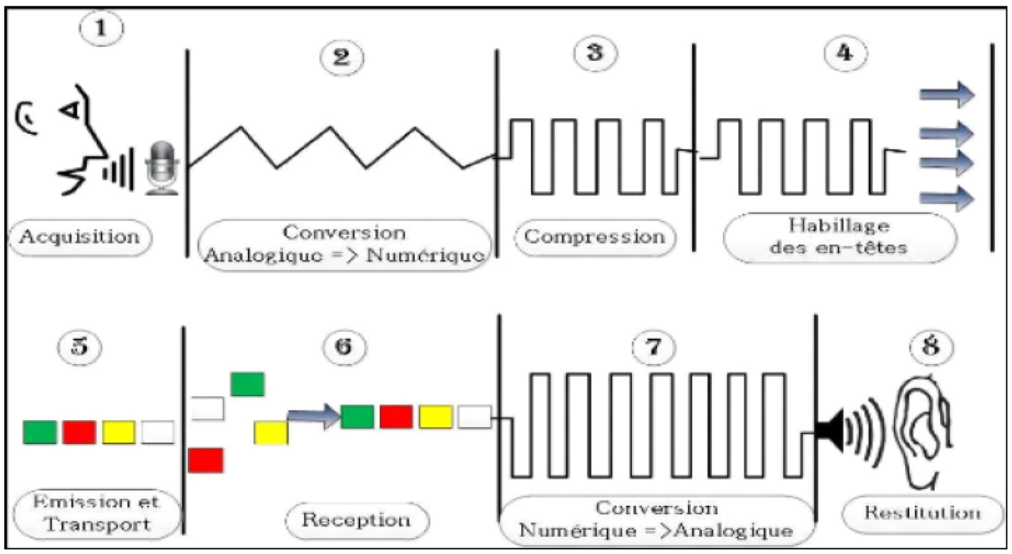


FIGURE 1.2 – Principe de fonctionnement de la VoIP
Source : http://memoireonline.com

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

- **L'acquisition :** C'est la première étape qui consiste à détecter la voix via un périphérique (téléphone ....).
- **La numérisation :** La bande voix qui est un signal électrique analogique utilisant une bande de fréquence de 300 à 3400 Hz. Ce signal doit d'abord être converti sous forme numérique suivant le format PCM (Pulse Code Modulation) ou G.711 à 64 Kbps.
- **La compression :** Cette opération consiste à réduire la taille physique de blocs d'informations numériques en utilisant un algorithme de compression.
- **L'habillage des entêtes :** le signal numérisé et compressé va être après découpé, en ajoutant des entêtes, il faut prendre en compte l'ordre du réassemblage du paquet, le type du trafic de synchronisation.
- **L'émission et transport :** C'est l'acheminement jusqu'au destinataire dans des paquets IP en utilisant les protocoles du routage.
- **La réception :** La réception des informations émis pendant la transaction.
- **La conversion numérique/analogique :** C'est l'étape inverse de la numérisation
- **La restitution :** Résultat finale l'écoute de la voix.

1.2 Description générale du protocole SIP

1.2.1 Informations sur le protocole SIP

Le protocole SIP est un protocole normalisé et standardisé par l'IETF (décrit par le RFC 3261 qui rend obsolète le RFC 2543, et complété par le RFC 3265) qui a été conçu pour établir, modifier et terminer des sessions multimédia. Il se charge de l'authentification et de la localisation des multiples participants. Il se charge également de la négociation sur les types de média utilisables par les différents participants en encapsulant des messages SDP (Session Description Protocol). SIP ne transporte pas les données échangées durant la session comme la voix ou la vidéo[3].
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 assure le plus souvent les sessions audio et vidéo. SIP remplace progressivement H323. SIP est le standard ouvert de VoIP, interopérable, le plus étendu et vise à devenir le standard des télécommunications multimédia (son, image, etc.). Skype par exemple, qui utilise un format propriétaire, ne permet pas l'interopérabilité avec un autre réseau de voix sur IP et ne fournit que des passerelles payantes vers la téléphonie standard. SIP n'est donc pas seulement destiné à la VoIP mais pour de nombreuses autres applications telles que la visiophonie, la messagerie instantanée, la réalité virtuelle ou même les jeux vidéo[10].

1.2.2 Capacités du protocole SIP

Le protocole SIP est capable de :

- localiser l'extrémité cible : SIP supporte la résolution d'adresses et la rédirection d'appels ;
- déterminer les capacités média de l'extrémité cible : SIP détermine le niveau de service commun le plus bas entre les deux extrémités. Les conférences sont établies en utilisant les capacités média qui peuvent être supportées par les deux extrémités ;
- déterminer la disponibilité de l'extrémité : si un appel ne peut pas aboutir car l'extrémité cible est indisponible, SIP détermine si l'extrémité appelée est déjà connectée avec un appel en cours ou ne répond pas après le nombre de sonneries paramétré ;
- établir une session entre les extrémités origine et cible : si l'appel peut aboutir, SIP établit une session entre les extrémités. SIP supporte également les modifications en cours de communication, telles que l'addition d'une autre extrémité à la conférence, le changement de caractéristiques de média ou de codec ;
- gèrer le transfert et la communication : SIP supporte le transfert d'appels d'une extrémité vers une autre. Pendant le transfert d'appels, SIP établit une session entre le transféré et la nouvelle extrémité (spécifiée par la partie transférante) et termine la session entre le transféré et la partie transférante[1].

1.2.3 Composants SIP

Dans un système SIP, on trouve deux types de composantes : les agents utilisateurs (UAS, UAC) et un réseau de serveurs (Registrar, Proxy) L'UAS représente l'agent de la partie appelée. C'est une application de type serveur qui contacte l'utilisateur lorsqu'une requête SIP est reçue. Et elle renvoie une

réponse au nom de l'utilisateur. L'UAC représente l'agent de la partie appelante. C'est une application de type client qui initie les requêtes. Le Registrar est un serveur qui gère les requêtes REGISTER envoyées par les «Users Agents» pour signaler leur emplacement courant. Ces requêtes contiennent donc une adresse IP, associée à une URI, qui seront stockées dans une base de données.
Les URI SIP sont très similaires dans leur forme à des adresses email : sip :utilisateur@domaine.com. Généralement, des mécanismes d'authentification permettent d'éviter que quiconque puisse s'enregistrer avec n'importe quelle URI[10].

1.2.4 Avantages et inconvénients SIP

- **Avantages :** L'implémentation de la voix sur IP avec le protocole de signalisation SIP fournit un service efficace, rapide et simple d'utilisation. SIP est un protocole rapide et léger. La séparation entre ses champs d'en-tête et son corps du message facilite le traitement des messages et diminue leur temps de transition dans le réseau.
  Les utilisateurs s'adressent à ces serveurs Proxy pour s'enregistrer ou demander l'établissement de communications. Toute la puissance et la simplicité du système viennent de là. On peut s'enregistrer sur le Proxy de son choix indépendamment de sa situation géographique. L'utilisateur n'est plus attaché à son autocommutateur. Une entreprise avec plusieurs centaines d'implantations physiques différentes n'a besoin que d'un serveur Proxy quelque part sur l'Internet pour établir son réseau de téléphonique gratuit sur l'Internet, un peu à la manière de l'émail. Les dizaines de milliers d'autocommutateurs peuvent être remplacés par quelques serveurs proxy. On imagine bien la révolution. Mais comme d'habitude rien n'empêchera de remplacer un autocommutateur par un serveur Proxy réduisant ainsi l'intérêt du système. SIP est un protocole indépendant de la couche transport. Il peut aussi bien s'utiliser avec TCP qu'UDP[4].

- **Inconvénients :** L'une des conséquences de cette convergence est que le trafic de voix et ses systèmes associés sont devenus aussi vulnérables aux menaces de sécurité que n'importe quelle autre donnée véhiculée par le réseau.
  En effet, SIP est un protocole d'échange de messages basé sur HTTP. C'est pourquoi SIP est très vulnérable face à des attaques de types Dos (dénis de service), détournement d'appel, trafic de taxation, etc. De plus, le protocole de transport audio associé RTP (Real Time Protocol) est lui aussi très peu sécurisé face à de l'écoute indiscrète ou des Dos.
  Le SIP est une norme pour la communication de multimédia, il devient de plus en plus utilisé pour la mise en place la téléphonie sur IP, la compréhension de ce protocole aidera le professionnel à l'épreuve de la sécurité sur le réseau[4].

1.2.5 Les messages SIP

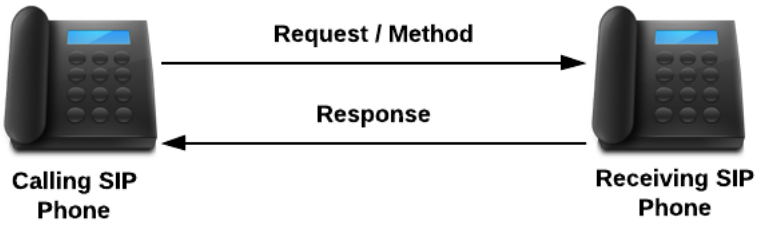


FIGURE 1.3 – Requêtes et réponses SIP
Source : http://3cx.fr

À part l'orientation client-serveur de SIP, les messages échangés sont soit des requêtes, soit des réponses. Dans les deux cas, les messages sont de nature textuelle (à l'instar des messages HTTP du World Wide Web), ce qui permet essentiellement une mise en œuvre facile et une bonne extensibilité du protocole.

1.2.5.1 Requêtes et réponses SIP

- **Requêtes SIP**

Il existe quatorze types de modes de requêtes dont les six premiers sont les modes de requêtes les plus basiques. Retrouvez toutes les requêtes du protocole SIP :

TABLE 1.1 – Requêtes du protocole SIP

Requêtes	Description
INVITE	Etablit une session
ACK	Confirme la requête INVITE
BYE	Met fin à la session
CANCEL	Annule l'établissement de la session
REGISTER	Donne l'emplacement de l'utilisateur (nom d'hôte, IP)
OPTIONS	Donne les informations sur les possibilités de recevoir et de passer des appels SIP
PRACK	Accusé de réception provisionnel
SUBSCRIBE	Souscrit à la notification du notifiant
NOTIFY	Prévient l'abonné d'un nouvel événement
PUBLISH	Publie un événement dans le serveur
INFO	Envoi des info de misession
REFER	Demande au destinataire d'émettre le transfert d'appel
MESSAGE	Transmet des messages instantanés
UPDATE	Modifie l'état d'une session

- **Reponses SIP**

Les Requêtes SIP reçoivent des réponses SIP. Il existe six catégories de réponses du protocole SIP :

TABLE 1.2 – Reponses du protocole SIP

Reponses	Description
1xx	réponses informatives
2xx	réponses réussies
3xx	réponses de renvoi
4xx	échecs des requêtes
5xx	erreurs du serveur
6xx	échec général

1.2.6 Fonctionnement du protocole SIP

Puisque nous avons choisi le protocole SIP pour effectuer la création des comptes utilisatéurs de notre serveur **VoIP**. Nous expliquerons les différents aspects, caractéristiques qui font du protocole SIP un bon choix pour l'établissement de la session, les principales caractéristiques du protocole SIP sont :

- Fixation d'un compte SIP
  Il est important de s'assurer que la personne appelée soit toujours joignable. Pour cela, un compte SIP sera associé à un nom unique. Par exemple, si 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 quelque soit son emplacement. Ce compte sera identifiable via son nom (ou pseudo).

- Changement des caractéristiques durant une session
  Un utilisateur doit pouvoir modifier les caractéristiques d'un appel en cours. Par exemple, un appel initialement configuré en (voix uniquement) peut être modifié en (voix + vidéo).

- Différents modes de communication
  Avec SIP, les utilisateurs qui ouvrent une session peuvent communiquer en mode point à point, en mode diffusif ou dans un mode combinant ceux-ci.

  – Mode Point à point : on parle dans ce cas d' « unicast » qui correspond à la communication entre deux machines.
  – Mode diffusif : on parle dans ce cas de « multicast » (plusieurs utilisateurs via une unité de contrôle MCU – Multipoint Control Unit).
  – Combinatoire : combine les deux modes précédents. Plusieurs utilisateurs interconnectés en multicast via un réseau à maillage complet de connexion.

- Gestion des participants
  Durant une session d'appel, de nouveaux participants peuvent joindre les participants d'une session déjà ouverte en participant directement, en étant transférés ou en étant mis en attente.

- Négociation des médias supportés
  Cela permet à un groupe durant un appel de négocier sur les types de médias supportés. Par exemple, la vidéo peut être ou ne pas être supportée lors d'une session.

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

- Modèle d'échange
  Le protocole SIP repose sur un modèle (Requête/Réponse). Les échanges entre un terminal appelant et un terminal appelé se font par l'intermédiaire de requêtes. La liste des requêtes échangées se présente de la façon suivante :

  – Invite : cette requête indique que l'application (ou utilisateur) correspondante à l'url SIP spécifié est invité à participer à une session. Le corps du message décrit cette session (par ex : média supportés par l'appelant). En cas de réponse favorable, l'invité doit spécifier les médias qu'il supporte.
  – Ack : cette requête permet de confirmer que le terminal appelant a bien reçu une réponse définitive à une requête Invite.
  – Options : un proxy server en mesure de contacter l'UAS (terminal) appelé, doit répondre à une requête Options en précisant ses capacités à contacter le même terminal.
  – Bye : cette requête est utilisée par le terminal de l'appelé afin de signaler qu'il souhaite mettre un terme à la session.
  – Cancel : cette requête est envoyée par un terminal ou un proxy server à fin d'annuler une requête non validée par une réponse finale comme, par exemple, si une machine ayant été invitée à participer à une session, et ayant accepté l'invitation ne reçoit pas de requête Ack, alors elle émet une requête Cancel.
  – Register : cette méthode est utilisée par le client pour enregistrer l'adresse listée dans l'URL TO par le serveur auquel il est relié[19].

1.3 Quelques attaques contre la VOIP

L'opportunité de migrer de la téléphonie classique vers la téléphonie IP, a offert plusieurs avantages pour les entreprises, et les a permis de bénéficier de nouveaux services tel que la vidéoconférence et la transmission des données. L'intégration de ces services dans une seule plateforme nécessite plus de sécurité.
Dans cette partie nous décrivons et détaillerons quelques attaques qui menacent la VoIP.

1.3.1 Le déni de service

C'est sûrement l'une des attaques les plus répandues. Comme pour un site internet, elle a pour but de rendre inopérant le système. Pour le réseau téléphonique, la personne malveillante peut s'attaquer à l'IPBX en saturant le serveur. Une mauvaise mise en oeuvre, par exemple, de la pile TCP/IP peut être fatale car elle favorise le **flooding**. Le serveur de communication ou encore la passerelle située entre le monde IP et le RTC sont deux autres cibles. Une manière différente de lancer un déni de service est de s'attaquer directement au téléphone IP. Cette méthode est totalement nouvelle puisque dans une architecture traditionnelle les téléphones dénués d'intelligence ne pouvaient pas servir de cibles. Les

experts, pour qui cette attaque est assez facile à réaliser, estiment qu'il ne faut pas omettre de sécuriser le lien entre le terminal et l'IPBX, particulièrement lorsqu'on procède aux actions d'enregistrement du premier sur le dernier[8].

1.3.2 La fraude téléphonique

Il s'agit de prendre la main sur l'IPBX et de le transformer, par exemple, en cabine téléphonique sauvage à l'aide de laquelle on va pouvoir passer des appels aux frais de l'entreprise[2].

1.3.3 L'écoute

A l'instar des paquets de données qui peuvent être interceptés par des attaques de type **man-in-the-middle**, il en va de même pour les paquets vocaux. Par **spoofing** (à savoir la falsication d'identité d'un ordinateur), tout le trafic entrant et sortant est orienté via le réseau du pirate. Ce dernier est donc capable de regrouper les paquets vocaux et de les écouter littéralement en direct. Le pirate a de ce fait à sa disposition les données sensibles, comme le nom de l'utilisateur, le mot de passe et l'information du système VoIP[2].

1.3.4 L'accès au système d'information

Les IPBX d'entreprise, au même titre que les postes clients équipés de logiciels de type Skype, doivent toujours être ouverts afin de recevoir les appels. Cela signifie que n'importe qui peut leur envoyer des messages. Le destinataire est alors totalement dépendant de l'intégrité du logiciel de VoIP, et de sa capacité à prévenir les attaques et à les empêcher de pénétrer dans le système d'information[2].

1.3.5 Vishing

Le vishing (contraction de VoIP et de phishing) est une attaque qui consiste à mettre en place un système de serveurs composant de façon aléatoire des numéros. Lorsqu'une personne finit par décrocher, elle entend un message, laissé par un serveur vocal se faisant passer, par exemple, pour un établissement financier et l'informant d'opérations débitrices inhabituelles. Un service comptabilité, par exemple, utilisant un service d'e-banking pourrait ainsi délivrer des informations confidentielles en toute innocence[16].

1.3.6 Spam via Internet Telephony (SPIT)

Tout comme d'autres pourriels (courriel indésirable) courants, le spam via la téléphonie internet peut aussi être généré et expédié par botnet (programme connecté à Internet). Il en résulte que des millions d'utilisateurs VoIP ne disposant pas d'un filtre correct, sont noyés sous ces messages SPIT. A l'instar du spam, SPIT ralentit les performances du système, engorge les boîtes de mail vocal et entrave la productivité des utilisateurs[16].

1.3.7 Détournement de données d'enregistrement

Il peut aussi arriver qu'un pirate annule un enregistrement SIP. Il remplace alors ce dernier par sa propre adresse IP, ce qui lui permet d'intercepter les communications entrantes, pour les réorienter, les reproduire, voire les interrompre[16].

1.3.8 Directory harvesting

Le **VoIP directory harvesting** signifie qu'un agresseur exploite des milliers d'adresses VoIP existantes pour lancer des attaques sur le réseau. L'attaque est généralement effectuée comme une attaque par dictionnaire standard, où des adresses électroniques sont générées par force brute en associant des lettres, des prénoms et des noms communs. Ces attaques sont plus efficaces pour générer des adresses électroniques d'employés d'entreprises, car ces adresses ont généralement un format standard (par exemple jacques.tremblay@compagnie.com, jtremblay@compagnie.com ou jeant@compagnie.com). Il peut ensuite les utiliser lui-même ou via un botnet pour expédier des messages SPIT ou procéder à du **vishing** (hameçonnage vocal)[16].

1.4 Etat de politique de sécurité de la VoIP existente

Pour les solutions de sécurité de la VoIP, plusieurs éfforts ont déjà été consentis pour définir des solutions plus éfficaces. Nous pouvons citer : Sécurisation protocolaire, sécurisation de l'application et sécurisation du système de l'exploitation[11].

1.4.1 Sécurisation protocolaire

La prévalence et la facilité de renifler des paquets et d'autres techniques pour la capture des paquets IP sur un réseau pour la voix sur IP font que le cryptage soit une nécessité.**IPsec** peut être utilisé pour réaliser deux objectifs. Garantir l'identité des deux points terminaux et protéger la voix une fois que les paquets quittent l'Intranet de l'entreprise. **VoIPsec** (VoIP utilisant IPsec) contribue à réduire les menaces, les sniffeurs de paquets, et de nombreux types de trafic « vocal analyze ». Combiné avec un pare-feu, IPsec fait que la VoIP soit plus sûr qu'une ligne téléphonique classique. Il est important de noter, toutefois, que IPsec n'est pas toujours un bon moyen pour certaines applications, et que certains protocoles doivent continuer à compter sur leurs propres dispositifs de sécurité[9].

1.4.1.1 VoIP VPN

Un VPN VoIP combine la voix sur IP et la technologie des réseaux virtuels privés pour offrir une méthode assurant la préservation de la prestation vocale. Puisque la VoIP transmet la voix numérisée en un flux de données, la solution VPN VoIP semble celle la plus approprié vu qu'elle offre le cryptage des données grâce à des mécanismes de cryptages et offre l'intégrité des paquets VoIP[9].

1.4.1.2 Secure RTP ou SRTP

Le service SRTP (Secure Realtime Transport Protocol) est conçu pour sécuriser la multiplication à venir des échanges multimédias sur les réseaux. Il couvre les lacunes de protocoles de sécurité existants comme IPsec, dont le mécanisme d'échanges de clés est trop lourd. Il est aussi bâti sur le protocole RTP. Il associe aussi une demi-douzaine de protocoles complémentaires. Il est donc compatible à la fois avec des protocoles d'initiation de session de voix sur IP tel que SIP, ainsi que le protocole de diffusion de contenu multimédia en temps réel RTSP[9].

1.4.2 Sécurisation de l'application

Plusieurs méthodes peuvent être appliquées pour sécuriser l'application, ces méthodes varient selon le type d'application (serveur ou client). Pour sécuriser le serveur il faut :

- L'utilisation d'une version stable, Il est bien connu que toute application non stable contient surement des erreurs et des vulnérabilités. Mais pour minimiser les risques, il est impératif d'utiliser une version stable.
- Tester les mises à jour des softwares dans un laboratoire de test, il est très important de tester toute mise à jour de l'application dans un laboratoire de test avant de les appliquer sur le système en production
- Ne pas tester les correctifs sur le serveur lui-même.
- Ne pas utiliser la configuration par défaut, qui sert juste à établir des appels. Elle ne contient aucune protection contre les attaques
- Ne pas installer une application cliente sur le serveur.

1.4.3 Sécurisation du système d'exploitation

Il est très important de sécuriser le système sur lequel est implémenté le serveur de VoIP. En effet, si le système est compromis, l'attaque peut se propager sur l'application serveur. Celle-ci risque d'affecter les fichiers de configuration contenant des informations sur les clients enregistrés. Il y a plusieurs mesures de sécurités à prendre pour protéger le système d'exploitation :

- Utiliser un système d'exploitation stable. Les nouvelles versions toujours contiennent des bugs et des failles qui doivent être corrigés et maîtrisés avant.
- Mettre à jour le système d'exploitation en installant les correctifs de sécurité recommandé pour la sécurité.
- Ne pas mettre des mots de passe simple. Ils sont fondamentaux contre les intrusions. Et ils ne doivent pas être des dates de naissances, des noms, ou des numéros de téléphones. Un mot de passe doit être assez long et former d'une combinaison de lettre majuscule et miniscule, de chiffres et des ponctuations.
- Ne pas exécuter le serveur VoIP avec un utilisateur privilège. Si un utilisateur malveillant arrive à accéder au système via une exploitation de vulnérabilité sur le serveur VoIP, il héritera tous les privilèges de cet utilisateur.
- Sauvegarde des fichiers log à distance : les fichiers log sont très importants, il est conseillé de les enregistrer sur un serveur distant.
- Installer seulement les composants nécessaires : pour limiter les menaces sur le système d'exploitation. Il vaut mieux installer sur la machine le système d'exploitation et le serveur.
- Supprimer tous programmes, logiciels ou des choses qui n'ont pas d'importance et qui peuvent être une cible d'attaque pour accéder au système.
- Renforcer la sécurité du système d'exploitation en installant des patches qui permettent de renforcer la sécurité générale du noyau[11].

1.4.4 Pare-feu

Le pare-feu surveille les intrusions vers l'extérieur afin de les empêcher de se produire.Il limite l'accès entre les réseaux pour prévenir les intrusions et ne signalent pas une attaque de l'intérieur du réseau.

Conclusion

Au terme de notre premier chapitre, il est d'une importance capitale d'affirmer que la VoIP est l'une des solutions la plus rentable pour effectuer des conversations. Actuellement il est évident que la VoIP va continuer à évoluer. Elle est une bonne solution en matière d'intégration, fiabilité et de coût. La voix sur IP est devenue de nos jours l'une des téchnologies la plus ciblée. Il existe plusieurs autres attaques qui menacent la sécurité du VoIP, les attaques citées dans ce chapitre sont les plus fameuses et courantes dans les réseaux VoIP.
Dans le chapitre suivant, nous allons présenter les systèmes IDS afin de comprendre le principe de fonctionnement de la mise en place de notre solution pour la sécurité des réseaux et services VoIP.

Chapitre 2

Les systèmes de détection d'intrusion

Introduction

Avec l'arrivée de l'Internet, est apparue l'interconnexion planétaire des réseaux avec pour corollaire une rapidité de plus en plus grande de diffusion et d'acquisition de toute forme d'information. Parallèlement, des menaces de tous genres sont apparues et se sont développées. On estime aujourd'hui à moins de quatre (04) minutes le temps moyen pour qu'un ordinateur non protégé connecté à Internet subisse une tentative d'intrusion ou soit contaminé par un programme malicieux. Pour détecter les attaques que peut subir un système, il est nécessaire d'avoir un logiciel spécialisé dont le rôle serait de surveiller les données qui transitent sur ce système, et qui serait capable de réagir si des données semblent suspectes. Communément appelé un IDS, les systèmes de détection d'intrusion conviennent parfaitement pour réaliser cette tâche[17].
Dans ce chapitre nous allons décrire les fonctionnalités de base des systèmes de détection d'intrusion.

2.1 Systèmes de détection d'intrusion

Un système de détection d'intrusion est un dispositif ou une application logicielle qui surveille un réseau ou des systèmes pour déceler toute activité malveillante ou toute violation de politique de sécurité. Toute activité malveillante ou violation est généralement signalée à un administrateur ou est recueillie de façon centralisée au moyen d'un système de gestion des informations et des événements de sécurité (SIEM). Un système SIEM combine des sorties provenant de sources multiples et utilise des techniques de filtrage des alarmes pour distinguer les activités malveillantes des fausses alarmes[18].

2.1.1 Choix du placement d'un IDS

Il existe plusieurs endroits stratégiques où il convient de placer un IDS. **La figure 2.1** illustre un réseau local ainsi que les trois positions que peut y prendre un IDS :

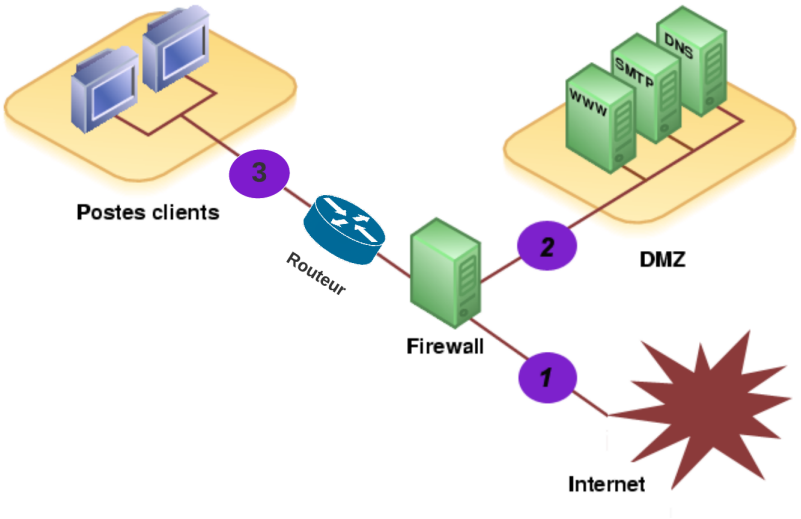


FIGURE 2.1 – Choix d'emplacement d'un système de détection d'intrusion
Source : http://www-igm.univ-mlv.fr/~dr/XPOSE2004/IDS/IDSSnort.html

Le placement des IDS va dépendre de la politique de sécurité définie dans le réseau. Mais il existe des positions qu'on peut qualifier de standards, par exemple il serait intéressant de placer des IDS :

- Dans la zone démilitarisée (position 2)(attaques contre les systèmes publics).
- Dans le (ou les) réseau(x) privé(s) (position 3) (intrusions vers ou depuis le réseau interne).
- Sur la patte extérieure du firewall (position 1)(détection de signes d'attaques parmi tout le traficentrant et sortant, avant que n'importe quelle protection intervienne).

2.1.2 Classification des IDS

En fonction des données qu'ils traiteront, les systèmes de détection d'intrusion peuvent être considérés comme ou étant des systèmes de détection d'intrusion hôtes (analysant les événements au niveau du système d'exploitation), ou réseaux (analysant les événements propres au trafic réseau).

2.1.2.1 Systèmes de détection d'intrusion réseaux

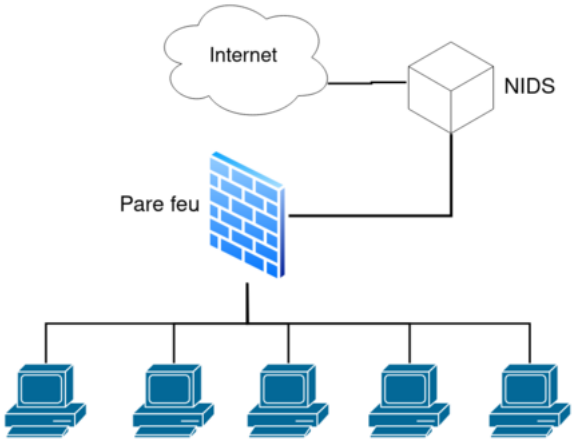


FIGURE 2.2 – Positionnement Nids
Source : https://www.wikiwand.com/fr/Système_de_détection_d%27intrusion

Les systèmes de détection d'intrusion réseaux ou NIDS sont les IDS les plus répandus. Ce sont des outils très utiles pour l'administrateur réseaux qui va pouvoir, en temps réel, comprendre ce qui se passe sur son réseau et prendre des décisions en ayant toutes les informations. Ces IDS vont analyser tout le trafic entrant et sortant du réseau afin d'y déceler des attaques. Cependant, un NIDS placé sur chaque hôte ne saura pas détecter toutes les attaques possibles comme les attaques par déni de service (DDoS) car il ne verra pas tout le trafic réseau, mais que celui qui arrive à l'hôte finale.
Quand un NIDS est positionné en amont d'un pare feu, il pourra alors générer des alertes pour le pare feu qui va pouvoir filtrer le réseau. Placé en aval du pare feu, le NIDS produira moins de faux positifs, car le trafic réseau qu'il analysera aura déjà été filtré par le pare feu. Dès qu'une attaque est détectée, que ce soit par signature (SIDS) ou anomalies (AIDS), une alerte est remontée afin de pouvoir prendre une décision sur l'action à effectuer, soit par un IPS, soit par l'administrateur[18].

2.1.2.2 Systèmes de détection d'intrusion hôtes

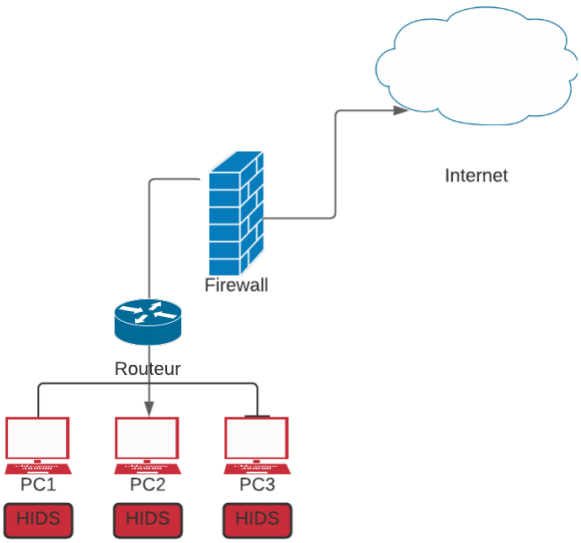


FIGURE 2.3 – Positionnement Hids

Les systèmes de détection d'intrusion hôte ou HIDS sont des IDS mis en place directement sur les hôtes à surveiller. Ils vont directement analyser les fichiers de l'hôte, les différents appels système et aussi les événements réseaux. Par conséquent ces analyses sont strictement limitées à l'hôte sur laquelle l'HIDS est installé et n'ont aucune vue sur le réseau. Les HIDS agissent comme des antivirus mais en plus poussé, car les antivirus ne sont intéressés que par les activités malveillantes du poste alors qu'un HIDS va pouvoir intervenir s'il détecte des attaques par dépassement de tampon et concernant les processus système par exemple.
La fonction de base d'un HIDS est l'inspection des fichiers de configuration du système d'exploitation afin d'y déceler des anomalies contre les rootkit notamment [18].

2.1.2.3 Systèmes de détection d'intrusion collaboratif

Les systèmes de détection d'intrusion collaboratif ou CIDS sont des systèmes reposant sur d'autres IDS. De ce fait le CIDS peut opérer sur des systèmes hétérogènes. Il existe trois façons de mettre en place un CIDS, l'approche centralisée, l'approche hiérarchique et l'approche distribuée.

- **L'approche centralisée :**

Elle se composée de deux éléments : le système expert et les IDS (HIDS ou NIDS). Les IDS vont pouvoir détecter, sur leur réseau local ou sur leur hôte, des anomalies qu'ils enverront au système expert. Il va permettre de déterminer s'il s'agit d'une attaque globale contre les différents systèmes ou plus locale, s'il n'a reçu qu'une seule alerte par exemple. Les CIDS déployés sur cette approche ont un très bon taux de détection. Mais ils ont deux désavantages majeurs, le premier est que si le système expert tombe en panne, tout le système est inutilisable, il s'agit d'un point de défaillance unique (single-point of failure en anglais, ou SPOF). Le deuxième inconvénient de cette approche est qu'en cas de grosse attaque, il est possible que certaines des alertes reçues soient ignorées en raison de la quantité reçue par le système expert, ou que ces alertes soient traitées plus tard et donc, possiblement, après l'attaque. Cette approche a été mise en place pour DIDS (Distributed Intrusion Detection System) par Snapp[17].

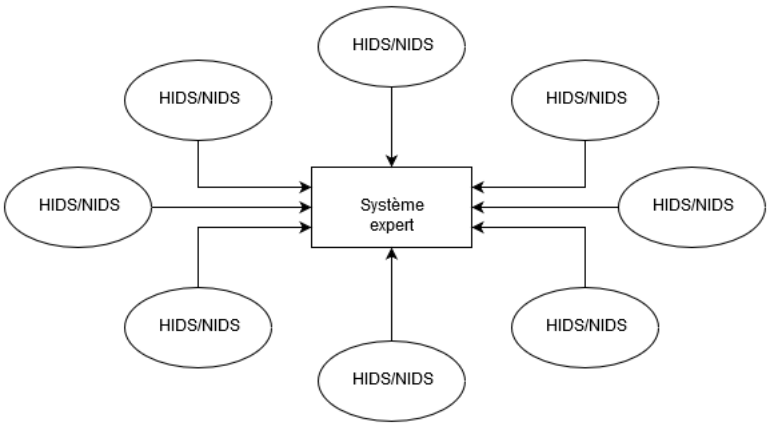


FIGURE 2.4 – L'approche centralisée

Source : https://www.wikiwand.com/fr/Système_de_détection_d%27intrusion

- **L'approche hiérarchique :**

Cette approche va permettre d'éviter le point de défaillance unique, mis en lumière par l'approche centralisée. En effet, dans cette solution, plusieurs nœuds (Système expert) sont chargés de la corrélation des alertes. Un nœud est désigné dans chaque groupe afin qu'il agisse en tant que nœud de corrélation et d'alerte, il va donc analyser les alertes qui viennent de son groupe, les corréler et transmettre une alerte, si besoin, au nœud supérieur. Cette fois-ci si un nœud intermédiaire vient à être désactivé, toute la sous-branche sera inutilisable.

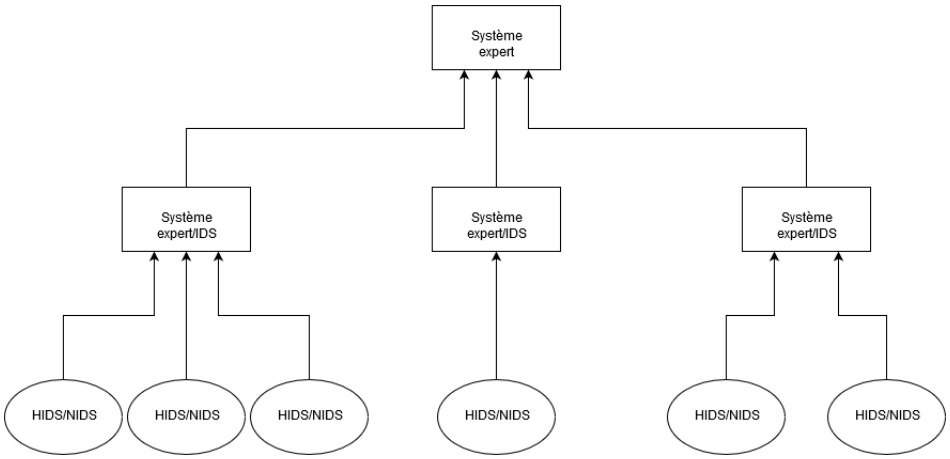


FIGURE 2.5 – L'approche hiérarchique

Source : https://www.wikiwand.com/fr/Système_de_détection_d%27intrusion

- **L'approche distribuée :**

La dernière approche, permet d'éviter d'avoir des points de défaillance, qui pourront mettre à mal tout le système de détection. Pour cela, chaque nœud va jouer le rôle d'un collecteur d'information et d'un analyseur d'information. Ces nœuds détectent localement les attaques et sont capables de corréler les informations des nœuds voisins pour détecter les attaques globales[17].

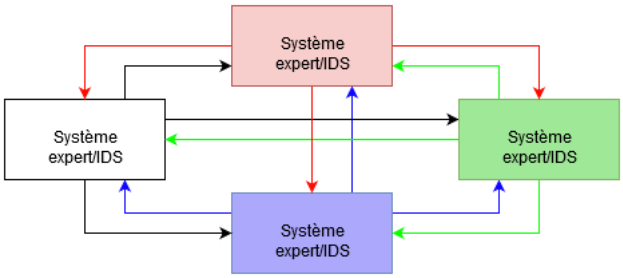


FIGURE 2.6 – L'approche distribuée

Sorce : https://www.wikiwand.com/fr/Système_de_détection_d%27intrusion

2.1.3 Méthodes de détection des IDS

2.1.3.1 Systèmes de détection d'intrusion par signatures

Les systèmes de détection d'intrusion par signature ou SIDS, reposent sur des bibliothèques de description des attaques (appelées signatures). Au cours de l'analyse du flux réseau, le système de détection d'intrusion analysera chaque événement et une alerte sera émise dès lors qu'une signature sera detectée. Cette signature peut référencer un seul paquet, ou un ensemble (dans le cas d'une attaque par déni de service par exemple). Cette méthodologie de détection se révèle être efficace uniquement si la base de signatures est maintenue à jour de manière régulière. Dans ce cas, la détection par signatures produit peu de faux-positifs[17].
Cependant, une bonne connaissance des différentes attaques est nécessaire pour les décrire dans la base de signature. Dans le cas d'attaques inconnues de la base, ce modèle de détection s'avérera inefficace et ne générera donc pas d'alertes. La base de signature est donc très dépendante de l'environnement (système d'exploitation, version, applications déployées, ...).

2.1.3.2 Systèmes de détection d'intrusion par anomalies

Contrairement aux SIDS, les systèmes de détection d'intrusion par anomalies (ou AIDS : Anomaly-based Intrusion Detection System) ne se reposent pas sur des bibliothèques de description des attaques. Ils vont se charger de détecter des comportements anormaux lors de l'analyse du flux réseau[12]. Pour cela, le système va reposer sur deux phases :

- Une phase d'apprentissage, au cours de laquelle ce dernier va étudier des comportements normaux de flux réseau.
- Une phase de détection, le système analyse le trafic et va chercher à identifier les événements anormaux en se basant sur ses connaissances.

  Cette méthode de détection repose sur de nombreuses techniques d'apprentissage supervisé, telles que :

- Les réseaux de neurones artificiels ;
- Le modèle de Markov caché ;
- Les machines à vecteurs de support.

2.1.3.3 Systèmes de détection d'intrusion Hybride

Cette méthodologie de détection consiste à reposer à la fois sur un système de détection par signature et sur un système de détection par anomalies. Pour cela, les deux modules de détection, en plus de déclencher des alertes si une intrusion est détectée, peuvent communiquer leurs résultats d'analyse à un système de décision qui pourra lui-même déclencher des alertes grâce à la corrélation des résultats remontés par les deux modules.
L'avantage de cette méthodologie de détection est la combinaison du faible taux de faux-positifs générés par les systèmes de détection d'intrusion par signature, tout en possédant la capacité de détecter des attaques inconnues dans la base de signature grâce à la détection par anomalie[12].

2.1.3.4 Systèmes de détection d'intrusion par analyse des protocoles

Les systèmes de détection d'intrusion peuvent également reposer sur l'analyse des protocoles. Cette analyse (appelée en anglais SPA : Stateful Protocol Analysis) a pour objectif de s'assurer du fonctionnement normal d'un protocole (par exemple de transport ou d' application). Celle-ci repose sur des modèles définis, par exemple par des normes RFC. Ces normes n'étant pas exhaustives, cela peut entraîner des variations dans les implémentations. De plus, les éditeurs de logiciels peuvent rajouter des fonctionnalités propriétaires, ce qui a pour conséquence que les modèles pour ces analyses doivent être régulièrement mis à jour afin de refléter ces variations d'implémentations.
Cette méthode d'analyse a pour principal inconvénient que les attaques ne violant les caractéristiques du protocole, comme une attaque par déni de service, ne seront pas détectées[12].

2.1.3.5 Systèmes de détection d'intrusion par temporalité de détection

Il existe deux types de temporalité dans les systèmes de détection d'intrusion : la détection en temps réel (système temps réel), et la détection post-mortem (analyse forensique). Le plus souvent, l'objectif est de remonter les alertes d'intrusion le plus rapidement possible à l'administrateur système. La

détection en temps réel sera donc privilégiée. Cette temporalité de détection présente des défis de conception pour s'assurer que le système puisse analyser le flux de données aussi rapidement qu'il est généré. Cependant, il est aussi envisageable d'utiliser un système de détection d'intrusion dans le cadre d'analyse post-mortem. Dans ce cas, ce dernier permettra de comprendre le mécanisme d'attaque pour aider à réparer les dommages subis et réduire le risque qu'une attaque du même genre se reproduise[12].

2.1.3.6 Systèmes de détection d'intrusion par corrélation des alertes

La corrélation des alertes a pour objectif de produire un rapport de sécurité de la cible surveillée (un réseau par exemple). Ce rapport sera basé sur l'ensemble des alertes produites par les différentes sondes de détection d'intrusion disséminées sur l'infrastructure[12]. Pour cela, il est nécessaire de différencier deux composants :

- **les sondes :** chargées de récupérer les données depuis les sources concernant leurs cibles (fichiers de logs, paquets réseaux ,...) et de générer, si nécessaire, des alertes ;
- **les composants d'agrégation et de corrélation :** chargés de récolter les données des sondes et des autres composants d'agrégation et de corrélation afin de les corréler et produire le rapport de sécurité transmis à l'administrateur.

2.1.4 Tableau comparatif des systèmes de détection d'intrusion

TABLE 2.1 – Comparaison des différents types de IDS

Types d'IDS	Avantages	Inconvenients
NIDS	Surveille un grand réseau ; Identifie les attaques de multiples hôtes ; Assure la sécurité contre les attaques puisqu'il est invisible ;	Ne voit qu'une copie du trafic du réseau à surveiller, Dysfonctionement dans un environnement crypté ; Ne permet pas d'assurer si une tentative d'attaque est couronnée de succès ; Difficile à traiter tous les paquets circulant sur un grand réseau
HIDS	Contrôle les activités locales des utilisateurs avec précision ; Capable de déterminer si une tentative d'attaque est couronnée de succès ; Capable de fonctionner dans des environnements cryptés ; Détecte des attaques qui ne sont pas vues par **NIDS** ;	La difficulté de déploiement et de gestion ; Incapable de détecter des attaques contre de multiples cibles dans le réseau
HYBRIDE	Moins de faux positifs ; Meilleure corrélation ; Possibilité de réaction sur les analyseurs ;	Taux élevé de faux positifs

2.2 Systèmes de prévention d'intrusion

Les systèmes de prévention des intrusions (IPS), également connus sous le nom de systèmes de détection et de prévention des intrusions (IDPS), sont des dispositifs de sécurité réseau qui surveillent les activités du réseau ou du système pour détecter toute activité malveillante. Les principales fonctions des systèmes de prévention des intrusions sont d'identifier les activités malveillantes, d'enregistrer des informations sur ces activités, de les signaler et de tenter de les bloquer ou de les arrêter[12].

2.2.1 Classification des IPS

Les systèmes de prévention des intrusions peuvent être classés en quatre types différents[7] :

- **Système de prévention des intrusions en réseau (NIPS) :** surveille l'ensemble du réseau à la recherche de trafic suspect en analysant l'activité du protocole.
- **Système de prévention des intrusions sans fil (WIPS) :** surveille un réseau sans fil pour détecter tout trafic suspect en analysant les protocoles de réseau sans fil.
- **Analyse du comportement du réseau (NBA) :** examine le trafic réseau pour identifier les menaces qui génèrent des flux de trafic inhabituels, telles que les attaques par déni de service distribué (DDoS), certaines formes de logiciels malveillants et les violations de règles.
- **Système de prévention des intrusions basé sur l'hôte (HIPS) :** un logiciel installé qui surveille l'activité suspecte d'un seul hôte en analysant les événements qui se produisent sur cet hôte. Il est capable de reporter des alertes ou d'y réagir lui-même.

les systèmes de prévention des intrusions (IPS) utilisent les mêmes architectures que les systèmes des détections d'intrusions (IDS). Car un IPS est juste un IDS améliorer capable de détecter et bloquer une intrusion.

2.2.2 Méthodes de détection des IPS

La majorité des systèmes de prévention des intrusions utilisent l'une des trois méthodes de détection suivantes :

- **Détection basée sur les signatures :** L'IPS basé sur les signatures surveille les paquets dans le réseau et compare avec les modèles d'attaque pré-configurés et prédéterminés connus sous le nom de signatures.
- **Détection statistique basée sur les anomalies :** Un IPS basé sur les anomalies surveillera le trafic réseau et le comparera à une base de référence établie. La ligne de base identifiera ce qui est "normal" pour ce réseau. quel type de bande passante est généralement utilisé et quels protocoles sont utilisés. Elle peut cependant déclencher une alarme de faux positif pour une utilisation légitime de la bande passante si les lignes de base ne sont pas configurées intelligemment.
- **Détection d'analyse de protocole dynamique** Cette méthode identifie les déviations des états du protocole en comparant les événements observés avec des profils prédéterminés de définitions généralement acceptées de l'activité bénigne[12].

2.3 Système de détection d'intrusion pour la VoIP

Il n'est pas trés courant de trouver des outils de détection pour des solutions VoIP. Mais néamoins il existe **SecAst** dédié uniquement pour le serveur Asterisk.

- SecAst

Sécurité pour Asterisk (SecAst) est un système de détection et de prévention des fraudes et des intrusions conçu spécifiquement pour protéger les systèmes téléphoniques basés sur Asterisk. SecAst utilise une VAR de techniques et de bases de données propriétaires pour détecter les tentatives d'intrusion, arrêter les attaques en cours et prévenir de futures attaques. En outre, SecAst utilise des techniques avancées pour détecter les informations d'identification valides qui ont été divulguées compromises et sont abusés, et utilise des algorithmes heuristiques pour apprendre le comportement de l'attaquant. Lors de la détection de fraude ou d'attaque, SecAst peut déconnecter les appels et bloquer l'attaquant Asterisk au niveau du réseau[13].
SecAst offre les fonctionnalités suivantes :

  - Base de données des numéros de téléphone sur les fraudes et d'adresses IP des pirates
  - Base de données IP géographique
  - Communiquant avec un certain nombre de sous-systèmes Asterisk réseau et Linux
  - Surveillance des tentatives de connexion et détection d'attaque par force brute
  - Arrêter les attaques dans ses traces et alerter l'administrateur avec des détails de chaque attaque
  - Offre des interfaces étendues pour interagir avec d'autres programmes, services publics, pare-feu, systèmes de facturation.
  - Disponible dans les éditions gratuites et commerciales

Cette solution protège le serveur voix sur IP en temps réel. Les limites se présentent comme suit :

- Pas de detéction en cas d'une attaque en dehors du serveur voix sur IP
- Pas d'ajout des règles dans la base de signature
- Elle ne surveille que le serveur Asterisk

Le but de ce projet est de protèger le réseau global et c'est véritablement la raison pour laquelle il faut compléter cet outil de sécurité au sein du réseau. Une combinaison pour la consolidation de la sécurité de VoIP est nécessaire. Pour notre projet, la sécurité c'est une étape primordiale. Après des recherches, nous avons choisi **Snort** qui est un système de détection et prévention d'intrusion réseau ou NIDS, qui permet de surveiller les données de package envoyées et reçues via une interface réseau spécifique. Il permet aussi de détecter les menaces ciblant les vulnérabilités et bloquer les paquets malveillants de votre système à l'aide de technologies de détection et d'analyse de protocole basées sur des signatures. Il existe plusieurs endroits où nous pouvons mettre en place notre NIDS.

Conclusion

Les systèmes de détection d'intrusion sont actuellement des produits employés et aboutis pour intervenir dans la detéction d'intrusion. Ils continuent d'évoluer pour répondre aux exigences technologiques du moment mais malgré les nouvelles attaques, ils ont des fonctionnalités capables de satisfaire les besoins de tous types d'utilisateurs. Néanmoins, comme tous les outils techniques, ils ont des limites que seule une analyse humaine peut compenser. Un peu comme les Firewalls, les IDS deviennent chaque jour meilleurs grâce à l'expérience acquise avec le temps mais ils deviennent aussi de plus en plus sensibles aux problèmes de configuration et de paramétrage.
Nous décrivons dans le chapitre suivant l'implémentation de ce travail suivi des captures d'écran.

Chapitre 3

Implémentation de la solution

Introduction

Après avoir présenté la partie réservée à l'étude générale sur la VoIP et la présentation des systèmes IDS, nous présenterons la phase de réalisation de notre projet. Dans une première étape on va passer à la configuration de notre serveur VoIP. En deuxième étape nous allons présenter un test de pénétration effectué sur le réseau. Et en troisième étape, on va présenter la sécurisation et répondre au besoin de sécurité de VoIP avec notre solution IDS (Snort) proposée.

3.1 Environnement de travail

La figure 3.1 présente l'environnement de travail avec les différentes machines installées et leur adressage IP.

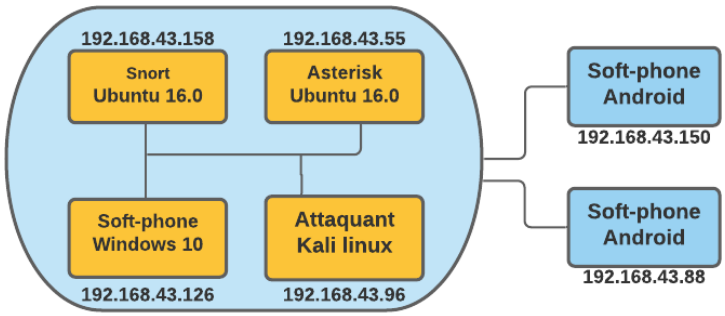


FIGURE 3.1 – Environnement de travail

3.2 Architecture du réseau d'étude

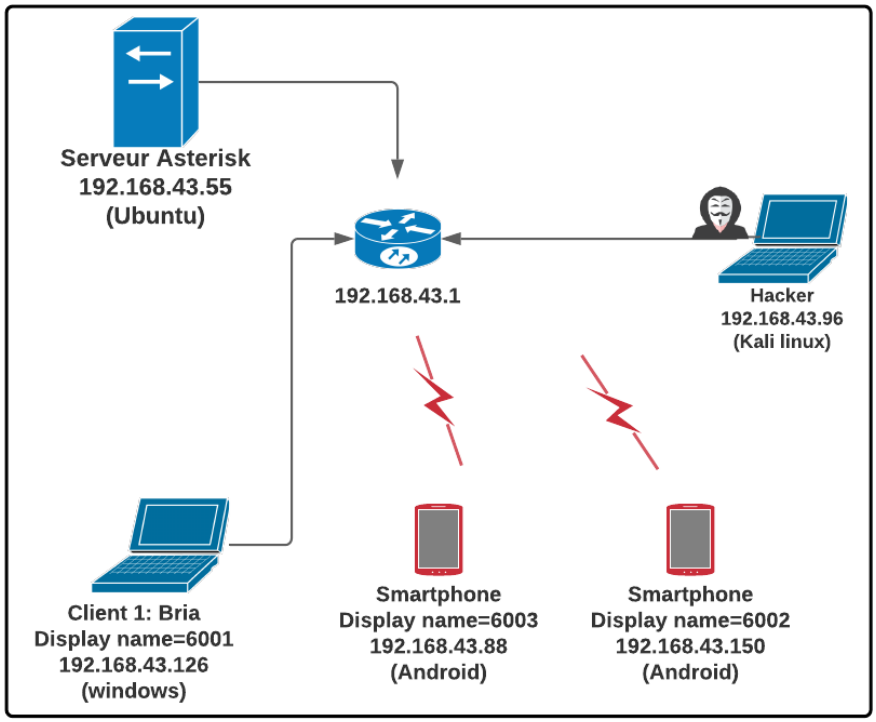


FIGURE 3.2 – Architecture du réseau d'étude

3.3 Les tâches réalisées

Au cours de l'implémentation de notre projet, nous avons eu à réaliser les tâches suivantes :

- Préparation de l'environnement de travail avec l'installation d'**Oracle VM VirtualBox**
- Installation, configuration et intégration du serveur **Asterisk sous Ubuntu 16.04**
- Installation et lancement des appels avec Softphone **MizuDroid** sous **Android** et **Bria** sous **Windows 10**
- Installation, lancement des attaques et analyse des paquets avec **Wireshark sous Kali Linux**
- Installation, configuration et détection des attaques avec Snort sous **Ubuntu 20.0**

  La **figure 3.1** présente l'environnement de travail avec les différentes machines installées

3.4 Installation et configuration du serveur Asterisk

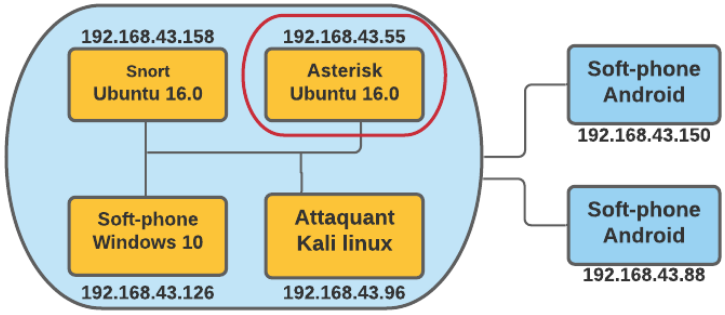


FIGURE 3.3 – Installation et configuration du serveur Asterisk dans l'environnement de travail

Le serveur Asterisk est un autocommutateur téléphonique privé (PABX) libre et propriétaire pour les systèmes GNU/Linux. Il permet la messagerie vocale ; les files d'attente ; les agents d'appels ; les musiques d'attente et les mises en garde d'appels ; la distribution des appels. Il est possible également d'ajouter l'utilisation des vidéo-conférences par le biais de l'installation de modules supplémentaires et la recompilation des binaires.[15]

Etapes d'installation

- apt-get update && apt-get upgrade
- apt-get install build-essential libxml2-dev libncurses5-dev linux-headers-'uname-r' libsqlite3-dev libssl-dev
- mkdir/usr/src/asterisk
- cd/usr/src/asterisk
- wget http ://downloads.asterisk.org/pub/telephony/asterisk/releases/asterisk10.7.0.tar.gz
- tar xvzf asterisk-13.33.0.tar.gz
- cd asterik-asterisk-13.33.0
- ./configure
- make
- make install
- make samples
- make config
- /etc/init.d/asterisk start

Après l'installation du serveur **Asterisk** il y a trois fichiers à configurer. Le fichier **sip.conf** pour changer de langue si l'on souhaite ; **users.conf** pour créer les comptes utilisateurs ainsi que leurs mots de passe et **extensions.conf** pour configurer le dialplan.

3.4.1 La mise en marche du serveur Asterisk

Pour démarrer notre serveur, on utilise la commande **/etc/init.d/asterisk start** et ensuite, la commande **Asterisk –r** permet la connexion au console CLI d'Asterisk.

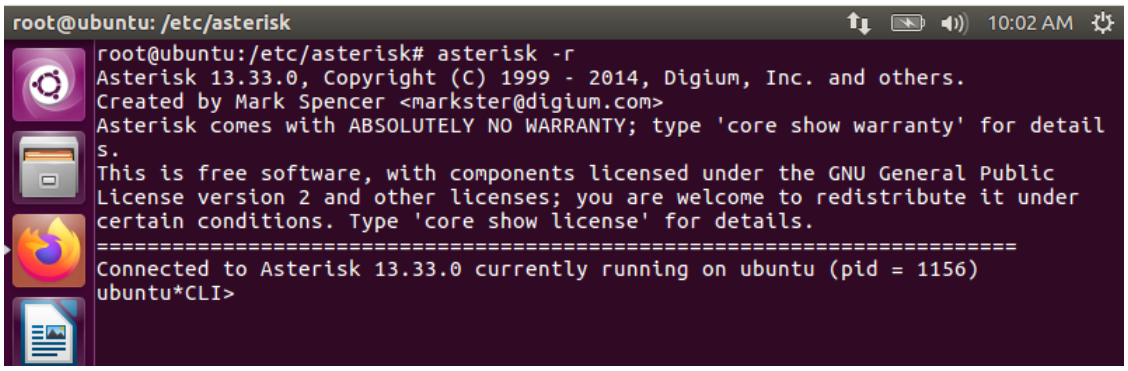


FIGURE 3.4 – Lancement du serveur Asterisk

3.4.2 Création des comptes et test d'appel

Pour la création des comptes des utilisateurs au niveau de notre serveur **Asterisk**, il faut modifier le fichier **/etc/asterisk/users.conf** ensuite on utilise la commande **sip show users** pour voir les comptes des utilisateurs. La commande **sip show peers** pour voir les utilisateurs connectés au serveur.

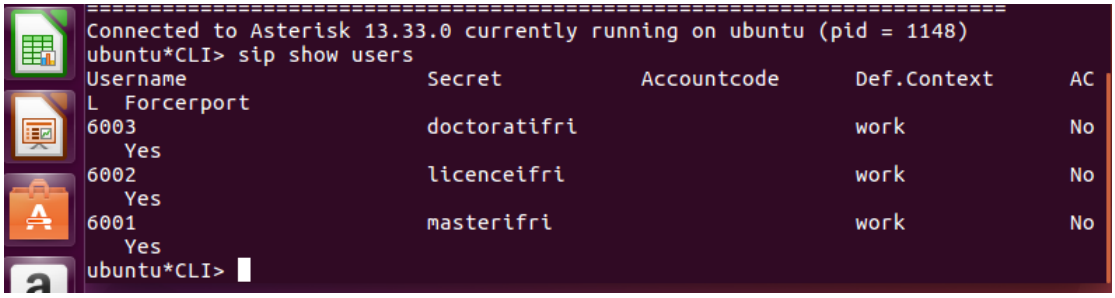


FIGURE 3.5 – Configuration des comptes utilisateurs

Sur la **figure 3.5** on voit les utilisateurs de notre serveur Asterisk avec leurs différents mots de passe.

3.4.2.1 Test d'un appel entre deux clients (via MizuDroid)

Pour effectuer un test d'appel sur le serveur, on télécharge des soft-phone (Un soft-phone est un type de logiciel utilisé pour faire de la téléphonie par Internet depuis un ordinateur plutôt qu'un téléphone[14]). Avant de passer des appels, on enregistre d'abord les informations des utilisateurs créées au niveau de notre serveur Asterisk dans le fichier **/etc/asterisk/users.conf**.
On va décrire le lancement des appels avec Softphones **MuziDroid** sous **Andoid**.

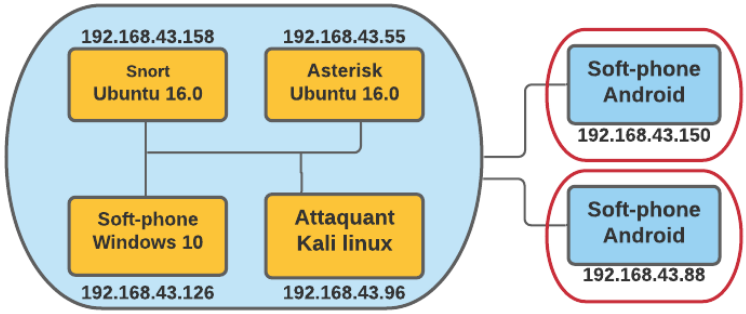


FIGURE 3.6 – Lancement d'appel

L'utilisateur ayant l'extension **6003** effectue un appel avec l'utilisateur qui a une extension **6002**, il suffit de composer le numéro de l'appelant, si la ligne est libre, une sonnerie se déclenche chez le récepteur avec l'affichage du numéro de l'appelé. Ci-dessous (**figure 3.7**) un test réussi d'un appel entre deux téléphones Android.

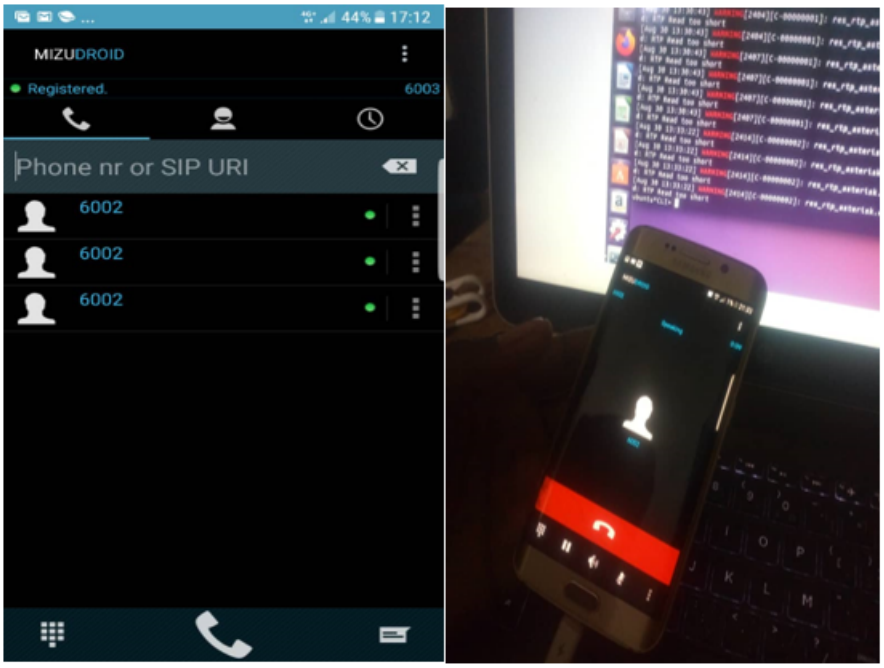


FIGURE 3.7 – Lancement d'appel

La figure suivante nous présente la réception d'appel par l'utilisateur **6002**.

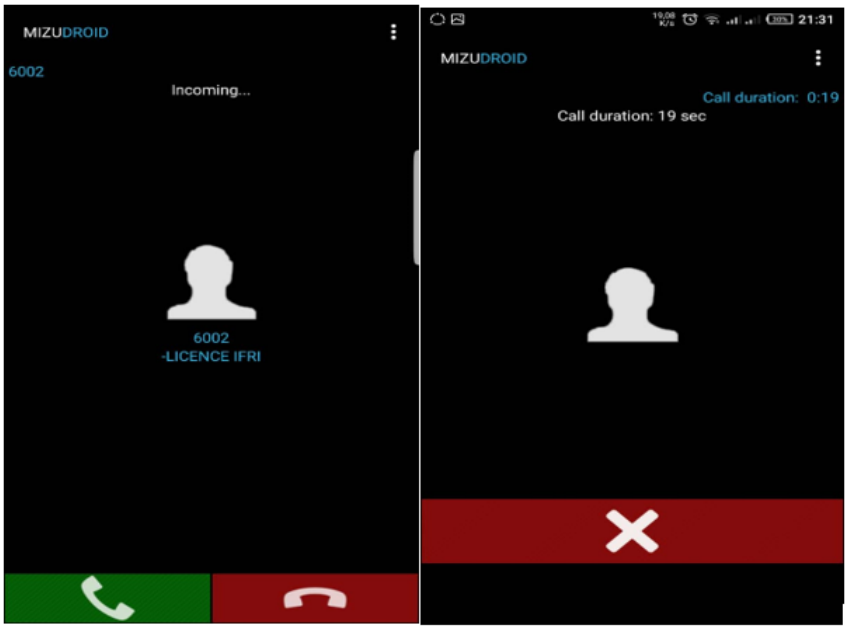


FIGURE 3.8 – Réception d'appel

3.5 Lancement des attaques et analyses des paquets sous Kali Linux

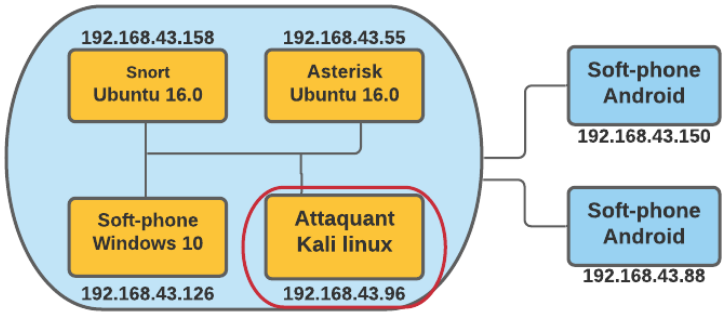


FIGURE 3.9 – Installation de Kali Linux dans l'environnement de travail

3.5.1 L'écoute clandestine avec Wireshark

Wireshark est un logiciel d'analyse réseau (sniffer) permettant de visualiser l'ensemble des données transitant sur la machine qui l'exécute et d'obtenir des informations sur les protocoles applicatifs utilisés. Les octets sont capturés en utilisant la librairie réseau PCAP puis regroupés en blocs d'informations et analysés par le logiciel.
Dans le cadre de notre projet, on a utilisé Wireshark sous la version 3.3.0 pour l'analyse des paquets et l'écoute des appels téléphonique via la voix sur IP.

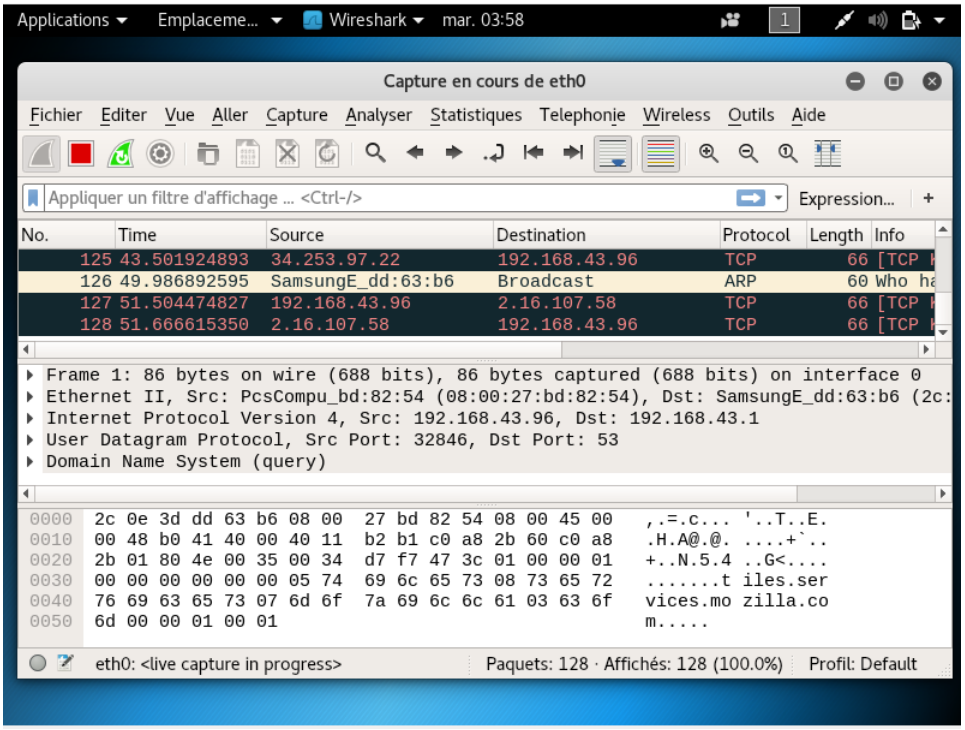


FIGURE 3.10 – Capture des paquets

La **figure 3.10** présente des exemples des paquets capturés par Wireshark à savoir les adresses IP, les numéros de ports, et d'autres informations.

3.5.2 Simulation SIP DoS

Pour lancer cette attaque, nous avons utilisé la commande **"svmap 192.168.43.1/24"** (adresse du réseau) afin de découvrir s'il y a un serveur **Asterisk** installé dans le réseau **192.168.43.1/24**. Sur **la figure 3.11** le résultat obtenu.

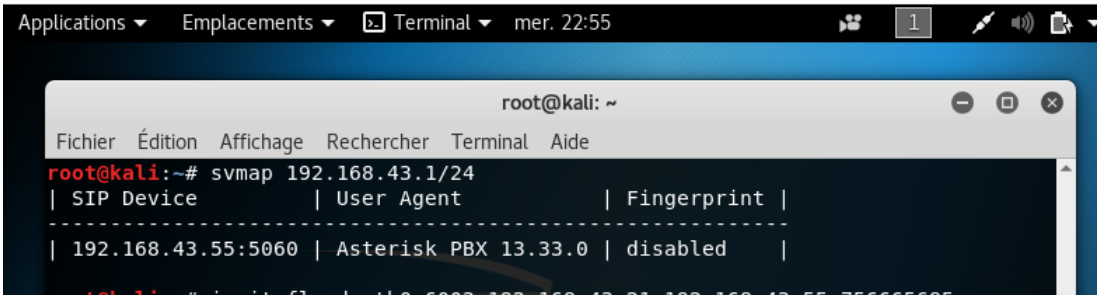


FIGURE 3.11 – Verification d'existance d'un serveur SIP

Nous avons un serveur **Asterisk PABX** sur la version *13.33.0*. On va ensuite attaquer notre serveur par une attaque **inviteflood** sur l'interface eth0 pour faire une simulation des appels à partir des numéro **6003** sur l'adresse de notre serveur qui est **192.168.43.55** et ensuite en va simulé des invites. Ici, nous avons simulé **756665685** invites. Nous avons choisi une adresse aléatoire **192.168.43.21** en utilisant la commande suivante :

"inviteflood eth0 6003 192.168.43.21 192.168.43.55 756665685"

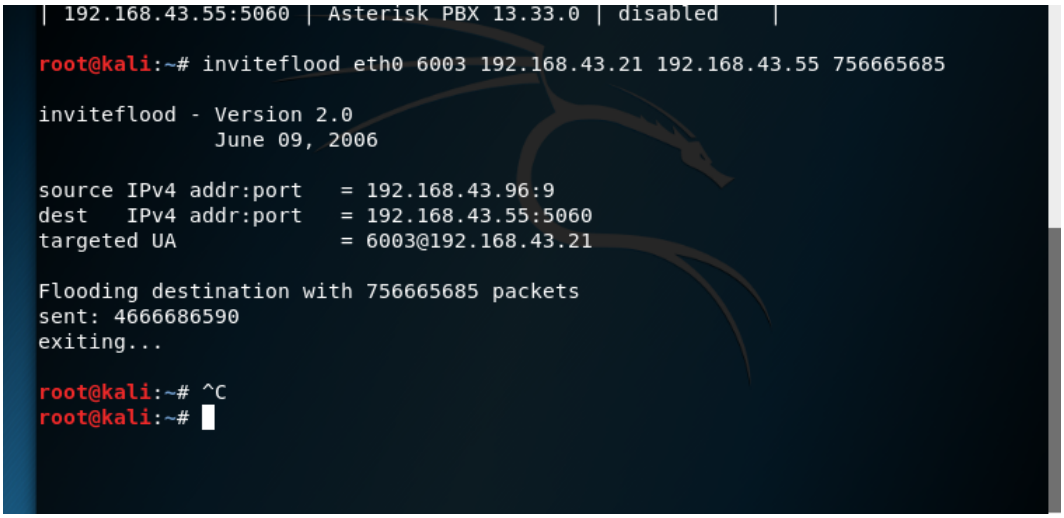


FIGURE 3.12 – Simulation d'attaque SIP DoS

Nous avons pu constater que, lorsque l'attaque est bien effectuée, le serveur Asterisk est complètement hors service, il est impossible d'obtenir une réponse provenant de celui-ci. Ensuite, nous avons refait les tests des appels avec les clients sip mais l'appel ne s'effectue pas car notre serveur est occupé par une attaque SIP DoS. Sur la **figure 3.13** nous voyons la réaction du serveur Asterisk lors de l'attaque.

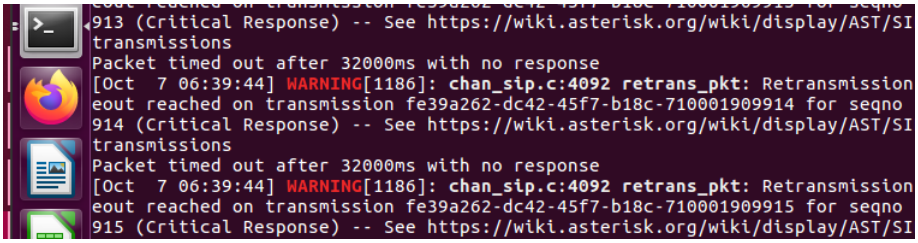


FIGURE 3.13 – Réaction du serveur Asterisk

3.5.3 Simulation d'attaque par SYN Flood

Le SYN flood est une attaque informatique visant à atteindre un déni de service. Elle s'applique dans le cadre du protocole TCP et consiste à envoyer une succession de requêtes SYN vers la cible.
Pour lancer cette attaque, nous avons utilisé la commande **"hping3 -S –flood 192.168.43.53"**(adresse IP du serveur Asterisk). Sur la figure3.14 le résultat obtenu.

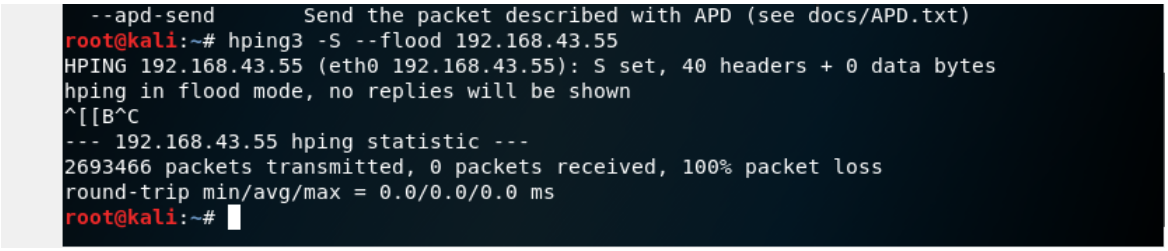


FIGURE 3.14 – Simulation d'attaque SYN Flood

3.6 Installation et configuration d'un IDS Snort

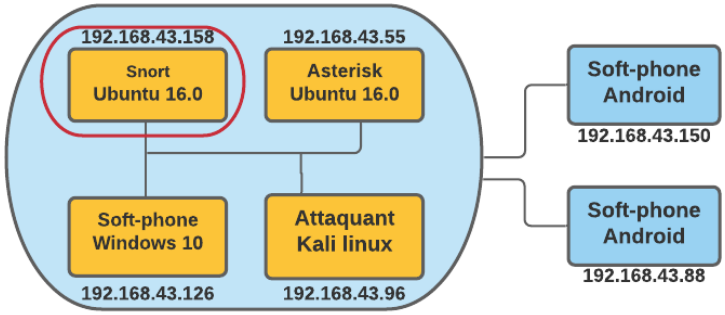


FIGURE 3.15 – Installation et configuration de Snort dans l'environnement du travail

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

3.6.1 Choix de Snort

Snort est un Système de detéction et prévention d'intrusion gratuit disponible dans sa version 3.0.0-270 (25 mars 2020) (www.snort.org). A l'origine, c'est un un sniffer utiliser dans le monde de la détection d'intrusion en s'appuyant sur une base de signature régulièrement enrichie par le "monde du libre". En se basant sur le système Snort , les auteurs implantent une unité de prétraitement logique des messages SIP composé par plusieurs modules : vérification et analyse de syntaxe, vérification des entêtes, et vérification de l'état à partir d'un ensemble de messages. Une évaluation de performance de ce prototype est réalisé à l'aide de générateur de trafic BRUTE. Le système est démontré pour détecter des classes différentes d'intrusion : l'usurpation d'identité ; déni de service ; les attaques des flux média et la fermeture prématurée des sessions.
Sous Linux (comme sous Windows) son installation est simple et se résume pour Linux. Ce dernier permet d'analyser le trafic réseau de type IP, il peut être configuré pour fonctionner en quatre modes :

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

3.6.2 Etape d'installation

Installation du paquet :
Sous Linux avec les commandes suivantes, une fois l'archive téléchargée dans le répertoire **"cd /etc/snort"** :

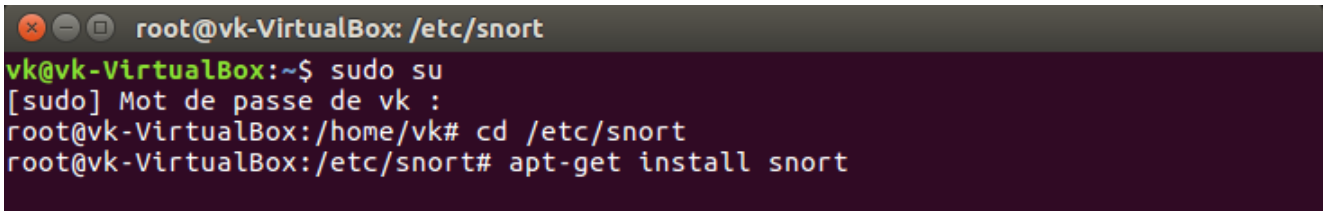


FIGURE 3.16 – Installation et configurasion de Snort

Une fois l'installation de Snort terminée, nous entrons la commande « dpkg-reconfigure snort » pour pouvoir procéder à la configuration de Snort.

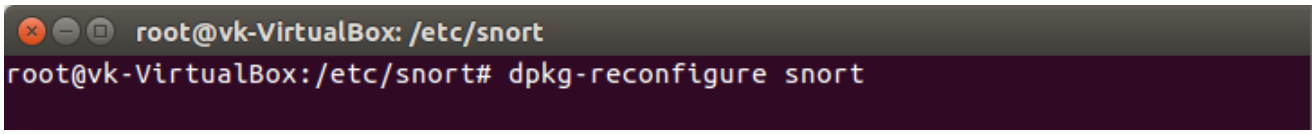


FIGURE 3.17 – Lancement de configuration de Snort

Choix du mode de lancement de Snort :

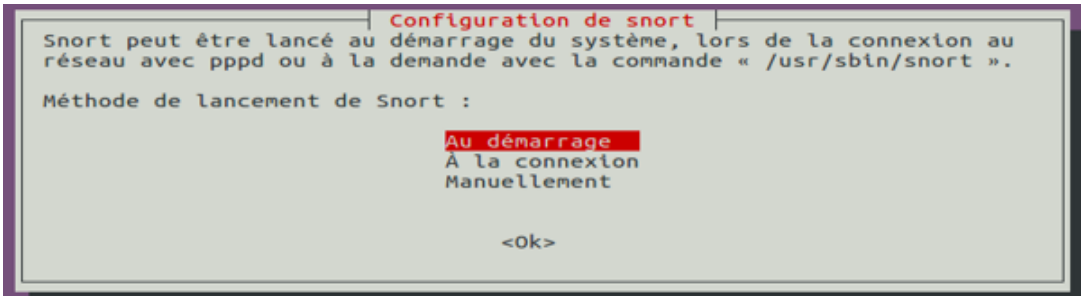


FIGURE 3.18 – Choix du mode de lancement de Snort

Dans cette même interface on peut aussi effectuer les configurations suivantes :

- Choix de l'interface d'écoute que Snort va utiliser pour analyser le trafic de notre réseau : dans notre cas c'est le **enp0s3**
- Indication de la plage d'adresse du réseau qui sera pris en compte par Snort : Dans notre cas, la plage est **192.168.43.0/24**
- L'activation ou non du mode promiscuité a pour conséquence respectivement de permettre à notre serveur Snort de pouvoir vérifier tous les paquets transitant au sein du réseau même ceux qui ne lui sont pas directement adressés
- La possibilité d'entrer des configurations personnelles supplémentaires
- L'activation de la fonctionnalité permettant à Snort de nous envoyer de manière quotidienne (tous les jours et à une heure fixe) des rapports de journaux d'évènements survenus sur le réseau à une adresse mail précise. Et par la suite, nous renseignons l'adresse mail où seront envoyés les rapports. Nous avons utilisé l'adresse suivante **oumarhisseinhassan75@gmail.com**
- Enfin, nous devons indiquer à Snort le nombre d'occurrences minimal d'un évènement donné (une alerte) pour que ce dernier soit comptabilisé dans les statistiques du rapport

Après la configuration de notre **Snort**, on redémarre le service Snort pour lui permettre de mettre à jour les nouveaux paramètres qui lui ont été indiqués.

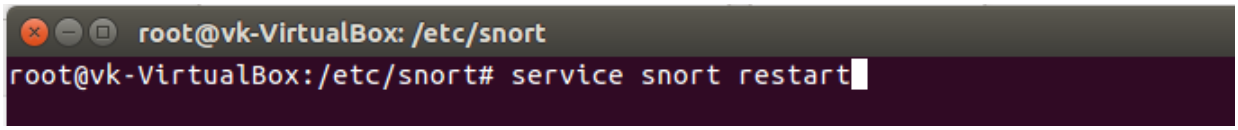


FIGURE 3.19 – Redémarage du service Snort

3.6.2.1 Définition des règles pour la détection

Les règles de Snort sont décrites dans un langage simple et suivent le schéma suivant :

L'entête de règle qui contient :

- l'action de la règle (la réaction de Snort) ;
- le protocole qui est utilisé pour la transmission des données (snort en considère trois : TCP, UDP et ICMP) ;
- les adresses IP source et destination et leur masque ;
- les ports source et destination sur lesquels il faudra vérifier les paquets.

Les options de la règle (entre parenthèse) comprennent :

- le message d'alerte ;
- les conditions qui déterminent l'envoi de l'alerte en fonction du paquet inspecté.

L'exemple de règle suivant est simple et permet de détecter les tentatives de login sous l'utilisateur root, pour le protocole ftp (port 21) :

alert tcp any any -> 192.168..0/24 21 (content : "USER root" ; nocase ; msg : "Tentative d'accès au FTP pour l'utilisateur root" ;)

Pour ajouter des régles il suffit d'utilIser la commande suivante :

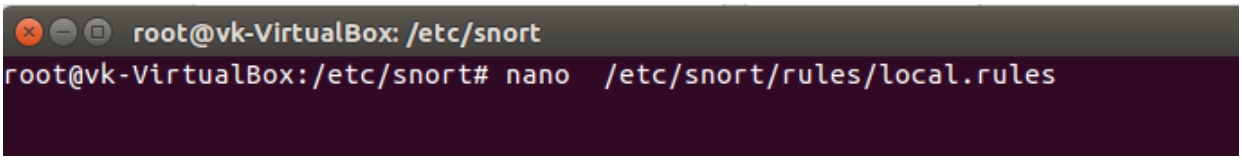


FIGURE 3.20 – Ouverture de fichiers d'ajout des régles de Snort

Dans notre cas, pour la création des règles, nous avons utilisé le fichier **local.rules** pour définir les règles

```
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# ----------------
# LOCAL RULES
# ----------------
# This file intentionally does not come with signatures.  Put your local
# additions here.
alert TCP $EXTERNAL_NET any -> 192.168.43.158/24 any (sid:1000001; msg:"Mon RSI OU$
alert UDP any any -> any any (sid:1000002; msg:"Mon RSI OUMAR un paquet UDP vient $
log TCP any any -> $EXTERNAL_NET any (sid:1000003; logto:"/etc/snort/log.log"; msg$
alert icmp any any -> $HOME_NET any (msg:"Tentative connexion ICMP"; sid:00001; re$
reject tcp any any <> any $HTTP_PORTS (msg:"Mon RSI Oumar je viens d'abandonné le $
```

FIGURE 3.21 – Fichier locale.rules

Ainsi, nous devons ajouter au niveau de la section « include » du fichier snort.conf la ligne suivante pour indiquer à Snort de prendre en considération les nouvelles règles.

```
include $RULE_PATH/community-web-dos.rules
include $RULE_PATH/community-web-iis.rules
include $RULE_PATH/community-web-misc.rules
include $RULE_PATH/community-web-php.rules
include $RULE_PATH/local.rules

##################################################
```

FIGURE 3.22 – Ajout au niveau de la section include

Lancement de la commande d'analyse de Snort en temps réel des différents paquets transitant dans le réseau et de spécifier le mode de sortie d'affichage des messages d'alertes, par exemple avec la commande suivante, on indique que les messages sont directement affichés sur le terminal.

```
root@vk-VirtualBox: /etc/snort
root@vk-VirtualBox:/etc/snort# snort -A console -c "/etc/snort/snort.conf" -i en
p0s3
```

Après validation de la commande, Snort est prêt à analyser les échanges au sein du réseau.

```
        --== Initialization Complete ==--

           -*> Snort! <*-
  ,,_      Version 2.9.7.0 GRE (Build 149)
 o"  )~    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
   ''''    Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.7.4
```

FIGURE 3.23 – Lancement de Snort

3.6.2.2 Test de fonctionnement de Snort

Il suffit de lancer la commande Ping sur l'adresse IP de la machine sur laquelle nous avons installé Snort. La **figure 3.23** montre la détection de la commande ping par Snort.

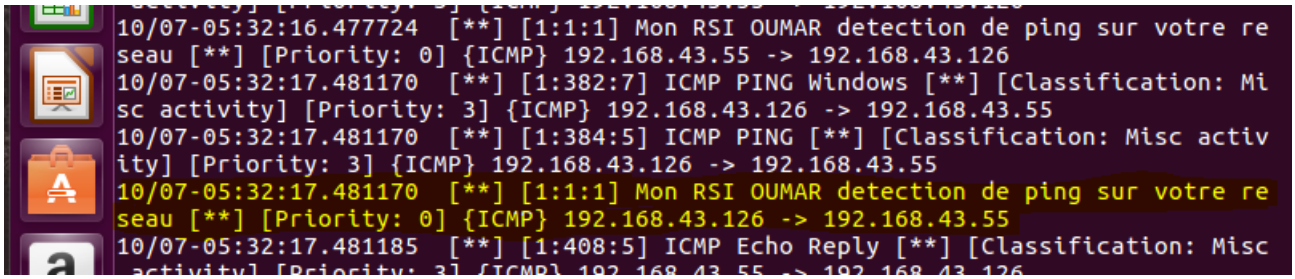


FIGURE 3.24 – Détection de ping

La **Figure 3.25** montre le résultat statistique d'analyse de Snort sur le réseau. Ici, nous avons **Received :263** donc 263 paquets reçus et analyser par Snort. On peut aussi voir les différents protocoles utiliser avec leurs statistiques.

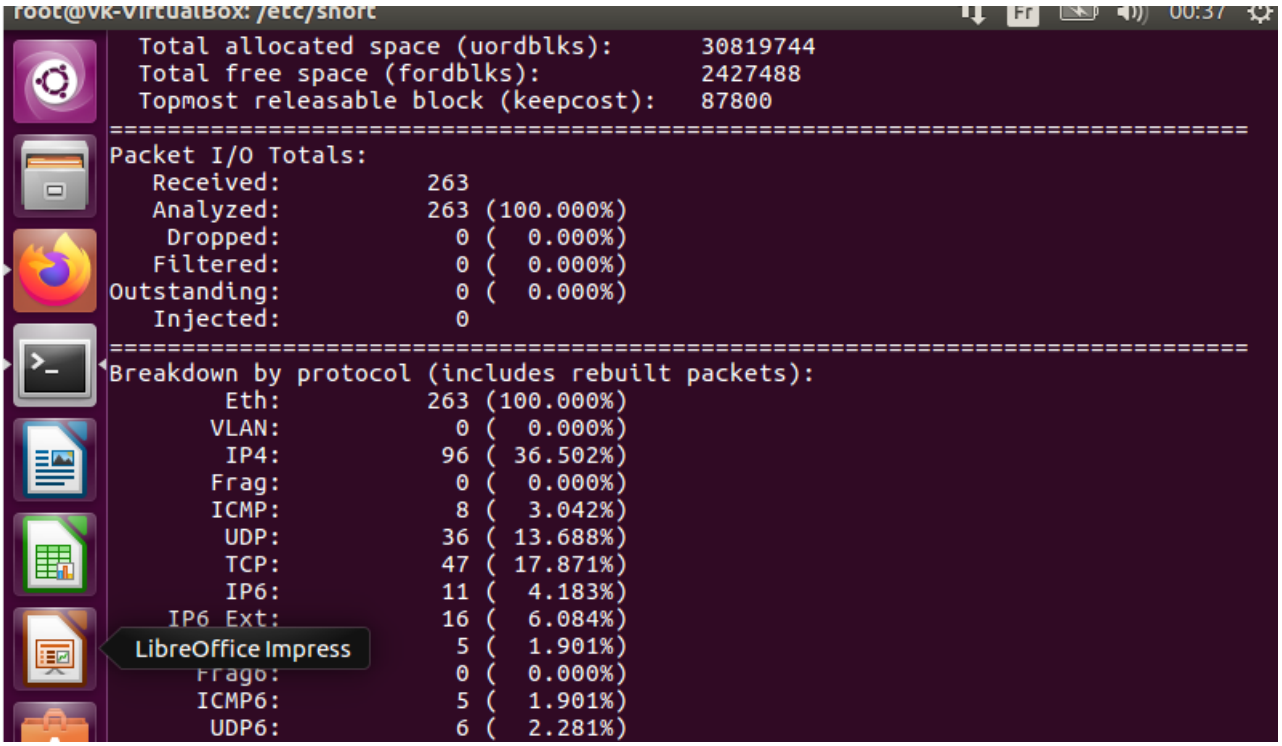


FIGURE 3.25 – Interface de supervision du réseau

3.6.3 Détection d'attaques par Snort

- Détection d'attaque SIP DoS

C'est une attaque DoS qui peut être directement dirigée contre les utilisateurs finaux ou les dispositifs tels que les téléphones IP, les routeurs et les proxys SIP, ou contre les serveurs concernés par le processus, en utilisant le mécanisme du protocole SIP ou d'autres techniques.

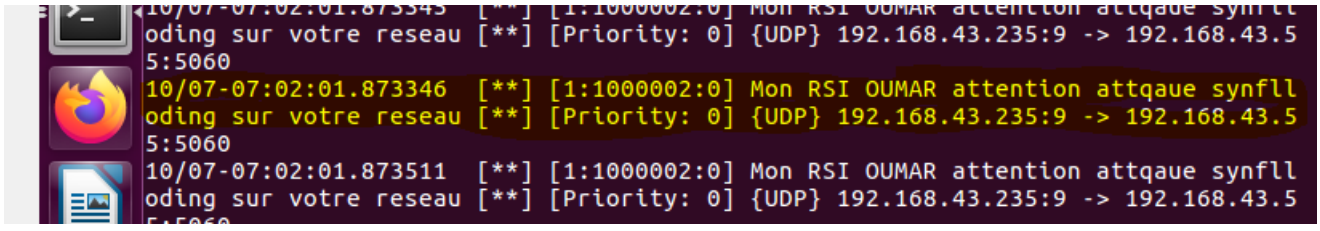


FIGURE 3.26 – Détection d'attaque SIP Dos

- Détection d'attaque SYN Flood

Pour la détection de cette attaque, nous avons créé notre propre règle de base dans le fichier **local.rules**. Notre règle permet à Snort de détecter tous les paquets de demande de connexion vers la cible. Dans notre cas, les critères de ces paquets sont :

  - Paquets de type TCP
  - Provenant de n'importe quelle source
  - À destination de la cible 192.168.43.55 et n'importe quelle port
  - Paquets vérifiés quelque soit l'état de la connexion (flow : stateless)
  - Paquets dont le flag SYN est positionné (flags : S)

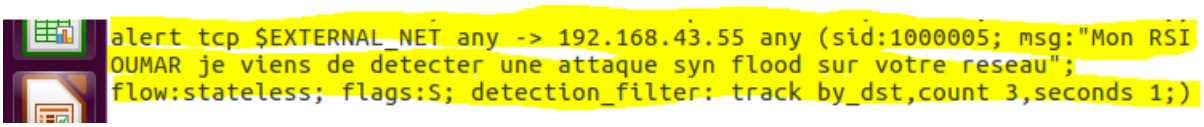


FIGURE 3.27 – Fichier local.rules

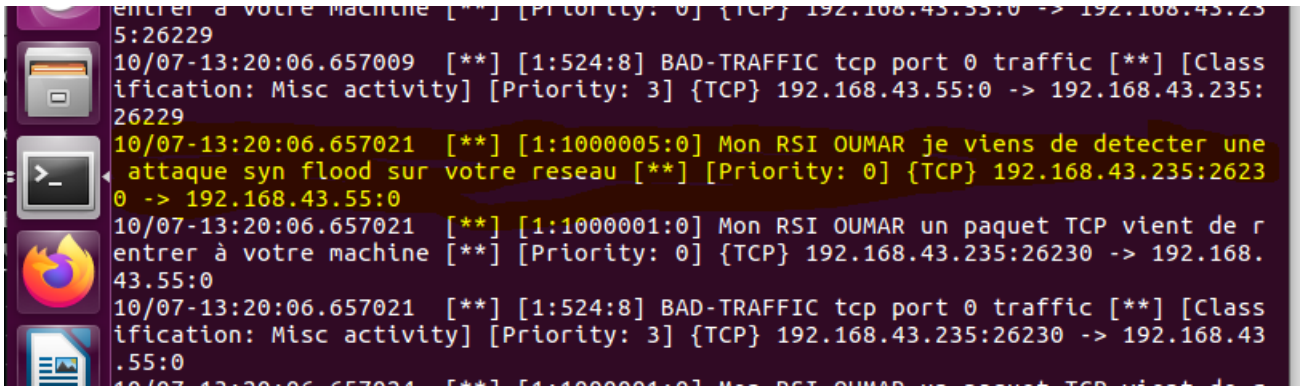


FIGURE 3.28 – Détection d'attaque SYN Flood

Conclusion

À travers ce chapitre, nous avons installé et configuré un système de détection d'intrusion (**Snort**) pour la sécurité de réseau VoIP. On a commencé par présenter l'environnement de travail, par la suite, nous avons énuméré l'ensemble des tâches réalisées en général et en détail.

Bibliographie

[1] P. cybersécurité. Communication avec voix sur ip (voip). 2015.

[2] DataNews. 7 menaces pour voip. 2019.

[3] J. DORDOIGNE. Voip. 2018.

[4] A. FRIJA. Etude et mise en place d'une solution voip securisee. 2018.

[5] C. informatiques. Description de la voip. 2018.

[6] Ipbx.pro. Standard téléphonique. 2020.

[7] SlideShare. Les sondes de sécurités ids_ips. 2017.

Webographie

[8] Consulté le 01 juin 2020 à l'adresse. https://blog.wildix.com/fr/comment-gerer-les-attaques-dos-dans-la-voip/.

[9] Consulté le 04 mai 2020 à l'adresse. http://www.chambet.com/publications/MISC%2016%20-%20Securite%20de%20la%20VoIP.pdf.

[10] Consulté le 10 août 2020 à l'adresse. https://fr.wikipedia.org/wiki/Session_Initiation_Protocol#:~:text=Session%20Initiation%20Protocol%20(SIP)%20est,par%20internet%20(la%20VoIP).

[11] Consulté le 16 juillet 2020 à l'adresse. https://www.idtexpress.com/fr/blog/voip-security-best-practice/.

[12] Consulté le 17 juillet 2020 à l'adresse. http://odile.papini.perso.luminy.univ-amu.fr/sources/SECURITE/cours-SSI-5.pdf.

[13] Consulté le 17 juillet 2020 à l'adresse. https://telium.io/fr/securite-pour-asterisk/.

[14] Consulté le 17 juillet 2020 à l'adresse. https://fr.wikipedia.org/wiki/Softphone#:~:text=Un%20softphone%20(anglicisme)%20est%20un,ordinateur%20plutôt%20qu%27un%20téléphone.

[15] Consulté le 19 juillet 2020 à l'adresse. https://fr.wikipedia.org/wiki/Asterisk_(logiciel).

[16] Consulté le 25 mai 2020 à l'adresse. https://bfmbusiness.bfmtv.com/01-business-forum/voix-sur-ip-les-5-menaces-qui-pesent-sur-votre-reseau-381864.html.

[17] Consulté le 28 juillet aout 2020 à l'adresse. https://fr.wikipedia.org/wiki/Système_de_détection_d%27intrusion.

[18] Consulté le 28 mai 2020 à l'adresse. http://www-igm.univ-mlv.fr/~dr/XPOSE2004/IDS/IDSPres.htmlhttp://www-igm.univ-mlv.fr/~dr/XPOSE2004/IDS/IDSPres.html.

[19] Consulté le 30 juillet 2020 à l'adresse. https://www.techniques-ingenieur.fr/base-documentaire/technologies-de-l-information-th9/reseaux-cellulaires-e

t-telephonie-42288210/protocole-sip-te7530/fonctionnement-d-un-syste
me-sip-te7530niv10003.html.

Table des matières

Remerciements ii

Table des figures iii

Liste des tableaux v

Liste des acronymes vi

Introduction 1

1 Etude générale sur la VoIP 3
Introduction . . . 3
1.1 Présentation de la VoIP . . . 3
1.1.1 Définition . . . 3
1.1.2 Architecture . . . 3
1.1.3 Le Processus du traitement de la voix IP . . . 5
1.2 Description générale du protocole SIP . . . 6
1.2.1 Informations sur le protocole SIP . . . 6
1.2.2 Capacités du protocole SIP . . . 6
1.2.3 Composants SIP . . . 6
1.2.4 Avantages et inconvénients SIP . . . 7
1.2.5 Les messages SIP . . . 8
1.2.5.1 Requêtes et réponses SIP . . . 8
1.2.6 Fonctionnement du protocole SIP . . . 9
1.3 Quelques attaques contre la VOIP . . . 10
1.3.1 Le déni de service . . . 10
1.3.2 La fraude téléphonique . . . 11
1.3.3 L'écoute . . . 11
1.3.4 L'accès au système d'information . . . 11
1.3.5 Vishing . . . 11
1.3.6 Spam via Internet Telephony (SPIT) . . . 11
1.3.7 Détournement de données d'enregistrement . . . 11
1.3.8 Directory harvesting . . . 12
1.4 Etat de politique de sécurité de la VoIP existente . . . 12
1.4.1 Sécurisation protocolaire . . . 12
1.4.1.1 VoIP VPN . . . 12
1.4.1.2 Secure RTP ou SRTP . . . 12
1.4.2 Sécurisation de l'application . . . 13

1.4.3 Sécurisation du système d'exploitation . . . 13
1.4.4 Pare-feu . . . 14

2 Les systèmes de détection d'intrusion 15
Introduction . . . 15
2.1 Systèmes de détection d'intrusion . . . 15
2.1.1 Choix du placement d'un IDS . . . 15
2.1.2 Classification des IDS . . . 16
2.1.2.1 Systèmes de détection d'intrusion réseaux . . . 16
2.1.2.2 Systèmes de détection d'intrusion hôtes . . . 17
2.1.2.3 Systèmes de détection d'intrusion collaboratif . . . 18
2.1.3 Méthodes de détection des IDS . . . 19
2.1.3.1 Systèmes de détection d'intrusion par signatures . . . 19
2.1.3.2 Systèmes de détection d'intrusion par anomalies . . . 20
2.1.3.3 Systèmes de détection d'intrusion Hybride . . . 20
2.1.3.4 Systèmes de détection d'intrusion par analyse des protocoles . . . 20
2.1.3.5 Systèmes de détection d'intrusion par temporalité de détection . . . 20
2.1.3.6 Systèmes de détection d'intrusion par corrélation des alertes . . . 21
2.1.4 Tableau comparatif des systèmes de détection d'intrusion . . . 21
2.2 Systèmes de prévention d'intrusion . . . 22
2.2.1 Classification des IPS . . . 22
2.2.2 Méthodes de détection des IPS . . . 22
2.3 Système de détection d'intrusion pour la VoIP . . . 23
Conclusion . . . 23

3 Implémentation de la solution 25
Introduction . . . 25
3.1 Environnement de travail . . . 25
3.2 Architecture du réseau d'étude . . . 26
3.3 Les tâches réalisées . . . 26
3.4 Installation et configuration du serveur Asterisk . . . 27
3.4.1 La mise en marche du serveur Asterisk . . . 28
3.4.2 Création des comptes et test d'appel . . . 28
3.4.2.1 Test d'un appel entre deux clients (via MizuDroid) . . . 28
3.5 Lancement des attaques et analyses des paquets sous Kali Linux . . . 30
3.5.1 L'écoute clandestine avec Wireshark . . . 30
3.5.2 Simulation SIP DoS . . . 31
3.5.3 Simulation d'attaque par SYN Flood . . . 32
3.6 Installation et configuration d'un IDS Snort . . . 33
3.6.1 Choix de Snort . . . 33
3.6.2 Etape d'installation . . . 33
3.6.2.1 Définition des règles pour la détection . . . 35
3.6.2.2 Test de fonctionnement de Snort . . . 36
3.6.3 Détection d'attaques par Snort . . . 37
Conclusion . . . 38

Bibliographie 39

Webographie 40

Table des matières 42