

---

الجمهورية الجزائرية الديمقراطية الشعبية  
République Algérienne démocratique et populaire  
وزارة التعليم العالي والبحث العلمي  
Ministère de l'enseignement supérieur et de la recherche scientifique  
جامعة سعد دحلب البلدية  
Université SAAD DAHLAB de BLIDA  
كلية التكنولوجيا  
Faculté de Technologie  
قسم الإلكترونيك  
Département d'Électronique



## Mémoire de Master

En Télécommunication

Spécialité : Réseaux & Télécommunications

Présenté par

MOUSSIDEN Meriem

---

# Etude sur la sécurité d'Openstack

---

Proposé par : Mr.BENSEBTI Messaoud & Mlle.AMALOU Warda

Année Universitaire 2021-2022

## Remerciements

---

Je tiens tout d'abord à exprimer ma gratitude envers Allah tout-puissant pour la force, la santé, la volonté et le courage qu'Il m'a accordés pour mener à bien ce travail. C'est avec une immense joie et le cœur ému que je remercie mes chers parents pour leur affection inépuisable et leurs précieux conseils. Ils n'ont jamais cessé de prier pour moi tout au long de mon cursus scolaire et m'ont encouragé régulièrement. Je remercie également tous les membres de ma famille.

Je tiens sincèrement à remercier mon encadreur, le Pr. BENSEBTI Messaoud, qui m'a guidé tout au long de la réalisation de ce mémoire.

Je souhaite également exprimer ma reconnaissance envers le Dr. Mehdi MEROUANE pour les précieuses informations qu'il nous a fournies tout au long de notre parcours universitaire, ce qui a enrichi notre domaine d'études.

Enfin, je tiens à remercier chaleureusement Mlle. AMALOU Warda pour sa confiance en mes capacités et pour m'avoir proposé ce sujet de mémoire.

MERCI

---

## ملخص :

عالم الإنترنت يحتوس على العديد من الثغرات الأمنة التي تهدد الأفراد و المستخدمين الذي يستعملونه لتخزين بياناتهم.

ففي هذا المشروع قمنا باختيار إحدى خزائن هذا العالم و التي تسمى بالسحابة الإلكترونية باستعمال إحدى الوسائل مفتوحة المصدر و المجانية OpenStack حيث قمنا بعرض طرق تثبيتها باستعمال نظام التشغيل Ubuntu الذي يعتبر هو الخادم, ثم قمنا بعملية التهكير بالرجل ف الوسط و الحرمان من الخدمة باستعمال Kali linux ثم قمنا بحماية هذا النظام عن طريق خلق قواعد جديدة في واجهة Suricata IDS/IPS و التي تستعمل للتنبيه و تقف الهجوم تحت قواعد خاصة.

كلمات المفاتيح: تهكير, السحابة الإلكترونية, أمن السحابة

---

**Résumé :** Le monde d'Internet contient de nombreuses failles de sécurité qui menacent les individus et les utilisateurs qui l'utilisent pour stocker leurs données.

Dans ce projet, nous avons choisi l'un des coffre-fort de ce monde, qui s'appelle le Cloud électronique, en utilisant l'un des moyens gratuits et open source, qui est OpenStack, où nous avons présenté les moyens de l'installer à l'aide du système d'exploitation Ubuntu, qui est le serveur, puis nous avons effectué le processus de piratage de l'homme du milieu et de déni de service à l'aide de Kali linux, puis nous avons protégé ce système en créant de nouvelles règles dans l'interface Suricata IDS/IPS qui sont utilisées pour alerter et arrêter le attaquer selon des règles spéciales.

**Mots clés :** Nuage informatique ; OpenStack; attaque, sécurité.

---

**Abstract:** The world of the Internet contains many security vulnerabilities that threaten individuals and users who use it to store their data.

In this project, we chose one of the safes of this world, which is called the electronic cloud, using one of the free and open source means, which is OpenStack, where we presented the ways to install it using the Ubuntu operating system, which is the server, and then we carried out the process of hacking the man in the middle and denial of service using Kali linux and then we protected this system by creating new rules in the Suricata IDS/IPS interface which are used to alert and stop the attack under special rules.

**Keywords :** Cloud computing, Openstack, Security , Attack.

# LISTES DES ACRONYMES ET ABBREVIATIONS

<b>AWS</b>	Amazon Web Services.
<b>API</b>	cloud application programming interface.
<b>ARP</b>	Address Resolution Protocol.
<b>ASII</b>	American Standard Code for Information Interchange.
<b>CPU</b>	Central Processins Unit.
<b>CSF</b>	ConfigServer Security & Firewall.
<b>DoS</b>	Deny of Service.
<b>DDoS</b>	Distributed Denial of Service.
<b>DNS</b>	Domain Name System.
<b>EDA</b>	Event Driven Architecture.
<b>FTP</b>	File Transfer Protocol.
<b>Http</b>	HyperText Transfer Protocol.
<b>HIDS</b>	Système de détection d'intrusion basé sur l'hôte.
<b>IAS</b>	the international Accreditation Service.
<b>IP</b>	Internet Protocol.
<b>ICMP</b>	HostBased Intrusion Detection System
<b>Id</b>	Identity.
<b>IPS</b>	système de prévention des intrusions.
<b>IDPS</b>	système de prévention de détection d'intrusion.
<b>laaS</b>	Infrastructure-as-a-service.
<b>IDS</b>	Un système de détection d'intrusion.
<b>LAN</b>	Local Area Network.
<b>MAC</b>	Media Access Control.
<b>MITM</b>	Man in the Middle.
<b>Nmap</b>	Network Mapper.
<b>NIDS</b>	Système de détection d'intrusion réseau.
<b>PC</b>	Personal Computer.
<b>PME</b>	Petites et moyennes entreprises.
<b>PoD</b>	Ping of Death.

<b>PaaS</b>	Platform-as-a-service.
<b>RAM</b>	Random Access Memory
<b>SDN</b>	Software-Defined Networking
<b>SSH</b>	Secure Shell.
<b>SLA</b>	Cloud service-level agreement.
<b>SOA</b>	Service Oriented Architecture.
<b>SYN</b>	Synchronize.
<b>SaaS</b>	Software-as-a-service.
<b>SQL</b>	Structured Query Language.
<b>SMB</b>	Server Message Block.
<b>TLS</b>	Transport Layer Security.
<b>TCP</b>	Transmission Control Protocol.
<b>UDP</b>	User Datagram Protocol.
<b>VPN</b>	Virtual Private Network.
<b>Web</b>	The World Wide Web.

# Table des matières

<b>Chapitre 1</b>	<b>Généralité sur le Cloud Computing</b>	<b>2</b>
1.1	Introduction :	2
1.2	L'origine du terme Cloud Computing :	3
1.3	Historique :	3
1.4	Types de Cloud Computing :	4
1.4.1	Modèle de déploiement :	4
1.4.2	Model de service :	6
1.4.3	Différence entre Iaas, Paas et Saas :	10
1.5	Les avantages :	12
1.5.1	Faible coût d'entretien :	12
1.5.2	Excellente accessibilité :	12
1.5.3	Fiabilité :	12
1.5.4	La vitesse :	13
1.5.5	Échelle globale :	13
1.5.6	Productivité :	13
1.5.7	Performance :	13
1.5.8	Sécurité des données :	13
1.6	Les inconvénients :	14
1.6.1	Nécessite une connexion Internet constante :	14
1.6.2	Les données stockées peuvent ne pas être sécurisées :	14
1.7	Exemples de Cloud Computing :	14
1.7.1	Applications sociales :	14
1.7.2	Banque, services financiers :	15
1.7.3	Soins de santé :	15
1.7.4	Éducation :	16
1.7.5	Jeux en ligne :	16
1.8	Architecture informatique en nuage :	16
1.8.1	Front-end :	17
1.8.2	Backend :	17
1.8.3	Application :	18

1.8.4	Un service :	18
1.8.5	Cloud Runtime :	18
1.8.6	Stockage :	18
1.8.7	Infrastructure :	18
1.8.8	La gestion :	18
1.8.9	Sécurité :	19
1.8.10	L'Internet :	19
<b>1.9</b>	<b>Virtualisation dans le Cloud Computing :</b>	<b>19</b>
1.9.1	Types de virtualisation :	20
<b>1.10</b>	<b>Cloud service :</b>	<b>22</b>
1.10.1	Openstack :	22
1.10.2	IBM Cloud Private :	22
1.10.3	Apache CloudStack :	22
1.10.4	Amazon EC2 :	23
1.10.5	La Comparaison :	23
<b>1.11</b>	<b>Conclusion :</b>	<b>23</b>
<b>Chapitre 2</b>	<b>Attaques et sécurité du Cloud Computing</b>	<b>24</b>
<b>2.1</b>	<b>Introduction :</b>	<b>24</b>
<b>2.2</b>	<b>Les attaques et l'impact sur le Cloud Computing :</b>	<b>24</b>
2.2.1	Définition d'une attaque :	24
2.2.2	Anatomie d'une attaque :	25
2.2.3	Types d'attaques :	25
2.2.4	Les attaques contre Cloud Computing :	26
<b>2.3</b>	<b>Sécuriser un serveur Cloud :</b>	<b>30</b>
2.3.1	Utilisation des clés SSH :	30
2.3.2	Installer un pare-feu :	30
2.3.3	Le VPN :	31
2.3.4	Utiliser Le Protocole TLS :	31
2.3.5	Système de détection d'intrusion (IDS) :	32
<b>2.4</b>	<b>Wireshark :</b>	<b>33</b>
2.4.1	Présentation de l'interface Wireshark :	34
<b>2.5</b>	<b>Conclusion :</b>	<b>35</b>
<b>Chapitre 3</b>	<b>La réalisation d'Openstack</b>	<b>36</b>

<b>3.1</b>	<b>Introduction :</b> .....	36
<b>3.2</b>	<b>Présentation d'Openstack :</b> .....	36
3.2.1	Definition :	36
3.2.2	Architecture d'Openstack :	37
<b>3.3</b>	<b>Environnement :</b> .....	38
3.3.1	Environnement matériel :	38
3.3.2	Travail à faire :	38
3.3.3	Installation d'Openstack :	39
3.3.4	Création d'un espace Cloud :	39
<b>3.4</b>	<b>Mise en place d'un IDS :</b> .....	48
3.4.1	Suricata IDS :	48
3.4.2	Fonctionnalités :	49
3.4.3	La gestion des règles :	49
<b>3.5</b>	<b>Conclusion :</b> .....	50
<b>Chapitre 4 Les attaques et la sécurité dans l'Openstack .....</b>		<b>51</b>
<b>4.1</b>	<b>Introduction :</b> .....	51
<b>4.2</b>	<b>Simulation des attaques :</b> .....	51
4.2.1	Machine Kali linux :	51
4.2.2	Simulation et détection des attaques :	52
<b>4.3</b>	<b>Conclusion :</b> .....	63
<b>Conclusion générale .....</b>		<b>64</b>
<b>Annexes</b>		
<b>Bibliographie</b>		



## Liste des figures

Figure 1-1: Cloud Computing. ....	2
Figure 1-2 : L'histoire du Cloud Computing. ....	4
Figure 1-3 : Les modèles de déploiement du Cloud. ....	5
Figure 1-4 : Nuage hybride.....	6
la différence entre ce que nous gérons et le fournisseur de services gère dans IaaS.....	7
la différence entre ce que nous gérons et le fournisseur de services gère dans PaaS.....	9
La différence entre ce que nous gérons et le fournisseur de services gère dans SaaS. ....	10
L'architecture du Cloud Computing. ....	17
L'architecture du Virtualisation dans Cloud Computing. ....	20
Types de virtualisation. ....	22
Figure 2- 1: La différence entre le DoS et le DDoS. ....	26
Figure 2- 2: L'attaque SQL injection.....	28
Figure 2- 3: L'attaque de l'homme du milieu. ....	29
Figure 2- 4: Le protocole SSH. ....	30
Figure 2- 5: Le filtrage d'un trafic entrant pour bloquer les menaces sur notre ordinateur par le Pare-feu. ....	31
Figure 2- 6: Architecture VPN. ....	31
Figure 2- 7: L'architecture d'IPS/IDS. ....	32
<b>Figure 2- 8:</b> L'interface de Wireshark. ....	34
Figure 2- 9: Les paquets en Wireshark.....	35
Figure 3- 1: Présentation d'Openstack. ....	37
Figure 3- 2: L'installation d'OpenStack. ....	39
Figure 3- 3: L'interface d'OpenStack. ....	40
Figure 3- 4: Création d'un projet. ....	40
Figure 3- 5: Saisie le nom de projet. ....	41
Figure 3- 6: Création d'un User. ....	41
Figure 3- 7: Saisir le nom utilisateur. ....	42
Figure 3- 8: Création d'un groupe.....	42
Figure 3- 9: Saisir le nom de groupe. ....	42
Figure 3- 10: Ajouter les utilisateurs dans le groupe. ....	43
Figure 3- 11: L'interface d'utilisateur.....	43
Figure 3- 12: Création de réseaux. ....	44
Figure 3- 13: Création d'un réseau externe. ....	44
Figure 3- 14: Création d'un réseau interne. ....	44
Figure 3- 15: La conversation de réseau interne.....	45
Figure 3- 16: Création d'un routeur. ....	45
Figure 3- 17: Les paramètres de routeur. ....	45
Figure 3- 18: Network Topology. ....	46
Figure 3- 19: Création d'instance. ....	46
Figure 3- 20: Saisir le nom d'instances. ....	47
Figure 3- 21 : Les paramètres d'instance. ....	47

<i>Figure 3- 22</i> : Le terminal d'instance. ....	47
<i>Figure 3- 23</i> : Network Topologie d'instance. ....	48
<i>Figure 3- 24</i> : L'architecture d'un Suricata IDS. ....	49
<i>Figure 3- 25</i> : L'emplacement de Suricata. ....	50
<i>Figure 4- 1</i> : Schéma de simulation d'attaques.....	51
<i>Figure 4- 2</i> : L'adresse mac du système cible.....	53
<i>Figure 4- 3</i> : Les adresses mac qui Connecté avec le serveur. ....	53
<i>Figure 4- 4</i> : L'interface d'Ettercap. ....	54
<i>Figure 4- 5</i> : La liste des host. ....	54
<i>Figure 4- 6</i> : Lancement d'ARP Poisoning. ....	55
<i>Figure 4- 7</i> : Le changement qui s'est dans l'adresse mac. ....	55
<i>Figure 4- 8</i> : L'analyse des paquets sur wireshark. ....	55
<i>Figure 4- 9</i> : La captation du mot de passe et le nom d'utilisateur. ....	56
<i>Figure 4- 10</i> : L'activation de pare-feu.....	57
<i>Figure 4- 11</i> : Création des règles. ....	57
<i>Figure 4- 12</i> : Les règles sur le pare-feu. ....	57
<i>Figure 4- 13</i> : Création d'un groupe de sécurité. ....	58
<i>Figure 4- 14</i> : Ajouter les règles pour groupe de sécurité. ....	58
<i>Figure 4- 15</i> : Création d'un Key Pair. ....	59
<i>Figure 4- 16</i> : La forme d'un Key Pair.....	59
<i>Figure 4- 17</i> : L'attaque DoS. ....	60
<i>Figure 4- 18</i> : Les capturassions des paquets d'attaque DoS. ....	61
<i>Figure 4- 19</i> : L'attaque DoS avec Hping3. ....	61
<i>Figure 4- 20</i> : Les capturassions des paquets avec wireshark. ....	62
<i>Figure 4- 21</i> : Lancement de Suricata. ....	62
<i>Figure 4- 22</i> : Les alertes sur Suricata. ....	63
<i>Figure 4- 23</i> : Drop les attaque DoS. ....	63

## Liste des tableaux

<b>Tableau 1- 1:</b> La différence entre IaaS, PaaS, SaaS .....	13
<b>Tableau 1- 2:</b> La comparaison entre différents programmes d'un Cloud Computing .....	27
<b>Tableau 3-1:</b> Les caractéristiques de PC serveur .....	44
<b>Tableau 4- 1:</b> Les ports d'Openstack .....	65



# Introduction générale

---

La sécurité revêt une importance cruciale dans le domaine des réseaux sans fil, tels que le Wi-Fi et le Bluetooth, ainsi que dans le domaine de l'informatique en général. Les technologies numériques présentent de nombreuses vulnérabilités, qu'il s'agisse de la facilité avec laquelle des personnes mal intentionnées peuvent compromettre la sécurité depuis l'extérieur ou l'intérieur, ou encore des failles qui peuvent résulter d'erreurs de conception ou de configuration. Ces failles peuvent entraîner le vol d'informations sensibles et de données privées sans que l'utilisateur ne se sente en sécurité.

Par conséquent, les grandes entreprises considèrent une approche globale de la sécurité des systèmes comme essentielle pour protéger leurs utilisateurs contre les voleurs d'informations. Elles s'efforcent de réduire les vulnérabilités et d'élever le niveau de protection en développant des programmes de sécurité robustes et en utilisant des clés hautement confidentielles.

Avec l'avancement de la technologie, ces entreprises déplacent de plus en plus leurs informations vers le Cloud, rendant ainsi leur traitement informatique accessible à tous. Cependant, malgré les avantages attrayants de l'informatique en nuage en termes de facilité d'utilisation et de coûts, cela présente également de nouveaux défis en matière de sécurité et de fiabilité. Un aspect critique du Cloud est l'interconnexion avec différents appareils, ce qui rend la sécurisation de ces données à la fois difficile et essentielle.

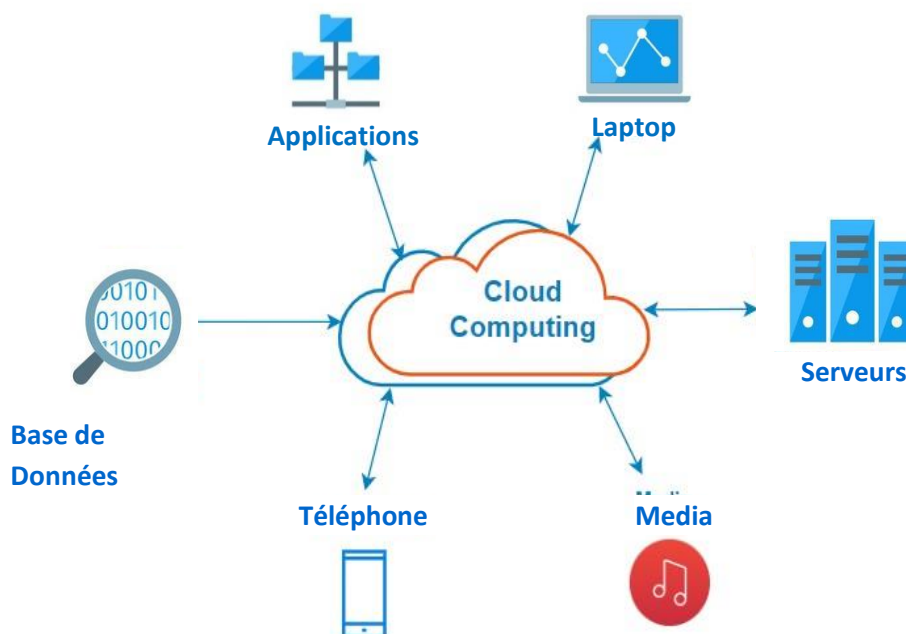
# Chapitre 1 Généralité sur le Cloud Computing

---

## 1.1 Introduction :

Avec l'ère du progrès et de la technologie et le développement de l'informatique, de nombreux facteurs sont apparus qui ont conduit à un grand saut dans le monde de la technologie. Aujourd'hui, je parle du projet que tout le monde utilise sans même les voir, que ce soit sur des sites bien connus ou bien des applications telles que Netflix, Instagram, Office 365 et LinkedIn, ou dans les startups, les institutions et les professionnels de l'informatique, les analystes et les utilisateurs individuels.

Dans ce chapitre, on parlera de Cloud Computing ou informatique en nuage qui est représenté dans une infrastructure dans laquelle la puissance de calcul et le stockage sont gérés par des serveurs distants auxquels les usagers se connectent via une liaison Internet sécurisée, et fournissent des services comme serveurs, le stockage, les bases de données, la mise en réseau, les logiciels, l'analyse, l'intelligence sur le Cloud (Internet).



**Figure 1- 1** : Cloud Computing.

## 1.2 L'origine du terme Cloud Computing :

Il existe en effet plusieurs histoires sur l'origine du terme "nuage électronique" (cloud computing), mais son origine exacte reste quelque peu floue. La plupart des sources s'accordent pour dire que le concept de l'informatique en nuage est souvent attribué au département des systèmes Internet de Compaq Computer, bien qu'ils n'aient pas atteint la véritable origine. Certaines de ces histoires disent :

- L'expression "nuage" est couramment utilisée en science pour décrire une grande agglomération d'objets qui apparaissent visuellement de loin comme un nuage, et elle sert à décrire tout groupe d'objets dont les détails ne sont pas examinés dans un contexte particulier.
- Dans l'usage courant, le terme "Cloud" est essentiellement une analogie avec Internet. Les spécialistes du marketing ont popularisé l'expression « dans le Cloud » pour désigner les logiciels, les plates-formes et l'infrastructure qui sont vendus « en tant que service », c'est-à-dire à distance sur Internet.
- Le terme "Cloud" en informatique trouve son origine dans le domaine de la téléphonie. Jusqu'aux années 1990, les entreprises de télécommunications se concentraient principalement sur la fourniture de circuits de données point à point. Cependant, elles ont commencé à proposer des services VPN (Virtual Private Network) offrant une qualité de service similaire, mais à un coût bien inférieur. En déplaçant le trafic vers l'équilibrage de charge selon leurs besoins, elles ont pu utiliser leur bande passante réseau de manière plus efficace. [1]

## 1.3 Historique :

De nos jours, de nombreux internautes considèrent le terme "informatique en nuage" comme un concept relativement nouveau dans le monde d'Internet. Cependant, il convient de noter que ce concept remonte aux années 1960. En 1961, l'informaticien John McCarthy a introduit publiquement l'idée de l'"informatique utilitaire" lors d'un discours célébrant le centenaire de la fondation du Massachusetts Institute of Technology. McCarthy a évoqué la possibilité d'organiser l'informatique

comme un service public, tout comme le système téléphonique. Cette vision préfigurait le développement que nous connaissons aujourd'hui.

Dans les années 60, les serveurs faisaient partie intégrante des ordinateurs, mais les choses ont considérablement évolué depuis. Entre 1961 et 1966, le technologue Douglas Barkhill a écrit "The Computer Utility Challenge," où il a exposé les avantages potentiels de l'informatique en nuage et a évoqué l'émergence de ce qu'il a appelé les "gadgets informatiques."

La véritable transformation a commencé à partir du milieu des années 90, avec l'avènement des moteurs de recherche tels que Google et Yahoo, ainsi que l'émergence de plateformes de publication ouvertes comme YouTube et Myspace, ainsi que l'apparition des médias sociaux comme Facebook et Twitter.

À la fin des années 90, Salesforce.com est devenu populaire en proposant des services à distance. En 2002, Amazon.com a lancé Amazon Web Services (AWS), une plateforme fournissant un stockage à distance, des ressources informatiques et d'autres fonctionnalités. Cela a marqué un tournant majeur dans le développement de l'informatique en nuage.

En 2006, Amazon Web Services a connu une refonte majeure, introduisant des publicités pour l'AMAZON Flexible Computing EC2, qui permettait aux organisations de louer la puissance de calcul et de traitement pour exécuter leurs applications d'entreprise. La même année, Google a commencé à fournir des services basés sur un navigateur pour les applications d'entreprise.

Cette évolution montre comment l'informatique en nuage a émergé comme un concept clé de la technologie au fil des décennies, transformant la manière dont les entreprises et les utilisateurs interagissent avec la technologie informatique.[2]



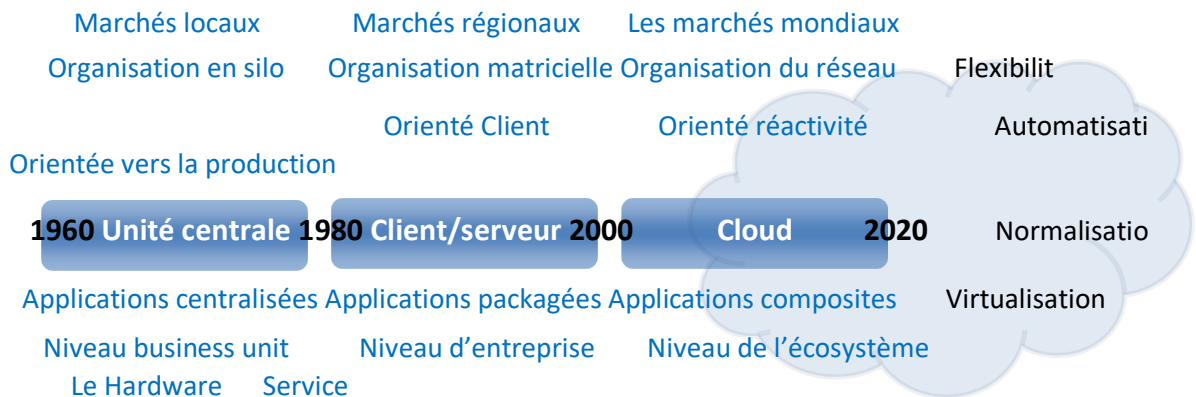


Figure 1- 2: L'histoire du Cloud Computing.

## 1.4 Types de Cloud Computing :

nous pouvons catégoriser les différentes formes de Cloud Computing en deux grandes classifications :

### 1.4.1 Modèle de déploiement :

Le modèle de déploiement se divise en trois types : le Cloud public, le Cloud privé et le Cloud hybride.

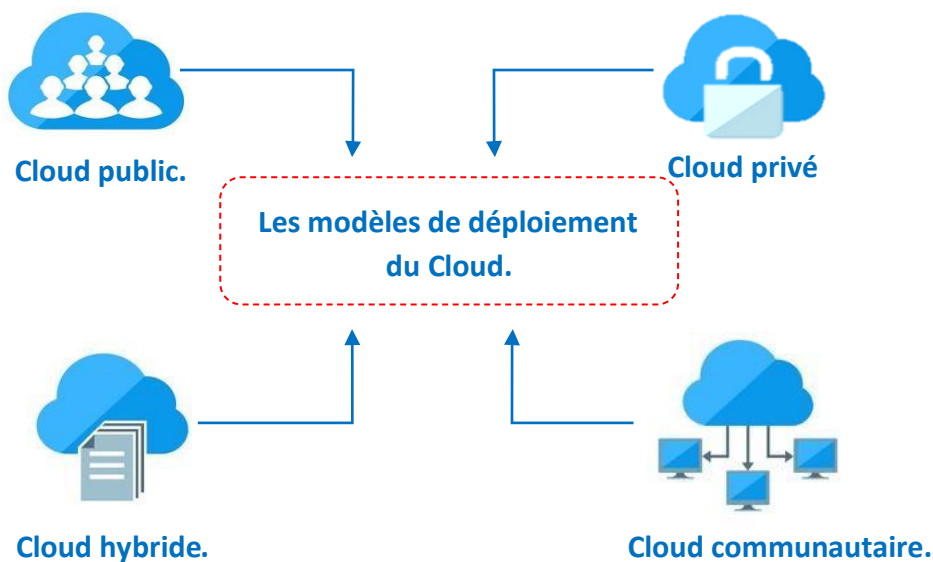


Figure 1- 3: Les modèles de déploiement du Cloud.

**a. Nuage public :**

Le Cloud public est une infrastructure Cloud mise à la disposition du grand public via Internet et gérée par un fournisseur de services Cloud. Ce modèle permet aux utilisateurs d'accéder au Cloud à travers des interfaces Web. Les utilisateurs ne paient que pour la quantité de services qu'ils utilisent, similaire à la façon dont nous payons pour l'électricité à la maison en fonction de notre consommation. Cette approche contribue à réduire les coûts d'exploitation par rapport aux dépenses informatiques traditionnelles. Cependant, il est important de noter que le Cloud public est généralement considéré comme moins sécurisé que d'autres modèles, car toutes les données et applications qu'il héberge sont vulnérables aux attaques malveillantes. Parmi les principaux fournisseurs de services Cloud public, on trouve AWS, Microsoft Azure, IBM Blue Cloud et Sun Cloud.

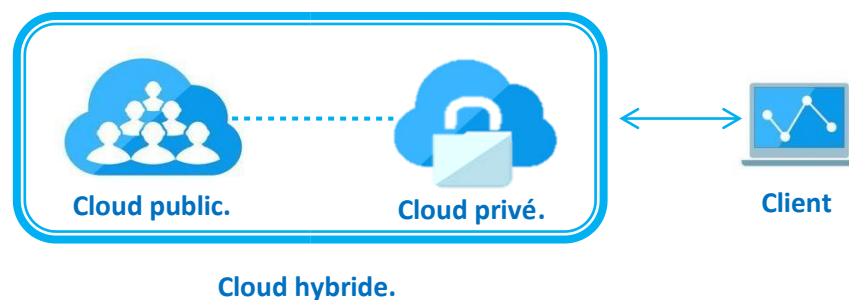
**b. Nuage privé :**

Un Cloud privé est une infrastructure Cloud exclusivement exploitée par une seule organisation. Il peut être géré en interne par l'organisation elle-même ou être pris en charge par un tiers, qu'il soit situé sur site ou hors site. L'élément clé ici est qu'il est réservé à l'usage exclusif d'une seule organisation. L'avantage principal du Cloud privé réside dans sa gestion plus aisée en termes de sécurité, de maintenance et de mises à jour, tout en offrant un contrôle total sur le déploiement et l'utilisation des ressources. On peut le comparer à une infrastructure réseau privée par rapport à Internet. Contrairement au Cloud public, où toutes les ressources et applications sont gérées par un fournisseur de services tiers, dans le Cloud privé, ces services sont consolidés et mis à disposition au niveau organisationnel. Les ressources et applications sont gérées directement par l'organisation elle-même. Étant donné que seuls les utilisateurs de l'organisation ont accès au Cloud privé, la sécurité est renforcée. Certaines entreprises qui proposent des services de Cloud privé incluent AWS et VMware.

**c. Nuage hybride :**

Le Cloud hybride combine les avantages du Cloud public et du Cloud privé en intégrant un Cloud privé avec un ou plusieurs services de Cloud public, le tout géré par un logiciel propriétaire qui facilite la communication entre ces services distincts. Cette approche offre aux entreprises une flexibilité accrue pour déplacer leurs charges de travail entre les solutions Cloud en fonction de l'évolution de leurs besoins et de leurs coûts.

Les services de Cloud hybride sont particulièrement puissants car ils permettent aux entreprises de mieux contrôler leurs données privées. Par exemple, les agences fédérales peuvent opter pour des Clouds privés pour stocker et gérer des données sensibles, tout en utilisant le Cloud public pour partager des données non sensibles, telles que des ensembles de données, avec le grand public ou d'autres départements gouvernementaux. Cette approche garantit la sécurité des données sensibles tout en permettant une collaboration efficace sur les informations non sensibles.[3]



**Figure 1- 4:** Nuage hybride.

**1.4.2 Model de service :**

Pour une classification plus globale, les services Cloud peuvent être catégorisés en trois grandes catégories : Infrastructure en tant que Service (IaaS), Plate-forme en tant que Service (PaaS), et Logiciel en tant que Service (SaaS), parfois abrégés respectivement en I, P, et S.

La question cruciale qui se pose est la suivante : quel service Cloud convient le mieux à nos besoins spécifiques ?

Si notre objectif est simplement d'utiliser une machine virtuelle (VM) et que nous disposons de l'expertise nécessaire pour installer et gérer les logiciels, alors le choix logique serait IaaS.

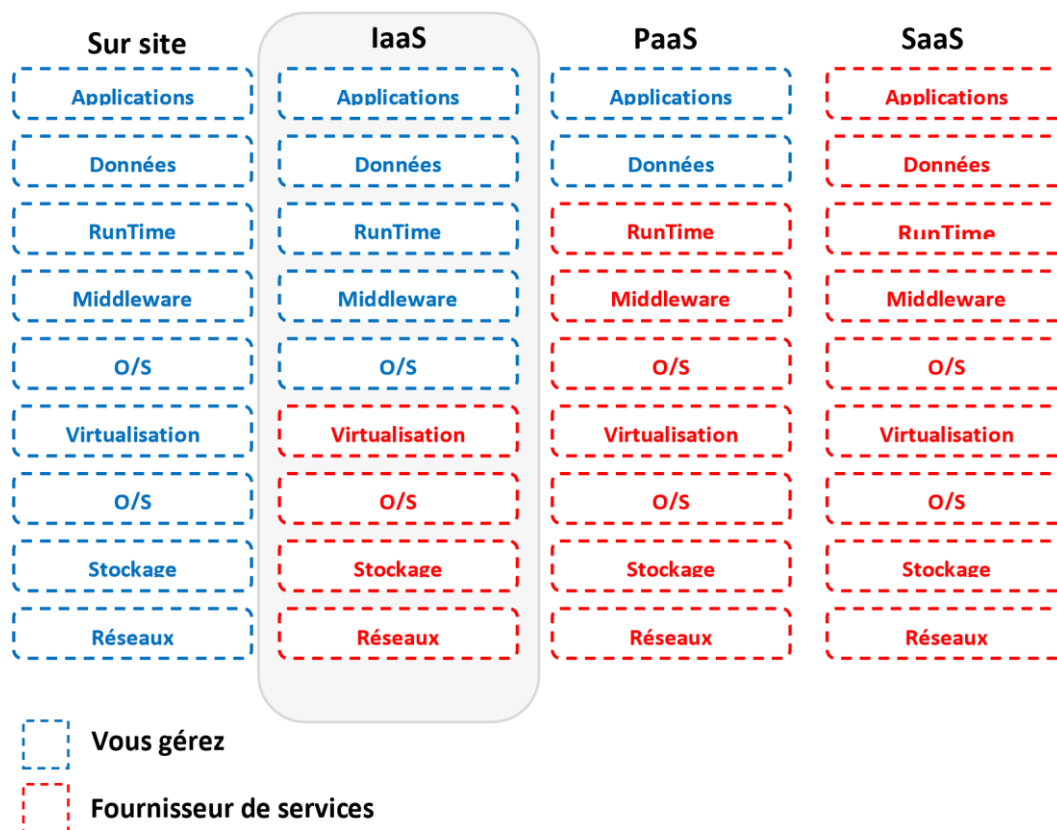
En revanche, si nous cherchons uniquement une plate-forme ou une interface pour développer des applications ou exécuter des programmes, alors PaaS serait l'option à privilégier.

Enfin, si notre besoin se résume à un produit fini hébergé dans le Cloud, accessible via Internet avec un simple nom d'utilisateur et un mot de passe, alors SaaS s'avère la solution idéale. Avec SaaS, nous pouvons immédiatement personnaliser l'application en fonction de nos besoins spécifiques.

**a *Infrastructure as a Service (IaaS) :***

Le modèle de prestation IaaS offre une infrastructure informatique de base basée sur le principe du paiement à l'utilisation. Il représente un environnement informatique autonome composé de ressources informatiques axées sur l'infrastructure. Ces ressources peuvent être consultées et gérées à l'aide d'interfaces et d'outils basés sur les services Cloud. Cet environnement comprend généralement du matériel, des réseaux, des connexions, des systèmes d'exploitation et d'autres ressources informatiques fondamentales. Contrairement aux environnements d'hébergement ou d'externalisation traditionnels, les ressources informatiques en IaaS sont souvent virtualisées et regroupées en ensembles pour simplifier le dimensionnement initial et la personnalisation de l'infrastructure.

L'objectif principal d'un environnement IaaS est de fournir aux utilisateurs de services Cloud un niveau élevé de contrôle et de responsabilité sur la configuration et l'utilisation de leur infrastructure. Certains des principaux fournisseurs de services IaaS incluent AWS, Azure, et Google. Dans ce contexte, les utilisateurs sont généralement des administrateurs système expérimentés.



**Figure 1- 5:** la différence entre ce que nous gérons et le fournisseur de services gère dans IaaS.

### **b Platform-as-a-Service(PaaS):**

Un fournisseur de services Cloud offre une plate-forme ou un environnement d'exécution prêt à l'emploi pour le développement, les tests et la gestion d'applications. Avec PaaS, vous achetez essentiellement une plate-forme, téléchargez votre code, et commencez à travailler dessus. Cela permet aux développeurs de logiciels de déployer des applications sans avoir à gérer l'infrastructure sous-jacente.

Les raisons courantes pour lesquelles un utilisateur de services Cloud opterait pour un environnement PaaS comprennent les suivantes :

Extension d'environnements sur site vers le Cloud pour des raisons de scalabilité et d'efficacité économique.

Remplacement complet d'un environnement sur site par une solution prête à l'emploi en Cloud.

Transformation en fournisseur de services Cloud, proposant ses propres services Cloud à d'autres utilisateurs de Cloud externes.

En travaillant au sein d'une plate-forme prête à l'emploi, les utilisateurs de Cloud se libèrent de la gestion administrative liée à la configuration et à la maintenance des ressources informatiques sous-jacentes, telles que celles fournies par le modèle IaaS. Cependant, cela signifie également qu'ils ont un contrôle moindre sur les ressources informatiques sous-jacentes qui hébergent et provisionnent la plate-forme. Les produits PaaS sont disponibles avec diverses piles de développement. Par exemple, Google App Engine offre un environnement pour les langages Java et Python.

Les principaux utilisateurs de PaaS sont généralement les développeurs de logiciels, car cela leur permet de se concentrer sur le développement d'applications plutôt que sur la gestion de l'infrastructure.[4]

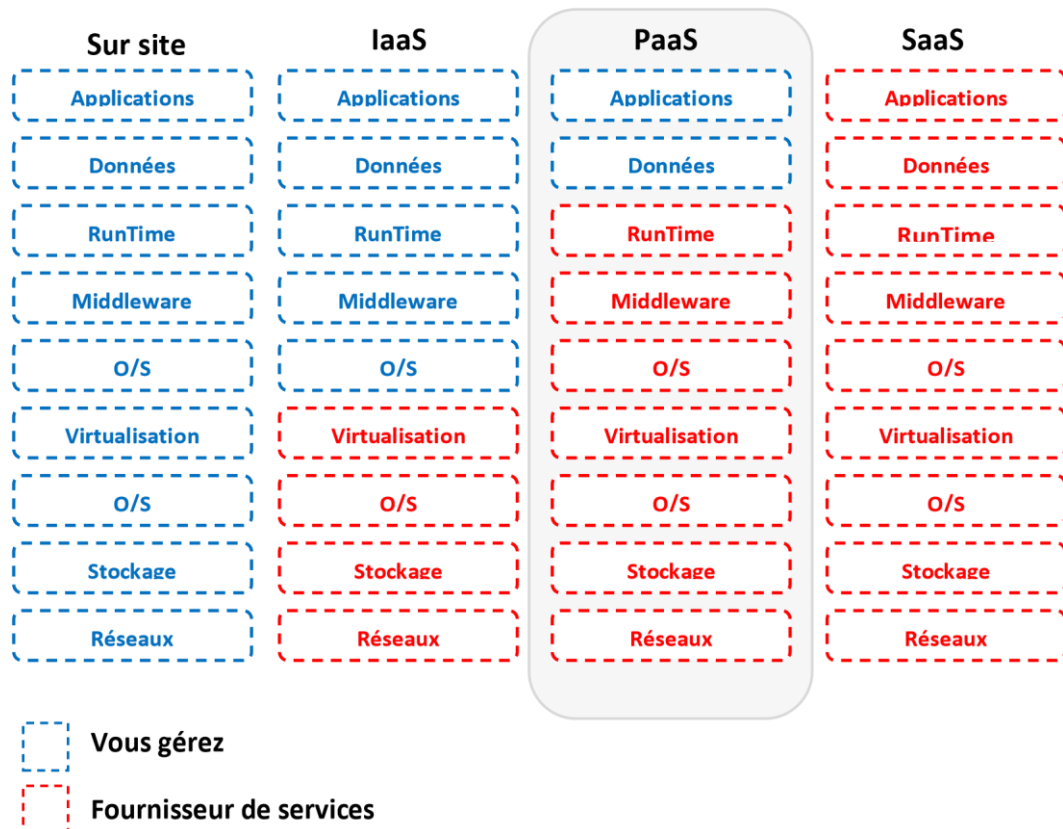


Figure 1- 6: la différence entre ce que nous gérons et le fournisseur de services gère dans PaaS.

**c *Logiciel en tant que service (SaaS) :***

Un logiciel positionné en tant que service Cloud, partagé et mis à disposition comme un "produit" ou un utilitaire générique, représente le profil type d'une offre SaaS. Le modèle de livraison SaaS est généralement utilisé pour rendre un service Cloud réutilisable largement disponible, souvent à des fins commerciales, pour une gamme de consommateurs de Cloud. Un marché entier gravite autour des produits SaaS, qui peuvent être loués et utilisés à diverses fins, selon des conditions variées.

Les consommateurs de Cloud se voient généralement accorder un contrôle administratif très limité sur une implémentation SaaS. Ce modèle de service est généralement fourni par le fournisseur de Cloud, bien qu'il puisse légalement appartenir à l'entité qui joue le rôle de propriétaire du service Cloud. Par exemple, une organisation agissant en tant que consommateur de Cloud, tout en utilisant un environnement PaaS, peut créer un service Cloud qu'elle décide de déployer dans le même environnement en tant qu'offre SaaS. Dans ce cas, la même organisation assume le rôle de fournisseur de Cloud, car le service Cloud basé sur SaaS est mis à la disposition d'autres organisations qui agissent en tant que consommateurs de Cloud lorsqu'elles utilisent ce service.

En ce qui concerne le SaaS, tout, du matériel au logiciel, est géré par le fournisseur de services. Les utilisateurs paient pour le service via un modèle d'abonnement payant. Dans ce modèle, les utilisateurs finaux sont généralement les clients finaux eux-mêmes. Quelques exemples de produits SaaS bien connus incluent Google Workspace, Dropbox, Salesforce et Cisco WebEx.

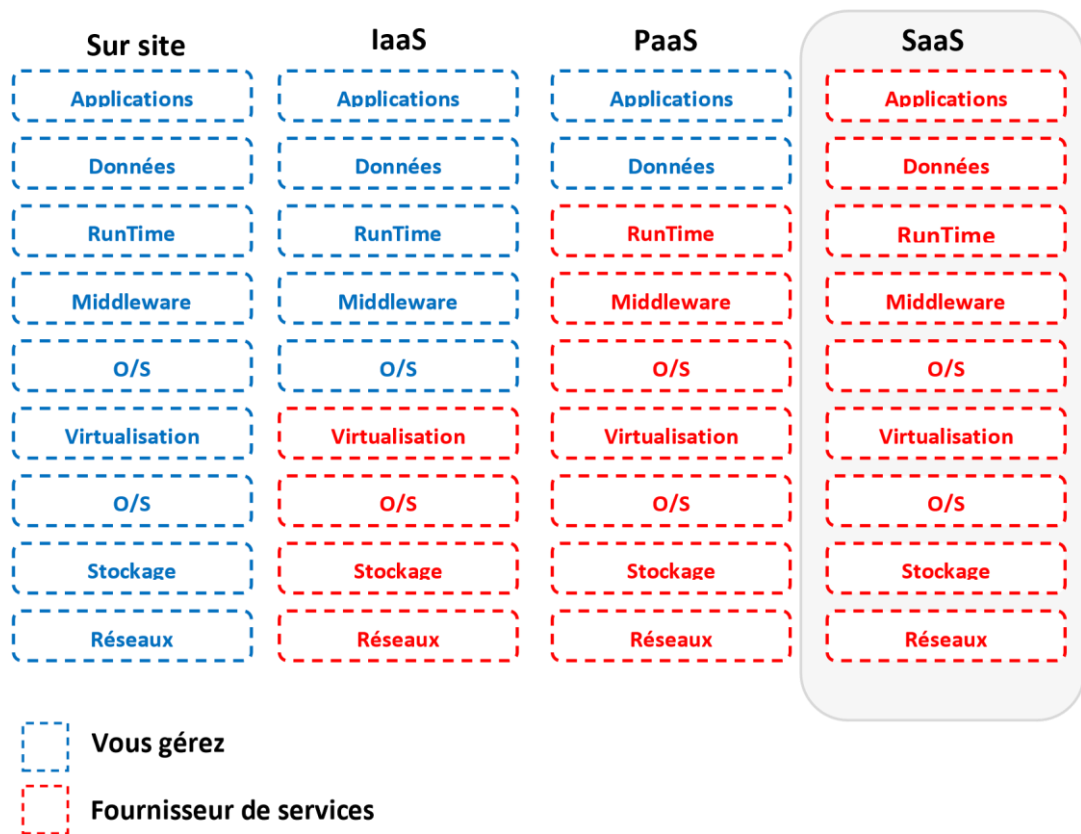


Figure 1- 7: La différence entre ce que nous gérons et le fournisseur de services gère dans SaaS.

### 1.4.3 Différence entre IaaS, PaaS et SaaS :

Base de	IaaS	PaaS	SaaS
<b>représente</b>	Infrastructure as a services.	Platform as a services.	Software as a services.
	IAAS est utilisé par les architectes de	PAAS est utilisé par le développeur.	SAAS est utilisé par l'utilisateur final. <b>Les usages</b> réseau.
<b>Accéder</b>	IAAS donne accès aux ressources telles que les machines virtuelles et le stockage virtuel.	PAAS donne accès à l'environnement d'exécution aux outils de déploiement et de développement pour l'application.	SAAS donne accès à l'utilisateur final.



<b>Modèle</b>	C'est un modèle de service qui fournit des ressources informatiques virtualisées sur Internet.	Il s'agit d'un modèle de cloud computing qui fournit des outils utilisés pour le développement d'applications.	Il s'agit d'un modèle de service dans le cloud computing que le logiciel hôte met à la disposition du client.
<b>Compréhension technique.</b>	Cela nécessitait des connaissances techniques.	Dans lequel vous avez besoin de connaissances sur le sujet pour comprendre la configuration de base.	Il n'y a aucune exigence sur les détails techniques que l'entreprise gère tout.
<b>Popularité.</b>	Il est populaire entre développeur et chercheurs.	Il est populaire parmi les développeurs qui se concentrent sur le développement d'applications et de scripts.	Il est populaire entre le consommateur et l'entreprise, comme le partage de fichiers, le courrier électronique et le réseautage.
<b>Services en nuage.</b>	Services Web Amazon, soleil, vcloud express	Facebook et de moteur recherche google.	M.S office web, applications Facebook et google.
<b>Services aux entreprises.</b>	AWS virtual private cloud.	Microsoft azure.	IBM cloud analysis.
<b>Services infonuagiques externalisés.</b>	Salesforce.	Force.com, Gigaspaces.	AWS, terremark

**Tableau 1- 1:** La différence entre IaaS, PaaS, SaaS.[5]

## **1.5 Les avantages :**

Les entreprises se posent des questions dans ce domaine, qui représente une excellente opportunité dans le domaine des technologies de l'information. C'est une porte d'entrée rapide vers certains des avantages les plus importants qui ont profondément impacté le monde d'Internet.

### **1.5.1 Faible coût d'entretien :**

Le Cloud Computing est probablement la méthode la plus rentable pour l'utilisation, la maintenance et la mise à niveau de l'infrastructure informatique, tout comme l'électricité alimente les horloges et le refroidissement, et les experts en informatique gèrent l'infrastructure.

### **1.5.2 Excellente accessibilité :**

Le Cloud nous permet d'accéder rapidement et facilement aux informations stockées n'importe où, à n'importe quel moment, dans le monde entier, grâce à une connexion Internet. Une infrastructure Cloud sur Internet améliore la productivité et l'efficacité de l'organisation en garantissant que nos données sont toujours accessibles.

### **1.5.3 Fiabilité :**

Traditionnellement, de nombreuses organisations pensent que leur centre de données sur site est plus fiable que l'hébergement ailleurs. Selon l'étude de comScore, 42 % des PME qui n'ont pas encore adopté le Cloud ont exprimé des inquiétudes quant à la fiabilité du Cloud. Cependant, pour leurs homologues qui ont adopté le Cloud, 75 % des PME ont déclaré avoir constaté une amélioration de la disponibilité des services depuis le passage au Cloud. Le changement de perception est crédité d'une meilleure disponibilité des serveurs et du niveau de support fourni par les fournisseurs de Cloud public.

La disponibilité du serveur est vraiment l'une des principales préoccupations de tout centre de données. Si le système tombe en panne, cela pourrait coûter à l'entreprise des milliers, voire des millions de dollars. De nombreux systèmes sur site semblent avoir une disponibilité de pratiquement 100 % puisqu'ils sont "toujours" opérationnels.

Cependant, l'exécution de serveurs 24 heures sur 24, 7 jours sur 7 pour des charges de travail de 8 à 5 est tout simplement un gaspillage, et pourtant, ces systèmes connaissent périodiquement des problèmes d'indisponibilité, de mise à niveau ou de maintenance. Au contraire, la plupart des services Cloud de Microsoft Azure sont assortis d'une garantie SLA de 99,95 %, ce qui est bien supérieur à ce que la plupart des centres de données sur site peuvent espérer offrir.

#### **1.5.4 La vitesse :**

La plupart des services de Cloud Computing sont proposés en libre-service et à la demande, ce qui signifie que de grandes quantités de ressources informatiques peuvent être provisionnées en quelques minutes, souvent en quelques clics de souris. Cela offre aux entreprises une grande flexibilité et allège la pression liée à la planification des capacités.

#### **1.5.5 Échelle globale :**

Les avantages des services de Cloud Computing incluent la possibilité d'évoluer de manière élastique. Dans le langage du Cloud, cela signifie fournir la bonne quantité de ressources informatiques (par exemple, plus ou moins de puissance de calcul, de stockage, de bande passante) au bon moment et à partir du bon emplacement géographique.

#### **1.5.6 Productivité :**

Les centres de données sur site nécessitent généralement beaucoup de "mise en rack et d'empilage" configuration du matériel, correctifs logiciels et autres tâches de gestion informatique chronophages. Le Cloud Computing élimine le besoin d'un grand nombre de ces tâches, de sorte que les équipes informatiques peuvent consacrer du temps à la réalisation d'objectifs commerciaux plus importants.

#### **1.5.7 Performance :**

Les plus grands services de Cloud Computing fonctionnent sur un réseau mondial de centres de données sécurisés, qui sont régulièrement mis à niveau vers la dernière génération de matériel informatique rapide et efficace. Cela offre plusieurs avantages

par rapport à un seul centre de données d'entreprise, notamment une latence réseau réduite pour les applications et de plus grandes économies d'échelle.

### **1.5.8 Sécurité des données :**

De nombreux fournisseurs de Cloud proposent un large éventail de politiques, de technologies et de contrôles qui renforcent globalement votre posture de sécurité, aident à protéger vos données, vos applications et votre infrastructure contre les menaces potentielles et garantissent que les données sont stockées et gérées en toute sécurité.[6]

## **1.6 Les inconvénients :**

Malgré les nombreux avantages du Cloud, il n'est pas sans inconvénients, comme tous les autres programmes électroniques. Ses inconvénients sont :

### **1.6.1 Nécessite une connexion Internet constante :**

Le Cloud Computing dépend entièrement d'une connexion Internet. Pour accéder à toutes les applications et documents, une connexion Internet constante est nécessaire. De plus, une connexion Internet à faible vitesse peut rendre l'utilisation du cloud computing difficile, voire souvent impossible. Il est donc essentiel d'avoir une connexion Internet à haute vitesse pour garantir une expérience optimale.

### **1.6.2 Les données stockées peuvent ne pas être sécurisées :**

Avec le Cloud Computing, toutes vos données sont effectivement stockées dans le Cloud. Cependant, se pose la question de la sécurité : est-ce que vos données confidentielles peuvent être accessibles par des utilisateurs non autorisés ? Toutes ces interrogations indiquent que le Cloud ne peut pas garantir une sécurité totale à 100 %.

La plupart des fournisseurs de services Cloud mettent en place des normes de sécurité et obtiennent des certifications sectorielles pertinentes pour assurer la sécurité de leur environnement Cloud. Néanmoins, le stockage de données et de fichiers critiques de l'entreprise dans des centres de données virtuels peut potentiellement vous exposer à des risques.

### **A Les risques courants sont :**

- Perte ou vol de données.
- Fuite de données.
- Piratage de compte ou de service.
- Interfaces et API non sécurisées.
- Attaques par déni de service.
- Vulnérabilités technologiques, en particulier sur les environnements partagés.

## **1.7 Exemples de Cloud Computing :**

### **1.7.1 Applications sociales :**

Les applications de Cloud social permettent à un grand nombre d'utilisateurs de se connecter entre eux à l'aide d'applications de réseaux sociaux telles que Facebook, Twitter, LinkedIn, etc.

Il existe les applications sociales basées sur le Cloud suivantes :

#### **a Facebook :**

Facebook est un site web de réseau social qui permet aux utilisateurs actifs de partager divers contenus tels que des fichiers, des photos, des vidéos, des statuts, etc., avec leurs amis, leur famille et leurs partenaires commerciaux grâce à son système de stockage en nuage. Sur Facebook, les notifications nous informent toujours lorsque nos amis aiment ou commentent nos publications.

#### **b Twitter :**

Twitter est un site de réseau social qui fonctionne comme un système de microblogging. Il permet aux utilisateurs de suivre des célébrités, des amis, et des proches, tout en recevant des actualités. Sur Twitter, les utilisateurs échangent de courts messages appelés "tweets".

#### **c LinkedIn**

LinkedIn est un réseau social destiné aux étudiants, aux débutants et aux professionnels.

### **1.7.2 Banque, services financiers :**

Les consommateurs stockent des informations financières auprès de fournisseurs de services de cloud computing. Ils utilisent ces services pour conserver leurs dossiers fiscaux en tant que sauvegarde en ligne, par exemple:

- ***Pay Pal :***

PayPal offre la méthode de paiement en ligne la plus pratique grâce à un compte internet sécurisé. PayPal accepte les paiements par cartes de débit, cartes de crédit, ainsi que par les titulaires de comptes PayPal.

### **1.7.3 Soins de santé :**

Grâce au Cloud Computing, les professionnels de la santé peuvent héberger des informations médicales, des analyses, et effectuer des diagnostics à distance. Les soins de santé sont un exemple concret de l'utilisation de l'informatique en nuage, ce qui permet à des médecins du monde entier d'accéder instantanément à ces données médicales pour des prescriptions et des mises à jour plus rapides. Les applications de l'informatique en nuage dans le domaine de la santé englobent la télémédecine, les soins de santé publics et personnels, les services de santé en ligne, ainsi que la bioinformatique.

### **1.7.4 Éducation :**

Ceci est particulièrement bénéfique pour les établissements d'enseignement supérieur, qui peuvent ainsi profiter d'avantages considérables. L'éducation est désormais un domaine où l'informatique en nuage est largement adoptée. Des entreprises telles que Google et Microsoft offrent gratuitement une variété de services aux membres du personnel et aux étudiants de divers établissements d'enseignement. De nombreux établissements d'enseignement aux États-Unis ont opté pour ces services afin d'améliorer leur efficacité et de réduire leurs coûts.

- a. ***Google Apps pour l'éducation:***

Google Apps for Education est la plate-forme la plus largement utilisée pour les e-mails, les calendriers, les documents et la collaboration en ligne, le tout gratuitement sur le Web.

**b. *Tablettes avec Google Play for Education:***

Il permet aux enseignants de mettre rapidement en œuvre les toutes dernières solutions technologiques dans la salle de classe et de les rendre disponibles pour leurs élèves.

**1.7.5 Jeux en ligne :**

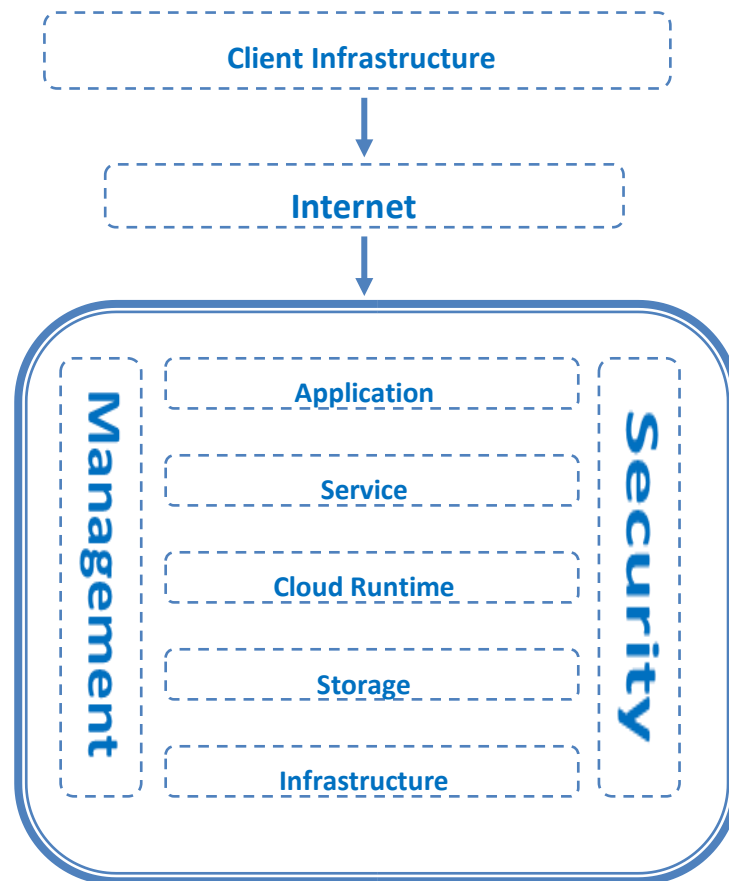
Aujourd'hui, le Cloud gaming est devenu l'un des médias de divertissement les plus essentiels, offrant une variété de jeux en ligne qui s'exécutent à distance depuis le Cloud. Parmi les meilleurs services de jeux en nuage figurent Shadow, GeForce Now, Vortex, Project xCloud et PlayStation Now.

**1.8 Architecture informatique en nuage :**

L'architecture Cloud se divise en deux parties :

- L'extrémité avant (frontend)
- l'arrière-plan (backend)

La figure ci-dessous illustre une vue interne de l'architecture du Cloud Computing.



**Figure 1- 8:** L'architecture du Cloud Computing.

L'architecture du Cloud Computing est une combinaison de SOA (Service-Oriented Architecture) et d'EDA (Event-Driven Architecture). Les composants de l'architecture du Cloud Computing incluent l'infrastructure client, l'application, le service, l'exécution, le stockage, l'infrastructure, la gestion et la sécurité.

### **1.8.1 Front-end :**

Le frontend de l'architecture Cloud représente la facette client du système de Cloud computing. Il englobe toutes les interfaces utilisateur et applications utilisées par le client pour accéder aux services et ressources du Cloud Computing. Un exemple concret serait l'utilisation d'un navigateur Web pour accéder à la plate-forme Cloud.

L'infrastructure client, quant à elle, se réfère aux composants frontaux, comprenant les applications et les interfaces utilisateur essentielles pour accéder à la plate-forme Cloud.



### **1.8.2 Backend :**

Le backend, dans le contexte de l'architecture Cloud, désigne l'infrastructure du Cloud elle-même utilisée par le fournisseur de services. Cette partie du Cloud contient les ressources, les gère et offre des mécanismes de sécurité. Elle comprend également des éléments tels qu'un vaste espace de stockage, des applications virtuelles, des machines virtuelles, des mécanismes de gestion du trafic, des modèles de déploiement, et bien plus encore.

### **1.8.3 Application :**

L'application en backend désigne un logiciel ou une plate-forme auxquels le client accède, fournissant ainsi le service conforme aux besoins du client.

### **1.8.4 Un service :**

Le service en backend englobe les trois principaux types de services Cloud : SaaS, PaaS et IaaS. Il gère également le type de service auquel l'utilisateur accède.

### **1.8.5 Cloud Runtime :**

Le Cloud d'exécution dans le backend fait référence à la fourniture d'une plateforme/d'un environnement d'exécution et d'exécution à la machine virtuelle.

### **1.8.6 Stockage :**

Le stockage en backend se réfère à la fourniture d'un service de stockage souple et extensible, ainsi qu'à la gestion des données qui y sont stockées.

### **1.8.7 Infrastructure :**

L'infrastructure Cloud en backend désigne les composants matériels et logiciels du Cloud, notamment les serveurs, le stockage, les dispositifs réseau, les logiciels de virtualisation, et bien d'autres éléments.

### **1.8.8 La gestion :**

La gestion en backend englobe la gestion des divers composants du backend, tels que les applications, les services, l'infrastructure Cloud, le stockage, ainsi que d'autres mécanismes de sécurité, entre autres.

### **1.8.9 Sécurité :**

La sécurité en backend se réfère à l'implémentation de divers mécanismes de sécurité destinés à protéger les ressources, les systèmes, les fichiers et l'infrastructure Cloud à l'usage des utilisateurs finaux.

### **1.8.10 L'internet :**

La connexion Internet agit comme un lien ou un pont entre le frontend et le backend, établissant ainsi l'interaction et la communication entre les deux.

#### **Les avantages de l'architecture informatique en nuage incluent :**

- Simplification du système global de Cloud Computing.
- Amélioration des capacités de traitement des données.
- Fourniture d'un niveau de sécurité élevé.
- Accroissement de la modularité.
- Amélioration de la reprise après sinistre.
- Offre d'une excellente accessibilité aux utilisateurs.
- Réduction des coûts d'exploitation informatique. [8]

## **1.9 Virtualisation dans le Cloud Computing :**

La virtualisation est une technique qui transforme l'infrastructure physique, telle que le système d'exploitation, les périphériques de stockage, le réseau, etc., en une

infrastructure virtuelle. Elle permet à plusieurs utilisateurs d'exécuter simultanément plusieurs logiciels et applications sur le même serveur.

La virtualisation est l'un des composants essentiels du Cloud Computing. Par exemple, si vous souhaitez créer un Cloud privé, vous aurez besoin d'un logiciel de virtualisation pour créer une infrastructure virtuelle comprenant des réseaux, des serveurs, du stockage, etc. La virtualisation permet le partage des mêmes ressources entre plusieurs utilisateurs, ce qui contribue à réduire les coûts du Cloud Computing, à maximiser l'utilisation des serveurs, à améliorer l'accessibilité et à accroître la scalabilité.

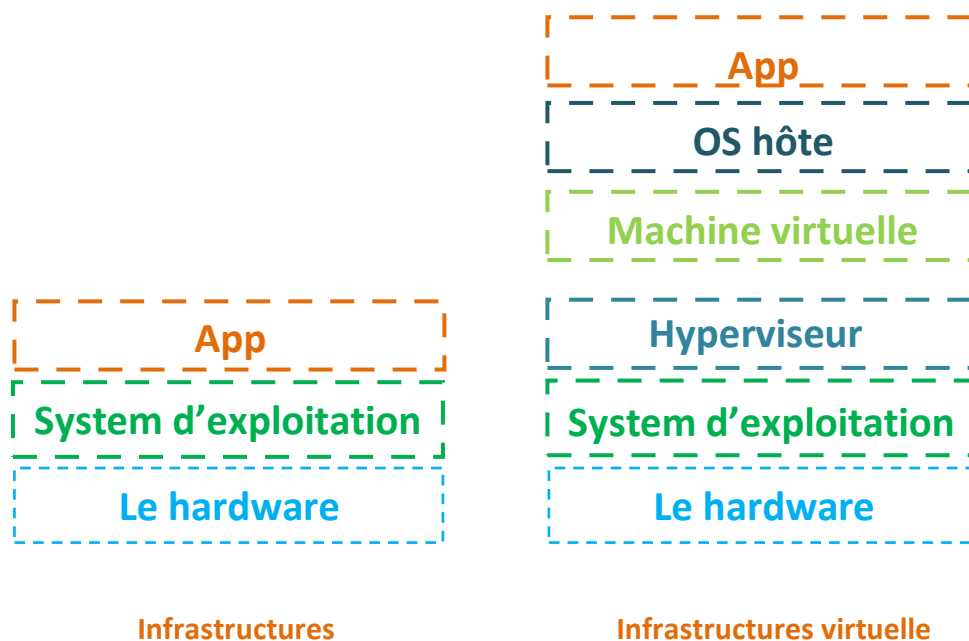


Figure 1-9 : L'architecture du Virtualisation dans Cloud Computing.

### 1.9.1 Types de virtualisation :

Il existe de nombreux types de virtualisation différents, et il est important de comprendre que la virtualisation du Cloud n'est qu'un type de technologie de virtualisation. Le Cloud Computing ne diffère pas fondamentalement de la virtualisation, mais il s'appuie sur cette dernière pour fonctionner. Avant d'aborder la virtualisation dans le Cloud, il convient de mentionner d'autres types de virtualisation :

#### a- Virtualisation des postes de travail :

La virtualisation des postes de travail est généralement réalisée à l'aide d'hyperviseurs, surtout lorsque le système d'exploitation installé sur l'appareil de

l'utilisateur diffère de celui qu'il souhaite utiliser. Par exemple, un utilisateur ayant un ordinateur avec Windows installé peut utiliser un hyperviseur pour virtualiser un poste de travail Linux, lui permettant ainsi de tester des programmes en développement dans un environnement Linux.

**b- Virtualisation des données :**

La virtualisation des données est une approche où les données sont gérées de manière à permettre à l'utilisateur de modifier ou d'accéder aux données sans avoir besoin de connaître précisément leur emplacement ou leur format. Les données sont agrégées sans être déplacées ni modifiées dans leur forme originale, ce qui facilite leur accès rapide depuis n'importe quel appareil.

**c- Virtualisation du réseau :**

La virtualisation réseau consiste à regrouper des réseaux physiques en un réseau virtuel géré par un logiciel, plutôt que par des équipements matériels. Toutes les composantes physiques du réseau, tels que les commutateurs et les routeurs, sont consolidées, et leurs ressources peuvent être assignées dynamiquement aux utilisateurs ou aux dispositifs du réseau en fonction des besoins. Cette opération est réalisée au moyen d'un système central de gestion du réseau virtuel. Un exemple courant de réseau virtuel est le VLAN (Virtual Local Area Network). Un VLAN rassemble plusieurs périphériques réseau au sein d'un même groupe, simulant ainsi un réseau local (LAN), même si ces périphériques ne sont pas physiquement situés à proximité les uns des autres.

**d- Virtualisation du stockage :**

La virtualisation du stockage est le processus de regroupement d'un ensemble de dispositifs de stockage physiques en une seule unité, semblable à un seul périphérique. Un type couramment utilisé de stockage virtuel est appelé réseau de stockage ou SAN (Storage Area Network). La virtualisation du stockage permet aux applications et aux serveurs d'accéder aux données stockées sans avoir besoin de connaître leur emplacement physique ou virtuel. Cela facilite la sauvegarde et le déplacement des données entre différents emplacements, tout en améliorant l'accessibilité aux données.

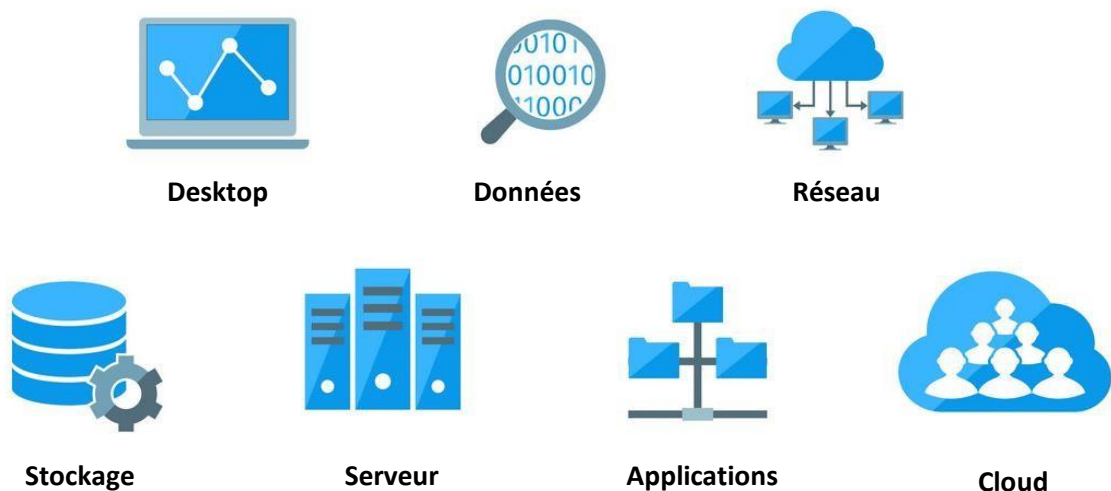
### **e- Virtualisation de serveur :**

Cela fait référence à la possibilité de stocker plusieurs serveurs virtuels sur un seul serveur physique. Au lieu d'acquérir davantage de serveurs physiques, cette approche permet d'économiser de l'espace dans une salle ou un centre de données en virtualisant plusieurs serveurs et en les hébergeant sur une seule machine. De plus, cela facilite l'allocation et la modification des ressources physiques entre différents serveurs selon les besoins. La mobilité des serveurs virtuels est également simplifiée, car il est possible de les déplacer facilement d'un serveur hôte à un autre. Pour en savoir plus sur la virtualisation de serveur, vous pouvez consulter mon guide détaillé sur ce sujet.

### **f- Virtualisation des applications :**

Cela désigne le stockage virtuel d'une application sur un serveur, avec un accès depuis l'appareil de l'utilisateur via ce serveur, au lieu d'une installation directe sur l'appareil. Cela signifie que les utilisateurs n'ont pas besoin d'accéder à un ordinateur spécifique pour utiliser une application, car ils peuvent y accéder depuis n'importe quel appareil ayant une connexion au serveur (par exemple, via Internet). Cette approche élimine également la nécessité d'avoir suffisamment d'espace de stockage sur l'appareil pour l'installation de l'application, car celle-ci est hébergée ailleurs sur le serveur.[9]

## **Types de Virtualisation**



**Figure 1- 10:** Types de virtualisation.

## **1.10 Cloud service :**

### **1.10.1 Openstack :**

OpenStack est un ensemble de modules logiciels, appelés projets, qui coopèrent pour créer et gérer des infrastructures Cloud. L'installation d'OpenStack au-dessus d'un environnement virtualisé permet de constituer un système d'exploitation Cloud, élargissant ainsi le pool de ressources informatiques disponibles pour des utilisations telles que l'hébergement d'applications ou la gestion de tâches liées au Big Data.

### **1.10.2 IBM Cloud Private :**

IBM Cloud Private est une plateforme d'applications conçue pour le développement et la gestion d'applications conteneurisées en local. Cette plateforme offre un environnement intégré pour la gestion des conteneurs, comprenant un orchestrateur de conteneurs basé sur Kubernetes, un registre d'images privées, une console de gestion, ainsi que des outils de surveillance.

### **1.10.3 Apache CloudStack :**

Apache CloudStack est un logiciel open source conçu pour le déploiement et la gestion de vastes réseaux de machines virtuelles. Il fonctionne en tant que plateforme de cloud computing Infrastructure en tant que service (IaaS) hautement disponible et hautement évolutive. CloudStack est utilisé par plusieurs fournisseurs de services pour proposer des services de cloud public, ainsi que par de nombreuses entreprises pour mettre en place une infrastructure de cloud sur site (privé) ou dans le cadre de solutions de cloud hybrides.

### **1.10.4 Amazon EC2 :**

Amazon Elastic Compute Cloud, également connu sous le nom d'EC2, est un service proposé par Amazon qui permet à des tiers de louer des serveurs pour exécuter leurs propres applications web. EC2 offre la possibilité de déployer des applications de manière évolutive en fournissant une interface web qui permet aux clients de créer des machines virtuelles, appelées instances de serveur. Sur ces instances, les clients peuvent charger et exécuter le logiciel de leur choix. [10]

### 1.10.5 La Comparaison :

avis d'entreprises	Openstack	IBM Cloud Private	Apache CloudStack	Amazon EC2
Notes	8.4	8.1	8.1	9.2
Petite entreprise	19.1%	8.6%	33.3%	44.2%
moyenne entreprise	31.9%	31.4%	29.2%	32.7%
grande entreprise	48.9%	60%	37.5%	23%

**Tableau 1- 2:** La comparaison entre différents programmes d'un Cloud Computing.

### 1.11 Conclusion :

Le domaine du Cloud Computing est très vaste. C'est pourquoi, dans ce chapitre, nous avons introduit les définitions de base du Cloud Computing, en mentionnant son évolution historique et en explorant ses principaux avantages et inconvénients. De plus, nous avons identifié les différents types de services Cloud tels que IaaS, PaaS et SaaS, ainsi que son infrastructure sous-jacente.

En conclusion, nous avons fourni des exemples d'utilisation du Cloud Computing dans divers domaines et effectué une comparaison des programmes les plus populaires dans ce domaine.

# Chapitre 2 Attaques et sécurité du Cloud Computing

---

## 2.1 Introduction :

La sécurité du Cloud englobe un ensemble de tactiques, de procédures et de technologies visant à protéger les données, les applications et les services d'infrastructure contre les menaces et les vulnérabilités, qu'elles proviennent de sources externes ou internes liées à la cybersécurité.

Dans ce chapitre, nous explorerons les méthodes de sécurisation du Cloud, ainsi que les types d'attaques couramment rencontrées, tels que les attaques par déni de service, les attaques de l'homme du milieu et les injections SQL, entre autres. De plus, nous examinerons les logiciels et programmes conçus pour identifier et se prémunir contre ces attaques.

## 2.2 Les attaques et l'impact sur le Cloud Computing :

### 2.2.1 Définition d'une attaque :

Une attaque informatique est une exploitation complète ou partielle d'une vulnérabilité dans un système informatique, généralement menée par un attaquant dans le but de compromettre la sécurité du système. Une attaque peut également entraîner une perturbation du fonctionnement normal du système. Selon une étude menée par l'Université du Maryland, un appareil connecté à Internet est susceptible d'être piraté toutes les 39 secondes, soulignant ainsi la vulnérabilité potentielle de tout dispositif connecté à Internet.

Les motivations derrière les attaques informatiques peuvent être variées, notamment :

- ✓ Obtenir un accès non autorisé au système.
- ✓ Voler des informations confidentielles, sensibles ou personnelles.
- ✓ S'emparer de données bancaires.
- ✓ Perturber le fonctionnement normal d'un service ou d'un système.
- ✓ Collecter des informations sur des tiers.



Les attaques informatiques peuvent avoir diverses origines et sont généralement classées en différentes catégories, telles que :

- ✓ Attaques physiques, incluant le vandalisme, l'extinction manuelle ou les pannes d'électricité.
- ✓ Interception des communications, notamment l'usurpation d'identité, le cyberharcèlement et l'attaque de l'homme du milieu.
- ✓ Ingénierie sociale, comme les cyberarnaques.
- ✓ Intrusions, généralement impliquant des logiciels malveillants (malwares).
- ✓ Attaques de déni de service (DoS ou DDoS), visant à saturer ou à perturber un service ou un réseau.

Il est essentiel de comprendre ces différentes formes d'attaques pour mettre en place des mesures de sécurité adéquates et protéger les systèmes et les données contre de telles menaces. [11]

### 2.2.2 Anatomie d'une attaque :

Dans le contexte des activités de piratage informatique, l'attaque est souvent subdivisée en cinq éléments, communément appelés "les 5 P", qui demeurent inchangés et caractérisent chaque attaque.

- a. **Probe** : C'est l'opération de la collecte d'information sur le système cible. Cette collecte peut se faire à l'aide d'outils déjà disponibles (ou gardés secrets).
  - b. **Penetrate** : Une fois les informations collectées vient la phase de la pénétration du réseau. Nous détaillerons dans les prochains paragraphes les différents types d'attaques.
  - c. **Persist** : Il s'agit de la création à l'intérieur du système pénétré d'un compte super utilisateur pour pouvoir s'y introduire une prochaine fois.
  - d. **Propagate** : Il s'agit de l'étape d'observation du réseau pour déceler ce qui est accessible et ce qui est disponible.
  - e. **Paralyse** : Il s'agit du coup de grâce qui peut s'exprimer, par exemple, par l'usage du serveur pénétré pour attaquer d'autres serveurs, ou tout simplement par la destruction de ses données et de son système d'exploitation.
- [12]

### 2.2.3 Types d'attaques :

Les pirates utilisent une variété de techniques d'attaque. Ces attaques peuvent être divisées en trois familles distinctes :

#### **a Les attaques directes :**

C'est l'attaque la plus simple. Le pirate attaque sa victime directement depuis son ordinateur. La plupart des "script kiddies" utilisent cette technique. En fait, les programmes de piratage qu'ils utilisent ne sont que peu configurables, et un grand nombre de ces programmes envoient des paquets directement à la victime.

#### **b Les attaques indirectes par rebond :**

Cette attaque est très populaire auprès des pirates. En effet, le rebond présente deux avantages :

- Il permet de masquer l'identité du pirate (adresse IP).
- Il utilise le CPU et la bande passante de l'ordinateur intermédiaire pour l'attaque.

Les attaques indirectes par réponse :

Cette attaque offre les mêmes avantages qu'une attaque par rebond du point de vue du pirate. La différence réside dans le fait que l'attaquant envoie une requête à l'ordinateur intermédiaire, et la réponse à cette requête est ensuite redirigée vers l'ordinateur de la victime. [13]

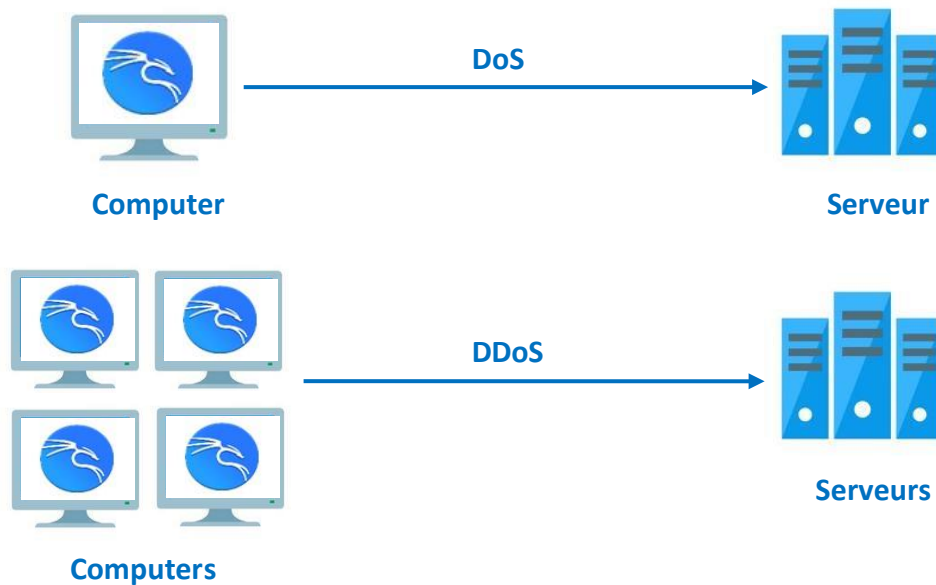
### 2.2.4 Les attaques contre Cloud Computing :

#### **A Les attaques par déni de service (DoS) :**

Les attaques par déni de service (DoS) ou déni de service distribué (DDoS) visent à empêcher l'accès autorisé à une ressource système pour les utilisateurs légitimes, ou à retarder les opérations et les fonctions d'un système, principalement dans le but de priver la ou les victimes de l'accès à une ressource particulière. En général, les cibles de ces attaques sont des

serveurs Web de haut niveau, où l'objectif est de rendre les pages Web hébergées indisponibles sur Internet.

En fin de compte, il y a une différence entre une attaque DoS et une attaque DDoS. Une attaque DoS est menée depuis un seul ordinateur ou serveur, tandis qu'une attaque DDoS implique plusieurs ordinateurs ou serveurs différents. [14]



**Figure 2- 1:** La différence entre le DoS et le DDoS.

Voici les types d'attaques sur DoS :

➤ **SYN Flood :**

Une attaque par déni de service SYN flood (attaque semi-ouverte), comme son nom l'indique, vise à empêcher les utilisateurs d'accéder à un site ou à un service. Avec le protocole TCP, le système de l'utilisateur tente d'établir une connexion avec le site (serveur), cette tentative étant connue sous le nom de "Three-Way Handshake". En envoyant de manière répétée des paquets SYN, l'attaquant est capable d'inonder tous les ports disponibles sur la machine serveur cible. Cela provoque des problèmes pour l'ordinateur cible, qui peut répondre lentement ou cesser de répondre de façon permanente. [15]

➤ **UDP Flood :**

Une attaque UDP Flood est un type d'attaque par déni de service (DoS) qui consiste à envoyer un grand nombre de paquets UDP à un serveur cible dans le but de perturber le traitement et la réactivité de cette machine. Le pare-feu qui protège le serveur peut également tomber en panne en cas d'afflux massif de paquets UDP, ce qui entraîne un déni de service pour le trafic légitime. [16]

➤ **http Flood :**

Une attaque HTTP Flood est un type d'attaque par déni de service distribué (DDoS) qui cible la couche d'application du site Web ou du service visé. En général, les attaques de la couche réseau ont tendance à être de grandes attaques volumétriques qui rendent un site ou un service indisponible en consommant la bande passante disponible, tandis que les attaques de la couche application sont une variété plus sophistiquée qui utilise une stratégie pour épuiser les ressources côté serveur.

Pour ce faire, les attaques HTTP Flood utilisent soit des requêtes GET qui demandent au serveur des composants de contenu statiques, soit des requêtes POST qui demandent des composants de contenu dynamiques. Quel que soit le type de requête utilisé, les attaquants utilisent les attaques HTTP Flood pour solliciter les composants les plus gourmands en ressources du site Web ciblé afin d'épuiser le serveur de la manière la plus efficace possible. [17]

➤ **ICMP Flood :**

Une attaque ICMP Flood (Internet Control Message Protocol), également connue sous le nom d'attaque par Ping Flood, est une attaque par déni de service (DoS) courante dans laquelle un attaquant tente de submerger un appareil ciblé avec des requêtes d'écho ICMP (pings). Normalement, les messages ICMP de demande d'écho et de réponse d'écho sont utilisés pour tester la connectivité et la santé d'un périphérique réseau ainsi que la connexion entre l'expéditeur et le périphérique. En inondant la cible de paquets de demande, le réseau est contraint de répondre avec un nombre égal de paquets de réponse. Cela rend la cible inaccessible au trafic normal. Cette forme d'attaque réussit généralement lorsque l'attaquant dispose d'une bande passante supérieure à celle de sa victime, par exemple, un hacker avec une connexion Internet qui transmet 20 millions de bits par seconde à une victime ayant une connexion Internet de 10 millions de bits par seconde. [18]

➤ **Ping of Death :**

Le Ping of Death (PoD) est un type d'attaque par déni de service (DoS) au cours de laquelle un attaquant tente de planter, de déstabiliser ou de geler l'ordinateur ou le service ciblé en envoyant des paquets malformés ou surdimensionnés à l'aide d'une simple commande "ping". Cette attaque, communément appelée "inondation Ping", vise le système ciblé en envoyant rapidement des paquets ICMP via la commande "ping" sans attendre de réponse.[19]

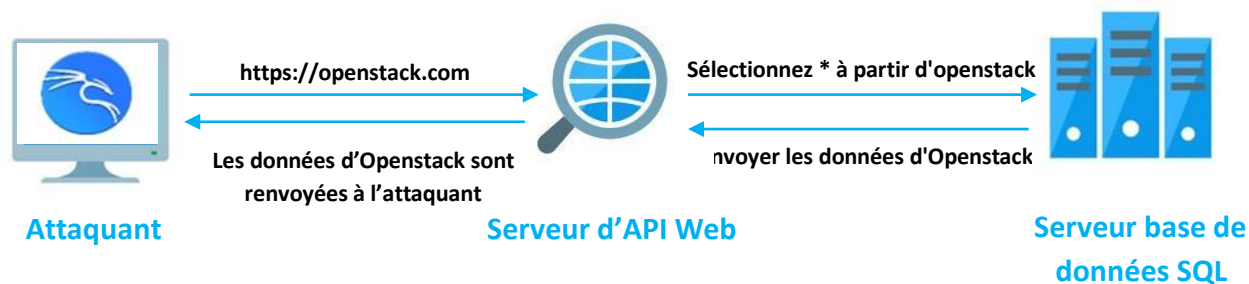
Le tableau suivant présente les différents outils d'attaque par déni de service (DoS) disponibles sur Kali Linux.

Outils d'attaque DoS	À propos de l'attaque
<b>Slowloris</b>	Envoyer le trafic HTTP autorisé au serveur.
<b>Hping3</b>	hping3 est un outil réseau capable d'envoyer des paquets ICMP/UDP/TCP personnalisés et d'afficher les réponses cibles comme le fait ping avec les réponses ICMP.
<b>LOIC</b>	Requêtes UDP, TCP et HTTP au serveur

**Tableau 2-1 :** Les différents outils de L'attaque DoS.

**B Les attaques SQL injection :**

L'injection SQL, également connue sous le nom de SQLI, est une technique d'attaque courante qui exploite un code SQL malveillant pour manipuler la base de données principale, permettant ainsi l'accès à des informations qui n'auraient pas dû être révélées. Ces informations peuvent comprendre divers éléments, tels que des données sensibles de l'entreprise, des listes d'utilisateurs ou des informations privées sur les clients. [20]



**Figure 2- 2:** L'attaque SQL injection.

✓ **Comment fonctionne une attaque par injection SQL ?**

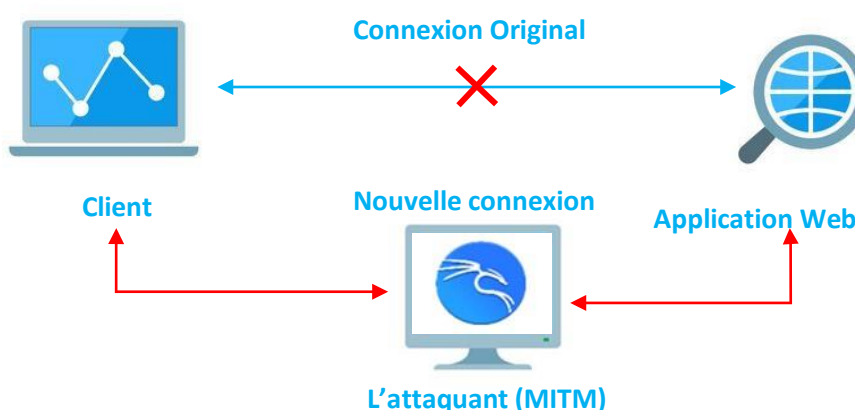
Une attaque par injection SQL vise les vulnérabilités des instructions SQL dynamiques. De manière similaire, une instruction SQL dynamique repose sur un ensemble préétabli de paramètres, tels qu'un formulaire Web, où l'instruction complète n'est générée qu'après que l'utilisateur a rempli ses informations.

Une fois que l'utilisateur a soumis son nom d'utilisateur et son mot de passe, une requête est envoyée au serveur pour récupérer les informations de l'utilisateur depuis la base de données. Lorsqu'une vulnérabilité existe dans une instruction SQL dynamique, un attaquant peut saisir des scripts complexes dans les formulaires pour manipuler les paramètres existants, modifiant ainsi le sens de l'instruction complète. [21]

**C L'attaque de l'homme du milieu:**

Les attaques de type Man-in-the-Middle (MITM) se manifestent sous deux formes principales : l'écoute clandestine et la manipulation. L'écoute clandestine survient lorsqu'un attaquant intercepte un flux de communication de données. Il ne s'agit pas tant d'une attaque directe que d'une fuite d'informations. Un espion peut enregistrer et analyser les données qu'il intercepte. En revanche, une attaque par manipulation nécessite que l'attaquant possède non seulement la capacité de recevoir les données de la victime, mais également la capacité de les retransmettre après les avoir

modifiées, comme illustré dans la figure 2.3.



**Figure 2- 3:** L'attaque de l'homme du milieu.

Les attaques MITM (Man-in-the-Middle) sur un réseau filaire nécessitent généralement un accès au réseau par lequel le trafic de la victime transite. Cela peut impliquer un accès physique à un câble afin de "s'insérer" dans le flux de données. Alternativement, cela peut signifier être connecté au même réseau local (LAN) que la victime et forcer le trafic à transiter par l'ordinateur de l'attaquant. Un attaquant peut accomplir cette redirection de trafic en effectuant une attaque d'empoisonnement ARP, où il falsifie les tables ARP du réseau local pour faire passer le trafic par une machine malveillante.

#### **ARP Poisoning :**

L'ARP (Address Resolution Protocol) est le mécanisme utilisé par les périphériques compatibles Ethernet et IP pour déterminer quelle adresse MAC correspond à une adresse IP spécifique sur un réseau. Lorsqu'un hôte souhaite communiquer avec un autre hôte, il envoie une requête ARP demandant : "Qui possède l'adresse IP 192.168.0.106 ?" Tous les hôtes du réseau local reçoivent cette requête, et le périphérique qui détient l'adresse IP 192.168.0.106 répond en indiquant sa propre adresse MAC. L'hôte initial utilise ensuite cette adresse MAC pour établir la communication avec l'autre périphérique. Il convient de noter que l'ARP, bien que fondamental pour la communication sur un réseau local, peut également être utilisé de manière malveillante dans des attaques, telles que celle que nous allons explorer dans ce projet à l'aide de l'outil Ettercap de Kali Linux . [22]

## 2.3 Sécuriser un serveur Cloud :

Il existe plusieurs méthodes de sécurité pour renforcer la sécurité dans le Cloud. Dans les sections suivantes, nous aborderons ces méthodes et proposerons également d'autres approches qui sont spécifiquement efficaces contre les types d'attaques que nous avons précédemment examinés.

### 2.3.1 Utilisation des clés SSH :

Le SSH (Secure Shell) est à la fois un programme informatique et un protocole de communication sécurisé. Pour sécuriser l'accès aux serveurs Cloud, il est recommandé d'éviter l'utilisation de mots de passe, car ils sont vulnérables aux attaques par force brute et peuvent être compromis facilement. Au lieu de cela, utilisez des clés SSH qui reposent sur la cryptographie à clé publique/privée pour un accès plus sécurisé.

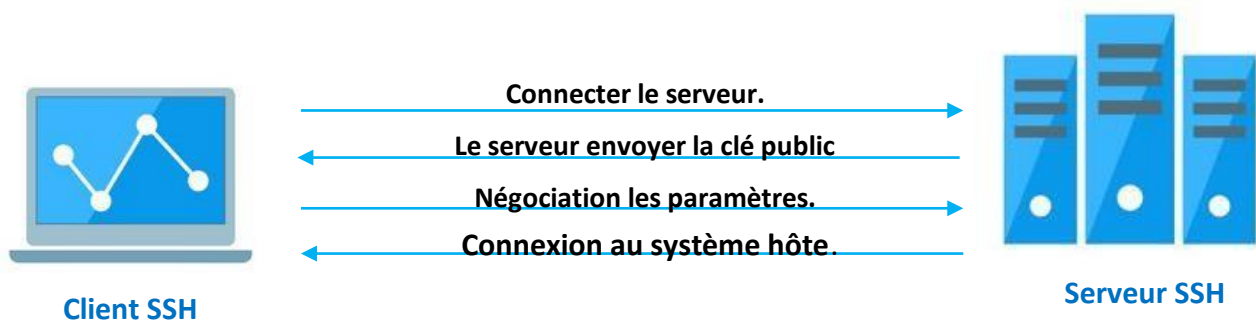


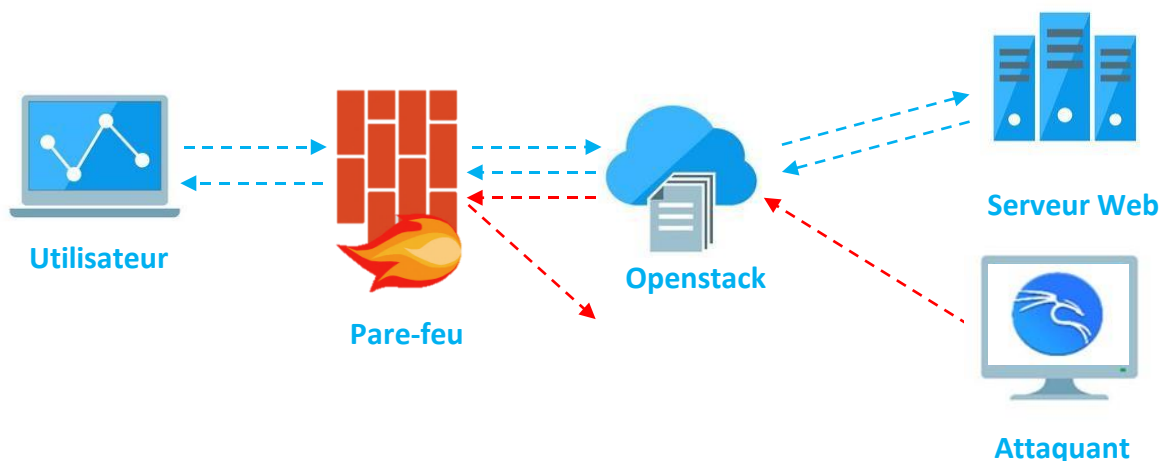
Figure 2- 4: Le protocole SSH.

### 2.3.2 Installer un pare-feu :

Toutes les distributions Linux incluent un logiciel de pare-feu ou permettent de facilement en ajouter un, tel que :

CSF, également connu sous le nom de ConfigServer Security & Firewall, est un pare-feu gratuit qui permet de protéger votre serveur contre différents types d'attaques. Il surveille les tentatives de connexion infructueuses sur des services tels que le serveur SSH, le serveur de messagerie, le serveur FTP, cPanel, DirectAdmin et Webmin, et il peut les bloquer instantanément pour renforcer la sécurité de votre système. [23]

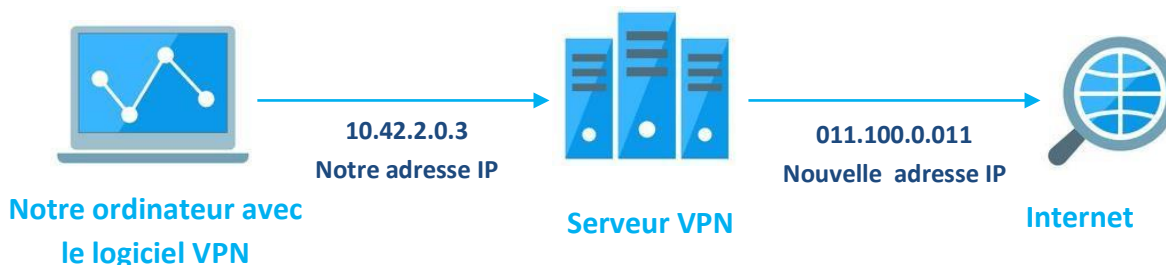




**Figure 2- 5:** Le filtrage d'un trafic entrant pour bloquer les menaces sur notre ordinateur par le Pare-feu.

### 2.3.3 Le VPN :

Un Virtual Private Network (VPN) crée une connexion sécurisée entre vous et Internet. Il vous offre une couche supplémentaire de confidentialité et d'anonymat en attribuant une nouvelle adresse IP.



**Figure 2- 6:** Architecture VPN.

### 2.3.4 Utiliser Le Protocole TLS :

Le TLS (Transport Layer Security) est un protocole de chiffrement qui permet de sécuriser les communications sur Internet. Il existe des situations où une sécurité renforcée est nécessaire pour garantir la confidentialité et l'intégrité du trafic réseau dans un déploiement OpenStack. Cette sécurisation est généralement configurée en utilisant des mesures cryptographiques telles que le protocole TLS. Il ne suffit pas de se fier uniquement à la séparation des zones de sécurité pour assurer la protection. En cas d'accès d'un attaquant à l'hyperviseur, aux ressources de l'hôte, à un point de

terminaison d'API ou à tout autre service, il ne devrait pas être en mesure d'injecter, de capturer facilement des messages ou des commandes, ou d'affecter autrement les capacités de gestion du cloud.

### 2.3.5 Système de détection d'intrusion (IDS) :

Un système de détection d'intrusion (IDS) est un dispositif de surveillance qui identifie les activités suspectes et génère des alertes en cas de détection. Les systèmes de détection d'intrusion sont conçus pour être déployés dans divers environnements, et comme de nombreuses solutions de cybersécurité, un IDS peut être basé soit sur l'hôte, soit sur le réseau.

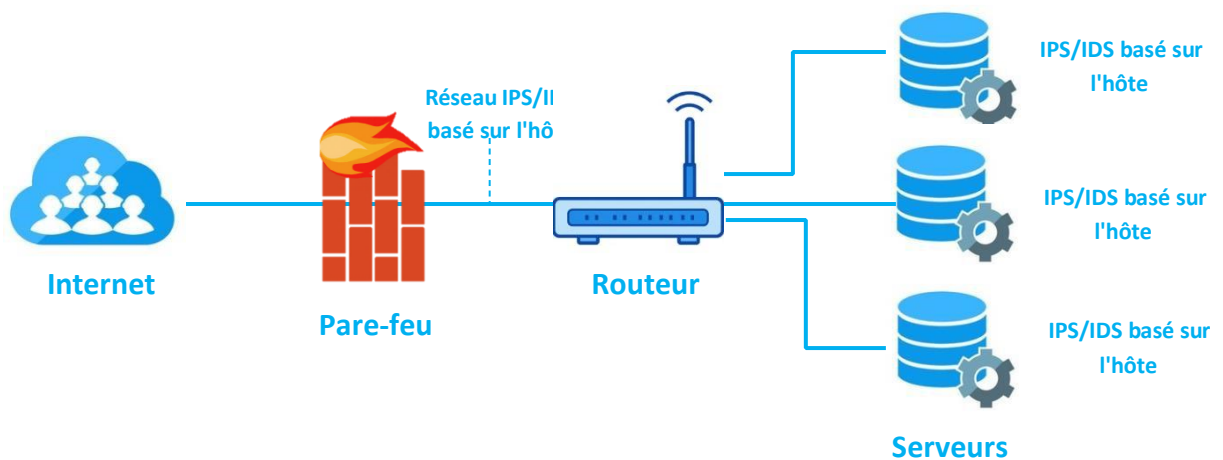


Figure 2- 7: L'architecture d'IPS/IDS.

#### A Différents types d'IDS :

Les systèmes IDS sont principalement de trois types :

➤ **Système de détection d'intrusion réseau (NIDS) :**

Le NIDS (Network Intrusion Detection System) est conçu pour surveiller l'ensemble d'un réseau protégé. Il dispose d'une visibilité sur l'ensemble du trafic circulant sur le réseau et prend des décisions en se basant sur les métadonnées et le contenu des paquets.

➤ **Système de détection d'intrusion basé sur l'hôte (HIDS) :**

Le HIDS (Host Intrusion Detection System) est déployé sur une machine particulière et est conçu pour la protéger contre les menaces internes et externes. Un tel IDS peut avoir la capacité de surveiller le trafic réseau entrant et sortant de

la machine, d'observer les processus en cours d'exécution et d'inspecter les journaux du système. [25]

➤ **système de prévention des intrusions (IPS) :**

L'IPS, parfois appelé système de prévention de détection d'intrusion (IDPS), est une technologie de sécurité réseau et un élément essentiel de tout système de sécurité d'entreprise. Il surveille en permanence le trafic réseau afin de détecter toute activité suspecte et prend des mesures pour la prévenir.

**B Les alertes IDS :**

Il existe plusieurs méthodes et de nombreux logiciels open source pour capturer et détecter les alertes. Dans les lignes suivantes, je parlerai des règles que nous allons utiliser dans ce projet avec le moteur de sécurité réseau Suricata.

Une règle ou signature comprend les éléments suivants :

- ✓ **L'action** : Détermine ce qui se passe lorsque la règle correspond, les actions valides sont : alert, pass, drop...
- ✓ **L'en-tête** : Définissant le protocole, les adresses IP (source et destination), les ports et la direction de la règle, il y a quatre protocoles de base : TCP,UDP, ICMP, IP.
- ✓ **Les options de la règle** : Définissant les spécificités de la règle.

Voici un exemple sur une règle :

```
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"HTTP GET Request Containing Rule in URI"; flow:established,to_server; http.method; content:"GET"; http.uri; content:"rule"; fast_pattern; classtype:bad-unknown; sid:123; rev:1;)
```

- **Alert** : Correspond à l'action à effectuer en cas de détection.
- **http \$HOME\_NET any ->** : correspond à l'en-tête. C'est cette partie qui permet de définir le sens de l'alerte ainsi que les réseaux et protocoles.
- La dernière partie correspond aux options appliquées à la règle. C'est ici que vous pouvez configurer plus particulièrement la règle en fonction des informations.

## 2.4 Wireshark:

Wireshark est un analyseur de paquets réseau qui présente les données des paquets capturés avec le plus de détails possible, y compris les adresses IP, les ports, etc. Il permet d'analyser le trafic enregistré dans un fichier annexe, mais il est surtout utilisé pour l'analyse en direct du trafic sur des interfaces réseau. Cependant, cette dernière fonction nécessite des droits administrateurs ou l'appartenance à un groupe ayant de tels privilèges [26].

### 2.4.1 Présentation de l'interface Wireshark :

#### a Capture des paquets :

Lorsque vous cliquez sur l'interface, il ouvre une fenêtre divisée en 3 sections, et c'est cette fenêtre qui capture les paquets :

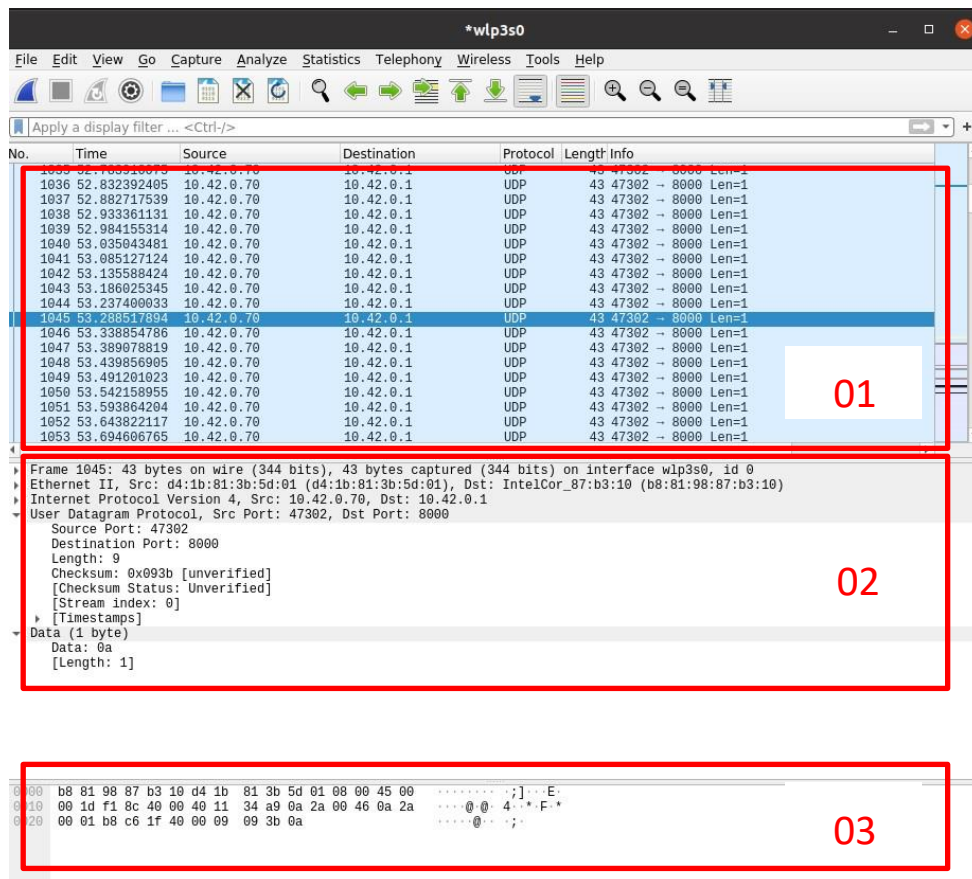
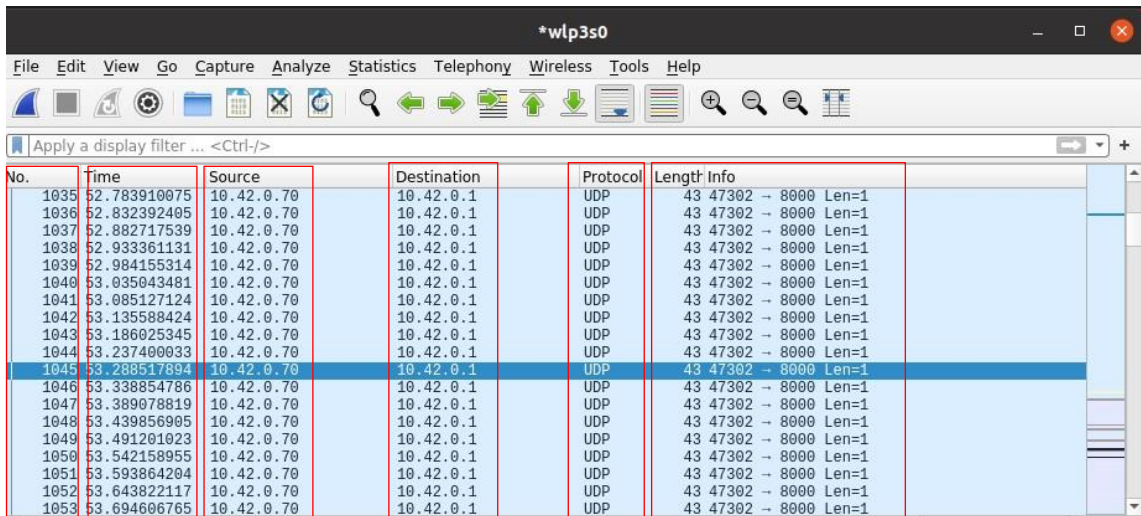


Figure 2- 8: L'interface de Wireshark.

- (1) Affiche l'ensemble des paquets capturés.
- (2) Affiche les détails d'un paquet sélectionné.
- (3) Présente l'ensemble du paquet sous forme octale et ASCII.

## b Liste des paquets capturés :

La section des paquets capturés est divisée en 7 unités :



No.	Time	Source	Destination	Protocol	Length	Info
1035	52.783910075	10.42.0.70	10.42.0.1	UDP	43	47302 → 8000 Len=1
1036	52.832392405	10.42.0.70	10.42.0.1	UDP	43	47302 → 8000 Len=1
1037	52.882717539	10.42.0.70	10.42.0.1	UDP	43	47302 → 8000 Len=1
1038	52.933361131	10.42.0.70	10.42.0.1	UDP	43	47302 → 8000 Len=1
1039	52.984155314	10.42.0.70	10.42.0.1	UDP	43	47302 → 8000 Len=1
1040	53.035043481	10.42.0.70	10.42.0.1	UDP	43	47302 → 8000 Len=1
1041	53.085127124	10.42.0.70	10.42.0.1	UDP	43	47302 → 8000 Len=1
1042	53.135588424	10.42.0.70	10.42.0.1	UDP	43	47302 → 8000 Len=1
1043	53.186025345	10.42.0.70	10.42.0.1	UDP	43	47302 → 8000 Len=1
1044	53.237400033	10.42.0.70	10.42.0.1	UDP	43	47302 → 8000 Len=1
1045	53.288517894	10.42.0.70	10.42.0.1	UDP	43	47302 → 8000 Len=1
1046	53.338854786	10.42.0.70	10.42.0.1	UDP	43	47302 → 8000 Len=1
1047	53.389078819	10.42.0.70	10.42.0.1	UDP	43	47302 → 8000 Len=1
1048	53.439856905	10.42.0.70	10.42.0.1	UDP	43	47302 → 8000 Len=1
1049	53.491201923	10.42.0.70	10.42.0.1	UDP	43	47302 → 8000 Len=1
1050	53.542158955	10.42.0.70	10.42.0.1	UDP	43	47302 → 8000 Len=1
1051	53.593864204	10.42.0.70	10.42.0.1	UDP	43	47302 → 8000 Len=1
1052	53.643822117	10.42.0.70	10.42.0.1	UDP	43	47302 → 8000 Len=1
1053	53.694606765	10.42.0.70	10.42.0.1	UDP	43	47302 → 8000 Len=1

Figure 2- 9: Les paquets en Wireshark.

- (1) Numéro du paquet.
- (2) Le temps.
- (3) L'adresse IP source.
- (4) L'adresse IP destination.
- (5) Le protocole.
- (6) La longueur du paquet.
- (7) Information sur le paquet.

## 2.5 Conclusion :

Dans ce chapitre, nous avons exploré les répercussions des attaques sur le Cloud Computing, ainsi que les actions à entreprendre pour garantir sa sécurité. La sécurité du cloud représente un élément essentiel de la vie d'une entreprise, car elle assure la confidentialité, l'intégrité, la fiabilité et la disponibilité des informations.

# Chapitre 3 La réalisation d'Openstack

---

## 3.1 Introduction :

Après avoir exploré le Cloud Computing, ses avantages et inconvénients, ainsi que les stratégies théoriques de piratage et de protection, ce chapitre se tournera vers une approche plus pratique en se concentrant sur l'une des différentes plateformes cloud, à savoir OpenStack. Nous examinerons en détail sa structure, comment la déployer, et nous discuterons également d'un des programmes open source de protection que nous avons mis en œuvre dans ce projet.

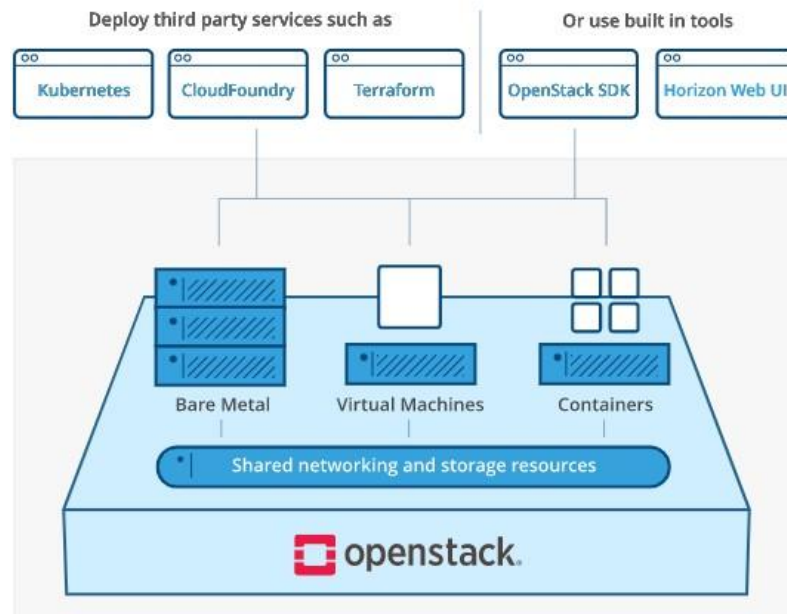
## 3.2 Présentation d'Openstack :

### 3.2.1 Definition :

OpenStack est une plateforme et un ensemble de programmes conçus pour créer un environnement cloud. Cette plateforme gère de vastes pools de ressources de calcul, de stockage et de mise en réseau au sein d'un centre de données. Toutes ces ressources sont gérées et provisionnées via des API avec des mécanismes d'authentification communs.

Un tableau de bord est également disponible, permettant aux administrateurs d'exercer un contrôle total tout en permettant aux utilisateurs de provisionner des ressources via une interface Web conviviale.

Au-delà des fonctionnalités de base d'infrastructure en tant que service (IaaS), OpenStack propose des composants supplémentaires pour l'orchestration, la gestion des pannes, la gestion des services, et d'autres services visant à garantir une haute disponibilité des applications utilisateur. [27]



**Figure 3- 1:** Présentation d'Openstack.

### 3.2.2 Architecture d'OPENstack :

#### a **OpenStack Identity Service (Keystone) :**

Le service OpenStack Identity, également connu sous le nom de Keystone, offre des fonctionnalités d'authentification et de gestion des comptes d'utilisateurs, ainsi que des informations sur les rôles pour l'environnement cloud OpenStack. Il s'agit d'un service essentiel qui assure l'authentification et l'autorisation entre tous les services du cloud OpenStack, et il est généralement le premier service à être installé dans un environnement OpenStack.

#### b **OpenStack Image Service (Glance) :**

OpenStack Image Service, également connu sous le nom de Glance, est un service qui vous permet de vous inscrire, de découvrir et de récupérer des images de machines virtuelles à utiliser dans l'environnement OpenStack. Les images mises à disposition via le service OpenStack Image peuvent être stockées dans divers emplacements backend, allant du stockage du système de fichiers local aux systèmes de fichiers distribués, tels que le Stockage d'objets OpenStack.

**c OpenStack Networking (Neutron) :**

OpenStack Networking est le composant Software Defined Networking (SDN) d'OpenStack, et son nom de projet est Neutron. Avec Neutron, nous avons la capacité de connecter et de gérer divers commutateurs, pare-feu et équilibreurs de charge, ainsi que d'accéder à diverses fonctionnalités telles que le Firewall-as-a-Service. Tout cela est configuré dans le logiciel pour vous offrir un contrôle précis sur l'ensemble de votre infrastructure cloud.

**d OpenStack Compute (Nova) :**

OpenStack Compute, également connu sous le nom de Nova, est le composant qui vous permet d'exécuter plusieurs instances de divers types sur n'importe quel nombre d'hôtes exécutant le service OpenStack Compute. Cela vous offre la possibilité de créer un environnement Cloud hautement évolutif et redondant.

[28]

### 3.3 Environnement :

#### 3.3.1 Environnement matériel :

**a Le serveur :**

Marque de PC	hp
Processeur	Intel core i5-6200U CPU @ 2.30GHZ* 4
RAM	12 GO
Type du système	64 bits
Système d'exploitation	Ubuntu 20.04 LTS
Disque DUR	500.1 GB

**Tableau 3-1:** Les caractéristiques de PC serveur.



### 3.3.2 Travail à faire :

➤ **Partie 1 :**

- ✓ L'installation et la configuration d'openStack.
- ✓ Simulation des attaques : DoS et DDoS attaque, l'homme du milieu, SQL injection et l'Analyse des paquets avec Wireshark.
- ✓ Comparaison les paquets des attaques avec les paquets normaux. **b Partie 2 :**
- ✓ Création des règles de détection en se basant sur les signatures obtenues en utilisant un logiciel open source de détection d'intrusion IDS Suricata.
- ✓ Tester la fiabilité des règles.

Dans notre recherche, nous utilisons les logiciels suivants :

- ✓ OpenStack.
- ✓ Ettercap.
- ✓ Wireshark version 3.0.0 64 bits sur Ubuntu 20.04 ✓ Suricata 1.0.0 sur Ubuntu 20.04.

### 3.3.3 Installation d'Openstack :

L'installation d'OpenStack sur Ubuntu peut être un processus assez complexe, mais cela est devenu plus simple grâce à Devstack. Il existe quelques prérequis de base que vous devez remplir avant de configurer OpenStack sur votre système :

- ✓ Un minimum de 8 Go de RAM
- ✓ Processeur compatible multicœur
- ✓ Au moins 10 Go d'espace libre sur le disque dur
- ✓ Une bonne connexion internet

Il existe également des exigences logicielles supplémentaires, que vous devez remplir :

- ✓ Git (comment installer git sur Ubuntu)
- ✓ Un navigateur Web

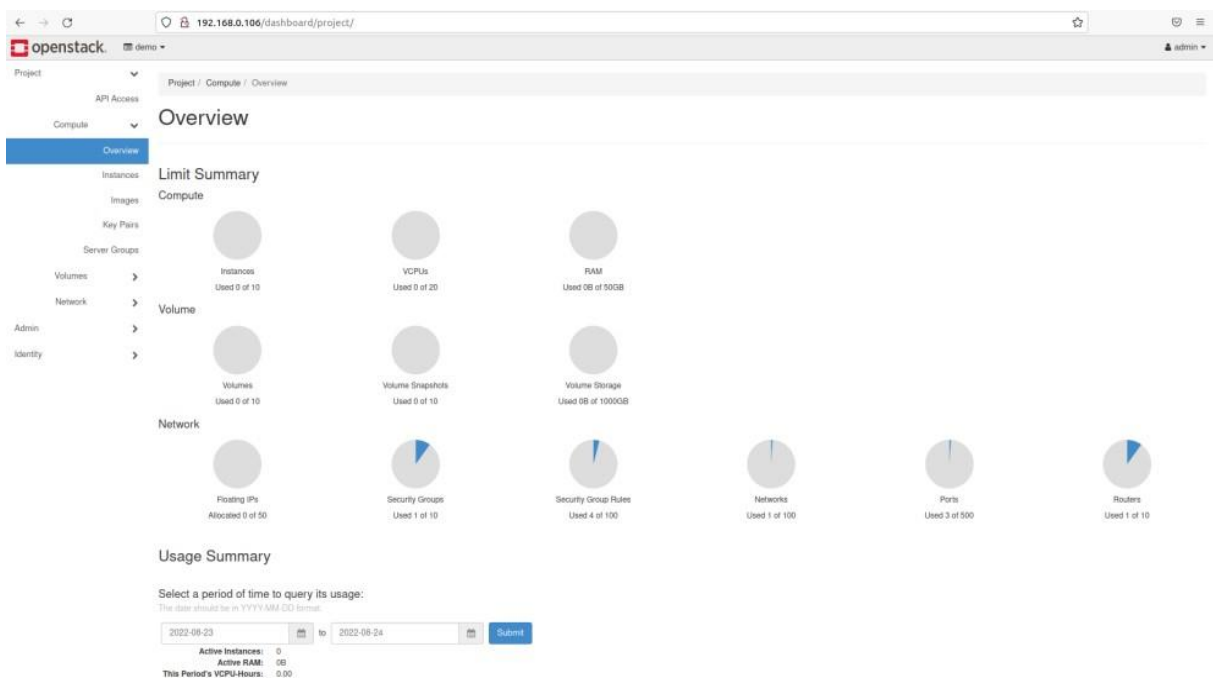
Une fois le téléchargement terminé, vous obtiendrez une adresse IP que vous devrez saisir dans votre navigateur web, ainsi que le nom d'utilisateur et le mot de passe, comme illustré dans l'image ci-dessous :

```
This is your host IP address: 192.168.0.106
This is your host IPv6 address: ::1
Horizon is now available at http://192.168.0.106/dashboard
Keystone is serving at http://192.168.0.106/identity/
The default users are: admin and demo
The password: root
```

**Figure 3- 2:** L'installation d'OpenStack.

### 3.3.4 Création d'un espace Cloud:

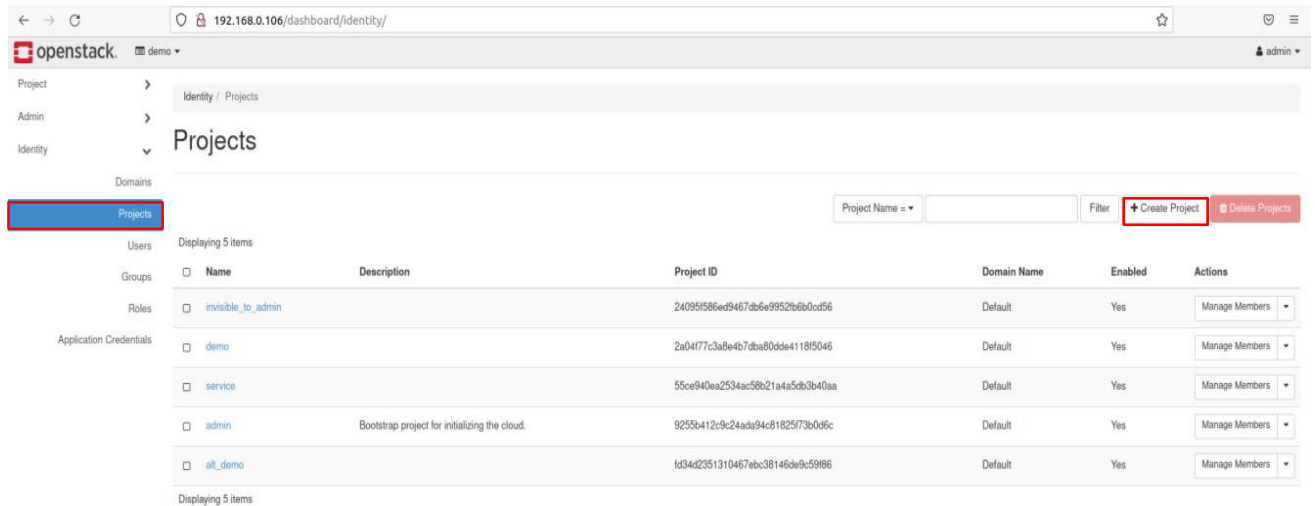
1. Après avoir téléchargé OpenStack, une interface s'affichera, où vous pourrez obtenir un aperçu de l'espace utilisé, du nombre d'instances, et du numéro du routeur tel qu'il apparaît à tous les utilisateurs.



**Figure 3- 3:** L'interface d'OpenStack.

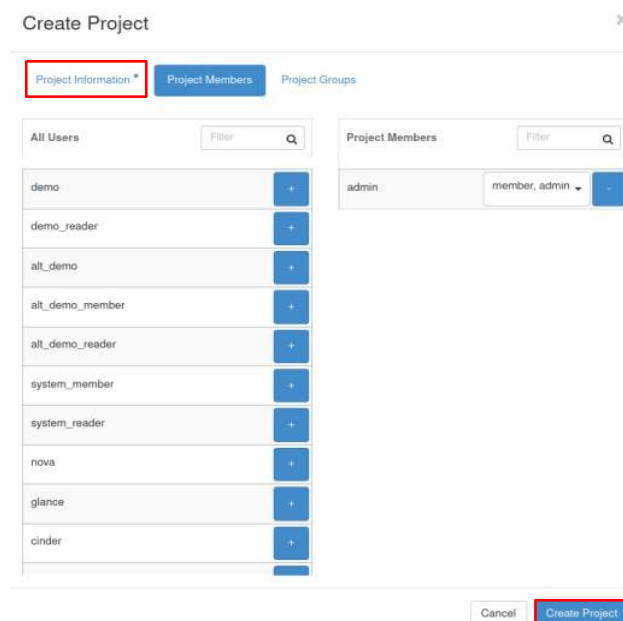
2. La première étape que nous allons suivre consiste à créer un projet et à y ajouter de nouveaux utilisateurs, transformant ainsi ces utilisateurs en clients. Cela permettra de limiter l'accès de certains utilisateurs au tableau de bord principal. Nous expliquerons la méthode dans les étapes suivantes :

- ✓ On clique sur projets dans le champ "Identité" puis sur "créer un projet".



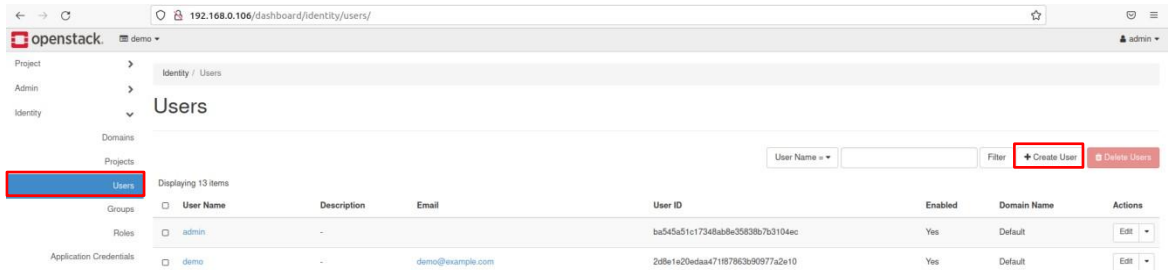
**Figure 3 - 4:** Creation d'un projet.

- ✓ Cette Une fois cette interface affichée, nous allons sélectionner le nom du projet, puis cliquer sur "Créer un projet".



**Figure 3-5 :** Saisie le nom de projet.

- ✓ Maintenant, nous allons créer un utilisateur en allant dans "Utilisateurs", puis en cliquant sur "Créer un utilisateur".

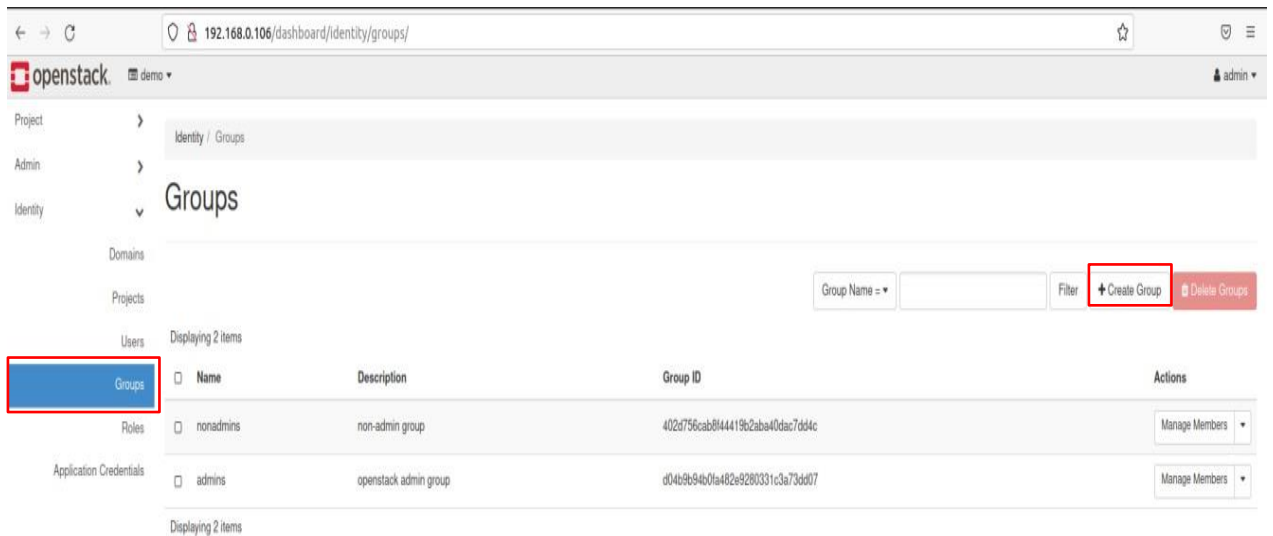


**Figure 3- 6:** Création d'un User.

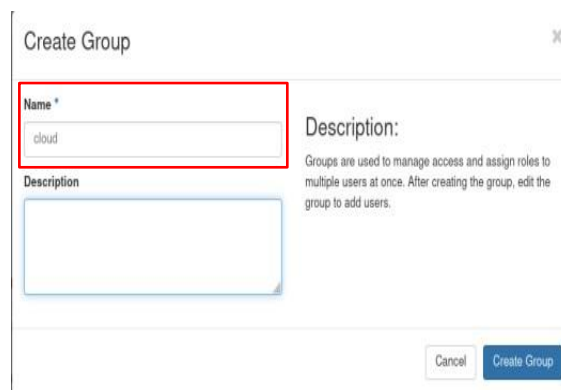
- ✓ Une fois cette interface affichée, nous allons entrer le nom d'utilisateur, sélectionner le projet auquel il sera associé et définir le mot de passe qui lui permettra d'accéder à son espace. Plusieurs utilisateurs peuvent être ajoutés à un projet, mais chaque utilisateur a son propre nom et mot de passe. Les champs qui ne sont pas marqués d'un astérisque (\*) sont facultatifs, tels que l'adresse e-mail. Enfin, nous allons créer un groupe pour cet utilisateur.

A screenshot of the 'Update User' form. The form contains several input fields: 'Domain ID' (default), 'Domain Name' (Default), 'User Name \*' (cloud), 'Description' (empty), 'Email' (cloud@cloud.com), and 'Primary Project' (cloud). The 'User Name \*' and 'Primary Project' fields are highlighted with red boxes. There are 'Cancel' and 'Update User' buttons at the bottom right.

**Figure 3 - 7:** Saisir le nom utilisateur.



**Figure 3 - 8:** Création d'un groupe .



**Figure 3 - 9:** Saisir le nom de groupe.

- ✓ Maintenant, nous allons placer les utilisateurs dans un groupe en cliquant sur le nom du groupe pour afficher cette interface. Ensuite, nous allons cliquer sur "Ajouter des utilisateurs" et sélectionner les utilisateurs que nous souhaitons ajouter.

Filter

Displaying 14 items

<input type="checkbox"/>	User Name	Email	User ID	Enabled
<input type="checkbox"/>	admin		ba545a51c17348ab8e35838b7b3104ec	Yes
<input type="checkbox"/>	demo	demo@example.com	2d8e1e20edaa471f87863b90977a2e10	Yes
<input type="checkbox"/>	demo_reader	demo_reader@example.com	2f2f37bdf2db4647bb2820fe76381ee7	Yes
<input type="checkbox"/>	alt_demo	alt_demo@example.com	708ac2908b8948f9bd5ceb3803dab57	Yes
<input type="checkbox"/>	alt_demo_member	alt_demo_member@example.com	d00bc9e1f3c74fa49e4e69dadfe1436c	Yes
<input type="checkbox"/>	alt_demo_reader	alt_demo_reader@example.com	6551c6e27ca046a7aae2c289a32a9646	Yes
<input type="checkbox"/>	system_member	system_member@example.com	4ef8291cb7cf448e9aad9b589693b0dd	Yes
<input type="checkbox"/>	system_reader	system_reader@example.com	226e9f2d8f5048908e7d1f17c1031af7	Yes
<input type="checkbox"/>	nova		ae9229c46bb34476a2a2479aa794ac16	Yes
<input type="checkbox"/>	glance		12c0a02e4d644cd9ac2d68b267ef8c50	Yes
<input type="checkbox"/>	cinder		a5807698adb049ceb3c3defa5a1d43a40	Yes
<input type="checkbox"/>	neutron		2870d4d76822413da82a131c818e4351	Yes
<input type="checkbox"/>	placement		5d324f236c544663bcf8c7c2f31884a3	Yes
<input type="checkbox"/>	cloud	cloud@cloud.com	9c36e73dca114a949b7916c798640c6b	Yes

Displaying 14 items

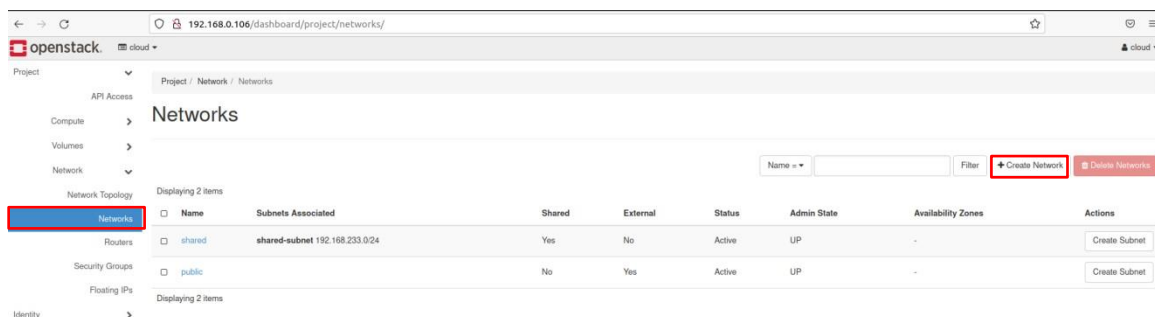
**Figure 3- 10:** Ajouter les utilisateurs dans le groupe.

- ✓ Après avoir terminé ces étapes, nous nous déconnectons de la session d'administration, puis nous nous reconnectons en utilisant le compte utilisateur que nous avons créé. Vous remarquerez une différence dans l'interface entre le compte administrateur et le compte utilisateur. Dans l'interface d'administration, vous verrez 3 éléments : Projet, Admin et Identité, tandis que dans l'interface utilisateur, il y aura seulement Admin et Identité.

The screenshot shows the OpenStack dashboard for a project. The 'Project' dropdown menu is highlighted with a red box. The 'Identity' menu item is also highlighted with a red box. The main content area shows a 'Limit Summary' for Compute resources, including Instances, VCPUs, and RAM. Below that, there is a 'Usage Summary' section with a date range selector and usage statistics for Active Instances, Active RAM, and VCPU-Hours.

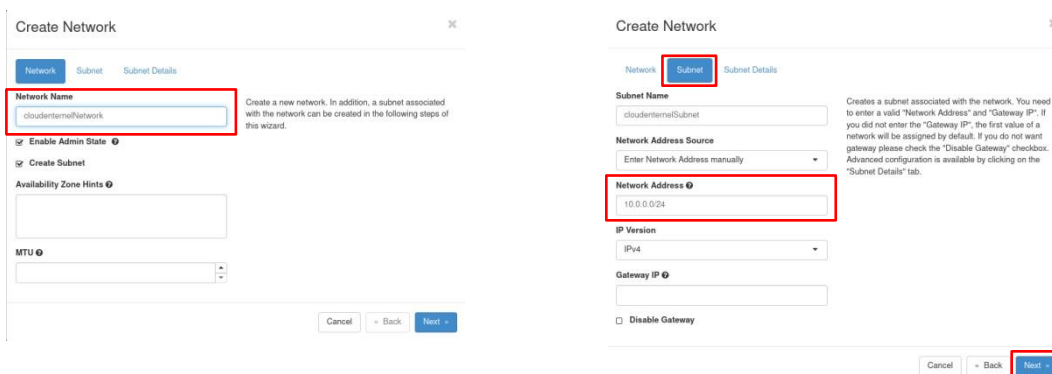
**Figure 3- 11:** L'interface d'utilisateur.

- ✓ Après vous être connecté, la première tâche consistera à créer un réseau. Nous allons créer deux réseaux : le premier sera interne et sera connecté à l'instance, tandis que le second sera externe.



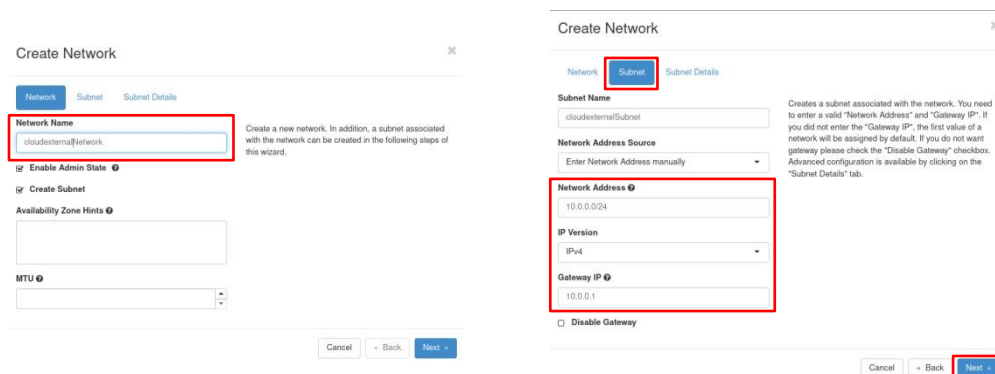
**Figure 3-12:** Création de réseaux.

- ✓ Pour le réseau externe, nous attribuons l'adresse IP :11.0.0.0/24



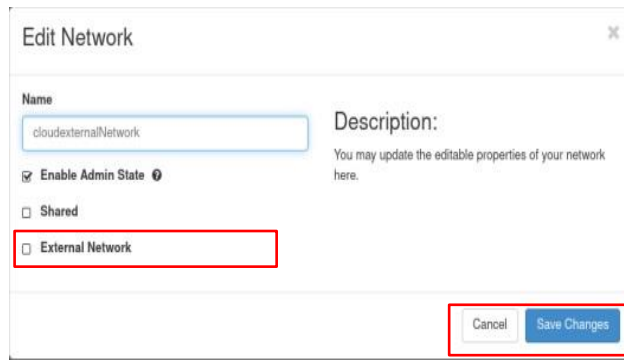
**Figure 3-13:** Création d'un réseau externe.

- ✓ Pour le réseau interne, nous attribuons l'adresse IP :10.0.0.0/24



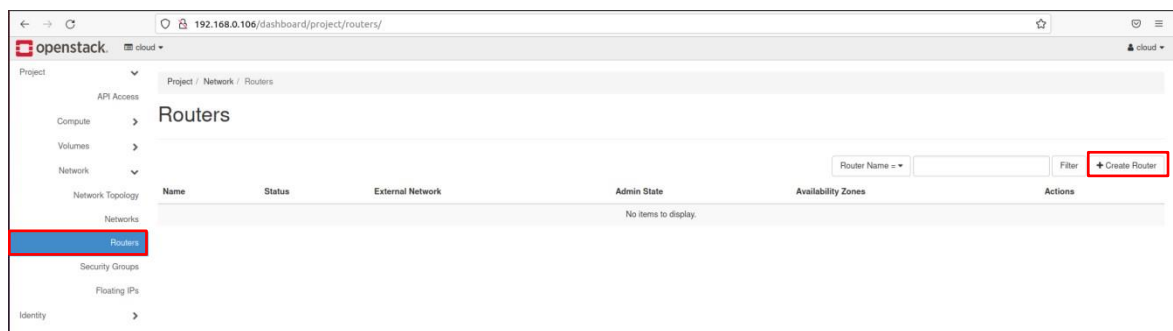
**Figure 3-14:** Création d'un réseau interne.

- ✓ Après avoir créé les deux réseaux internes, nous allons retourner à l'interface d'administration (ADMIN) et les configurer pour devenir des réseaux externes.

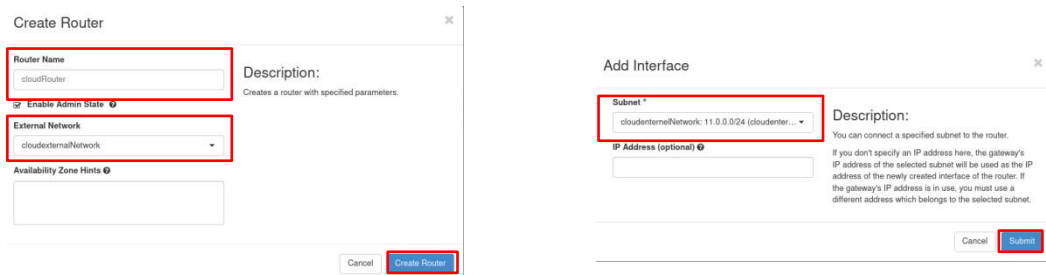


**Figure 3- 15:** La conversation de réseau interne.

- ✓ Nous allons maintenant créer un routeur et le connecter au réseau externe.



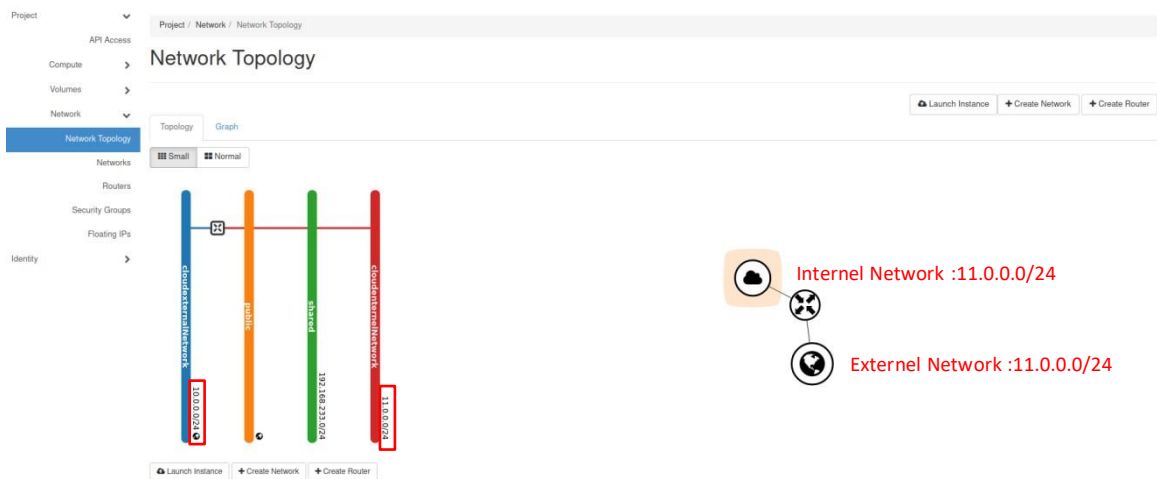
**Figure 3- 16:** Création d'un routeur.



**Figure 3- 17:** Les paramètres de routeur.

- ✓ Après avoir créé le routeur, nous double-cliquons sur son nom pour ajouter le réseau interne. Dans le schéma ci-dessous, nous verrons comment le réseau interne et le réseau externe sont connectés au routeur.



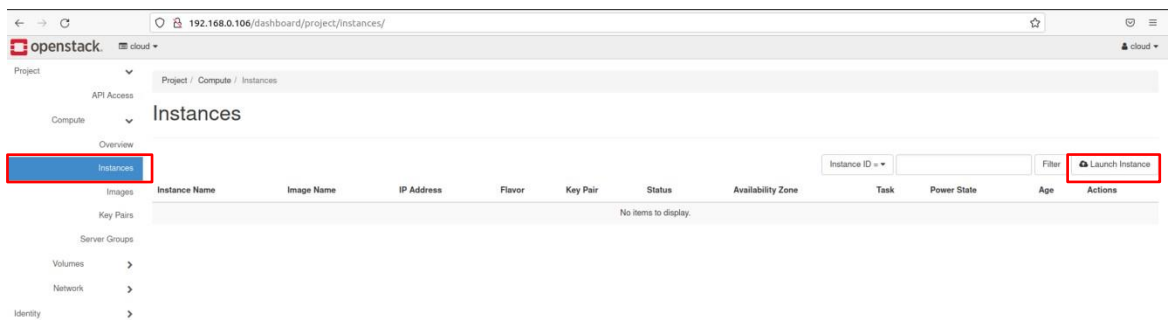


**Figure 3- 18:** Network Topology.

Nous pouvons observer ici l'association du réseau interne et externe avec le routeur :

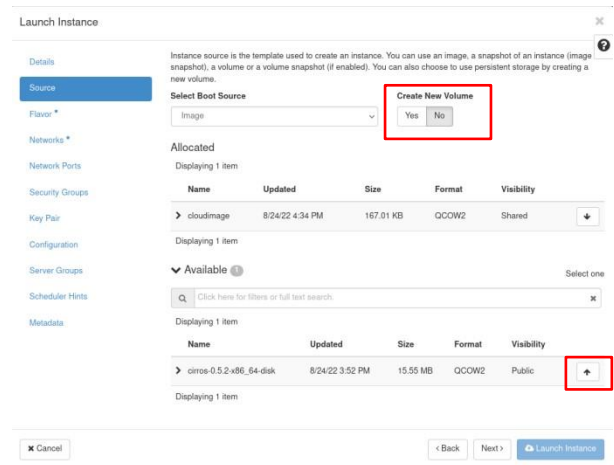
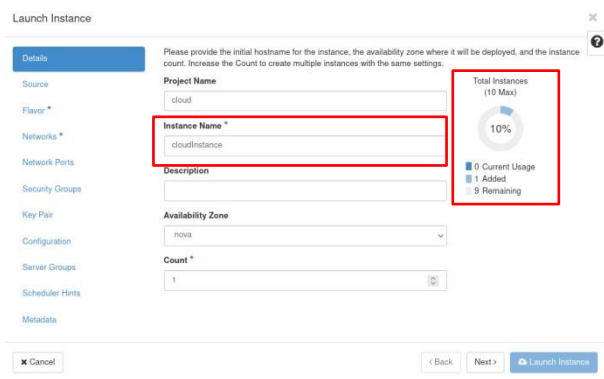
- Réseau Interne : 11.0.0.0/24
- Réseau Externe : 10.0.0.0/24

Enfin, nous allons créer une instance, qui est un lien entre les images et le réseau.



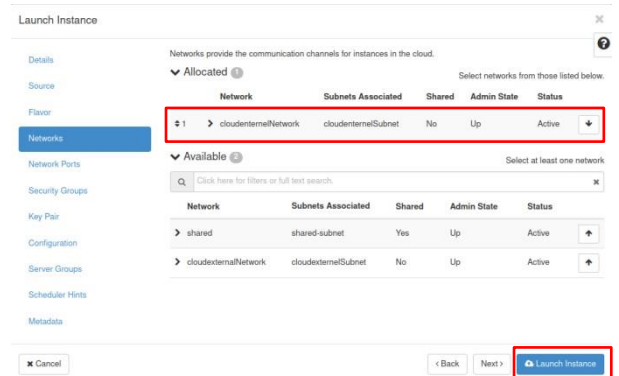
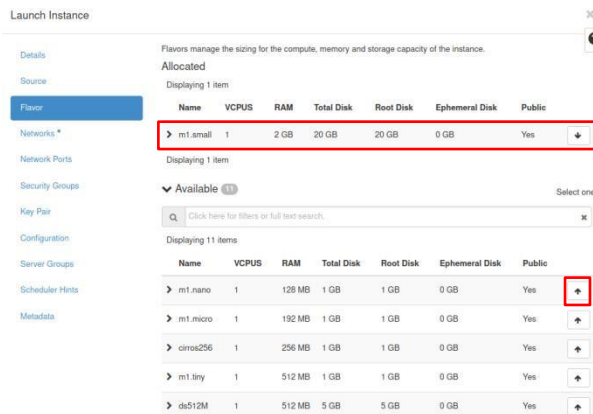
**Figure 3- 19:** Création d'instance.

- ✓ Nous commençons par saisir les informations sur l'instance, telles que son nom. Sur le côté droit, vous verrez le numéro d'instance que nous pouvons attribuer. Ensuite, nous sélectionnons la source, qui est une image préalablement chargée parmi nos images disponibles. En ce qui concerne le volume, nous choisissons de ne pas le spécifier, car cela pourrait compliquer la création de l'instance.



**Figure 3- 20:** Saisir le nom d'instances.

- ✓ Nous allons maintenant choisir le "Flavor" qui inclut la quantité de RAM et d'espace disque total, puis nous sélectionnerons le réseau interne. Ensuite, nous appuyons sur "Lancer l'instance".



**Figure 3- 21:** Les paramètres d'instance.

- ✓ Après avoir créé l'instance, nous double-cliquons sur son nom, puis nous accédons à la console pour nous assurer que l'instance fonctionne. Un tableau de bord s'affiche après avoir entré le nom d'utilisateur et le mot de passe. À partir de là, nous pouvons accéder à la page d'accueil pour vérifier que l'instance fonctionne correctement.

```

login as 'cirros' user. default password: 'gocubsgo'. use 'sudo' for root.
cloudinstance login: cirros
Password:
$
$ pwd
/home/cirros
$ cd ../../
$ ls
bin          etc          initrd.img  linuxrc     mnt         proc        sbin        usr
boot        home         lib         lost+found  old-root    root        sys         var
dev          init         lib64       media       opt         run         tmp         umlinux
$

```

Figure 3- 22: Le terminal d'instance.

- ✓ Nous pouvons observer ici une liaison entre l'instance et le réseau interne, ce qui confirme que nous avons réussi à créer une instance.

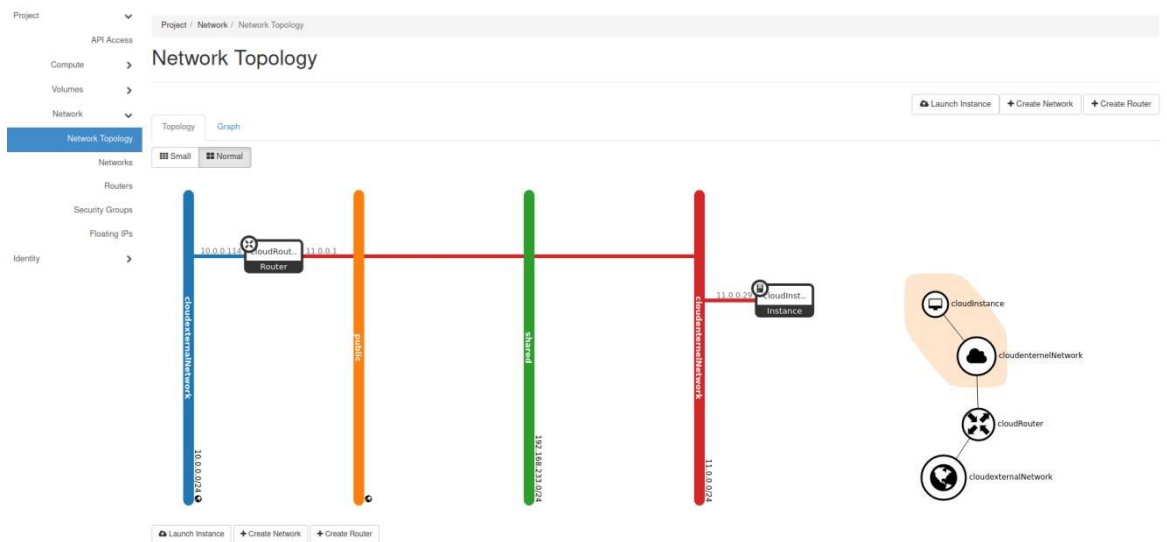


Figure 3- 23: Network Topologie d'instance.

### 3.4 Mise en place d'un IDS :

Dans ce projet, nous avons utilisé le logiciel de détection de menaces open source IDS/IPS Suricata.

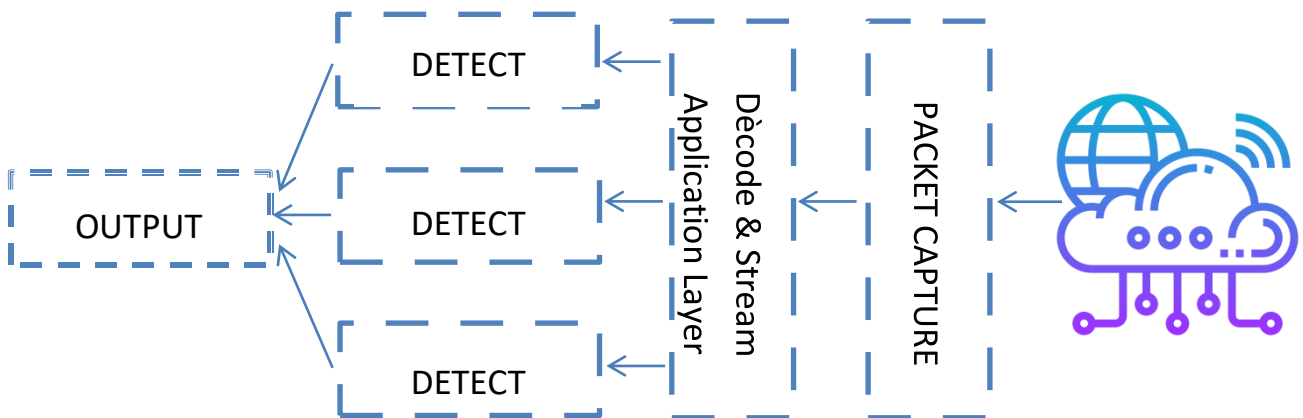
#### 3.4.1 Suricata IDS :

Suricata est un logiciel de détection de menaces réseau open source qui offre des fonctionnalités telles que la détection d'intrusion (IDS), la prévention d'intrusion (IPS), et la supervision de la sécurité réseau (NSM) basée sur des signatures.

Suricata permet l'inspection en profondeur des paquets (DPI) et offre de nombreuses possibilités d'utilisation éthique, notamment la collecte d'informations qualitatives et quantitatives.

Voici la liste des principales fonctionnalités de Suricata :

- ✓ IDS/IPS.
- ✓ Détection automatique de protocole (IPv4/6, TCP, UDP, ICMP, HTTP, TLS, FTP, SMB, DNS).
- ✓ Prise en charge de nombreux formats de sortie, notamment Unified2, JSON, et Prelude.
- ✓ Possibilité d'écrire des scripts en Lua pour l'analyse avancée.



**Figure 3- 24:** L'architecture d'un Suricata IDS.

### 3.4.2 Fonctionnalités :

Suricata analyse le trafic sur une ou plusieurs interfaces réseau en fonction des règles activées et abandonne les paquets en cours s'il détermine qu'une règle correspond à ces paquets. Par défaut, il génère un fichier au format JSON. Ce fichier peut ensuite être utilisé par des logiciels de type Extract-Transform-Load, tels que Logstash, souvent utilisés avec Elasticsearch. [29]

### 3.4.3 La gestion des règles :

L'efficacité du système IDS Suricata dépend de la gestion appropriée des règles. Il est essentiel d'éviter les faux positifs, de maintenir à jour les règles utilisées, et de permettre la détection des menaces récentes.

Les règles Suricata activées par défaut génèrent de nombreuses alertes sous forme de faux positifs. Nous examinons attentivement ces alertes dans le fichier fast.log et désactivons certaines règles. Par exemple, si nous utilisons Skype, nous devons désactiver les règles correspondantes pour éviter de générer des alertes réseau inutiles. Pour renforcer la sécurité de nos installations, nous ajoutons de nouvelles sources de règles ou créons les nôtres.

Dans la gestion des règles, nous pouvons effectuer les actions suivantes :

- ✓ Désactiver certaines règles.
- ✓ Ajouter de nouvelles sources de règles.
- ✓ Mettre à jour les règles manuellement.
- ✓ Mettre à jour automatiquement les règles.

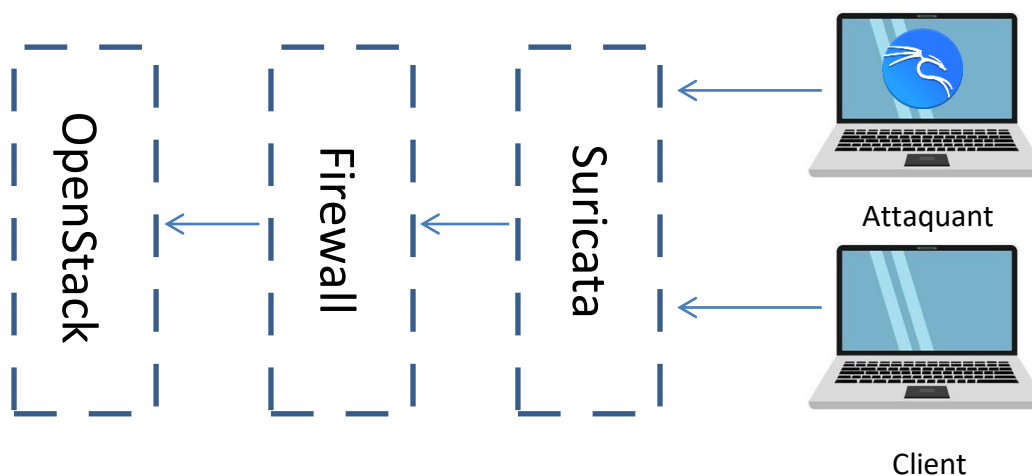


Figure 3- 25: L'emplacement de Suricata.

### 3.5 Conclusion :

Dans ce chapitre, nous avons exploré OpenStack et sa structure. Nous avons créé des utilisateurs et les avons connectés au réseau en créant une instance. Bien que l'installation puisse sembler facile à première vue, nous avons dû surmonter de nombreux défis en cours de route. Chaque fois qu'un problème surgissait, nous devons le résoudre pour progresser vers l'étape suivante.

En fin de compte, nous avons également mis en place le programme Suricata IDS/IPS, qui sera utilisé pour protéger OpenStack dans la prochaine partie de notre projet.

## Chapitre 4 Les attaques et la sécurité dans l'Openstack

---

### 4.1 Introduction :

Dans ce chapitre, nous présenterons une simulation de plusieurs types d'attaques, notamment l'attaque de l'homme du milieu, les attaques par déni de service (DoS) et les attaques par déni de service distribué (DDoS), ainsi que l'injection SQL, qui ont un impact sur la sécurité du cloud. Ensuite, nous nous pencherons sur les aspects de sécurité liés à OpenStack, expliquant comment utiliser des outils pour analyser les vulnérabilités et mener des attaques contre un environnement Cloud.

En fin de compte, nous réfléchirons à des solutions fiables et efficaces pour renforcer la sécurité du Cloud.

### 4.2 Simulation des attaques :

Dans ce projet, nous allons utiliser une machine Kali Linux pour simuler des attaques. Vous trouverez ci-dessous un schéma illustrant cette simulation :

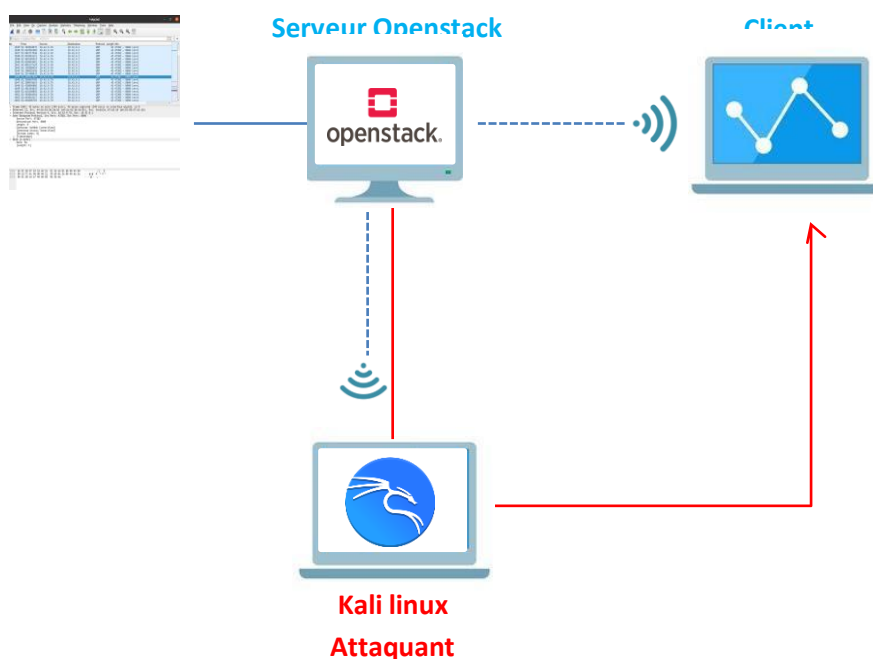


Figure 4- 1: Schéma de simulation d'attaques.

### 4.2.1 Machine Kali linux :

Kali Linux est une distribution open-source basée sur Debian, conçue pour des tests d'intrusion avancés et des audits de sécurité. Cette distribution est axée sur diverses tâches liées à la sécurité de l'information, notamment les tests d'intrusion, la recherche en sécurité, l'informatique légale et l'ingénierie inversée. Elle propose un ensemble d'outils, de configurations et d'automatisations qui permettent à l'utilisateur de se concentrer sur la tâche à accomplir plutôt que sur les activités périphériques. [29]

Parmi les outils disponibles dans Kali Linux que nous avons utilisés figurent :

- ✓ **Nmap** : un utilitaire d'exploration de réseau et d'audit de sécurité prenant en charge diverses techniques d'analyse de port, la détection de versions et l'empreinte TCP/IP.
- ✓ **Wireshark** : un outil de capture et d'analyse de paquets réseau.
- ✓ **Hping3** : un outil réseau capable d'envoyer des paquets ICMP/UDP/TCP personnalisés et d'afficher les réponses cibles, similaire à l'utilitaire ping.
- ✓ **Ettercap** : un outil prenant en charge la dissection active et passive de nombreux protocoles, y compris ceux cryptés, avec de nombreuses fonctionnalités d'analyse réseau et d'hôte.

### 4.2.2 Simulation et détection des attaques :

#### ***A Attaque de l'homme du milieu :***

Dans cette attaque, nous avons utilisé la méthode ARP Poisoning avec les outils Ettercap et Wireshark.

#### ➤ **ARP Poisoning :**

De manière simple, je vais vous expliquer comment fonctionne cette attaque. Supposons que nous ayons un système d'exploitation Ubuntu dont l'adresse MAC est enregistrée auprès du routeur. Lorsque cet Ubuntu envoie un message et que le message revient, il revient par le biais de la passerelle (le routeur) qui connaît



désormais l'adresse MAC de l'appareil Ubuntu. Ainsi, le routeur sait quelles adresses MAC sont associées à quels appareils.

Maintenant, imaginons qu'il y ait un attaquant au milieu, que nous appelons l'homme du milieu. Lorsque l'utilisateur demande une adresse, par exemple, "OpenStack", l'attaquant va tromper l'utilisateur en lui faisant croire que son propre système est le serveur recherché. Ensuite, l'attaquant dirigera le trafic par le biais de son propre système et enverra une demande d'adresse au serveur en se faisant passer pour l'utilisateur. C'est précisément cette manipulation de redirection du trafic en se faisant passer pour une autre entité qui constitue ce que l'on appelle l'empoisonnement ARP.

- ✓ Pour comprendre le fonctionnement de cette attaque, commençons par examiner Kali Linux. Nous allons exécuter la commande indiquée dans l'image ci-dessous pour obtenir l'adresse MAC du système cible. Dans l'image, nous pouvons voir le nom de l'ordinateur, l'adresse IP et l'adresse MAC, et c'est cette dernière information qui revêt une importance particulière pour nous.

```
(kali㉿kali)-[~]
└─$ arp -a
cloud (10.42.0.1) at b8:81:98:87:b3:10 [ether] on wlan0
```

**Figure 4- 2:** L'adresse mac du système cible.

- ✓ Ensuite, nous passerons à la machine cible et exécuterons la même commande pour voir tous les systèmes connectés à cette machine, car elle est considérée comme un serveur. Nous effectuons cette étape car nous prévoyons de surveiller un changement dans la sortie (OUTPUT) après avoir exécuté l'attaque.

```
cloud@cloud:~$ arp -a
gateway (192.168.0.1) at c8:ea:f8:a5:03:80 [ether] on enp2s0
? (10.42.0.231) at 4e:85:b6:86:2b:7e [ether] on wlp3s0
? (10.42.0.70) at d4:1b:81:3b:5d:01 [ether] on wlp3s0
cloud@cloud:~$
```

**Figure 4- 3:** Les adresses mac qui Connecté avec le serveur.

- ✓ Ensuite, nous reviendrons au périphérique Kali Linux, et avant de commencer le processus de piratage, nous devons entrer la commande suivante, qui est responsable de la redirection du trafic.

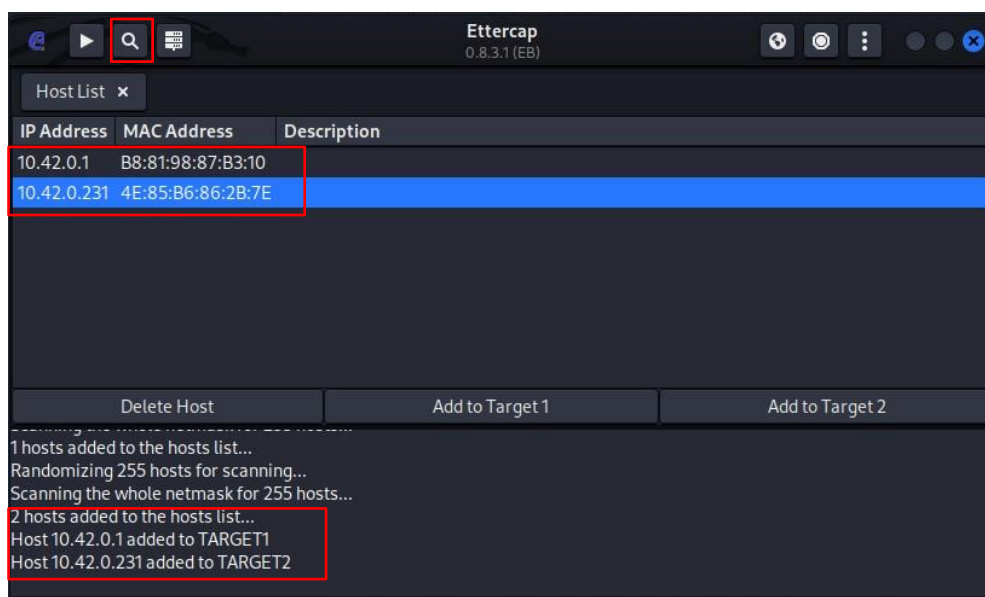
**Sysctl net.ipv4.ip\_forward=1**

- ✓ Maintenant, nous allons ouvrir Ettercap et sélectionner l'interface principale à partir de laquelle nous allons établir la connexion.



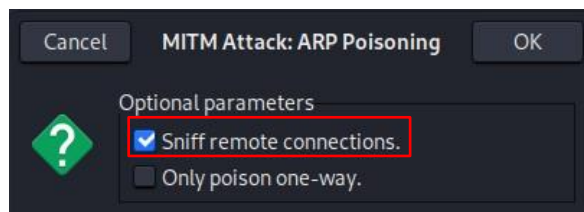
**Figure 4- 4:** L'interface d'Ettercap.

- ✓ La première étape consiste à informer Ettercap des cibles et de la passerelle afin qu'il puisse construire une table ARP. Pour ce faire, nous allons cliquer sur l'onglet de recherche pour extraire chaque hôte. Comme illustré dans l'image, nous observons la présence de deux hôtes. Le premier correspond à Ubuntu, tandis que le second concerne les utilisateurs. À présent, nous avons deux cibles que nous ajouterons ensuite à la liste des cibles (Target).



**Figure 4- 5:** La liste des host.

- ✓ À présent, nous allons lancer l'attaque en accédant au menu, puis en sélectionnant "ARP Poisoning". Une interface apparaîtra en bas de l'écran. Nous choisirons le premier et le second, en les laissant pour les connexions virtuelles à distance.



**Figure 4- 6:** Lancement d'ARP Poisoning.

- ✓ Dans Wireshark, nous pourrions capturer les attaques ARP en utilisant le champ de protocole. Nous allons définir le filtre ARP afin de ne visualiser que les attaques ARP. À ce stade, nous vérifierons si l'attaque fonctionne. Cependant, avant de faire cela, nous retournerons à Ubuntu. Là, nous observerons un changement dans l'adresse MAC de l'utilisateur, qui deviendra identique à celle de Kali Linux.

```
cloud@cloud:~$ arp -a
gateway (192.168.0.1) at c8:ea:f8:a5:03:80 [ether] on enp2s0
? (10.42.0.231) at 4e:85:b6:86:2b:7e [ether] on wlp3s0
? (10.42.0.70) at d4:1b:81:3b:5d:01 [ether] on wlp3s0
cloud@cloud:~$ arp -a
gateway (192.168.0.1) at c8:ea:f8:a5:03:80 [ether] on enp2s0
? (10.42.0.231) at d4:1b:81:3b:5d:01 [ether] on wlp3s0
? (10.42.0.70) at d4:1b:81:3b:5d:01 [ether] on wlp3s0
```

Avant

Après

**Figure 4- 7:** Le changement qui s'est dans l'adresse mac.

- ✓ Maintenant, nous allons retourner sur Wireshark et sélectionner les paquets que nous allons analyser. J'ai opté pour le premier groupe qui est apparu après l'attaque. En examinant les adresses MAC, nous notons une discordance entre l'adresse MAC et l'adresse IP, ce qui indique clairement une attaque ARP.

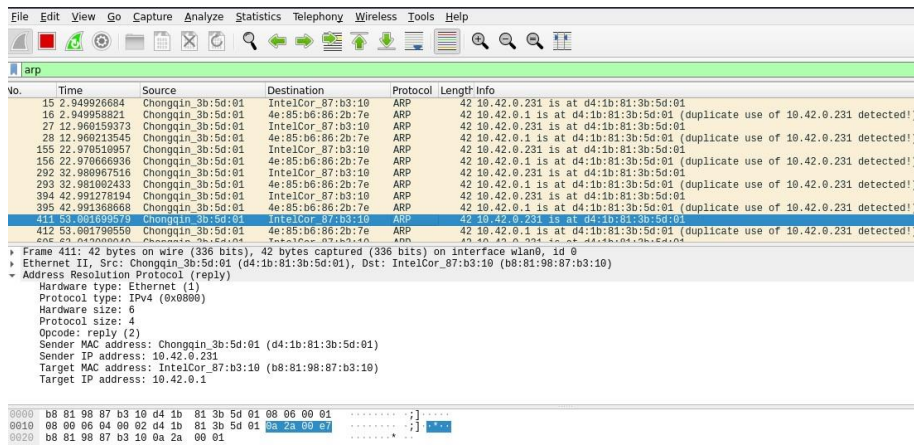


Figure 4- 8: L'analyse des paquets sur wireshark.

- ✓ En retournant à Ettercap, nous constatons qu'il a intercepté le nom d'utilisateur et le mot de passe, ce qui permettrait au pirate d'accéder facilement au compte de l'utilisateur.

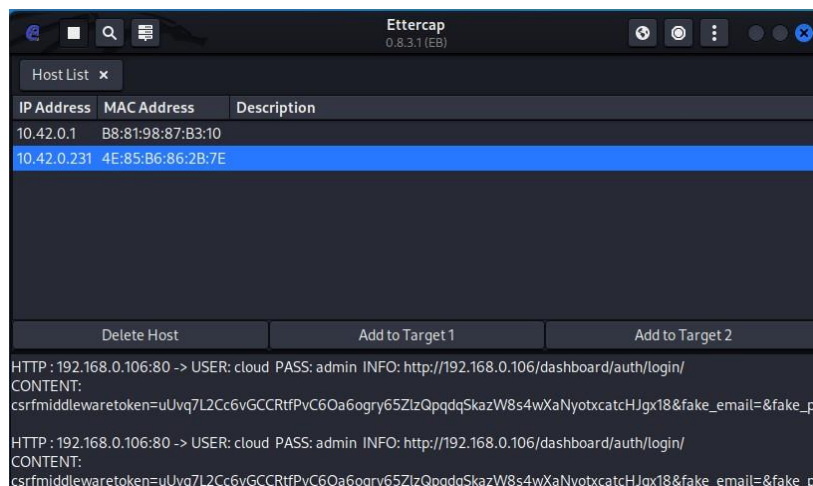


Figure 4- 9: La captation du mot de passe et le nom d'utilisateur.

➤ **Solution entre attaque l'homme de milieu :**

✓ **Active le firewall :**

Tout d'abord, nous allons activer le pare-feu. Cependant, cela entraînera un problème : l'utilisateur ne pourra pas accéder à Openstack car tous les ports seront fermés. Par conséquent, nous devons ouvrir certains ports pour Openstack. Il est important de noter que cette méthode n'est pas très sécurisée, car elle implique l'ouverture de la plupart des ports.

Dans le tableau suivant, nous listerons les ports que nous devons activer :

Le port	Service
80	OpenStack dashboard (Horizon)
8080	OpenStack Object Storage (swift)
443	Tout service OpenStack activé pour SSL, en particulier le tableau de bord d'accès sécurisé.
873	OpenStack Object Storage.
3260	Stockage par Blocs d'OpenStack
3306	La plupart des composants OpenStack.
5672	Service OpenStack de Stockage par Blocs, Réseau, Orchestration, et Compute.

I. **Tableau 4- 1:** Les ports d'Openstack.

Maintenant, nous allons configurer un pare-feu et rédiger des règles pour les ports d'Openstack.

```
root@cloud-HP-ENVY-Notebook:~# ufw status
Status: inactive
root@cloud-HP-ENVY-Notebook:~# ufw enable
Firewall is active and enabled on system startup
root@cloud-HP-ENVY-Notebook:~# ufw status
```

**Figure 4- 10:** L'activation de pare-feu.

```
root@cloud-HP-ENVY-Notebook:~# ufw allow 6000
Rule added
Rule added (v6)
root@cloud-HP-ENVY-Notebook:~# ufw allow 6001
Rule added
Rule added (v6)
root@cloud-HP-ENVY-Notebook:~# ufw allow 6002
Rule added
Rule added (v6)
root@cloud-HP-ENVY-Notebook:~# ufw allow 8004
Rule added
Rule added (v6)
```

**Figure 4- 11:** Création des règles.

8082	ALLOW	Anywhere
9090	ALLOW	Anywhere
8386	ALLOW	Anywhere
8776	ALLOW	Anywhere
8777	ALLOW	Anywhere
8774	ALLOW	Anywhere
6080	ALLOW	Anywhere
6081	ALLOW	Anywhere
9511	ALLOW	Anywhere

**Figure 4- 12:** Les règles sur le pare-feu.

### ✓ Création d'un groupe de sécurité :

Pour gérer les droits des utilisateurs de manière plus efficace et renforcer la sécurité, nous pouvons créer un groupe de sécurité spécifique pour les utilisateurs, configurer les autorisations du groupe et attribuer des ports pour une protection plus efficace.

Pour créer un groupe de sécurité, suivez ces étapes :

- Cliquez sur l'onglet "Groupe de sécurité".
- Sélectionnez "Créer un groupe de sécurité".
- Entrez le nom du groupe, puis cliquez sur "Créer le groupe de sécurité" ("Create Security Group").

Create Security Group
✕

---

**Name \***

**Description:**

Security groups are sets of IP filter rules that are applied to network interfaces of a VM. After the security group is created, you can add rules to the security group.

**Description**

**Figure 4- 13:** Création d'un groupe de sécurité.

- Cliquez deux fois sur le nom du groupe pour ajouter des règles. Ensuite, sélectionnez "Ajouter une règle" ("Add Rule").
- Une fois que vous avez ajouté une règle, spécifiez le port. Par exemple, pour autoriser les connexions SSH entrantes sur le port 22, configurez la règle correspondante.

**Add Rule** [X]

**Rule \***  
Custom TCP Rule

**Description ⓘ**  
[Text Area]

**Direction**  
Ingress

**Open Port \***  
Port

**Port\* ⓘ**  
[Text Input]

**Remote \* ⓘ**  
CIDR

**CIDR\* ⓘ**  
0.0.0.0/0

**Description:**  
Rules define which traffic is allowed to instances assigned to the security group. A security group rule consists of three main parts:  
**Rule:** You can specify the desired rule template or use custom rules, the options are Custom TCP Rule, Custom UDP Rule, or Custom ICMP Rule.  
**Open Port/Port Range:** For TCP and UDP rules you may choose to open either a single port or a range of ports. Selecting the "Port Range" option will provide you with space to provide both the starting and ending ports for the range. For ICMP rules you instead specify an ICMP type and code in the spaces provided.  
**Remote:** You must specify the source of the traffic to be allowed via this rule. You may do so either in the form of an IP address block (CIDR) or via a source group (Security Group). Selecting a security group as the source will allow any other instance in that security group access to any other instance via this rule.

[Cancel] [Add]

**Figure 4- 14:** Ajouter les règles pour groupe de sécurité.

✓ **Création d'un Key pair :**

La meilleure façon de fournir un accès sécurisé et facile à nos instances OpenStack consiste à utiliser des paires de clés pour l'authentification SSH. Pour chaque machine virtuelle, une paire de clés distincte est associée à l'utilisateur par défaut.

Pour créer une paire de clés, suivez ces étapes :

- Cliquez sur l'onglet "Key Pairs".
- Ensuite, cliquez sur "Créer une paire de clés" ("Create Key Pair") et choisissez un nom ainsi qu'un type pour la paire de clés.

**Create Key Pair** [X]

**Key Pair Name \***  
mykeypair ✓

**Key Type \***  
SSH Key

[Cancel] [Create Key Pair]

**Figure 4- 15:** Création d'un Key Pair.

- ✓ Une paire de clés appartient à un utilisateur individuel, et non à un projet. Pour partager une paire de clés entre plusieurs utilisateurs, chaque utilisateur doit importer cette paire de clés.

```

1 -----BEGIN RSA PRIVATE KEY-----
2 MIIEpAIBAAKCAQEAt/+06+PuRVuOCfQdMYH65ILZQtsd/LTb1mDogELIkU7m3MWA
3 vQhGsTotL1+qAkNZbRzerHORdEPppZTDoTRbhXhE9APwrt/+UCxJPpn/6mEKJ7FK
4 5xGUKYLLaLdaahrP5nwvYXedBp4LYUSffXP6jrqD5VnYwPzTNe4Chr4xmz5mZad
5 lliIPEZaefkFLon/tto6cMds83D9ba2zF90dV5QS/m7eeBw+22u+XUARm2A74LH
6 r/AP21utR2r0xig55kV0eWbohAJBdeb/6s3u8LPd5Eb6VGqUK/2IituUklWkJ3LZo
7 /5Jo2jjuf8m9Joa3xk95Ep6ecX0Xm6HJ05X5pQIDAQABAoIBAQCyz0TM05vbtAHS
8 uvG0jfDuT9DIehyBQftFyYClNbtMiOxfc0B4COZCQN4+6Mq2lwbGPQ/KteN6j76j
9 xbJJQ7LZntt8nbVoWdcDdW0vPbJdVum5wrWVhf3aoe8JlNkduBGMsSxFmyGuAvw1
10 BsM0/nox6h24Lmymj8hr4V2YqHDSMoHqZ9koRBwmt+cTntPgzt0APFV/7IEg1+JB
11 rgeQwa+T3M8b1KWZqQp+EV4cwtiL7cItnoFueWMqqvJXMuyMld3cRv5VxSP7oxKF
12 Ymv89uUn66RDFFunzJbY0hrb0axxbup6+9nFmsGmU0316KOTvs3fSEVQ/ynJRuug
13 JD4f9/KhAoGBA0VycB0QGc+rVw5j80x9hi1DwP2SwfIqQzB09oHskC0Thnp/rToj
14 2G+cjXJljqQOLhI6dLzkHa0i9s3swhYEweDHxreEyWSNJhRBxgh1KgHkG69tXvtK
15 TUZZLDTjJ24jrcYLubbPIIPwZnkQY6rBAFKCn453AyKNapC8KAH5/XvAoGBAM1K
16 1Bd+9LzcX0tJsf+25KY2VmAh6g47UiLtzHL9ky6S8YKcnbgZ3TAK7zTh5Eb9i6Sd
17 K2ci9yctAipHhrLofcyPXgv2obsCZu69ofnxLXqEJPzuxAh3Tres2jCxBGBMdb6G
18 itdRqhadhKZDHZeZDjp5NxiqxMavLVzjLU2PYX2rAoGBALzL61jNi8+LzVjAwYop
19 B00boS0FrLy89chblLBNG1BMbh+cmWStccl5NF6X0ohdRN8Vy0P48FZBuRoyph
20 A9kXyXWcd7KbsigE7xRqhARGVfMH06alvc5+1Zc3CmzgQXiU0V2RFw07VmAd0kT
21 gxokeHnAvv6hWnx6C+z0bRVAoGAVuacDS4ir2egtcDGZnanJ2zM93ijUu6HIx5L
22 cy/AA/ET5rQhV3MrXFvMHj6ZASwG1rHpU4LLkfvNdNQ+RwBifZsatnm6UI1dwSXo
23 0QLgwbH6bk8sEGFgow06g04N6ji1EueLEixkY0wP6kdd7TEfyAcncYY8foVgFJw
24 l0pi3G0CgyARNM/THvLJHjZ8N0imBhNJ6xsov3xKAIwdZkM/vSm4jIYlRnGCa+Ty
25 m43QW3mAFUja0Mh3D37vK1+4LBJUouqKYV8tELeZqxqkg5rPrkUQwJtRZcVWtnyR
26 ex/02yQ7huhtCTqLmJU0o7WntUoz9/ZPvmL+jK9i9WvfVbB12mMWLg==
27 -----END RSA PRIVATE KEY-----

```

Figure 4- 16: La forme d'un Key Pair.

## B Attaque DDOS :

Comme nous l'avons indiqué dans le chapitre 2, nous avons exploré plusieurs types et outils d'attaques DoS. Dans les lignes suivantes, nous allons détailler les méthodes utilisées par Kali Linux ainsi que les moyens de stopper ces attaques.

### ➤ Avec Slowloris :

- La meilleure méthode que nous avons employée dans ce projet, car OpenStack a été définitivement arrêté, et nous ne pouvons plus y accéder de manière complète.



```
(root@kali) - [~/home/kali/Desktop/Slowloris/slowloris]
# python3 slowloris.py 192.168.0.106 -s 500
[11-04-2022 23:24:19] Attacking 192.168.0.106 with 500 sockets.
[11-04-2022 23:24:19] Creating sockets ...
[11-04-2022 23:24:19] Sending keep-alive headers ... Socket count: 500
[11-04-2022 23:24:34] Sending keep-alive headers ... Socket count: 500
[11-04-2022 23:24:49] Sending keep-alive headers ... Socket count: 500
[11-04-2022 23:25:05] Sending keep-alive headers ... Socket count: 500
[11-04-2022 23:25:20] Sending keep-alive headers ... Socket count: 500
[11-04-2022 23:25:36] Sending keep-alive headers ... Socket count: 500
[11-04-2022 23:25:51] Sending keep-alive headers ... Socket count: 500
[11-04-2022 23:26:07] Sending keep-alive headers ... Socket count: 500
[11-04-2022 23:26:22] Sending keep-alive headers ... Socket count: 500
[11-04-2022 23:26:37] Sending keep-alive headers ... Socket count: 500
[11-04-2022 23:26:53] Sending keep-alive headers ... Socket count: 500
[11-04-2022 23:27:08] Sending keep-alive headers ... Socket count: 500
[11-04-2022 23:27:24] Sending keep-alive headers ... Socket count: 500
[11-04-2022 23:27:39] Sending keep-alive headers ... Socket count: 500
□
```

**Figure 4- 17:** L'attaque DoS.

- ✓ S : Spécifie le nombre cible de connexions à établir pendant le test (dans cet exemple 500, normalement avec 200 devrait être suffisant pour bloquer un serveur qui n'a pas de protection contre cette attaque).

➤ **L'analyse des paquets**

Dans Wireshark, nous avons observé une tentative du serveur pour répondre à une attaque DoS, qui a complètement perturbé le fonctionnement d'OpenStack via le port 80 vers divers types de portails. Nous avons également détecté un grand nombre de paquets TCP portant les flags (RST, ACK), ce qui indique que les ports de l'attaquant sont fermés.

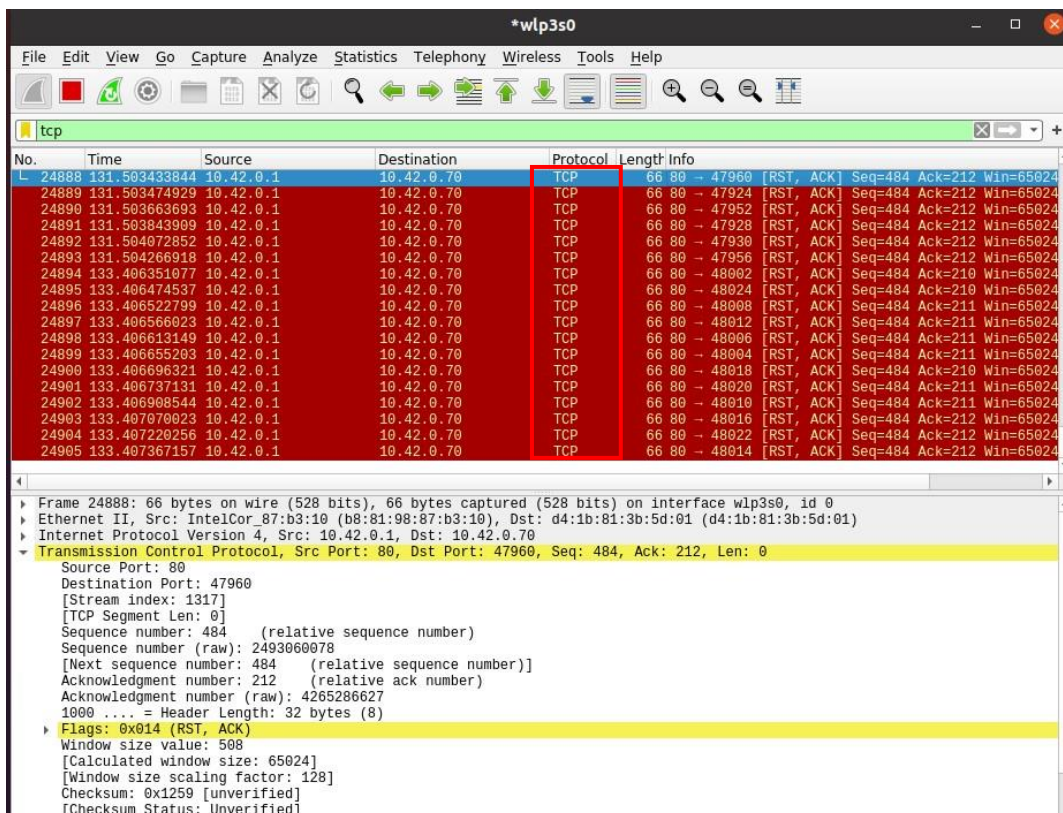


Figure 4- 18: Les capturations des paquets d’attaque DoS.

➤ Avec Hping 3 :

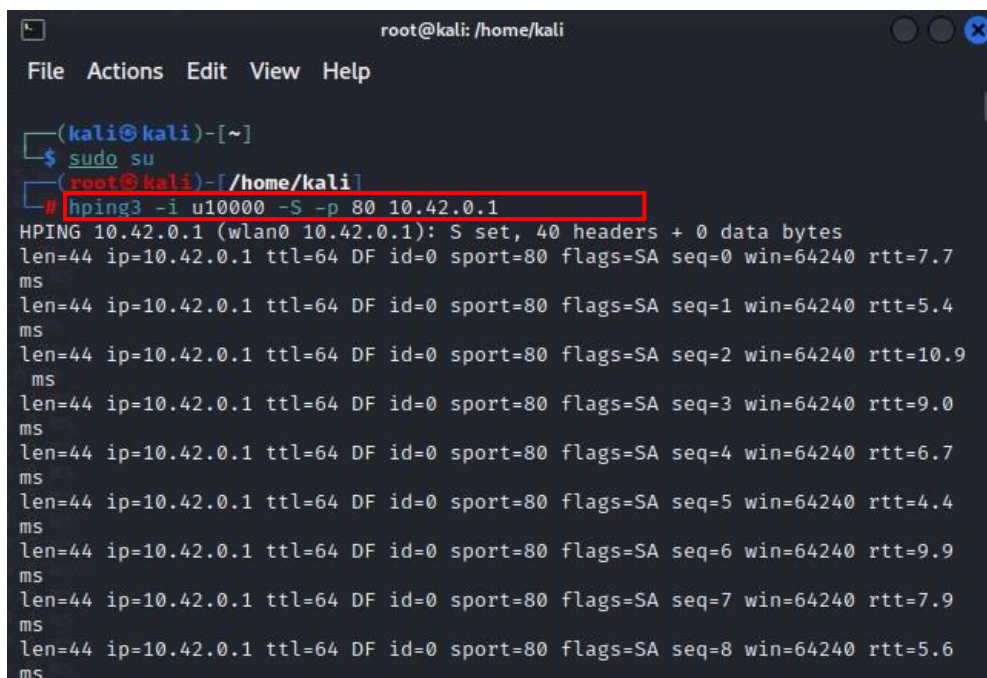


Figure 4- 19: L’attaque DoS avec Hping3.

- ✓ **I** : définit l’intervalle de temps entre chaque attaque.
- ✓ **U10000** : (u) pour microsecondes.
- ✓ **P** : Définit le port.

- ✓ S : Nous spécifions que le drapeau SYN (-S) doit être activé
- ✓ ✓ L'analyse des paquets :

Pendant l'analyse, nous avons remarqué la réception d'une grande quantité de paquets TCP portant le flag RST (RST=) en provenance de l'adresse 10.42.0.70 (l'attaquant). Ce flag indique que le récepteur doit supprimer la connexion. La suppression de la connexion est effectuée en fonction du numéro de séquence et des informations d'en-tête. Le paquet RST est envoyé après la réception du SYN/ACK, comme illustré dans l'image suivante.

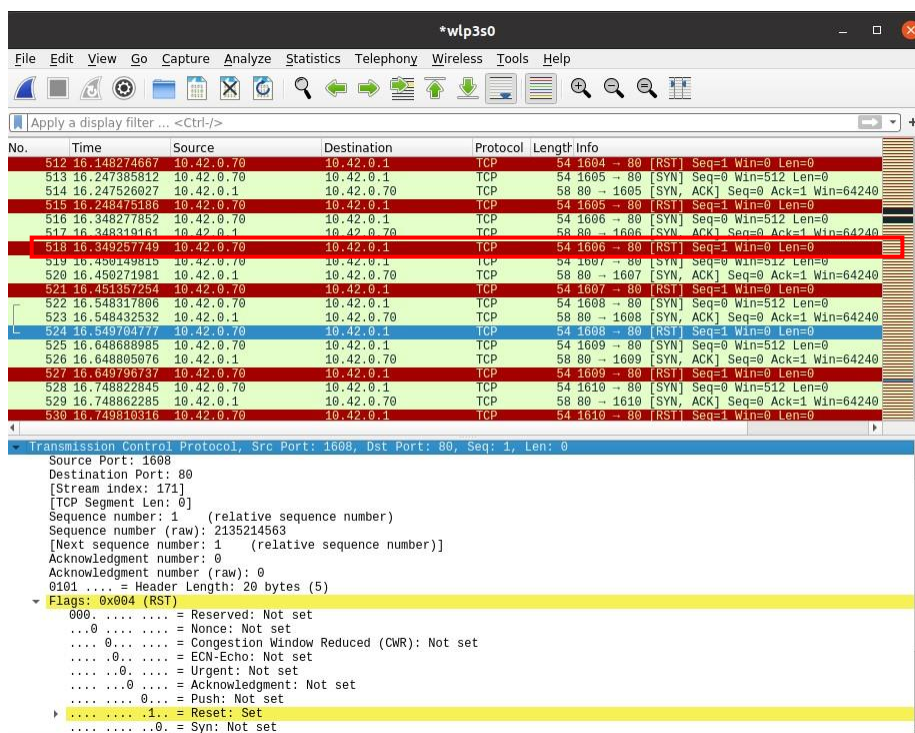


Figure 4- 20: Les capturations des paquets avec wireshark.

### ➤ Le Lancement de Suricata :

Dans OpenStack, le pare-feu n'offrira pas de nombreux avantages car la plupart des ports seront ouverts. Par conséquent, nous avons installé Suricata IDS/IPS, et nous allons maintenant expliquer la différence entre les deux.

Nous allons commencer par exécuter Suricata en utilisant la commande indiquée dans l'image ci-dessous :

```
root@cloud-HP-ENVY-Notebook:~# suricata -c /etc/suricata/suricata.yaml -q 0
7/9/2022 -- 19:27:16 - <Notice> - This is Suricata version 6.0.6 RELEASE running in SYSTEM mode
7/9/2022 -- 19:27:17 - <Notice> - all 6 packet processing threads, 4 management threads initialized, engine started.
```

Figure 4- 21: Lancement de Suricata.

- ✓ Nous allons maintenant capturer les alertes en utilisant la commande suivante :

```
cloud@cloud-HP-ENVY-Notebook:~$ tail -f /var/log/suricata/fast.log
09/07/2022-18:25:27.921439  [**] [1:1000001:1] tcp alert, DDOS ATTACK [**] [Classification: (null)] [Priority: 3] {TCP} 10.42.0.70:56788 -> 10.42.0.1:80
09/07/2022-18:25:30.409285  [**] [1:1000001:1] tcp alert, DDOS ATTACK [**] [Classification: (null)] [Priority: 3] {TCP} 10.42.0.70:57252 -> 10.42.0.1:80
09/07/2022-18:26:01.577795  [**] [1:1000001:1] tcp alert, DDOS ATTACK [**] [Classification: (null)] [Priority: 3] {TCP} 10.42.0.70:58310 -> 10.42.0.1:80
09/07/2022-18:26:32.305987  [**] [1:1000001:1] tcp alert, DDOS ATTACK [**] [Classification: (null)] [Priority: 3] {TCP} 10.42.0.70:59364 -> 10.42.0.1:80
```

Figure 4- 22: Les alertes sur Suricata.

- ✓ Ici, nous avons remarqué des alertes concernant des attaques de Déni de Service (DoS) utilisant le protocole TCP. Dans le dernier cas, nous avons identifié l'adresse IP qui envoie les attaques à partir de différents ports.
- ✓ Maintenant, notre prochaine étape consistera à tenter d'arrêter ces attaques en utilisant IPTABLES en convertissant Suricata du mode IDS (Détection d'Intrusion) en mode IPS (Prévention d'Intrusion).

```
[wDrop] [**] [1:1000001:1] tcp alert, DDOS ATTACK [**] [Classification: (null)] [Priority: 3] {TCP} 10.42.0.70:34208 -> 10.42.0.1:80
[**] [1:1000001:1] tcp alert, DDOS ATTACK [**] [Classification: (null)] [Priority: 3] {TCP} 10.42.0.70:34208 -> 10.42.0.1:80
[**] [1:9999:2] http alert [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.0.106:37012 -> 34.107.221.82:80
[**] [1:9999:2] http alert [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.0.106:37010 -> 34.107.221.82:80
[wDrop] [**] [1:1000001:1] tcp alert, DDOS ATTACK [**] [Classification: (null)] [Priority: 3] {TCP} 96.96.102.192:1778 -> 10.42.0.1:80
[**] [1:1000001:1] tcp alert, DDOS ATTACK [**] [Classification: (null)] [Priority: 3] {TCP} 98.179.46.94:1852 -> 10.42.0.1:80
[wDrop] [**] [1:1000001:1] tcp alert, DDOS ATTACK [**] [Classification: (null)] [Priority: 3] {TCP} 150.180.37.30:56098 -> 10.42.0.1:80
[**] [1:1000001:1] tcp alert, DDOS ATTACK [**] [Classification: (null)] [Priority: 3] {TCP} 105.43.245.173:56476 -> 10.42.0.1:80
[wDrop] [**] [1:1000001:1] tcp alert, DDOS ATTACK [**] [Classification: (null)] [Priority: 3] {TCP} 146.63.42.195:47272 -> 10.42.0.1:80
[**] [1:1000001:1] tcp alert, DDOS ATTACK [**] [Classification: (null)] [Priority: 3] {TCP} 168.109.59.51:47721 -> 10.42.0.1:80
[wDrop] [**] [1:1000001:1] tcp alert, DDOS ATTACK [**] [Classification: (null)] [Priority: 3] {TCP} 168.49.173.11:38476 -> 10.42.0.1:80
[**] [1:1000001:1] tcp alert, DDOS ATTACK [**] [Classification: (null)] [Priority: 3] {TCP} 95.30.66.230:38675 -> 10.42.0.1:80
```

Figure 4- 23: Drop les attaque DoS.

- ✓ Après avoir exécuté Suricata IPS, nous avons constaté que nous pouvions désormais accéder à OpenStack, ce qui signifie que nous avons réussi à arrêter l'attaque de Déni de Service (DoS).

### **4.3 Conclusion :**

Dans ce chapitre, nous avons exploré plusieurs types d'attaques, mais nous nous sommes concentrés sur deux d'entre elles en raison de leur succès : l'attaque de l'homme du milieu (ARP Poisoning) et l'attaque de Déni de Service (DoS). Ces attaques ont été exécutées à l'aide de Kali Linux.

Ensuite, nous avons abordé la sécurité en mettant en place plusieurs mesures. Nous avons configuré un pare-feu et déployé Suricata IDS/IPS pour détecter les alertes et mettre en place des mécanismes de blocage (Drop) en réponse à ces alertes. De plus, nous avons exploité les fonctionnalités de sécurité disponibles dans OpenStack pour renforcer davantage la protection de notre environnement.

## Conclusion générale

---

La sécurité du Cloud consiste en un ensemble de stratégies, de contrôles et de technologies conçues pour protéger les données, les applications et les services d'infrastructure. Notre projet vise principalement à créer un environnement sécurisé pour le Cloud, mais en raison de la complexité et de la sensibilité des grands services comme Google Drive ou iCloud, nous avons opté pour l'installation d'un Cloud open source sur un système d'exploitation Ubuntu. Cela nous a permis de tester les vulnérabilités et la sécurité.

Dans le cadre de notre projet, nous avons configuré un environnement avec OpenStack, en créant un nouvel utilisateur et un réseau privé. Nous avons ensuite créé une image et une instance. Pour renforcer la sécurité, nous avons commencé par mettre en place un groupe de sécurité avec des règles appropriées. De plus, nous avons généré une paire de clés pour l'accès SSH, que nous avons partagée avec les utilisateurs autorisés.

La phase suivante de notre projet a consisté à tester la vulnérabilité de notre environnement à des attaques. Nous avons utilisé Kali Linux pour mener des attaques telles que l'ARP Poisoning (empoisonnement ARP) et des attaques de type DoS (Déni de Service) avec Slowloris et Hping3. Nous avons également exploré d'autres attaques telles que ICMP et Syn-Flood, bien que celles-ci n'aient pas été couronnées de succès. L'attaque ARP Poisoning nous a permis d'extraire des informations d'identification utilisateur, tandis que l'attaque DoS a causé l'arrêt temporaire d'OpenStack.

Dans le but de renforcer la sécurité d'OpenStack, nous avons activé un pare-feu avec des règles personnalisées. Cependant, cela a laissé la plupart des ports ouverts pour permettre l'accès à OpenStack. En outre, nous avons installé Suricata IDS/IPS et créé des règles spécifiques pour détecter et contrer les attaques. Cette étape a été

couronnée de succès, car nous avons réussi à rétablir le fonctionnement d'OpenStack même lors d'une attaque DoS active.

Il est essentiel de souligner que, dans le monde d'Internet, il n'existe pas de protection complète. Les menaces évoluent constamment. Cependant, il est crucial de suivre des procédures de sécurité strictes, notamment :

- ✓ Créer des mots de passe complexes.
- ✓ Crypter les communications pour éviter les attaques de l'homme du milieu, en utilisant des protocoles sécurisés tels que HTTPS.
- ✓ Maîtriser la communication entrante et sortante en autorisant les connexions uniquement vers des réseaux et des plages d'adresses IP spécifiques.

### ✓ L'installation d'Openstack :

1. Avant Avant de commencer, nous devons nous assurer que notre système est à jour. Pour ce faire, exécutez la commande suivante, puis redémarrez votre système.

```
sudo apt-get update && sudo apt-get upgrade -y
```

2. Nous allons d'abord créer un nouvel utilisateur nommé "stack" dans notre système afin de configurer OpenStack :

```
sudo useradd -s /bin/bash -d /opt/stack -m stack
```

3. Nous devons également accorder à l'utilisateur "stack" des privilèges root et lui permettre de s'exécuter sans mot de passe. Pour ce faire, exécutez la commande suivante :

```
echo "stack ALL=(ALL) NOPASSWD: ALL" | sudo tee /etc/sudoers.d/stack
```

4. Le "OUTPUT" ressemblera à ceci :

```
cloud@cloud:~$ sudo useradd -s /bin/bash -d /opt/stack -m stack
[sudo] password for cloud:
cloud@cloud:~$ echo "stack ALL=(ALL) NOPASSWD: ALL" | sudo tee /etc/sudoers.d/stack
stack ALL=(ALL) NOPASSWD: ALL
```

5. Une fois que nous avons créé l'utilisateur "stack", il est temps de se connecter avec cet utilisateur en utilisant la commande suivante :

```
sudo su - stack
```

6. Maintenant, nous allons entrer cette commande pour télécharger/cloner Devstack depuis son référentiel vers notre système :

```
git clone https://opendev.org/openstack/devstack
```



7. Maintenant que nous avons téléchargé DevStack et configuré nos fichiers de configuration, nous devons accéder d'abord au dossier DevStack en exécutant :

```
cd devstack
```

8. Ensuite, nous avons créé un fichier local.conf en exécutant :

```
nano local.conf
```

et collez le contenu suivant :

```
[local|localr]]
ADMIN_PASSWORD=StrongAdminSecret
DATABASE_PASSWORD=$ADMIN_PASSWORDcinder
RABBIT_PASSWORD=$ADMIN_PASSWORD
SERVICE_PASSWORD=$ADMIN_PASSWORD
```

9. Maintenant Maintenant que nous avons correctement configuré les fichiers de configuration, exécutons le script pour configurer OpenStack sur notre système :

---

```
./stack.sh
```

10. Une fois notre installation terminée avec succès, notre terminal ressemblera à l'image ci-dessous.

```
This is your host IP address: 192.168.0.106
This is your host IPv6 address: ::1
Horizon is now available at http://192.168.0.106/dashboard
Keystone is serving at http://192.168.0.106/identity/
The default users are: admin and demo
The password: root

Services are running under systemd unit files.
For more information see:
https://docs.openstack.org/devstack/latest/systemd.html

DevStack Version: zed
Change: 8fa03a37adb7a4b818b410db9463f9661715eeda Merge "Clean up neutron cleanup code" 2022-08-23 20:05:48 +0000
OS Version: Ubuntu 20.04 focal

2022-08-24 15:55:27.571 | stack.sh completed in 4098 seconds.
stack@cloud:~/devstack$
```

## Bibliographie

---

- [1] International Journal of Advent Research in Computer and Electronics (IJARCE) (E ISSN: 2348-5523) Special Issue
- [2] National Conference "CONVERGENCE 2015", 28 March 2015 -page 104
- [3] <https://www.citrix.com/solutions/app-delivery-and-security/what-is-hybrid>
- [4] Cloud Computing concepts, Technology & Architecture by Top-selling Author Thomas ert Page 97,98,99
- [5] <https://www.geeksforgeeks.org/difference-between-iaas-paas-and-saas/>
- [6] <https://www.journaldunet.com/solutions/cloud-computing/1134148-sixraisonspour-lesquelles-la-technologie-determinera-la-reussite-future-desentreprises/>
- [7] <https://www.educba.com/example-of-cloud-computing/>
- [8] <https://www.geeksforgeeks.org/architecture-of-cloud-computing/>
- [9] <https://www.g2.com/categories/infrastructure-as-a-service-iaas>
- [10] <https://fr.wikipedia.org/wiki/OpenStack>
- [11] <https://www.serenicity.fr/attaque-informatique-definition/>
- [12] [http://igm.univ-mlv.fr/~dr/XPOSE2007/plebacco\\_ids/A\\_attaque.html](http://igm.univ-mlv.fr/~dr/XPOSE2007/plebacco_ids/A_attaque.html)
- [13] <https://www.securiteinfo.com/attaques/hacking/typesattaques.shtml>
- [14] New York Institute of Technology (NYIT), Amman's campus-2006, Prepared By : Murad M. Ali
- [15] <https://www.cloudflare.com/fr-fr/learning/ddos/syn-flood-ddos-attack/>
- [16] <https://www.cloudflare.com/fr-fr/learning/ddos/udp-flood-ddos-attack> .
- [17] <https://www.technology.org/2018/12/06/a-guide-to-http-floods-what-they-areand-what-it-means-to-get-hit-with-one/>

- [18] <https://www.netscout.com/what-is-ddos/icmp-flood>
- [19] [https://fr.wikipedia.org/wiki/Ping\\_flood](https://fr.wikipedia.org/wiki/Ping_flood)
- [20] <https://www.imperva.com/learn/application-security/sql-injection-sqli>
- [21] <https://www.pentasecurity.com/blog/how-sql-injection-attacks-work/>
- [22] 802.11 Security by Bruce Potter, Bob Fleck, Publisher(s): O'Reilly Media, Inc.
- [23] <https://www.codeur.com/blog/securiser-serveur/>
- [24] [https://access.redhat.com/documentation/enus/red\\_hat\\_openstack\\_platform/14/htmlsingle/security\\_and\\_hardening\\_guide/index#managing\\_instance\\_security](https://access.redhat.com/documentation/enus/red_hat_openstack_platform/14/htmlsingle/security_and_hardening_guide/index#managing_instance_security)
- [25] <https://www.checkpoint.com/cyber-hub/network-security/what-is-an-intrusiondetection-system-ids/#>
- [26] <http://www.machaon.fr/isn/reseaux/Fiche-Wireshark.pdf>
- [27] <https://www.openstack.org/software/>.
- [28] OpenStack cloud Computing Cookbook, Foreword by tim Bell, Infrastructure Manager
- [29] <https://www.kali.org/docs/introduction/what-is-kali-linux/n>