République Algèrienne Démocratique et Populaire
Ministère de L'Enseignement Supérieur et de la Recherche Scientifique
Université A/Mira de Béjaia
Faculté des Sciences Exactes
Département Informatique

Mémoire de fin de cycle

En vue de l'obtention du Diplome de Master Recherche

Option :

Réseaux et Systèmes Distribués

Thème :

Etude de sécurité d'une extension Cloud

réalisé par :

Mr BENKOUIDER SAHRAOUI Soufyane
Mlle MANSOURI Yasmine

Soutenu devant le jury composé de :

Président :	Mr	BOUDRAHEM Nassim	U.A/ Mira Béjaia.
Examinateur :	Mr	OMAR Mawloud	U.A/ Mira Béjaia.
Examinatrice :	Mme	OUYAHIYA Souraya	U.A/ Mira Béjaia.
Encadreur :	Mr	TOUAZI Djoudi	U.A/ Mira Béjaia.

Juin 2017.

TABLE DES MATIÈRES

LISTE DES TABLEAUX

TABLE DES FIGURES

INTRODUCTION GÉNÉRALE

Problème et objectif : L'ordinateur est devenu un élément central de notre vie. Que l'on soit jeune ou âgé, travailleur ou chômeur, on a souvent recours à internet, qui, au fil des années est devenu incontournable.

Certains utilisent leurs ordinateurs comme espace de stockage pour leurs données personnelles et/ou professionnelles. D'autres ayant besoin de plus d'espace ou pour partager leurs données utilisent des supports de stockage externe : disque dur ; clef USB ; ou, via internet, des supports de stockage externalisés proposés par des fournisseurs, que l'on désigne par le terme Cloud.

Avec l'adoption croissante des dispositifs IoT et l'intégration de nombreuses applications intelligentes et afin d'éviter la surcharge des dispositifs Cloud, une nouvelle technologie fait son apparition nommé FOG COMPUTING, en utilisant cette dernière le traitement et les applications sont concentrés dans les dispositifs à la périphérie du réseau plutôt qu'entièrement dans le Cloud, comme nous le savant tous aucune nouvelle technologique n'est parfaitement sécurisée et n'est a l'abri du piratage informatique.

Dans ce projet nous allons définir le ClOUD ses types ainsi que ses avantages et inconvénients, on passera ensuite au FOG COMPUTING afin de pouvoir étudier son fonctionnement et le comparer a celui du CLOUD, pour finir avec un test d'intrusion qui visera une architecture FOG.

CHAPITRE 1

CLOUD COMPUTING

1.1 Introduction

La technologie de l'Internet se développe de manière exponentielle depuis sa création. Actuellement, une nouvelle tendance a fait son apparition dans le monde des IT (Technologies de l'information et de la communication), il s'agit du Cloud computing. Cette technologie, s'appuyant sur le WEB 2.0, offre des occasions aux sociétés de réduire les couts d'exploitation des logiciels par leurs utilisations directement enligne [3].

Dans ce premier chapitre nous allons donner des idées générales sur le fonctionnement et les fonctionnalités du Cloud computing.

1.2 Définition

Le Cloud computing (L'informatique en nuage en Français) fournit des services ou des applications informatiques en ligne, accessibles partout, à tout moment, et de n'importe quel terminal (Smartphone, PC, tablette). Pour étre plus précis, le Cloud computing permet de partager, chez un fournisseur d'offres Cloud, une infrastructure, une solution applicative ou encore une plateforme à tout utilisateur qui en fait la demande via un simple site internet (appelé aussi portail) en libre-service [2].

1.3 Historique

Bien avant la naissance du terme de Cloud computing, les informaticiens utiilisaient déjà des services de Cloud computing comme le webmail2, le stockage de données en ligne ou encore le partage d'informations sur les réseaux sociaux. Dans les années 90, un

autre concept avait déjà préparé le terrain au Cloud computing. Il s'agit de l'ASP qui permettait au client de louer l'accés à un logiciel installé sur les serveurs distants d'un prestataire, sans installer le logiciel sur sa propre machine. Le Cloud computing ajoute à cette offre la notion d'élasticité avec la possibilité d'ajouter de nouvel utilisateurs et de nouveaux services d'un simple clic de souris.

Le Cloud computing est enfin apparu avec les différents progrés technologiques réalisés durant ces 50 dernières années, tant que sur le plan matériel, logiciel et conceptuel, qu'aux avancées des mécanismes de sécurité et l'élaboration de réseaux standardisés comme l'internet, et l'expèrience dans l'édition et la gestion de logiciels, services, infrastructures et stockage des données [1].

1.4 Services du Cloud computing

Trois grands modèles d'usage du Cloud se dégagent actuellement, tous présentent des caractéristiques différentes et n'ont pas le même niveau de maturité : [4] :

1.4.1 SaaS (Software as a Service)

Dans ce type de service, des applications sont mises à la disposition des consommateurs. Les applications peuvent être manipulées à l'aide d'un navigateur web, et le consommateur n'a pas à se soucier d'effectuer des mises à jour, d'ajouter des patches de sécurité et d'assurer la disponibilité du service. Gmail est un exemple de tel service. Il offre aux consommateurs un service de courrier électronique et le consommateur n'a pas à se soucier de la manière dont le service est fourni. D'autres exemples de logiciels mis à disposition en SaaS sont Google Apps, Office Web Apps, Adobe Creaitve Cloud ou LotusLive (IBM).

En effet un fournisseur de software as a service peut exploiter des services de type plateforme as a service, qui peut lui-même se servir de infrastructure as a service. D'autres services également disponibles sont :

-Le Data as a Service correspond à la mise à disposition de données délocalisées quelque part sur le réseau. Ces données sont principalement consommées par ce que l'on appelle des mashups.

-BPaaS : il s'agit du concept de Business Process as a service (BPaaS) qui consiste à externaliser une procédure d'entreprise suffisamment industrialisée pour s'adresser directement aux managers d'une organisation, sans nécessiter l'aide de professionnels de l'informatique

-Desktop as a Service : le Desktop as a Service (DaaS ; aussi appelé en français " bureau en tant que service ", " bureau virtuel " ou " bureau virtuel hébergé ") est l'externalisation d'une Virtual Desktop Infrastructure auprès d'un fournisseur de services. Généralement, le Desktop as a Service est proposé avec un abonnement payant.

-Network as a Service (NaaS) : le Network as a Service correspond à la fourniture de services réseaux, suivant le concept de Software Defined Networking (SDN).

-Software Defined Networking : c'est un modèle d'architecture réseau qui permet aux administrateurs de réseaux de gérer les services de réseaux par Abstraction de fonctionnalités.

1.4.2 PaaS (Platform as a Service)

En français plate-forme en tant que service. Dans ce type de service, situé juste au-dessus du précédent, le système d'exploitation et les outils d'infrastructure sont sous la responsabilité du fournisseur. Le consommateur a le contrôle des applications et peut ajouter ses propres outils. La situation est analogue à celle de l'hébergement web où le consommateur loue l'exploitation de serveurs sur lesquels les outils nécessaires sont préalablement placés et contrôlés par le fournisseur. La différence étant que les systèmes sont mutualisés et offrent une grande élasticité - capacité de s'adapter automatiquement à la demande, alors que dans une offre classique d'hébergement web l'adaptation fait suite à une demande formelle du consommateur.

1.4.3 IaaS (Infrastructure as a Service)

L'infrastructure en tant que service : c'est le service de plus bas niveau. Il consiste à offrir un accès à un parc informatique virtualisé. Des machines virtuelles sur lesquelles le consommateur peut installer un système d'exploitation et des applications. Le consommateur est ainsi dispensé de l'achat de matériel informatique. Ce service s'apparente aux services d'hébergement classiques des centres de traitement de données, et la tendance est en faveur de services de plus haut niveau, qui fait d'avantage abstraction de détails Techniques. .

Les services du Cloud computing offrent plusieurs avantages aux clients en économisant du temps et de l'argent, néanmoins des inconvénients sont soulevés qui limite leurs utilisations par les clients. Les avantages et les inconvénients des services du Cloud sont présentés dans le tableau suivant :

Types	Avantages	Inconvénients
SaaS	Pas d'installation	Dépendances des prestataire
PaaS	Environnement hétérogène	Pas de personnalisation de la machine virtuelle
IaaS	Flexibilité d'utilisation	Besoin d'un administrateur systèmes

TABLE 1.1 – Avantages et inconvénients des services du Cloud [4]

1.5 Différentes solutions Cloud

1.5.1 Le Cloud Privé

Le Cloud Privé est un mode de consommation de l'informatique (IaaS, PaaS, SaaS, ...) s'appuyant sur des ressources (serveur, stockage, réseau, licences logicielles...) mises à disposition exclusive d'une entreprise. Les ressources peuvent être géographiquement situées dans le périmètre de l'entreprise (on parlera d'un Cloud privé interne) ou chez un intégrateur/service provider (on parlera d'un Cloud privé managé ou hosté). L'exploitation du Cloud privé peut être réalisée uniquement par les équipes informatiques du client (Cloud privé interne), ou par un prestataire externe (Cloud privé interne, Cloud privé hosté). Les services disponibles le sont via un catalogue de services exposés dans un portail, leur mise en service est automatisés, et peut faire l'objet d'une facturation liée à la consommation.

1.5.2 le Cloud public

Le Cloud public est une structure souple et ouverte, géré par un fournisseur tiers. Plusieurs utilisateurs (individuels ou entreprises) peuvent y accéder via Internet. Avec le Cloud public, de multiples entités se partagent les mêmes ressources informatiques (mises à disposition par le fournisseur).

1.5.3 le Cloud hybride

Le Cloud hybride est une structure mixte qui permet de combiner les ressources internes du Cloud privé à celles externes du Cloud public. Une entreprise qui utilise un Cloud hybride peut par exemple avoir recours au Cloud public ponctuellement, lors de pics d'activité et le reste du temps se contenter des ressources à disposition en interne.

1.5.4 Les solutions open source du Cloud Computing

Le magazine JDN l'économie de demain dans sa parution du 12/06/2013 avait signifié que : " le Cloud n'est pas la chasse gardée des solutions propriétaires ".En effet plusieurs

solutions de Cloud Computing open source ont émergées dans le domaine du Cloud ; Dans cet article six de ces solutions d'open Cloud vous serons décrites.

1.5.4.1 Eucalyptus

Issue d'un projet de recherche de l'université de Californie, cette plate-forme Cloud open source est intégrée dans Ubuntu Server et Debian. Ecrite en C, Java et Python, elle permet de créer des Cloud Iaas (Infrastructure as a service) de type privé ou hybride, supporte des machines virtuelles Linux ainsi que les hyperviseurs Xen et

KVM. Par ailleurs, elle est compatible avec EC2 d'Amazon, S3, EBS IAM Auto Scaling

Elastic Load Balancing et CloudWatch. Il existe également une version propriétaire commercialisée par la société Eucalyptus Systems. Il apporte des fonctionnalités supplémentaires comme le support de VMware, celui des machines virtuelles

Windows et l'intégration SAN. Les avantages de ce logiciel open source pour le Cloud privé sont notamment une évolutivité très efficace, une organisation agile.

1.5.4.2 OpenNebula

Cette plateforme purement open source permet de déployer des Cloud privés, hybrides et publics. Ecrite en C++, Ruby et Shell, elle supporte les hyperviseurs Xen, KVM et VMware. Comme Eucalyptus, elle permet de s'interfacer avec le cloud d'Amazon, EC2. Le projet est publié sous licence Apache 2.0. Par ailleurs, OpenNebula est soutenu par le projet européen Reservoir, qui propose une architecture complète pour la gestion de datacenters et la création de services cloud

1.5.4.3 OpenStack

Créé en juillet 2010 par la Nasa et l'hébergeur américain Rackspace, ce projet purement open source .Le projet vise à fournir des solutions pour tous les types de nuages en étant simple à mettre en œuvre, hautement évolutive et riche en fonctionnalités. OpenStack est un système d'exploitation nuage qui contrôle de grandes surfaces de calcul, de stockage et les ressources réseau à travers un centre de données, le tout géré par un tableau de bord.

1.5.4.4 Niftyname

Ce projet d'origine française, la plate-forme Niftyname a été créée par l'hébergeur Ielo. Elle est diffusée sous licence GPLv3. Articulée autour d'un système de gestion écrit en Python, elle supporte l'hyperviseur KVM et permet de créer des machines virtuelles. Windows, Linux, BSD et Solaris. Elle sait également gérer les fonctionnalités de stockage et de réseaux associés à ces machines.

1.5.4.5 Stratuslab

Le projet StratusLab est née d'une collaboration académique informelle en 2008, co-financé par la Commission Européenne afin d'elaborer une plateforme open source sur infrastucture as a services.

Maintenant StratusLab est une collaboration ouverte des instituts (CNRSSixSQ, GRNET, et TCD) et les personnes continuent à évaluer le logiciel.

StratusLab fournit des fonctionnalités pour la gestion dynamique des ressources typiques de calcul d'un nuage IaaS. Mais il fournit également des fonctionnalités supplémentaires pour simplifier la gestion de l'image et la fédération du nuage.

1.6 Inconvénients du Cloud Computing

o La connexion internet

Le cloud utilisant de manière intensive le transfert de données, il faut avoir une connexion très performante. Plusieurs cas peuvent faire que le Cloud sera inadapté à votre entreprise :
- Si elle se situe dans un lieu éloigné
- Si la connexion ne dispose pas d'un débit garanti, une coupure peut survenir, privant l'entreprise de tous les accès au Cloud, et donc à toutes vos applications et données.

o Le coût du Cloud

Beaucoup d'entreprises ne regardent que les frais de stockage, mais il faut également prendre en compte les frais de transferts, qui peuvent s'avérer être importants, selon l'utilisation que l'entreprise faite du Cloud.

o L'optimisation des applications

Malgré une connexion internet rapide, avec un débit garanti, certaines applications web peuvent s'avérer être très lentes. Elles peuvent s'avérer être plus limitées que des applications fonctionnant sur les propres ordinateurs de l'entreprise.

o La sécurité du Cloud

Plusieurs points sont à étudier :
- La sécurité vis-à-vis du stockage : si les données sont conservées dans un seul disque, ou si elles sont entre plusieurs unités de stockage. - La sécurité et la confidentialité des données : si le fournisseur de service assure des tests portant sur sa sécurité informatique et si de tes tests sont faits de façon régulières.

- La sécurité des locaux : sont-ils inaccessibles pour des personnes malintentionnées ?

o Le piratage

Certaines applications comme Facebook et Twitter sont très sujets aux attaques. Le piratage d'un compte d'entreprise pourrait avoir des conséquences néfastes pour la réputation de l'entreprise, tandis que l'utilisation imprudente des applications par un salarié pourrait offrir aux cybercriminels l'opportunité d'entrer dans le réseau et de soustraire des données des clients.

o La pérennité du service

Il est nécessaire de se demander si l'hébergeur Cloud va durer dans le temps. Cet élément est important à prendre en compte car un changement d'hébergeur peut prendre du temps, et peut nécessiter un recodage des applications.

o La productivité des salariés

Il est nécessaire que les employés de l'entreprise sachent se servir du Cloud. En effet, même si l'entreprise fait des économies sur le stockage et le traitement d'informations, si les employés passent plus de temps pour leurs taches à cause du Cloud l'entreprise risque d'y perdre plus que d'y gagner.

o La plateforme

Il faut vérifier que l'hébergeur est capable de supporter de multiples plateformes car si ce n'est pas l'entreprise devra gérer plusieurs Clouds ce qui peut s'avérer vite très complexe.

o Les conditions de service

Il faut vérifier que les conditions de services sont conformes aux exigences de l'entreprise exigences. Vu que ces contrats sont très détaillés, mieux faut lire tout en détail avant de prendre une décision.

Le cloud computing n'est une mauvaise chose, bien au contraire, mais il est nécessaire avant de le mettre en place de peser le pour et le contre. En effet, certaines PME, de par leur activité, leur localisation, mais également par leurs applications utilisées, pourraient y percevoir plus de désavantages que de bénéfices.

1.7 Enjeux et perspectives

1.7.1 Enjeux et perspectives

Le premier avantage fournit par le Cloud Computing est l'automatisation de la maintenance des applications. Pas besoin d'acheter les nouvelles versions logicielles et de l'installer sur tous les PC de l'entreprise : tout se fait automatiquement par le fournisseur de l'application. Tous les utilisateurs bénéficient ensuite des nouveautés instantanément. Ainsi, on élimine les problèmes de compatibilité de fichiers, de versions obsolètes de logiciels. Cela permet d'être toujours en possession de la dernière version de l'application. Le Cloud a également un intérêt très important pour les travailleurs nomades voulant avoir accès aux fichiers de l'entreprise pendant leurs déplacements, et ceci à partir de n'importe quel appareil relié à internet. L'inconvénient est que bien sûr, sans connexion internet, toutes les données sont inaccessibles. En outre, le Cloud permet d'améliorer la sécurité des données : fini la perte de clé USB ou de PC contenant des informations confidentielles. Tout est centralisé et sécurisé par authentification de l'utilisateur. Ce partage des fichiers permet enfin de mieux diffuser l'information et d'encourager le travail collaboratif grâce par exemple à l'utilisation de wikis. Pour une installation informatique classique, les frais sont multiples : achat de logiciels, de serveurs, équipe informatique. Dans le cadre du Cloud Computing, il suffit de payer l'abonnement et les services désirés. Les ingénieurs informaticiens peuvent se dégager de certaines tâches comme l'entretien des serveurs, savoir si les serveurs pourront répondre aux pics d'activité, et ainsi se concentrer sur des tâches à plus forte valeur ajoutée.

L'entreprise profite également de l'expertise des fournisseurs de Cloud qui proposent des services adaptés. Certaines entreprises proposent des audits aux entreprises pour savoir s'il serait judicieux de basculer sur le Cloud. Néanmoins, il faut être vigilant lors de la signature du contrat et bien avoir réfléchi aux besoins de l'entreprise car la tarification des services proposés dans le Cloud est difficile à décrypter. La tarification peut se faire à la CPU 2, à la bande-passante, aux capacités de stockage, aux transactions. Il y a également des différences de tarifs en fonction de la zone géographique, des clauses minimales de durée de contrat.

1.7.2 Ce que change le Cloud Computing pour les revendeurs d'IT [12]

Le Cloud Computing est générateur d'un certain nombre de nouveautés pour les revendeurs de solutions relatives à l'IT :

Nouvelles compétences à acquérir : Le revendeur IT doit développer de nouvelles compétences autres que des compétences purement informatiques, notamment dans les domaines de la gestion des contrats, des audits des garanties de SLA4, de mise en place de plan de reprise d'activités.

Nouvelles missions : Le partenaire Cloud peut (et doit à terme) jouer le rôle de conseil technologique (web agency, experts verticaux) afin d'aider les PME à profiter efficacement et durablement des avantages liés aux Cloud et au SaaS.

Nouveaux services : Le Cloud est bien évidemment aussi générateur de nouveaux services (dématérialisation, archivage, sécurité, solutions de gestion...) dont beaucoup sont encore à inventer. De plus, les partenaires Cloud ont en effet tout intérêt à compléter leurs offres logicielles par toute une panoplie de " nouveaux " services : facilité d'accès, disponibilité, évolutivité, fonctions en self-service, souplesse et réactivité face aux montées et descentes en charge de l'utilisateur. Pour délivrer ces services, les fournisseurs de Cloud pourront s'appuyer sur des acteurs de BPO (Business Process Outsourcing). Ces derniers auront en charge certains processus métier de l'entreprise (exemple : achats, comptabilité, finance, gestion de la relation client ou en s'appuyant sur les solutions SaaS de l'éditeur). Le Cloud permet une démocratisation de l'accès à ces services qui jusqu'à présent étaient plutôt réservé aux seules grandes entreprises. Ces opportunités de nouveaux marchés se concrétisent par un accès facile et rapide à l'International, à des départements de grands comptes, à des petites entreprises traditionnellement inaccessibles (TPE, PME...).

Nouveaux modes de tarification : En mutualisant leurs offres, les fournisseurs de solution Cloud peuvent proposer des prix plus compétitifs, une tarification plus facilement adaptable et donc plus attractive pour de nouveaux clients.

Nouveaux modèles économiques : Le principe d'une tarification à l'abonnement (mode locatif) est pour l'éditeur synonyme de revenus récurrents. Le partenaire Cloud est ainsi en mesure de planifier des revenus récurrents prévisibles.

1.7.3 Enjeux de sécurité

Les entreprises ont souvent un a priori négatif sur la sécurité des infrastructures Cloud. Il est vrai que de multiples affaires de violations de données ou de pannes de Datacenter ternissent la réputation des fournisseurs de Cloud. On peut citer l'incident survenu en 2009 au service Ovi de Nokia qui, à la suite d'une panne de son système de refroidissement, avait perdu la totalité de ses données sans moyen de récupération, ou bien la panne des

serveurs d'Amazon ayant entrainé l'indisponibilité de sites web à fort trafic tels que Four square ou Quora. A l'heure actuelle, les entreprises, surtout les plus grandes, pour toutes ces raisons qui créent une zone d'ombre autour de la sécurité du Cloud public, préfèrent utiliser un Cloud privé interne à leur entreprise, plus rassurant. De plus, ce sont surtout les PME non spécialistes du secteur qui pourraient être intéressées par un passage sur le nuage, leurs données étant souvent stockées sur des serveurs peu adaptés et mal protégés, et qui ont tout intérêt à confier leurs systèmes IT à des fournisseurs de Cloud pouvant déployer des moyens de protection à grande échelle. Les problèmes de sécurité sont ainsi plus souvent imputables aux entreprises clientes qui se protègent mal et non pas aux hébergeurs qui sont des spécialistes et possèdent des moyens de défense efficaces (équipe informatique dédiée à la sécurité, moyens de cryptage, charte de qualité, etc.).

1.8 Conclusion

Le cloud représente une évolution pour certains, une révolution pour d'autres. Si la sémantique diverge, le constat est formel : le cloud computing transforme la façon d'utiliser l'outil informatique.

A la base, il y a toujours et même de plus en plus de gros serveurs installés dans des data center, qui vont abriter des logiciels puis stocker et diffuser des données, ce qui rend cette technologie indispensable aux grandes entreprises ainsi qu'aux particuliers

CHAPITRE 2

FOG COMPUTING

2.1 Introduction

La prolifération des capteurs intelligents, l'adoption croissante de dispositifs IoT et l'intégration de nombreuses applications intelligentes appellent la technologie de fog computing à devenir le concept le plus populaire dans des secteurs comme la fabrication, l'énergie, le transport et la logistique, et les soins de santé, Avec 50 milliards d'objets qui deviendront connectés dans le monde d'ici 2020, il serait un peu difficile de tout gérer dans le Cloud. Aussi appelé brouillard informatique, le fog est un modèle dans lequel les données, le traitement et les applications sont concentrés dans les dispositifs à la périphérie du réseau plutôt qu'entièrement dans le Cloud.

2.2 Définition

Egalement appelé fog networking ou fogging, le fog computing renvoie à une infrastructure matérielle et applicative distribuée, taillée pour stocker et traiter les données issues des objets connéctés. Au lieu de centraliser dans le cloud les informations produites par les capteurs, l'idée à travers cet environnement est de faire appel aux équipements situés à la périphérie du réseau (routeurs, passerelles, commutateurs, appareils mobiles...) pour réaliser les traitements. En créant cette surcouche intermédiaire au plus près de la production des données, l'objectif est in fine d'optimiser les délais de réponse des applications.

Le fog computing est considéré comme une extension locale du cloud. Par contraste avec le cloud, ou nuage, qui se forme dans le ciel (traduisant l'idée d'une informatique distante), le terme anglais fog (brouillard en français) se forme au dessus du sol. L'expression fog computing renvoie ainsi à la notion d'une informatique plus proche du monde

physique, des terminaux et de l'IoT [5].

2.3 Le plus du FOG

Face à l'explosion des volumes de données issus des objets connectés, les infrastructures actuelles de cloud, très centralisées, pourraient atteindre leur limite. Les capacités des réseaux et des Datacenters existants risquent en effet la saturation, ce qui ferait exploser les temps de latence et rendrait le traitement des données incompatible avec les besoins d'analyse en temps réel. Avec le cloud, les serveurs capables de traiter les données sont distants et leur temps de réponse dépend de facteurs que l'utilisateur ne peut pas contrôler : charge de travail des serveurs, encombrement du réseau... Le fog computing a pour but d'apporter une réponse à cette problématique. Il réduit le chemin à parcourir entre l'appareil qui produit les données et l'équipement qui les traite, et la nécessité de faire transiter les données vers les serveurs [8].

2.4 Consortium de l'OPENFOG

Cette collaboration a pour but de fédérer les entreprise impliquées dans le FOG autour de la définition de protocoles et standards technologies spécifiques au FOG afin de standardiser le marché .

L'OpenFog a défini une infrastructure pour mettre en œuvre une solution de FaaS (Fog as a Service). Celle-ci se décline en plusieurs couches calquées sur la logique d'empilement du cloud (IaaS, PaaS et SaaS). Une architecture à laquelle s'ajoutent des éléments spécifiques au FOG computing : des services d'interconnexion réseau, de collecte de données à partir des objets connectés, ou encore des applications de traitement. Le principe de fonctionnement est ainsi le même que celui du Cloud avec quelques particularités .

2.5 Fonctionnement du FOG

Les charges de travail du fog computing sont réparties entre environnements locaux et cloud, où différents objets (des dispositifs équipés de capteurs et connectés à un réseau) transmettent des données à des nœuds déployés localement en périphérie (d'où le concept du brouillard, ou "fog"), au lieu de communiquer directement avec le cloud. Un sous ensemble de données (pour lesquelles la rapidité de transmission n'est pas un élément critique) est alors transféré des nœuds d'extrémité vers un cloud centralisé ou un Datacenter, afin de procéder à des analyses et traitements supplémentaires. En plaçant

certaines fonctionnalités analytiques à proximité de la source des données, les architectures "en brouillard" ou de périphérie peuvent réduire le volume de données circulant sur le réseau, minimisant ainsi la latence et les coûts. [6]

2.6 Différence entre le FOG et le CLOUD [8]

L'edge computing se réfère à tous les équipements IT d'"extrémité", c'est-à-dire installés au plus près des utilisateurs et sources de données. Ces équipements informatiques et réseau peuvent faire partie d'une infrastructure de fog computing. Ils ne se limitent pas seulement aux équipements IT conventionnels. Les objets connectés capables de stocker et de traiter les données en local sont aussi considérés comme faisant partie d'une infrastructure d'edge computing.

Poin de différence	Cloud Computing	Fog Computing
Latence	élevée	basse
Localisation du service	dans l'internet	basse
Distance entre le client et le serveur	plusieurs sauts	un seul saut
Nombre de nœuds du serveur	Peu	beaucoup de nœuds
Support de mobilité	limité	supporté
Interaction en temps réel	supporté	supporté

TABLE 2.1 – FOG vs Cloud

2.7 Avantages du FOG

1. Réduction significative de la circulation des données à travers le réseau. Donc réduction de la congestion, du coût et de la latence. Elimination des goulets d'étranglement résultant de systèmes informatiques centralisés. Amélioration de la sécurité des données chiffrées qui restent plus proche de l'utilisateur final en réduisant leur exposition. Meilleure évolutivité découlant de systèmes virtualisés.
2. élimination de la dimension centralisée de l'environnement informatique, réduisant ainsi les points de blocage et de défaillance.
3. Amélioration de la sécurité, les données sont codées dès leur déplacement dans le réseau.
4. Amélioration des temps de réponse aux utilisateurs finaux. Meilleure évolutivité, fiabilité et tolérance aux pannes.
5. Consommation réduite de bande passante

Côté désagrément, il note surtout la complexité de mise en œuvre avec un choix restreint de plate-formes technologiques, d'applications Web disponibles ou encore de services par rapport à une infrastructure de cloud computing classique.

Le Fog computing s'avère donc plus performant que le cloud computing pour faire face aux nouvelles demandes induites par l'apparition de l'IoT. Mais il ne remplacera jamais totalement le cloud computing, qui restera privilégié pour le traitement de gros volumes de données, un scénario très répandu. En fait, l'industrie s'oriente vers une complémentarité des deux systèmes en fonction de besoins spécifiques.

2.8 Conclusion

Le Fog computing peut améliorer et rendre plus facile et plus rapide l'utilisation de l'internet des objets certes, mais peut aussi ouvrir la porte a plusieurs utilisateurs malveillants pour pouvoir infiltrer le réseau, car comme nous le savons tous aucune nouvelle technologie n'est à l'abri du piratage informatique.

CHAPITRE 3

SIMULATION

3.1 Introduction

Afin de pouvoir tester la sécurité du FOG COMPUTING on va procéder par simulation, comme nous l'avons déjà mentionné un périphérique FOG est situé à une distance d'un saut par rapport à son client, donc pour simuler une attaque, on procéder par substitution.

Le périphérique FOG sera représenté par une machine (serveur) qui est connectée à une autre machine directement, et l'attaquant est une troisième machine dans le réseau et qui a pour serveur la machine FOG aussi.

3.2 Environnement de travail

Avant de pouvoir faire la simulation une préparation à l'avance est requise, pour la faire nous avons besoin de quelques ressources matériel et logiciel.

3.2.1 Ressources matériel

Pour pouvoir réaliser notre simulation on aura besoin d'une machine tournant sous Windows, cette machine aura pour adresse IP : 192.168.164.1

3.2.2 Ressources logiciel

Afin de bien mener cette simulation on va installer :

3.2.2.1 VMWare workstation [9]

C'est la version station de travail du logiciel. Il permet la création d'une ou plusieurs machines virtuelles au sein d'un même système d'exploitation (généralement Windows ou Linux), ceux-ci pouvant être reliés au réseau local avec une adresse IP différente, tout en étant sur la même machine physique (machine existant réellement). Il est possible de faire fonctionner plusieurs machines virtuelles en même temps, la limite correspondant aux performances de l'ordinateur hôte. La version Linux présente l'avantage de pouvoir sauvegarder les fichiers de la machine virtuelle (* .vmsd) pendant son fonctionnement.

3.2.2.2 Cain [11]

C'est un outil gratuit de récupération de mot de passe fonctionnant sous Windows. Il permet la récupération facile de divers genres de mots de passe en sniffant le réseau, cassant des mots de passe hachés en utilisant des attaques par dictionnaire, par recherche exhaustive ou encore via des tables arc-en-ciel. Son code source n'est pas fourni.

Il peut être utile pour les administrateurs qui désirent élever le niveau de sécurité des stations. Il permet de vérifier si les mots de passe choisis par les utilisateurs sont suffisamment robustes contre les diverses attaques possibles, et d'émettre des directives de sécurité si nécessaire. L'outil est également didactique et s'adresse aux personnes intéressées par la sécurité et la cryptologie.

3.2.2.3 Wireshark [10]

Wireshark est un analyseur de paquets libre utilisé dans le dépannage et l'analyse de réseaux informatiques, le développement de protocoles, l'éducation et la rétro-ingénierie. Wireshark utilise la bibliothèque logicielle GTK+ pour l'implémentation de son interface utilisateur et pcap pour la capture des paquets ; il fonctionne sur de nombreux environnements compatibles UNIX comme GNU/Linux, Free BSD, Net BSD, Open BSD ou Mac OSX, mais également sur Microsoft Windows. Wireshark reconnaît 1 515 protocoles.

3.3 installation et configuration

La machine physique tournant sous Windows 7 aura pour adresse IP : 192.168.164.1 et elle représentera le périphérique FOG Sur VMware workstation on créera deux machines virtuelles sous Windows 7 aussi comme suit : Machine client avec l'adresse IP : 192.168.164.133 Machine pirate avec l'adresse IP : 192.168.164.132 Sur la machine pirate on installera Wireshark et Cain.

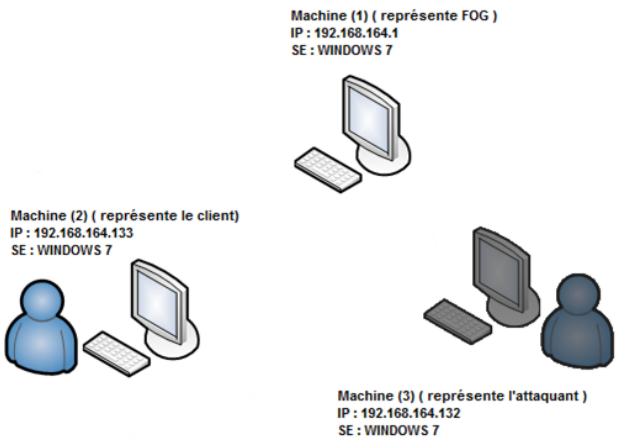

FIGURE 3.1 – Réseau établi

3.4 Test d'intrusion

3.4.1 Type de teste

Le scénario d'attaque qu'on a choisi pour pouvoir tester la sécurité de la connexion nœud a nœud du FOG est l'attaque MAN-IN-THE-MIDDLE ou l'homme du milieu, une attaque assez connu dans le monde de l'informatique qui a pour but d'intercepter les communications entre deux parties, sans que ni l'une ni l'autre ne puisse se douter que le canal de communication entre elles a été compromis. Le canal le plus courant est une connexion à Internet de l'internaute lambda. L'attaquant doit d'abord être capable d'observer et d'intercepter les messages d'une victime à l'autre. L'attaque " homme du milieu " est particulièrement applicable dans la méthode d'échange de clés Diffie-Hellman, quand cet échange est utilisé sans authentification.

3.4.2 Partie exploitée

L'attaque qu'on va tester va viser le protocole ARP (protocole de résolution d'adresse) est un protocole effectuant la traduction d'une adresse de protocole de couche réseau (typiquement une adresse IPv4) en une adresse MAC (typiquement une adresse éthernet), ou même de tout matériel de couche de liaison. Il se situe à l'interface entre la couche réseau (couche 3 du modèle OSI) et la couche de liaison (couche 2 du modèle OSI).

3.4.3 MITM en théorie

Dans notre cas la machine du pirate va envoyer une requête ARP au client et au serveur FOG afin d'empoisonner leurs table ARP, en falsifiant son adresse IP et en gardant son

adresse MAC pour obligé le trafic entre les deux machine a passer a travers la machine pirate.

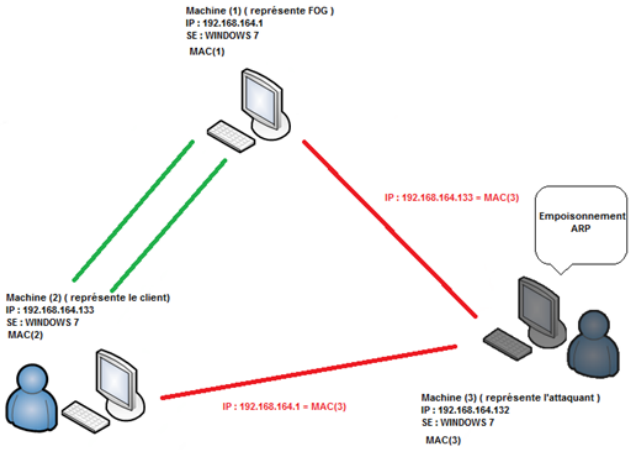

FIGURE 3.2 – Etape (1) de l'attaque

Quand la table de chaque machine sera mis a jour le pirate se placera au milieu et capturera tout le trafic circulant dans le canal.

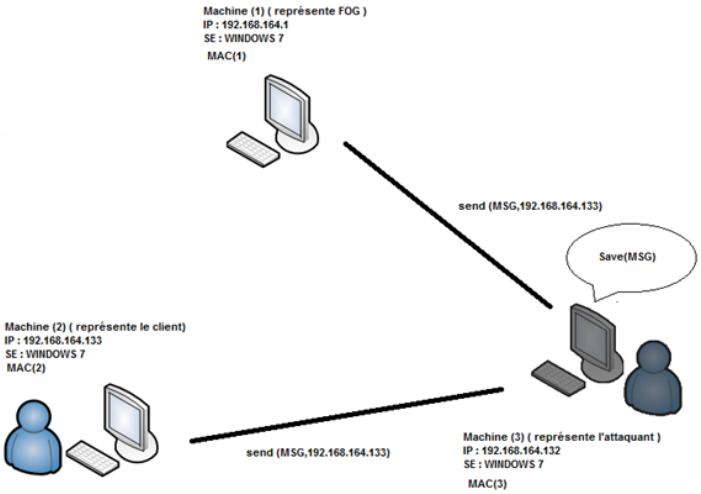

FIGURE 3.3 – Etape (2) de l'attaque

L'interception des messages y compris les mots de passes sera à présent facile vu l'emplacement de l'attaquant, surtout pour les communications non cryptés sachant que la plupart des nouveaux périphériques qui forment l'internet des objets sont à faibles ressources et n'ont ni la rapidité ni la mémoire suffisante pour pouvoir effectuer les opérations cryptographiques modernes.

3.5 Exemple concret de l'intrusion

Nous allumons la machine physique puis les deux machines virtuelles :

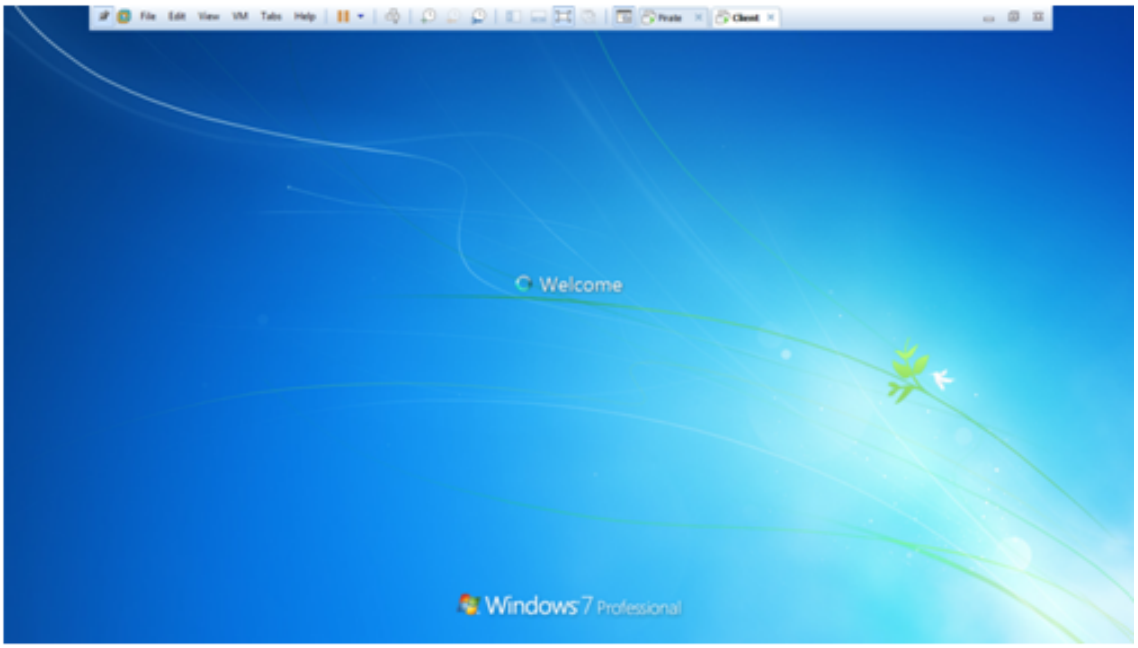

FIGURE 3.4 – Machines de simulation

Nous pourrons ensuite préparer l'attaque de l'homme du milieu sur la machine pirate en démarrant Cain, et en choisissant l'onglet Sniffer.

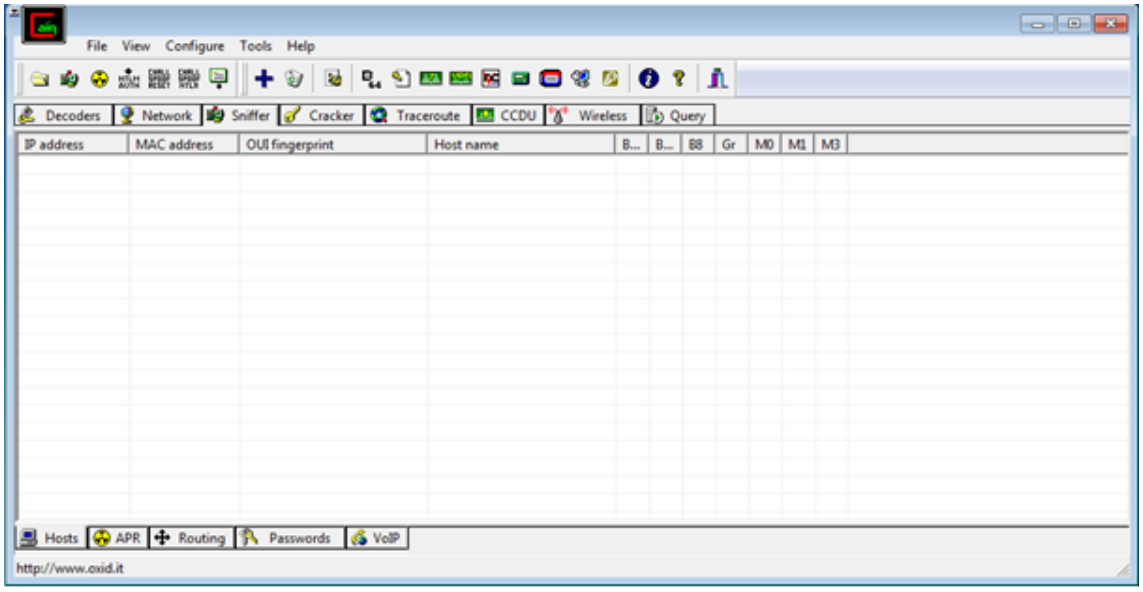

FIGURE 3.5 – Aperçu du logiciel Cain

Nous configurons ensuite la carte réseau avec la quelle on est connecté.

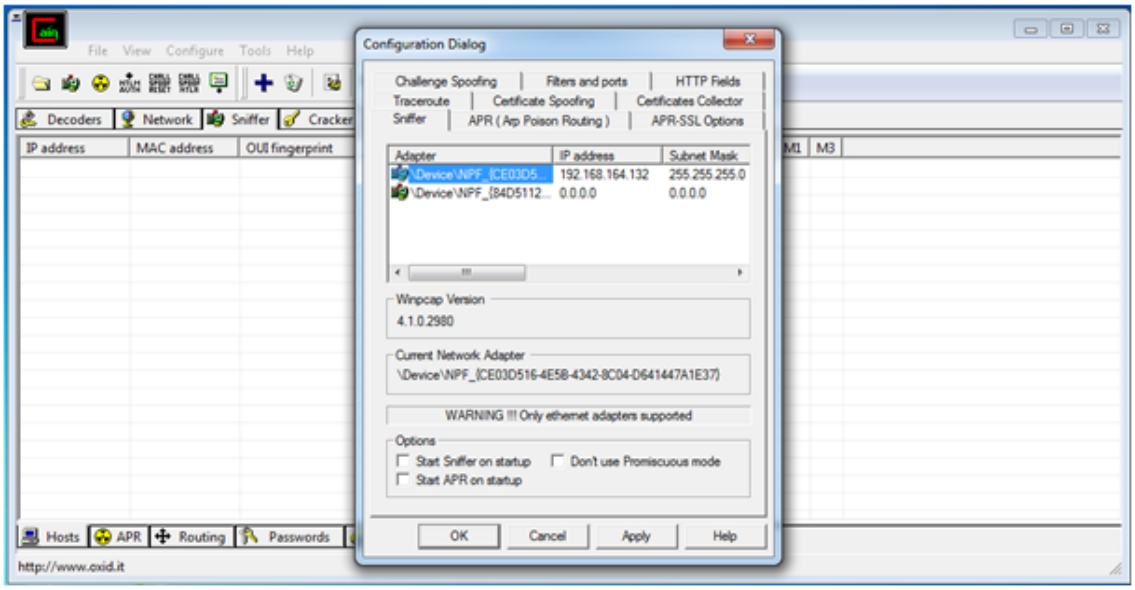

FIGURE 3.6 – Sélection de la carte réseau

Sur la machine client on pourra vérifier l'ensemble des hôtes connectées au client avec leurs adresses IP et MAC en tapant la commande " arp -a "

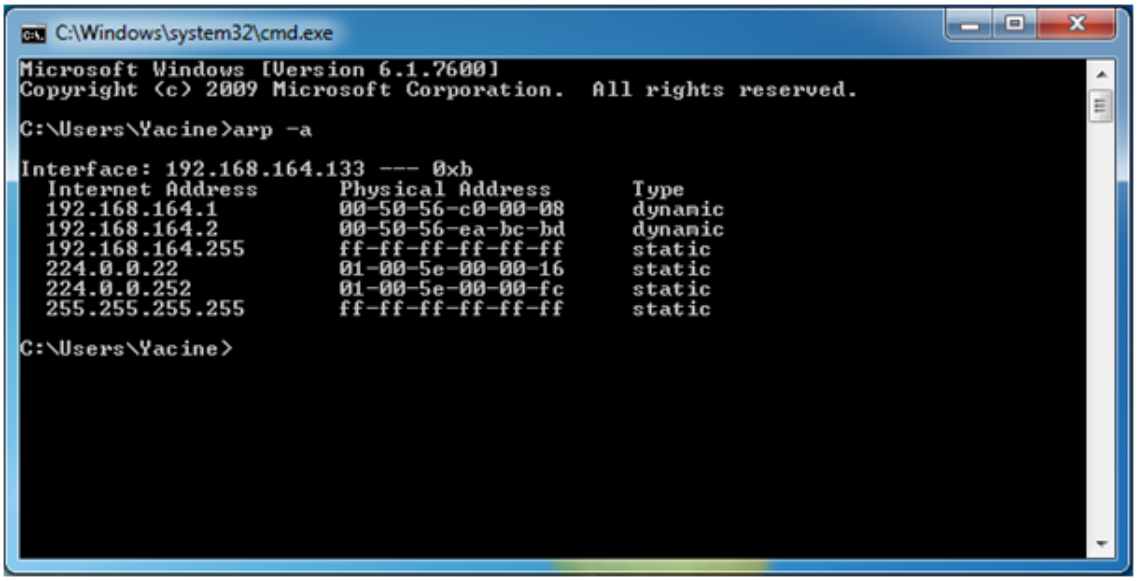

FIGURE 3.7 – Résultat de la commande " arp -a "

Dans l'onglet APR, on sélectionne les deux hôtes dont on veut sniffer le trafic, dans notre cas le client et le serveur FOG, ayant les adresse IP 192.168.164.133 et 192.168.164.1 respectivement.

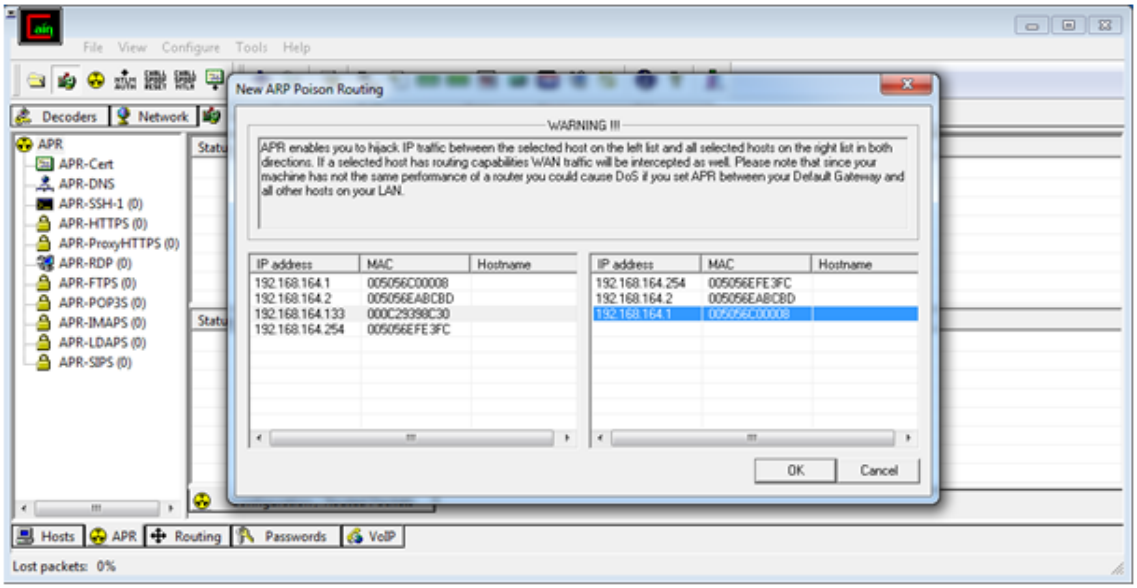

FIGURE 3.8 – Sélection du canal a sniffé

Nous démarrons ensuite l'empoisonnement ARP a partir de Cain pour se mettre au milieu des deux victimes.

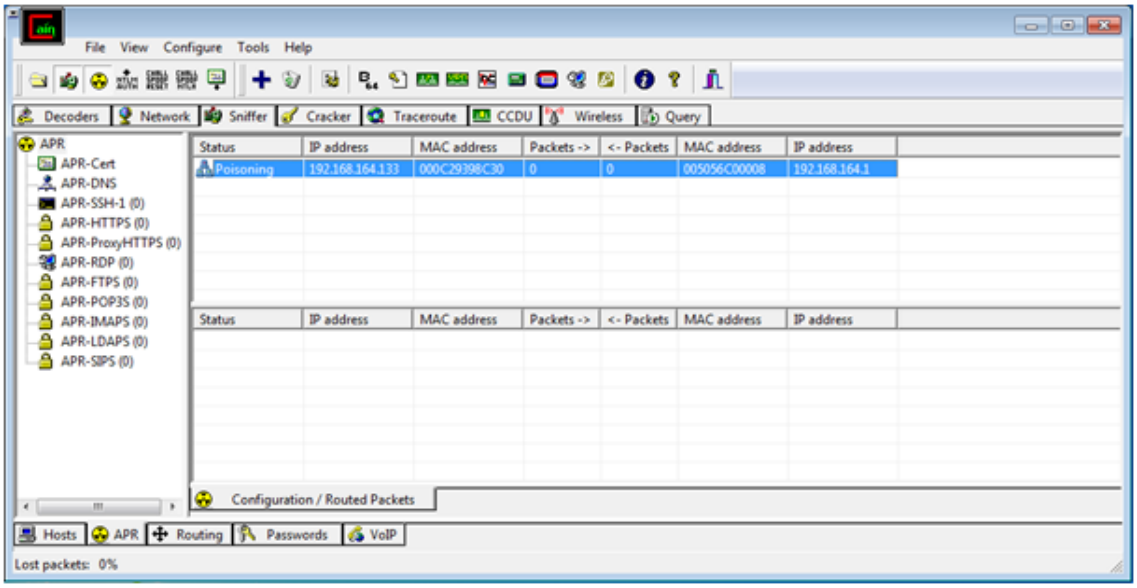

FIGURE 3.9 – Démarrage d'emploisonnement des tables ARP

On retape la commande " arp -a " pour revoir les adresses connectées à notre machine client.

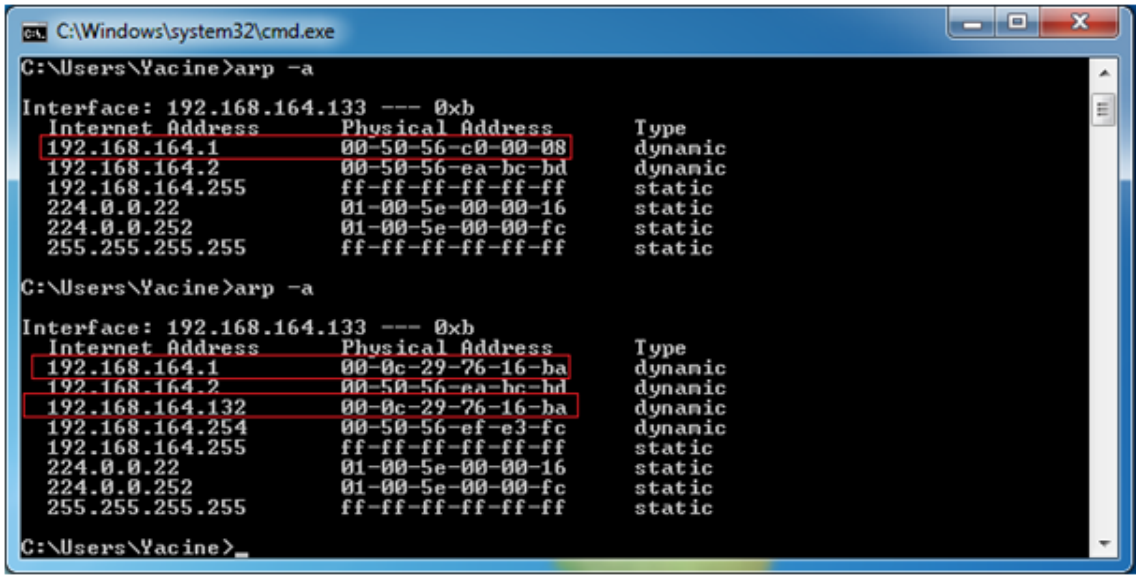

FIGURE 3.10 – Résultat de la commande " arp -a " après l'empoisonnement

Nous pourrons remarquer que l'adresse MAC associé a l'adresse IP 192.168.164.1 (serveur FOG) a changé, on remarque aussi que la nouvelle adresse MAC associé a l'adresse IP du FOG est la même que celle associé a l'adresse IP 192.168.164.132 (Pirate), On en conclus que le pirate a réussi a se mettre au milieu des deux hôtes.

Pour pouvoir tester l'écoute du canal, on envoi une requête ping du client vers le serveur et on voit si les paquets passent vraiment par le pirate.

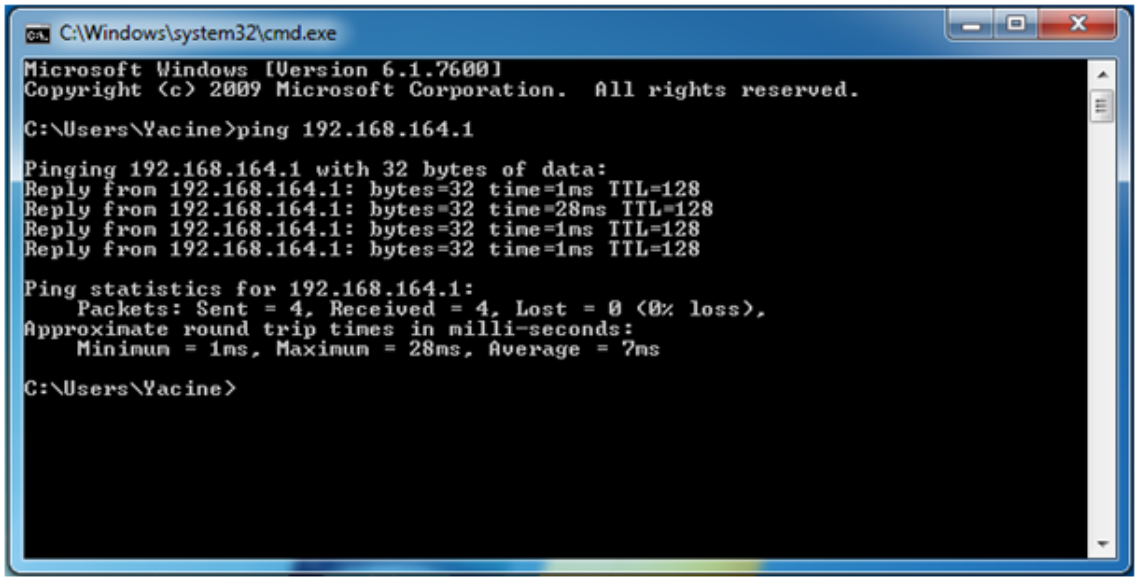

FIGURE 3.11 – Requête PING du client au serveur

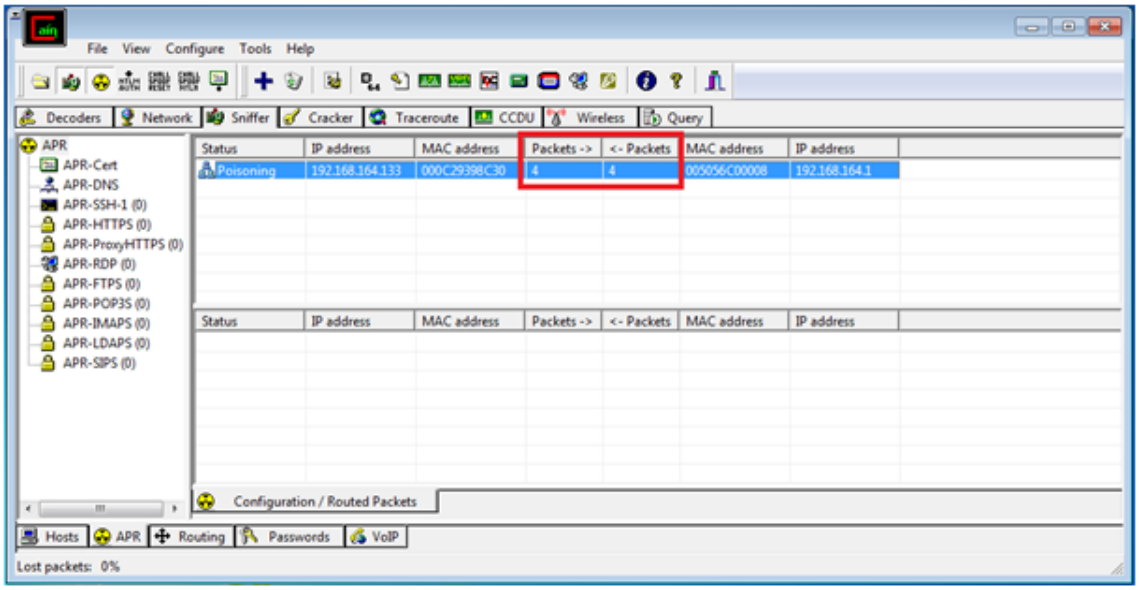

FIGURE 3.12 – Paquets capturés

Nous pouvons voir maintenant que les 4 paquets envoyés par la requête ping ont tous passer par la machine pirate.

Cette faille ne s'arrête pas la, Nous avons confirmé que les paquets circulant entre le client et le serveur peuvent être interceptés, mais es-qu'on peut capturer le mot de passe d'une session vu que le serveur est une passerelle du point de vu du client.

Nous allons essayer d'établir une connexion via le protocole FTP entre le client et un serveur distant, le serveur FOG étant une passerelle toutes données nécessaires pour établir cette connexion passeront par lui.

Coté client :

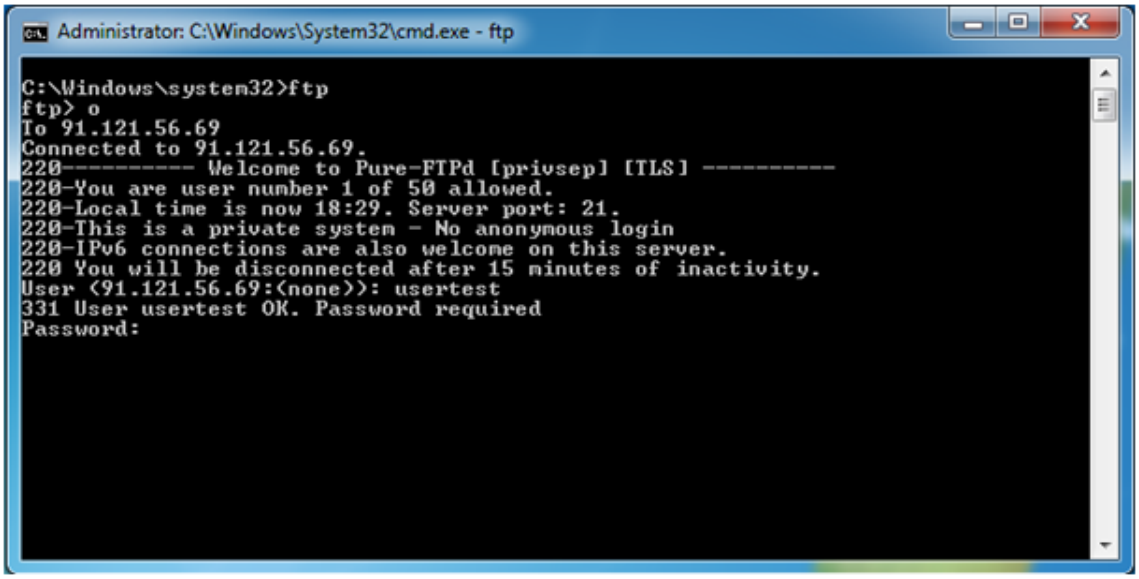

FIGURE 3.13 – Connexion FTP

Coté pirate :

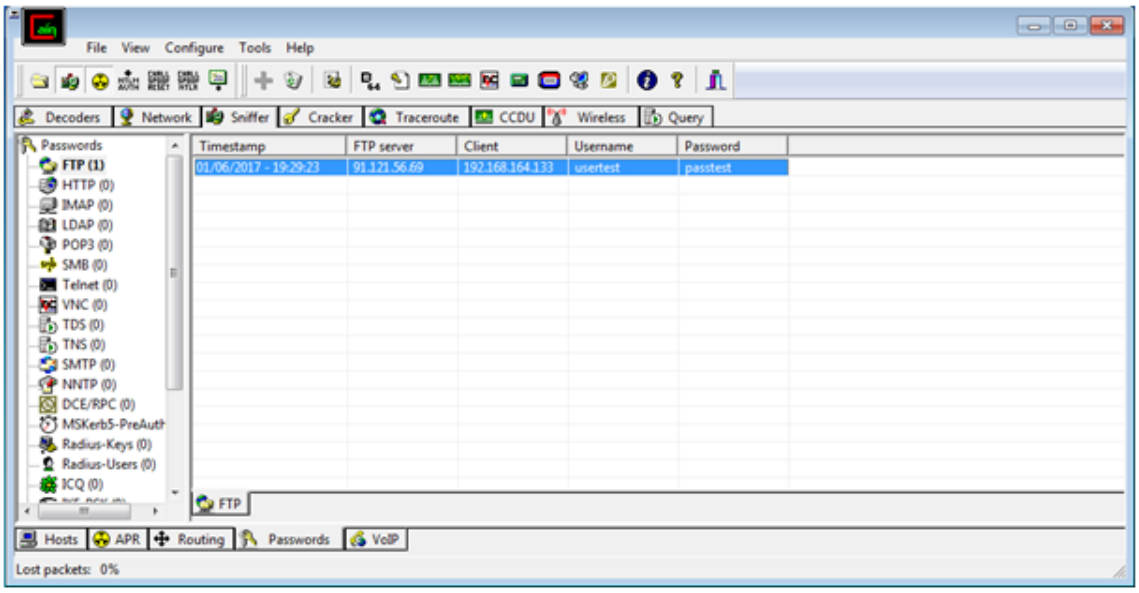

FIGURE 3.14 – Capture des informations d'authentification FTP

Nous remarquons que Cain peut capturer les identifiants nécessaires à une authentification non chiffrée [9]. Maintenant et pour mieux analyser les paquets circulant sur le canal intercepté, on fait appel à notre deuxième logiciel " Wireshark ". Nous commençons par sélectionner la carte réseau.

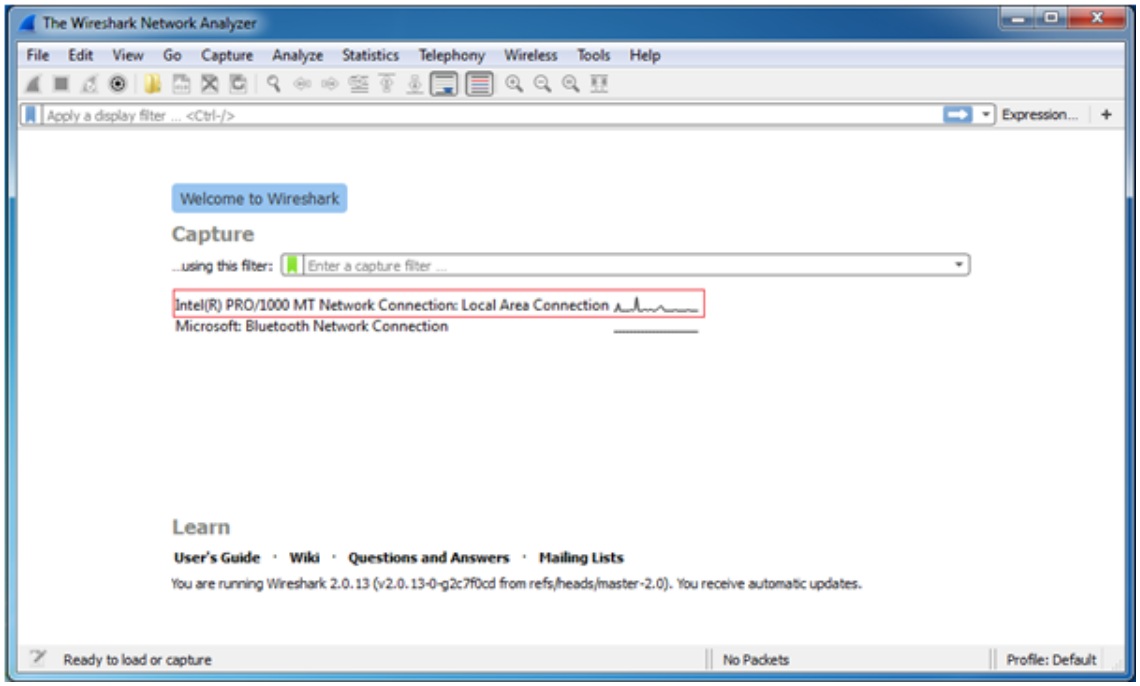

FIGURE 3.15 – Selection de carte réseau sur wireshark

Nous pourrons ensuite voir tout le trafic passant par notre carte réseau.

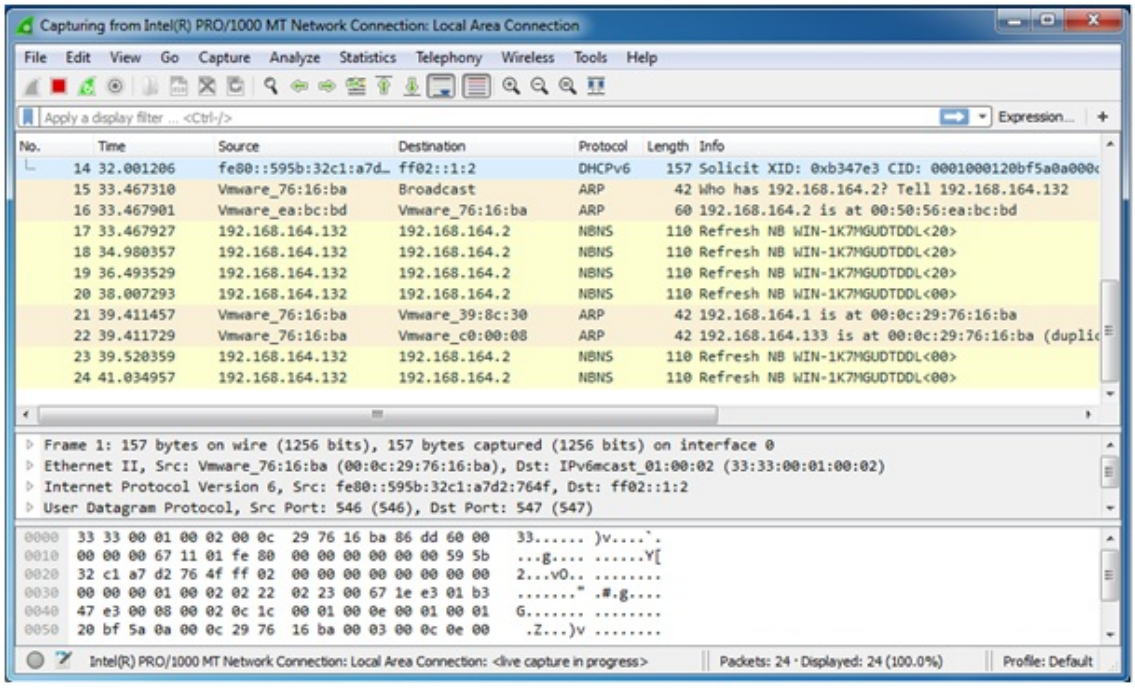

FIGURE 3.16 – Capture de paquets

Maintenant nous allons vers le PC client et on renvoi une requête PING vers le serveur, sachant que l'empoisonnement des tables ARP est toujours opérationnel, et on observe ce qui s'affiche au niveau de Wireshark.

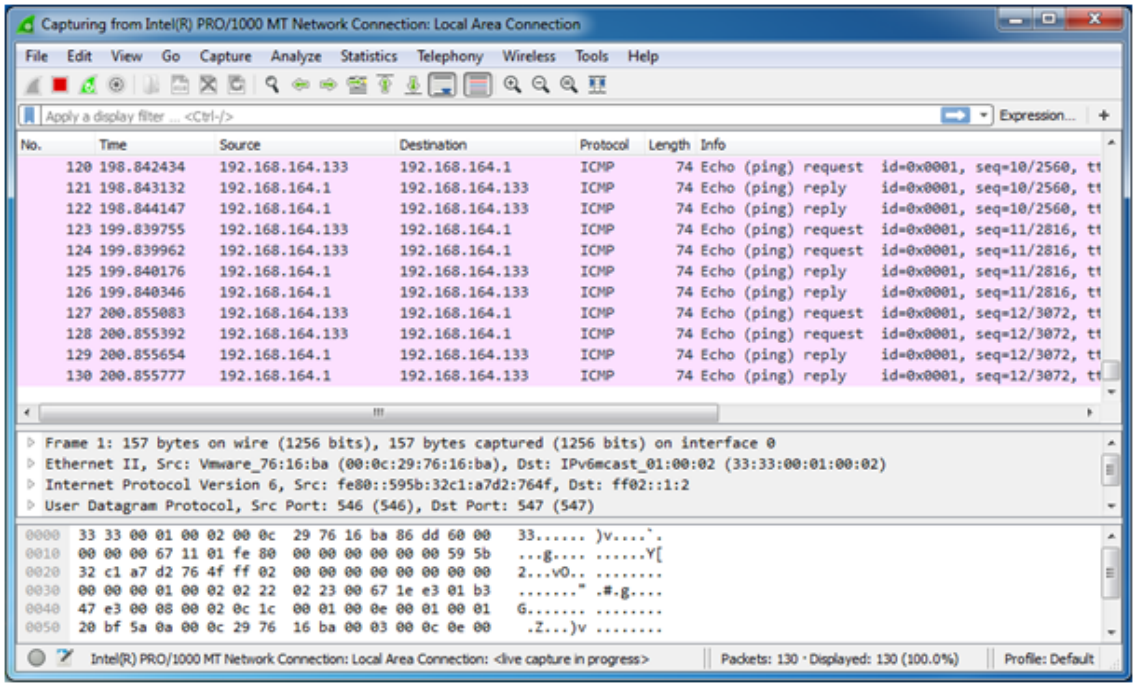

FIGURE 3.17 – Capture de paquets ICMP

Nous voyons bien que les paquets ont été bien capturés, on pourra même analyser leur contenu en appliquant un filtre ICMP sur Wireshark pour qu'on les confond pas avec d'autres paquets, et on sélectionnant l'un d'eux.

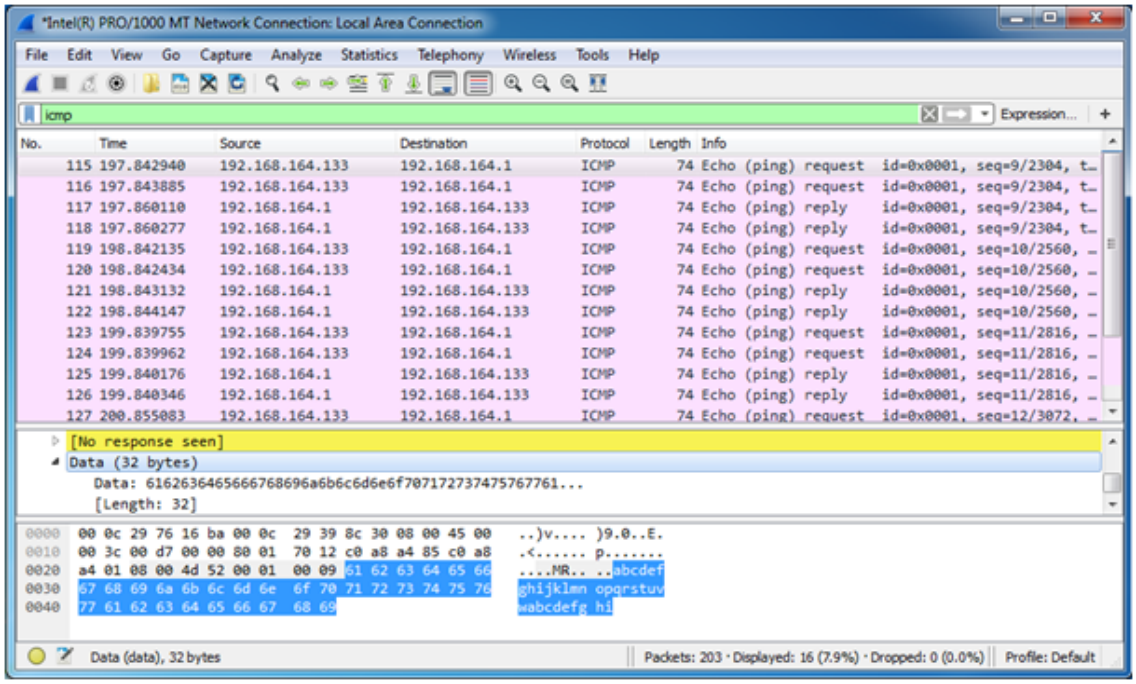

FIGURE 3.18 – Application du filtre et analyse d'un paquet

Cela s'implique à n'importe quel type de connexion, on pourra essayer une connexion

FTP.

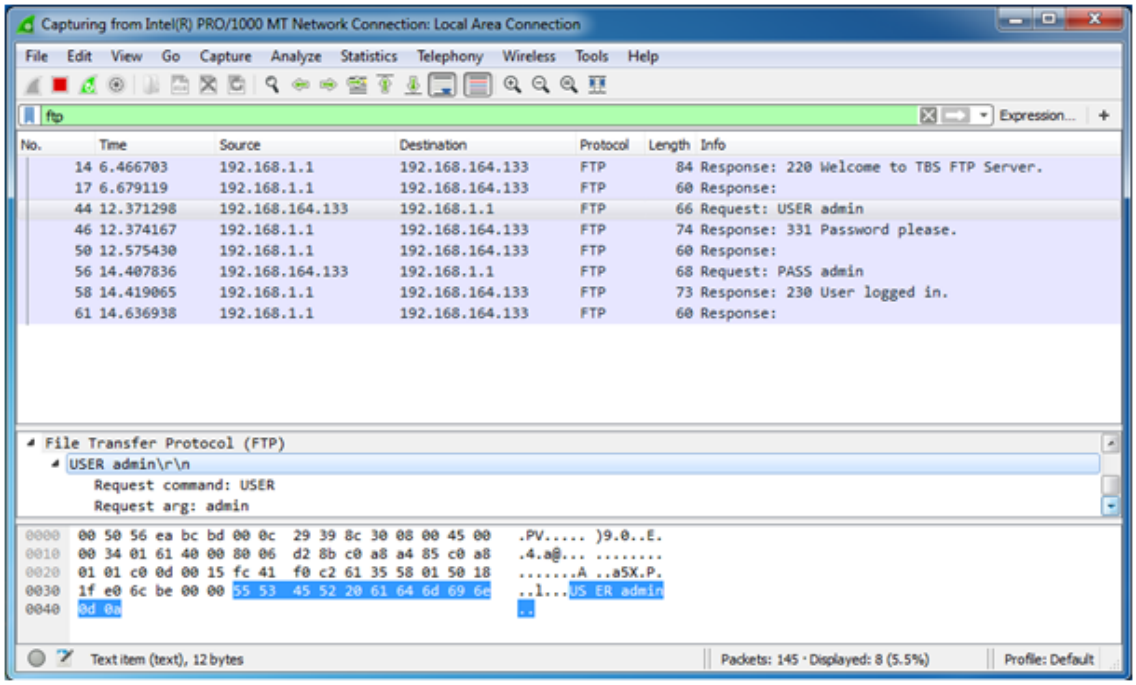

FIGURE 3.19 – Capture de paquets FTP

3.6 conclusion

Dans ce chapitre nous sommes arrivés à dévoiler une faille parmi plusieurs qui menace la sécurité du FOG computing, sachant que la majorité des périphériques de l'internet des objets sont des périphériques a faibles ressources, on doit soit créer de nouvels algorithmes adaptés a ces derniers, soit rendre ces périphériques plus puissants afin de pouvoir exécuter les algorithmes de cryptographie moderne, l'utilisation des protocole sécurité tel que SFTP, HTTPS pourra réduire le risque d'être visé par ce genre d'intrusion. Mais cela ne nous garanti pas une sécurité parfaite.

CONCLUSION GÉNERAL

Ce projet nous a permis d'approfondir nos connaissances sur les systèmes Cloud, leurs types, ainsi que leurs avantages et leurs inconvénients, tout en ce focalisant sur le brouillard informatique ou le FOG COMPUTING qui complète le Cloud et qui lui permet un traitement rapide des informations tout en diminuant les taches accordées a ce dernier.

La comparaison entre ces deux technologies nous a amené à déduire que ces dernières se complètent et que chacune dépend de l'autre.

L'audit de sécurité réalisé dans ce projet révèle une certaine insuffisance de sécurité dans le fonctionnement du brouillard informatique, sachant qu'on peut y remédier partiellement en appliquant des solutions déjà existantes ou complètement en trouvant une solution innovante au problème étudié.

La déduction qu'on peut tirer de ce qu'a été fait est que c'est presque impossible d'atteindre un niveau de sécurité parfait, et qu'il n'existe pas de systèmes infaillible.

Dans n'importe quelle nouvelle technologie il y'aura toujours des insuffisances, des failles, ou des bugs et c'est cela qui force l'avancement de la recherche scientifique.

LISTE DES ABREVIATIONS

1. USB : Universal Serial Bus
2. IoT : Internet of Things
3. IT : Information Technology
4. SaaS : Software as a Service
5. PaaS : Platform as a Service
6. IaaS : Interface as a Service
7. PC : Personal Computer
8. IP : Internet Protocol
9. MITM : Man In The Middle
10. FTP : File Transfer Protocol
11. ICMP : Internet Control Message Protocol
12. OSI : Open Systems Interconnection

BIBLIOGRAPHIE

[1] S. Belkadi et H. Harfi. Detection d'instrusion dans le cloud computing, mémoire master 2 "administration et sécurité des réseaux". *Université Abderrahmane Mira Béjaia*, 2016.

[2] N. Degroote. L'élasticité des bases de données sur le cloud computing, mémoire master 2 "réseaux et systèmes informatiques". *Université Libre de Bruxelles*, 2010.

[3] K. Maioua et A. Mansouri. Approche basée agents mobiles intelligents dans un environnement de cloud computing, mémoire master 2 " intelligence artificielle". *Université Kasdi Mrabah Ourgla*, 2014.

[4] P. Codo. Conception d'une solution de cloud computing privée basée sur un algorithme de supervision distribuée, mémoire d'ingéniorat " algorithmique distribuée". *Ecole Polytechnique d'Abomey-Calavi*, 2012.

[5] F. Bonomi et al. Fog computing and its role in the internet of things. *Systems Inc. 170 W Tasman Dr. San Jose, CA 95134, USA*, 2012.

[6] S. Yi et al. Fog computing : platform and applications, the college of william and marry. *Third IEEE Workshop on Hot Topics in Web Systems and Technologies*, 2015.

[7] OpenFog consortium architecture working group. Openfog reference architecture for fog computing. *OpenFog reference architecture for Fog computing*, Février 2017.

[8] Maher Abdelshkour. Iot, from cloud to fog computing. *Cisco*, Mars 2015.

[9] Vmware. "vmware workstation". http ://www.vmware.com/content/dam/digitalmarketing/vmware/fr Introduction-to-vSphere-PG-FR.pdf, Mis en ligne Mai 2015, consulté Fevrier 2017.

[10] SharkFest. "présentation wireshark". https ://www.wireshark.org/docs/, Mis en ligne septembre 2014, consulté Février 2017.

[11] Massimilano Montoro. "cain and abel user guide". http ://www.oxid.it/cain.html, Mis en ligne 2014, consulté Avril 2017.

[12] le cloud computing une nouvelle filière fortement structurante. www.idf.direccte.gouv.fr, Mis en ligne 2013, consulté Avril 2017.

RÉSUMÉ

Avec l'évolution croissante d'internet et les besoins énormes des utilisateurs particuliers les entreprises de nouvelles technologies on fait leur apparaitrions afin de satisfaire ces nouvelles contraintes, le stockage et le traitement enligne et distant aussi appelé CLOUD domine de plus en plus le marché et devient essentiel dans le monde de l'internet des objets, cette technologie possède plusieurs avantages certes mais n'empêche qu'elle contient plusieurs inconvénients majeurs, une nouvelle technologie nommé FOG ou brouillard informatique débarque sur le marché pour compléter son prédécesseur, cette dernière comme toute nouvelle technologie n'incarne pas la perfection non plus, ce projet est un audit de sécurité qui nous a permis de lever le voile sur certains besoins de sécurité de cette extension CLOUD.

Asbtract

With the increasing evolution of the Internet and the enormous needs of individual users, new technologies are making their appearance to satisfy these new constraints, storage and remote processing also called CLOUD dominates the market more and more Becomes essential in the world of the internet of objects, this technology has several advantages, but it does contain several major disadvantages, a new technology called FOG or computerized mist arrives on the market to complete its predecessor, the latter as Any new technology does not incarnate perfection either, this project is a security audit that allowed us to remove the veil on certain security needs of this CLOUD extension.