REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE M'HAMED BOUGARA-BOUMERDES

Faculté de **T**echnologie

Département **I**ngénierie des **S**ystèmes **E**lectriques

Mémoire de Master

Présenté par

CHERIFI CHAHRAZED **KHENAKA RIM**

Filière : Télécommunications

Spécialité : Réseaux et **T**élécommunications

Thème : **Implémentation d'une Stratégie de Sécurité dans un Réseau de Campus**

Soutenu le 02 /07 /2024 devant le jury composé de :

Sedjelmaci	Ibticeme	MCB	UMBB	Présidente
Akliouat	Hacene	MAA	UMBB	Examinateur
Mechid	Samira	MAA	UMBB	Promotrice

Année universitaire : 2023/2024

Remerciements

Nous commençons par exprimer notre gratitude envers Allah, le Tout-Puissant

Nous souhaitons exprimer notre profonde gratitude à nos parents pour leur amour, leur soutien inconditionnel et leurs encouragements constants tout au long de notre parcours académique.

Un immense merci à notre promotrice madame Mechid pour sa précieuse orientation, ses conseils avisés et son encadrement tout au long de ce projet.

Nous tenons également à exprimer notre gratitude aux encadrants de stage, monsieur Nighoud et monsieur Chettih pour leur accueil chaleureux, leur soutien technique et leurs enseignements pratiques.

Nous remercions également nos amis et camarades de classe pour leur camaraderie.

Enfin, nous remercions chaleureusement la faculté de technologie pour avoir fourni un environnement académique stimulant et des ressources nécessaires à la réalisation de ce projet. Votre soutien a été fondamental pour l'achèvement de ce travail.

Dédicace

Je dédie ce mémoire à mes parents, pour leur amour inconditionnel. Leurs encouragements ont été une source inestimable de motivation et de force tout au long de cette aventure. Ils sont, et resteront toujours, une source d'inspiration et de fierté pour moi.

Je dédie également ce mémoire à mes sœurs, Sarra et Rana, ainsi qu'à mon petit frère Anes. Leur affection, leur soutien moral et leurs encouragements ont été essentiels pour moi.

À mes amis et camarades Damia, Hassiba, Imene, et Manel, qui ont été à mes côtés tout au long de ce parcours et qui sont devenus ma deuxième famille, je vous dédie aussi ce mémoire. Votre soutien moral et votre camaraderie ont été des éléments essentiels pour surmonter les moments de doute et de stress. Les discussions et les moments de détente partagés ont grandement contribué à la réalisation de ce travail.

Un remerciement spécial à ma binôme, Chahrazed, pour son soutien tout au long de ce projet. Sa patience et ses compétences ont été d'une aide précieuse, et notre travail d'équipe a grandement facilité l'accomplissement de ce mémoire. Merci, Chahrazed, pour ton amitié et ton engagement.

Je dédie également ce mémoire à ma grand-mère décédée qu'**Allah** lui accorde Sa miséricorde. Elle aurait tant aimé être à mes côtés pour voir la réussite de mes études. Elle a toujours été fière de moi, simplement pour qui je suis. Elle restera toujours vivante dans mon cœur.

Rim

Dédicace

Ce mémoire est dédié principalement à mes parents même si aucune dédicace ne saurait exprimer ma profonde gratitude et ma vive reconnaissance envers tous leurs soutiens et leurs conseils et sacrifices tout au long de ce parcours académique. Merci pour tout ce que vous avez fait.

À mon défunt grand-père qui avait tant de rêves pour moi, j'espère qu'il est fier de ce que je suis devenu aujourd'hui.

À mon frère Idir et sœurs Liza et Dounia, Puisse mon travail et efforts vous montrer que tout est possible avec détermination et persévérance.

À mes amies Hassiba, Imene, Manel, et Damia, qui ont toujours été là pour me soutenir, me conseiller et me remonter le moral. Votre amitié précieuse a été un pilier essentiel dans les moments difficiles et de joie.

À ma binôme et meilleure amie Rim, en reconnaissance de tout ce que nous avons accompli ensemble et de ton rôle précieux dans ma vie. Merci pour tout ce que tu fais et pour être une amie exceptionnelle.

Chahrazed

Résumé

Les systèmes d’information sont désormais des éléments critiques et indispensables au bon fonctionnement des entreprises, assurant des services tels que le stockage, la gestion et le transport des données. Cela souligne l'impératif de sécuriser ces systèmes. Ce projet se concentre sur la sécurisation du réseau LAN d'un campus, en particulier au niveau de l'accès au réseau. Nous examinerons les diverses attaques potentielles au niveau deux (2) du modèle OSI, mettant en œuvre une stratégie de sécurité basée sur les bonnes pratiques et les dernières recherches pour repousser ces attaques préjudiciables au bon fonctionnement du réseau.

Mots-clés : LANs, Sécurité, Switches, couche 2.

Abstract

Information systems are now critical and indispensable to the smooth running of essential to the smooth running of businesses, providing services such as data storage data storage, management and transport. This underlines the imperative to secure these systems. This project focuses on securing a campus LAN network, particularly in terms of network access. We examine the various potential attacks at level two (2) of the OSI model, implementing a security strategy based on best practices and the latest research to repel these attacks, which are detrimental to the network operation.

Keywords: LANs, Security, Switches, layer 2.

ملخص

أصبحت أنظمة المعلومات الآن بالغة الأهمية ولا غنى عنها للتشغيل السلس للأنظمة الأساسية للتشغيل السلس للأعمال، وتوفير خدمات مثل تخزين البيانات، وتخزين البيانات، وإدارتها، ونقلها. وهذا يؤكد ضرورة تأمين هذه الأنظمة. يركز هذا المشروع على في الحرم الجامعي، خاصة فيما يتعلق بالوصول إلى الشبكة. نحن ندرس مختلف الهجمات المحتملة في المستوى LAN تأمين شبكة ، وننفذ استراتيجية أمنية تعتمد على أفضل الممارسات وأحدث الأبحاث لصد هذه الهجمات التي تضر OSI الثاني (2) من نموذج بتشغيل الشبكة.

الكلمات الرئيسية: الشبكات المحلية، الأمن، المفاتيح، الطبقة 2..

Table des matières

Liste des abréviations

LAN Local Area Network

CAN Campus Area Network

WAP Wireless Access Point

VLAN Virtual Local Area Network

QOS Quality of service

STP Spanning-Tree Protocol

IDS Intrusion Detection System

IPS Intrusion Prevention System

AAA Authentication Authorization Accounting

ASA Adaptive Security Appliance

CIA Confidentiality Integrity Availability

DOS Denial Of Service

DDOS Distributed Denial Of Service

ACL Access Control List

MDM Mobile Device Management

OSI Open Systems Interconnection

VTP Vlan Trunking Protocol

HSRP Hot StandbyRouter Protocol

CDP Cisco Discovery Protocol

DHCP Dynamic Host Configuration Protocol

TCP Transmission Control Protocol

VTY Virtual Teletype

SVI Switch Virtual Interfaces

DNS Domain Name System

SSH Secure Shell

SFTP Secure File Transfer Protocol

BPDU Bridge Protocol Data Unit

Table des figures

Table des tableaux

Introduction Générale

À l'ère d'une connectivité croissante, la sécurité des réseaux informatiques est devenue une préoccupation majeure pour les organisations. Divers réseaux campus, qui relient un grand nombre d'ordinateurs et d'appareils sur une vaste zone géographique, sont particulièrement exposés à diverses menaces en matière de sécurité. En effet, la nature étendue et ouverte des réseaux campus les rend vulnérables à des attaques telles que les écoutes clandestines, les attaques par déni de service, les intrusions non autorisées, et bien d'autres. Cette exposition accrue aux menaces nécessite une approche robuste et systématique pour protéger les données sensibles et assurer la continuité des opérations.

Les réseaux campus, en raison de leur complexité et de leur taille, présentent des défis uniques en matière de sécurité. Ils doivent non seulement être protégés contre les menaces externes mais aussi contre les risques internes, tels que les erreurs humaines et les comportements malveillants de l'intérieur. De plus, la diversité des dispositifs connectés, allant des ordinateurs et smartphones, agrandit la surface d'attaque potentielle, rendant la tâche de sécurisation encore plus ardue.

Il est impératif de mettre en place une stratégie de sécurité efficace pour protéger les ressources et les données contre les attaques potentielles, la problématique centrale de ce mémoire est la suivante : **comment peut-on définir et implémenter une stratégie de sécurité efficace dans un réseau de campus pour prévenir et atténuer les différentes menaces, tout en assurant la continuité et la fiabilité des services réseau ?** Cette question guidera notre exploration des concepts théoriques, des pratiques de configuration, des simulations d'attaques, et des solutions de sécurisation tout au long de ce mémoire.

Le premier chapitre de ce mémoire est consacré aux notions théoriques de la sécurité des réseaux IP. Nous y présentons une définition des réseaux locaux (LAN) et des réseaux de campus, les différents types d'attaques auxquels ces réseaux peuvent être exposés, ainsi que les contre-mesures appropriées pour chaque type d'attaque. Cette base théorique est essentielle pour comprendre les vulnérabilités potentielles et les mécanismes de défense qui peuvent être mis en place pour protéger un réseau.

Dans le deuxième chapitre, nous passons à des aspects plus pratiques en détaillant les configurations de base des commutateurs dans les couches core et accès. Nous explorons des protocoles et des configurations tels que HSRP, STP, les mots de passe, les VLANs, et d'autres éléments critiques pour la sécurité et la résilience du réseau. Ensuite, dans le troisième chapitre nous simulerons diverses attaques à l'aide de l'outil Kali Linux, incluant des attaques DHCP, le spoofing MAC, Telnet, HSRP, et bien d'autres. Chaque simulation nous permet d'examiner les failles potentielles et de développer des solutions appropriées pour y remédier.

Le Quatrième chapitre se concentre sur la sécurisation de notre réseau face aux attaques simulées. Nous proposons des solutions spécifiques pour chaque type d'attaque identifiée, en assurant que chaque mesure prise contribue à renforcer la robustesse et la sécurité globale du réseau de campus.

.

Chapitre 1 : Sécurité des réseaux informatiques

1.1 Introduction

L'architecture d'un réseau campus est essentielle pour garantir des communications efficaces et sécurisées au sein d'une organisation. Ce chapitre explore en détail les différents aspects de la conception et de la sécurisation d'un réseau campus, en commençant par une définition des réseaux LAN (Local Area Network) et en expliquant comment ils sont étendus pour former un réseau campus.

Nous examinerons ensuite les bases de la cybersécurité, en soulignant les principes fondamentaux de la CIA (confidentialité, intégrité, disponibilité) et en identifiant les types courants d'attaques auxquels sont confrontés les réseaux. Enfin, nous discuterons des technologies de sécurité et les protocoles utilisés pour renforcer la sécurité des réseaux campus, en mettant l'accent sur les meilleures pratiques pour protéger les données et garantir des communications fiables.

1.2 Définition d'un réseau LAN :

Un réseau local (LAN) est un groupe d'appareils interconnectés qui partagent la même infrastructure de communication dans une zone géographique limitée. Un réseau local permet aux utilisateurs de partager des ressources telles que des fichiers, des imprimantes, des applications et des périphériques réseau. Ils fournissent également une plateforme permettant aux utilisateurs de communiquer, de collaborer et d'accéder à des services réseau communs. [1]

Les réseaux locaux sont généralement conçus pour offrir un débit élevé allant de 10 Mbit/s à 10 Gbit/s selon la norme IEEE 802.3 et une faible latence, ce qui les rend adaptés aux besoins de communications en temps réel et de transfert de données rapide au sein d'une organisation. Les réseaux locaux ont une portée limitée, généralement jusqu'à quelques kilomètres, selon la technologie de transmission utilisée. [2]

1.3 Les réseaux campus :

1.3.1 Définition :

Un réseau campus (CAN) est un réseau informatique couvrant une zone étendue regroupant plusieurs bâtiments ou installations situés à proximité les uns des autres.

Contrairement à un réseau LAN (Local Area Network) qui se limite à une zone géographique restreinte comme un bureau ou un bâtiment. Un réseau campus facilite la communication et le partage de ressources entre différentes parties d'une organisation. Utilisant des technologies telles que des commutateurs Ethernet et des câbles à fibre optique, il supporte des services comme la voix sur IP, la vidéoconférence et la vidéosurveillance. [3]

Pour assurer la sécurité, l'accessibilité et les performances nécessaires, les réseaux campus doivent être planifiés et gérés de manière appropriée pour répondre aux besoins des utilisateurs répartis sur le campus. [4]

1.3.2 Les différentes couches d'un réseau campus :

Les réseaux campus sont fréquemment élaborés en adoptant une architecture à trois niveaux afin de satisfaire les exigences en matière de connectivité, de performance et de sécurité. Voici une description détaillée de chaque couche :

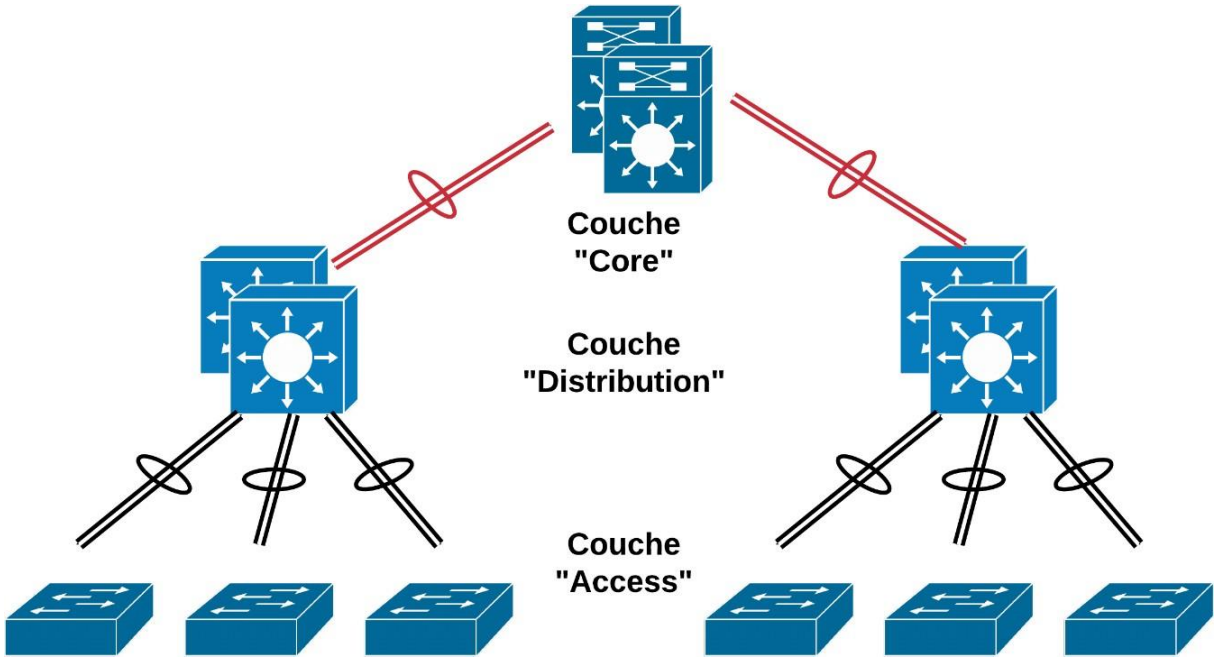

Figure 1.1 : Architecture réseau campus à trois couches [5]

- **Couche d'accès :** La couche d'accès est la première couche dans un réseau campus (du bas en haut comme le montre la figure 1.1). Elle représente la première interface entre les utilisateurs finaux et le réseau. Elle comprend les commutateurs d'accès

Ethernet pour les connexions filaires et les points d'accès sans fil (WAP - Wireless Access Points) pour les connexions sans fil. [6]

- **Caractéristique :** La fonction de la couche d'accès dans un réseau campus est de gérer les connexions des utilisateurs en connectant les différents appareils tels que les ordinateurs, les imprimantes et les téléphones IP au réseau. Elle assure également le contrôle de l'accès en mettant en place des mesures de sécurité telles que l'authentification des utilisateurs et la sécurisation des ports afin de limiter l'accès aux seuls appareils autorisés. De plus, elle utilise la segmentation VLAN pour diviser le réseau en segments logiques, ce qui permet d'améliorer les performances et la sécurité en isolant le trafic entre différents groupes d'utilisateurs. Enfin, la couche d'accès met en œuvre des politiques de qualité de service (QoS) afin de garantir des performances optimales pour les applications sensibles à la latence, telles que la voix et la vidéo.

➢ **Couche de distribution :** La couche de distribution est la deuxième couche dans un réseau campus. Elle relie les différents équipements d'accès à la couche cœur du réseau. Elle agit comme une couche d'agrégation pour regrouper le trafic provenant des segments d'accès et le transmettre vers la couche cœur. [7]

- **Caractéristique :** Outre l'agrégation du trafic, la couche de distribution joue un rôle clé dans le routage inter-VLAN. Cette fonctionnalité permet aux différents VLAN de communiquer entre eux en utilisant des routeurs ou des commutateurs de couche 3 pour diriger le trafic entre les segments. De plus, la couche de distribution met en place des politiques de contrôle de la bande passante afin d'optimiser l'utilisation des ressources réseau. Cela garantit que les applications critiques bénéficient d'une bande passante suffisante tout en évitant la congestion du réseau. [8]

➢ **Couche cœur :** La couche cœur est la troisième et dernière couche dans un réseau campus. Elle est responsable de l'acheminement du trafic entre les différents segments du réseau.

- **Caractéristique :** Pour garantir un acheminement rapide et fiable, la couche cœur utilise des commutateurs et des routeurs haut débit capables de traiter de grandes quantités de données. En matière de redondance et de tolérance aux pannes, la couche cœur met en place plusieurs mécanismes. Parmi eux, le Spanning Tree Protocol (STP) qui est souvent utilisé pour éliminer les boucles de commutation en désactivant sélectivement certains chemins redondants. En ce qui concerne la sécurité, la couche

cœur intègre des fonctionnalités avancées telles que les pares-feux, les systèmes de détection d'intrusion (IDS/IPS), et les VPN. [8]

1.3.3 Les équipements de base d'un réseau campus :

Lors de la conception d'un réseau, il est important de sélectionner le matériel approprié aux besoins actuels, tout en prévoyant la croissance du réseau. Au sein d'un réseau d'entreprise, les commutateurs et les routeurs jouent un rôle essentiel dans la communication réseau.

La commutation est un concept clé dans le domaine de télécommunication qui permet le transfert efficace des données entre les périphériques connectés. Elle repose sur l'utilisation de commutateurs réseau qui dirigent le trafic uniquement vers les ports destinataires, améliorant ainsi la performance du réseau en évitant les collisions et en optimisant la bande passante disponible. En créant des canaux virtuels et en maintenant une table associant les adresses MAC, les commutateurs permettent aux appareils de transmettre et de recevoir des données de manière simultanée, ce qui améliore l'évolutivité et la stabilité du réseau**.**

Il existe deux types de commutateurs utilisés dans un réseau CAN, chacun ayant des fonctionnalités spécifiques adaptées à différents besoins et environnements, comme décrit dans la suite :

- **Commutateur niveau 2 :** Un commutateur de niveau 2, est un dispositif réseau qui fonctionne au niveau de la couche 2 du modèle OSI. Il utilise les adresses MAC pour acheminer le trafic entre les périphériques, maintien des tables d'adresses MAC pour chaque port, ce qui lui permet de transférer les données uniquement vers les ports destinataires. Ces commutateurs permettent la segmentation du réseau en VLANs pour améliorer la sécurité et les performances, optimisent le trafic en évitant les collisions, offrent des fonctionnalités de sécurité avancées, et prennent en charge la redondance pour assurer la fiabilité du réseau.

  La gamme Catalyst 2960 est une famille de commutateurs Ethernet qui offre une sécurité intégrée avec contrôle d'admission par le réseau (NAC), qualité de service (QoS) évoluée, et résilience pour apporter des services intelligents à la périphérie du réseau. [9]

Figure 1.2 : Commutateur Cisco Catalyst 2960 *[9]*

- **Les commutateurs multicouches :** sont généralement déployés dans les couches principales et de distribution du réseau commuté d'une entreprise. Ils prennent en charge certains protocoles de routage et transmettent les paquets IP à un rythme proche de celui de la transmission de la couche 2.

  Les commutateurs multicouches prennent souvent en charge du matériel spécialisé, tels que des circuits intégrés spécifiques ASIC (Application Specific Integrated Circuits), Les ASIC, associés à des structures de données logicielles dédiées, peuvent rationaliser le réacheminement de paquets IP indépendamment du processeur.

Figure 1.3: Commutateur Cisco 3850 *[9]*

1.3.4 L'approche de la défense en profondeur dans un réseau campus :

La méthode de défense en profondeur est une approche de sécurité qui consiste à mettre en place plusieurs méthodes de défense pour protéger un réseau ou un système informatique. Dans un réseau campus, d'après Cisco la défense en profondeur implique généralement plusieurs mesures de sécurité à différents niveaux du réseau pour réduire les risques d'attaques et de compromissions. La figure ci-dessous montre un exemple de réseau de zone de campus utilisant l'approche de la défense en profondeur pour la sécurité. [10]

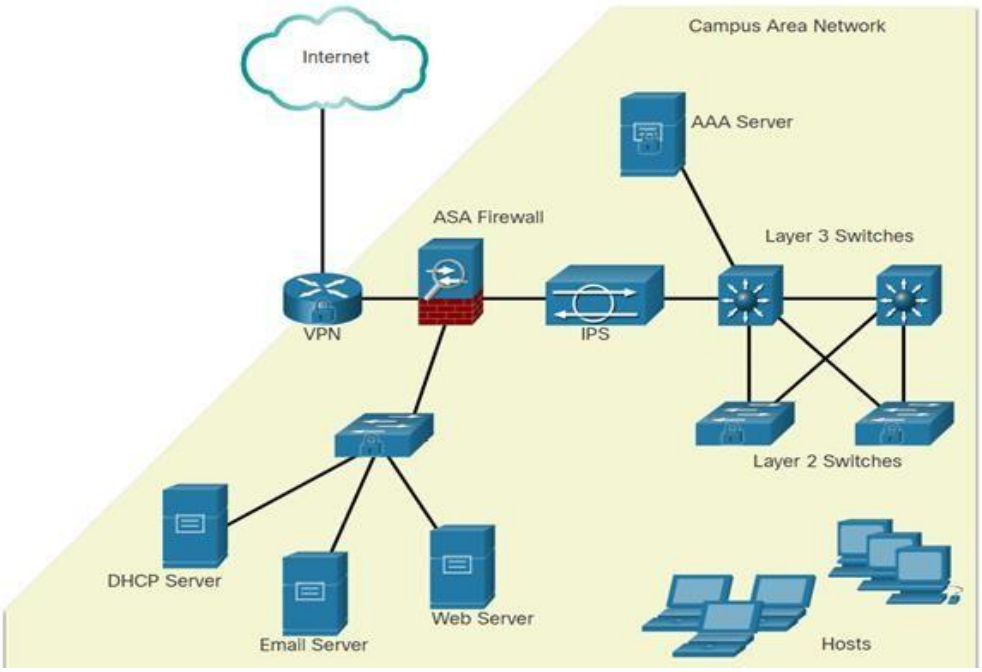

Figure 1.4 : Un exemple d'une approche de défense en profondeur dans un réseau campus [10]

Les méthodes de sécurisation utilisée dans l'exemple montré dans la figure 1.2 sont :

- **VPN :** Les réseaux privés virtuels (VPN) jouent un rôle crucial dans la sécurisation des réseaux campus. Ils garantissent un accès distant sécurisé aux utilisateurs en cryptant les données sensibles qui circulent sur Internet, assurant ainsi la confidentialité et l'intégrité des communications. Les VPN permettent aux employés, aux étudiants et aux partenaires externes d'accéder de manière sécurisée aux ressources du réseau campus, peu importe leur emplacement géographique. De plus, les VPN permettent de contourner les restrictions géographiques et de protéger les données contre les interceptions et les attaques en ligne. [11]

- **Le pare-feu ASA** : Dans un environnement de campus, un pare-feu Cisco ASA (Adaptive Security Appliance) peut jouer un rôle crucial dans l'amélioration de la sécurité. Il peut être positionné à la frontière du réseau pour filtrer le trafic entrant et sortant, empêchant les tentatives d'accès non autorisé et réduisant l'exposition aux attaques externes. Le pare-feu ASA peut également diviser le réseau en zones sécurisées, limitant ainsi la propagation des menaces en cas de compromission. Ainsi, le pare-feu ASA contribue de manière significative à renforcer la sécurité d'un réseau campus. [12]

- **Les serveurs AAA (Authentication, Authorization, and Accounting) :** jouent un rôle essentiel dans la gestion sécurisée des utilisateurs et de leurs accès au sein d'un réseau campus. Leur principale fonction est d'authentifier les utilisateurs qui souhaitent se connecter au réseau en vérifiant leurs informations d'identification. Une fois l'authentification réussie, les serveurs AAA déterminent les autorisations de chaque utilisateur en fonction de son identité et de son profil, ce qui leur permet de contrôler son accès aux différentes ressources du réseau campus. De plus, ces serveurs assurent également le suivi et l'enregistrement des activités des utilisateurs, ce qui permet aux administrateurs de réseau de superviser l'utilisation des ressources et de détecter les comportements suspects. En intégrant les serveurs AAA dans un réseau campus, les organisations peuvent ainsi garantir un accès sécurisé, contrôlé et traçable pour leurs utilisateurs. [13]

- **IPS :** Dans un environnement de réseau campus, un système de prévention des intrusions (IPS) joue un rôle essentiel dans la sécurisation du réseau en détectant et en empêchant les activités malveillantes. L'IPS surveille en permanence le trafic réseau afin de repérer tout comportement anormal ou toute signature d'attaque connue. Lorsqu'une menace est détectée, l'IPS peut prendre des mesures immédiates pour bloquer l'activité malveillante, assurant ainsi la protection du réseau contre les attaques et les compromissions. De plus, l'IPS contribue à la prévention des attaques par déni de service (DDoS) en bloquant le trafic malveillant et en maintenant la disponibilité des services réseau. En surveillant et en générant des rapports sur les activités détectées, l'IPS offre aux administrateurs réseau une meilleure visibilité sur les menaces potentielles, leur permettant ainsi de prendre des mesures préventives pour renforcer la sécurité du réseau campus. [14]

1.4 La sécurité des réseaux :

1.4.1 Importance de la sécurité des réseaux :

La cybersécurité est essentielle pour assurer la continuité des activités d'une organisation. Les failles de sécurité peuvent perturber le commerce en ligne, entraîner la perte de données commerciales, compromettre la confidentialité et l'intégrité des informations. Ces vulnérabilités peuvent entraîner des pertes financières, des vols de propriété intellectuelle, des poursuites judiciaires et même mettre en danger la sécurité publique.

Le maintien d'un réseau sécurisé protège les utilisateurs et les intérêts commerciaux. Les professionnels de la cybersécurité doivent rester vigilants et surveiller de près les nouvelles menaces et attaques ainsi que les vulnérabilités potentielles des appareils et des logiciels.

1.4.2 Principes de sécurité CIA :

La triade CIA, dans la sécurité de l'information, est un acronyme qui représente les trois principes fondamentaux de la sécurité de l'information : confidentialité, intégrité et disponibilité. Ces trois principes sont considérés comme les piliers de la sécurité de l'information et sont essentiels pour assurer la protection des données et des systèmes informatiques : [15]

- **Confidentialité :** Il est crucial de garantir que seules les personnes autorisées peuvent accéder aux informations, en utilisant des méthodes telles que le chiffrement, le contrôle d'accès strict, l'anonymisation des données et des politiques de confidentialité claires.
- **Intégrité :** l'intégrité des données garantit que les informations sont exactes, Complet et inchangé. Cela signifie que les données ne doivent pas être modifiées de manière non autorisée, que ce soit accidentellement ou intentionnellement, en utilisant des mesures comme le chiffrement, le contrôle d'accès, les sauvegardes régulières, les checksums et hachage et les journaux d'audit des systèmes.
- **Disponibilité :** Pour garantir que les données et les systèmes sont accessibles lorsque nécessaire, il est nécessaire d'utiliser des méthodes telles que la redondance des systèmes, les sauvegardes régulières, l'amélioration de la résilience des systèmes, la maintenance des équipements, les mises à jour régulières des systèmes et la mise en place de plans de reprise après sinistre pour faire face à des événements catastrophiques imprévus.

1.4.3 Types d'attaques :

Afin de réduire les attaques, il est recommandé de débuter par la classification des divers types d'attaques. En classifiant les attaques réseau, il devient possible de cibler des types d'attaques plutôt que des attaques individuelles. Bien qu'il n'existe pas de méthode normalisée pour classer les attaques de réseau, la méthode qu'on a décidé d'utiliser classe les attaques en trois grandes catégories : les attaques de reconnaissance, les attaques d'accès et les attaques Déni de service (DOS). [10]

1.4.3.1 Attaques de reconnaissance : Une attaque de reconnaissance représente la première étape au cours de laquelle un pirate informatique collecte des renseignements sur une cible spécifique avant de lancer une attaque plus précise. Voici quelques stratégies couramment employées lors d'une attaque de reconnaissance : [16]

- **Scan de ports :** L'attaquant utilise des outils comme Nmap pour scanner les ports ouverts sur un système. Cela permet de déterminer quels services sont disponibles et éventuellement de trouver des vulnérabilités.

- **Scan d'adresses IP :** L'attaquant recherche des adresses IP actives sur un réseau pour identifier des cibles potentielles. Cela peut être fait en utilisant des outils comme Ping ou des scans de plage d'adresses IP.

- **Scanners de vulnérabilité :** L'attaquant utilise des outils automatisés pour rechercher des vulnérabilités connues dans les logiciels ou les services utilisés par la cible pour déterminer le type et la version de l'application et du système d'exploitation qui s'exécutent sur l'hôte.

- **Recherche d'informations publiques :** autorise l'attaquant à rassembler des données provenant de sources publiques, telles que les sites Web de l'organisation cible, les réseaux sociaux ou les rapports annuels. Cette approche peut s'avérer pertinente pour identifier des informations concernant l'infrastructure, les employés ou les partenaires.

1.4.3.2 Attaques d'accès : Les attaques par accès exploitent les failles connues dans les services d'authentification, les services FTP et les services web. Elles visent à compromettre des comptes en ligne, des bases de données confidentielles et d'autres données sensibles**.** Les acteurs de la menace utilisent les attaques d'accès sur les appareils et les ordinateurs du réseau pour récupérer des données, obtenir un accès ou escalader les privilèges d'accès jusqu'au statut d'administrateur. Voici quelques techniques courantes utilisées lors d'une attaque d'accès : [10]

- **L'ingénierie sociale :** est une méthode utilisée par les attaquants pour manipuler les individus et obtenir des informations confidentielles ou un accès non autorisé à des systèmes. Cette technique exploite la crédulité, la peur ou la sympathie des personnes ciblées, et peut prendre différentes formes, telles que le phishing (par mail ou sur les réseaux sociaux), le vishing (par téléphone), l'ingénierie sociale en personne, où

l'attaquant se présente en personne pour obtenir des informations, et d'autres techniques de manipulation psychologique**.**

- **Attaque par force brute :** L'attaquant tente de deviner les identifiants de connexion en essayant différentes combinaisons de noms d'utilisateur et de mots de passe. Cette méthode est généralement automatisée à l'aide de scripts ou d'outils spécifiques.

- **Attaque par dictionnaire :** Similaire à l'attaque par force brute, mais au lieu de générer des combinaisons aléatoires, l'attaquant utilise une liste de mots couramment utilisés comme mots de passe potentiels. Cette approche est souvent plus efficace car de nombreux utilisateurs choisissent des mots de passe faibles.

- **Attaque par injection :** L'attaquant insère du code malveillant dans des champs de formulaire ou des requêtes afin de contourner les mécanismes d'authentification et d'accéder à des données sensibles ou à des fonctionnalités du système.

1.4.3.3 Attaques de déni de service :

- **DOS :** L'objectif d'une attaque par déni de service (DoS) est de rendre un service indisponible en submergeant le serveur cible avec un trafic malveillant. L'attaquant envoie un volume massif de requêtes ou de trafic à partir d'un seul système ou d'un petit groupe de systèmes, ce qui peut entraîner un ralentissement ou une interruption totale du service pour les utilisateurs légitimes. Les attaques DoS peuvent prendre différentes formes, telles que les attaques par inondation ou par épuisement des ressources.

- **DDOS :** Une attaque par déni de service distribué (DDoS) est une forme d'attaque plus avancée dans laquelle l'attaquant exploite un réseau de machines infectées, appelées "botnets", afin de coordonner l'envoi de trafic vers la cible. Chaque machine de la botnet envoie une quantité relativement modeste de trafic, mais l'effet cumulatif peut être dévastateur, car il est ardu pour la cible de filtrer ou de bloquer efficacement l'intégralité du trafic. Les attaques DDoS peuvent rendre un service indisponible en saturant la bande passante, la mémoire ou d'autres ressources du serveur ciblé. [17]

1.4.4 Contre-mesure pour chaque attaque :

1.4.4.1 Contre-mesure pour les attaques d’accès :

Pour se prémunir contre les attaques visant à obtenir un accès non autorisé à un système, différentes mesures de sécurité peuvent être mises en place. En premier lieu, il est recommandé d'adopter des méthodes d'authentification forte, telles que la double authentification, qui requièrent la fourniture de deux types de preuves d'identité distinctes. Ensuite, il convient d'établir une politique de gestion des accès afin de restreindre les privilèges des utilisateurs en fonction de leurs besoins réels, en suivant le principe du moindre privilège. Il est également primordial de surveiller régulièrement les journaux d'authentification afin de détecter toute activité suspecte ou tentative d'accès non autorisé. De plus, il est crucial de maintenir à jour les systèmes et les logiciels afin de réduire les vulnérabilités et les risques d'exploitation par des attaquants. Sensibiliser les utilisateurs aux risques de sécurité et aux bonnes pratiques en matière de sécurité informatique, notamment en ce qui concerne la protection des identifiants et des mots de passe, constitue également une mesure efficace. Enfin, l'utilisation de pare-feu et de systèmes de détection d'intrusion pour filtrer le trafic réseau et détecter les tentatives d'accès non autorisé, ainsi que le chiffrement des données sensibles en transit et au repos.

1.4.4.2 Contre-mesure pour les attaques de reconnaissance :

Pour contrer les attaques de reconnaissance il est essentiel de mettre en œuvre plusieurs mesures de protection. En premier lieu. Tout d'abord, il est recommandé de limiter les informations publiques disponibles sur l'organisation en limitant les informations sensibles sur les sites web et les réseaux sociaux. Ensuite, il est primordial de surveiller activement le trafic réseau et de détecter les schémas d'activité suspects, ce qui permet d'identifier les attaques de reconnaissance en cours. De plus, l'utilisation de pare-feu et de systèmes de détection d'intrusion peut contribuer à bloquer ou à signaler les activités malveillantes. La mise en place de politiques de sécurité strictes, telles que l'utilisation de mots de passe robustes et la limitation des droits d'accès, peut également contribuer à réduire les risques liés aux attaques de reconnaissance. Enfin, il est essentiel de sensibiliser les employés aux techniques de social engineering et aux bonnes pratiques en matière de sécurité informatique afin de renforcer la posture de sécurité globale de l'organisation. [16]

1.4.4.3 Contre-mesure pour les attaques de déni de service :

Afin de contrer les attaques de déni de service (DoS) et de déni de service distribué (DDoS), il est possible de mettre en place diverses mesures de sécurité. Par exemple, l'utilisation de services de protection contre les attaques DDoS fournis par des fournisseurs spécialisés peut

permettre de filtrer le trafic malveillant et de maintenir la disponibilité des services en ligne. De plus, la configuration de pare-feu, de systèmes de détection d'intrusion (IDS) et de systèmes de prévention d'intrusion (IPS) peut contribuer à bloquer le trafic nuisible et à repérer les attaques en cours. Il est conseillé de configurer les serveurs et les routeurs pour qu'ils résistent mieux aux attaques, par exemple en limitant le nombre de connexions simultanées ou en utilisant des listes de contrôle d'accès (ACL) pour filtrer le trafic indésirable. Enfin, la surveillance continue du trafic réseau et la mise en place de plans de réponse aux incidents peuvent permettre de détecter et de contrer rapidement les attaques de déni de service. [17]

1.4.5 La sécurité physique dans les réseaux informatiques :

La sécurité physique des réseaux informatiques est un pilier fondamental pour protéger les données et les ressources des entreprises. Voici quelques aspects clés mettant en évidence son importance et les actions à prendre pour la renforcer : [18]

1.4.5.1 Contrôle d'accès physique : il est essentiel de restreindre l'accès aux locaux contenant les équipements réseau afin d'assurer un contrôle d'accès physique adéquat. Cette mesure peut être mise en œuvre grâce à l'utilisation de serrures à clé ou électroniques, de cartes d'accès, de systèmes de contrôle d'accès biométriques tels que les empreintes digitales ou la reconnaissance faciale, ainsi que de caméras de surveillance. Par ailleurs, les entreprises doivent impérativement établir des politiques strictes pour réguler l'accès à ces locaux.

1.4.5.2 Protection contre le vol : Les serveurs, les commutateurs et les routeurs sont des objets de grande valeur et contiennent des données sensibles, ce qui en fait des cibles potentielles pour les voleurs. Afin de garantir leur protection, les entreprises peuvent mettre en place différentes mesures de sécurité. Tout d'abord, elles peuvent utiliser des câbles de sécurité pour attacher ces équipements à des points d'ancrage fixes, ce qui rend leur vol plus difficile. De plus, l'installation de systèmes d'alarme, de détecteurs de mouvement et de caméras de surveillance permet de détecter toute tentative de vol et de dissuader les voleurs potentiels. Enfin, il est recommandé de marquer les équipements de manière visible, ce qui peut dissuader les voleurs et faciliter leur récupération en cas de vol. Ces mesures combinées contribuent à renforcer la sécurité des équipements réseau et à réduire les risques de vol.

1.4.5.3 Protection contre les dommages physiques : Les équipements réseau doivent être sécurisés contre les dégâts physiques engendrés par les catastrophes naturelles telles que les incendies, les inondations, les tremblements de terre, etc., ainsi que les accidents tels que les chutes, les chocs, etc. Afin d'assurer cette protection, les entreprises ont la possibilité d'installer des systèmes de détection et d'extinction d'incendie, des systèmes d'alerte en cas d'inondation, des onduleurs et des générateurs de secours pour maintenir l'alimentation électrique en cas de panne.

1.4.5.4 Gestion des câbles : Pour minimiser les risques de perte de connectivité et de dommages physiques, il est essentiel d'adopter une gestion efficace des câbles. Il convient ainsi de veiller à leur organisation, leur étiquetage et leur fixation appropriés, afin d'éviter tout trébuchement, accident ou détérioration des équipements.

1.4.5.5 Sécurité des équipements mobiles : Afin de prévenir le vol et l'accès non autorisé, il est impératif de sécuriser les équipements mobiles tels que les ordinateurs portables, les tablettes et les smartphones lors de leur utilisation pour se connecter au réseau. Cette protection peut être mise en place en utilisant des logiciels de cryptage, des mots de passe solides et des solutions de gestion des appareils mobiles (MDM) pour surveiller et contrôler l'accès aux appareils.

1.5 Conclusion :

Pour conclure, la sécurisation des réseaux informatiques, en particulier des réseaux campus, est un défi majeur dans un contexte où les menaces sont de plus en plus nombreuses et sophistiquées. Ce chapitre a permis de définir les concepts clés liés aux réseaux locaux et campus, en soulignant l'importance de la sécurité des réseaux. Cette étude nous permettra de développer une stratégie de sécurité complète et adaptée pour notre réseau campus, en tenant compte des différents aspects de la sécurité des réseaux abordés dans ce chapitre.

Chapitre 2 : Paramétrage Initial des Commutateurs

2.1 Introduction

Dans ce chapitre, nous allons concevoir et construire le réseau et sa configuration. A partir des différentes configurations nécessaires au déploiement sur un LAN,

Dans ce cadre nous présenterons les configurations réalisées ainsi que les tests de validation pour confirmer le bon fonctionnement de ce réseau.

2.2 Présentation de l'architecture du réseau :

Nous avons réalisé les configurations initiales sur les commutateurs de l'entreprise afin de mettre en œuvre la stratégie de sécurité envisagée. Pour une documentation plus précise et une présentation éducative, nous allons reproduire ces configurations dans l'outil Cisco Packet Tracer dans cette partie du chapitre.

2.2.1 Présentation du simulateur Cisco « Packet Tracer »

Packet Tracer est un logiciel de CISCO permettant de construire un réseau physique virtuel et de simuler le comportement des protocoles réseaux sur ce réseau.

Cisco Packet Tracer est un moyen d'apprendre comment différents réseaux sont construits et de découvrir comment fonctionnent les différents composants qui composent un réseau informatique. Son objectif est de schématiser, configurer et visualiser tous les futurs déploiements réseau possibles.

2.2.2 Le réseau réalisé

Notre modèle d'entreprise est composé de :

- **Niveau CORE de réseau** : Il est composé de deux commutateurs de niveau 3. Il assure lesconnexions avec le commutateur d'accès.
- **Niveau ACCESS** : Il est composé d'un commutateur niveau 2, destiné àconnecter les périphériques finaux.

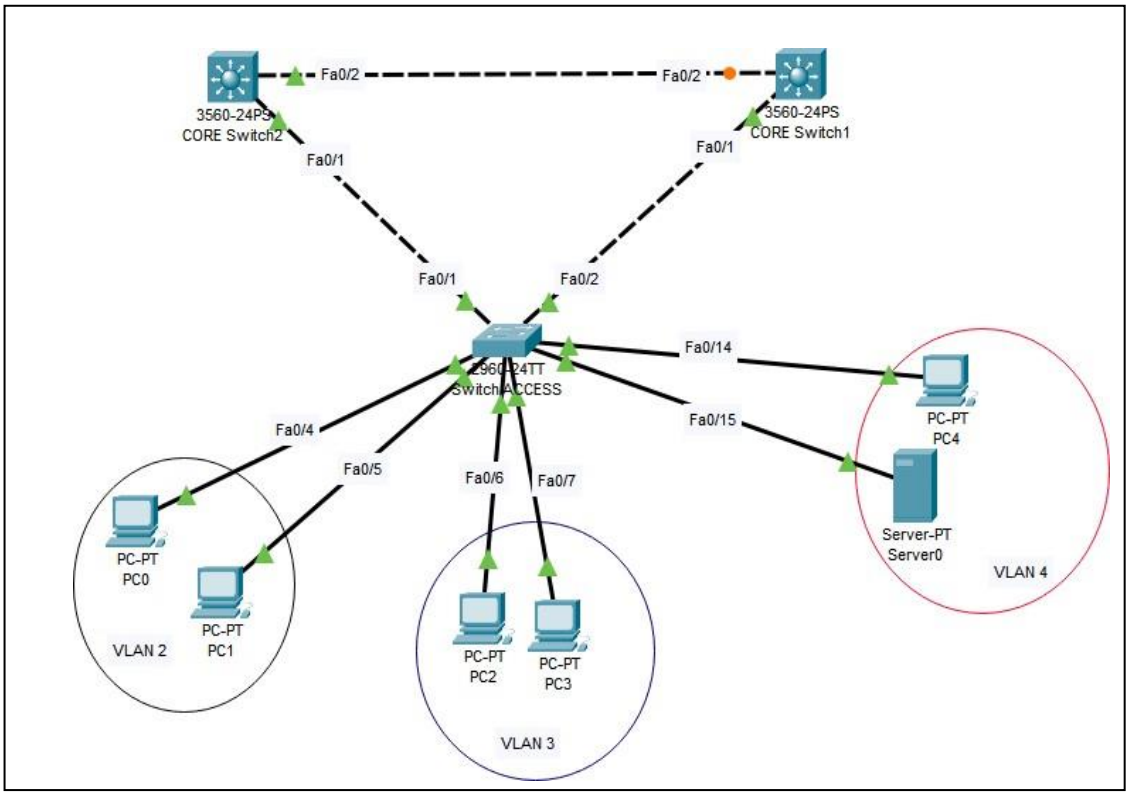

Figure 2.1 Architecture du réseau réalisé sur l'outil Packet tracer

2.3 Les protocoles implémentés

Tout au long de notre travail, nous exploiterons un certain nombre de protocoles et de technologies. Dans cette section nous décrirons le mode de fonctionnement du niveau réseau 2, ainsi que d'autres protocoles de couches supérieures nécessaires au bon fonctionnement de notre réseau, en décrivant comment les déployer.

2.3.1 Protocole VTP

Le protocole VTP est un protocole propriétaire de Cisco utilisé pour configurer et administrer les VLANs.

VTP permet d'ajouter, de renommer ou de supprimer un ou plusieurs réseaux locaux virtuels sur un seul commutateur, propageant cette nouvelle configuration à tous les autres commutateurs du réseau.

Trois modes de fonctionnement existent :

- **VTP server :** le commutateur permet à l'administrateur de faire des modifications sur les VLANs et chargé de diffuser la configuration aux commutateurs du domaine VTP.

- **VTP client :** ne permettent pas aux administrateurs de modifier les VLAN, ils envoient/transmettent les mises à jour.
- **VTP transparent :** le commutateur reçoit les mises à jour et ne fait que de les diffuser.

- **Segmentation VLANs**

La segmentation logique des ports au sein d'un ou plusieurs réseaux physiques permet plusieurs aspects positifs des VLANs, tel que la réduction de la diffusion du trafic sur le réseau et l'amélioration de la sécurité.

Le plan d'adressage VLANs :

N° de VLAN	Nom de VLAN	Plage d'adressage
2	Gestion	192.168.2.0 /24
3	Commercial	192.168.3.0 /24
4	Informatique	192.168.4.0 /24

Tableau 2.1 : adressage VLANs

- **Il est important de souligner que :** Nous avons décidé de ne pas mettre en place le VTP sur les commutateurs de l'entreprise en raison des risques associés à la perte de configuration VTP. Cette décision a été prise afin d'éviter tout problème de synchronisation inattendue des VLANs, de modification non autorisée des VLANs ou de déploiement de VLANs non intentionnels dans le réseau. Nous avons privilégié une approche manuelle pour la configuration des VLANs afin d'assurer un contrôle total sur les modifications apportées au réseau.

2.3.2 Protocole HSRP

HSRP est un protocole propriétaire Cisco. Il permet de gérer la redondance de commutateur, lorsqu'un commutateur tombe en panne un autre de secours prend le relais. Une élection déterminera le commutateur actif et les autres seront en "attente" (standby). [19]

La configuration HSRP dépend également du STP pour utiliser de manière optimale les deux protocoles.

2.3.3 Protocole STP

Le Spanning Tree Protocol est un protocole essentiel dans les réseaux informatiques car il permet d'éviter les boucles en désactivant sélectivement des liens redondants dans le réseau. [5]

STP bloque logiquement les boucles physiques dans un réseau de couche 2, empêchant les trames d'encercler le réseau pour toujours. STP compense une défaillance du réseau en recalculant et en ouvrant les ports précédemment bloqués.

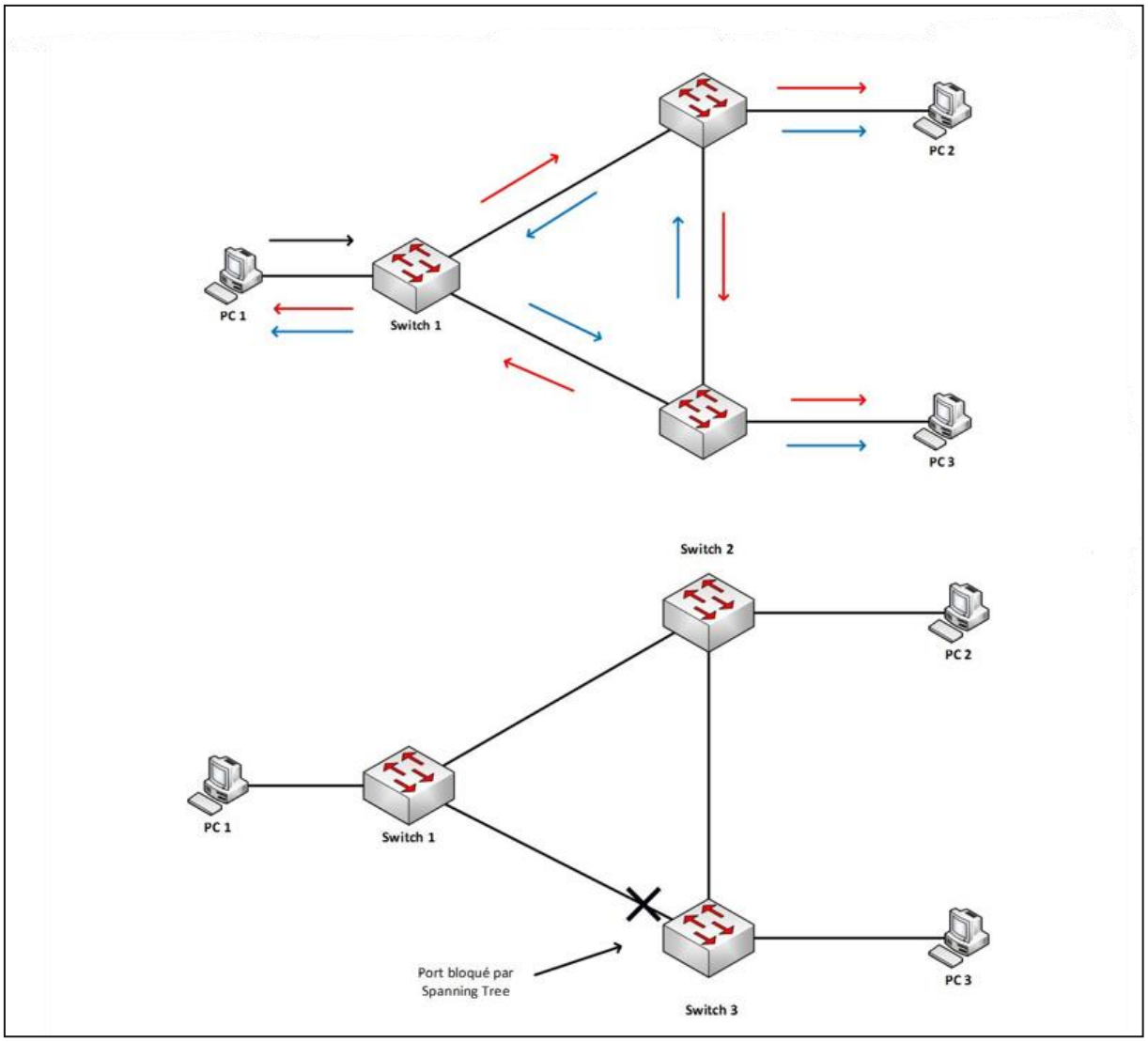

Figure 2.2 : Fonctionnement STP *[20]*

- La figure 2.2 montre une topologie redondante, un problème majeur est la tempête de broadcast, qui survient lorsque des messages de broadcast circulent indéfiniment dans le réseau. Par exemple, lorsque PC 1 envoie un message en broadcast, ce message circule indéfiniment entre les switches, saturant les liens et mettant à mal la CPU des switches. Cela peut rendre un switch hors service en quelques secondes, bloquant tout autre trafic. Le STP désactive les liens susceptibles de créer des boucles et les réactive en cas de panne d'un autre lien, permettant ainsi de profiter de la redondance des liaisons.

2.3.4 Protocole CDP

Le CDP est un protocole de couche 2 propriétaire de Cisco qui est utilisé pour recueillir des informations sur les appareils Cisco qui partagent la même liaison de données. CDP fonctionne indépendamment des supports et protocoles et s'exécute sur tous les périphériques Cisco, tels que routeurs, commutateurs et serveurs d'accès.

Le Cisco Discovery Protocol sera activé pour simplifier l'administration, le dépannage, et favoriser une meilleure intégration avec les solutions de téléphonie IP et sans fil. [21]

2.3.5 DHCP (Dynamic Host Configuration Protocol)

Le protocole DHCP offre une configuration automatique et dynamique des adresses IP ainsi que des informations associées aux ordinateurs configurés pour l'utiliser, appelés clients DHCP. Cela signifie que chaque hôte du réseau obtient sa configuration IP de manière dynamique au moment du démarrage.

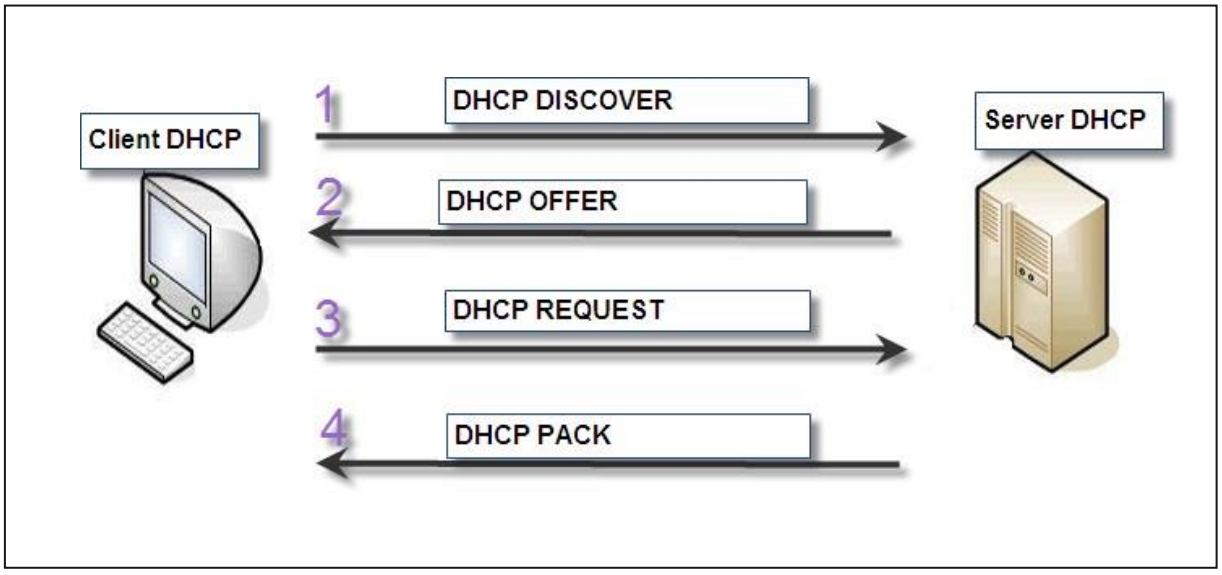

Figure 2.3: Fonctionnement du DHCP *[22]*

2.3.6 Accès distant Telnet

Le protocole Telnet est utilisé au niveau de la couche application pour permettre une communication bidirectionnelle, interactive et textuelle sur Internet ou les réseaux locaux (LAN). Il utilise une connexion de terminal virtuel pour transmettre les données de l'utilisateur en mode intra bande, où l'information de contrôle Telnet est encodée dans une connexion de données en utilisant le protocole TCP (Transmission Control Protocol) avec des octets de 8 bits. [23]

2.4 Configuration des équipements

2.4.1 Configuration initiale

- **Configuration du nom de périphérique**

La configuration implique d'assigner un nom au périphérique en utilisant la commande "hostname" dans le mode de configuration globale.

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname Access
Access(config)#
```

Figure2.4 : Nomination du switch Access

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname CORE_2
CORE_2(config)#
```

Figure2.5 : Nomination su switch core 2

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname CORE_1
CORE_1(config)#
```

Figure 2.6 : Nomination du switch core 1

- **Sécurisation d'accès aux périphériques**
- **Configurer le mot de passe du mode d'exécution privilégié :**

Le mot de passe du mode d'exécution privilégié secret (enable secret) est utilisé pour accéder au mode d'exécution privilégié (mode enable) d'un périphérique réseau.

```
Access>enable
Access#confi
Access#configure ter
Access#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Access(config)#enable secret cisco
Access(config)#
```

Figure 2.7: Configuration du mot de passe privilégié

- **Configurer la ligne console :**

Le mot de passe "console 0" fait référence au mot de passe utilisé pour accéder à la console de gestion (port console 0) d'un périphérique réseau.

```
Access(config)#line console 0
Access(config-line)#password cisco123
Access(config-line)#login
Access(config-line)#loggin syn
Access(config-line)#loggin synchronous
Access(config-line)#
```

Figure 2.8: Configuration de la line console

- **Cryptage des mots de passe :**

La commande **service password encryption** sert à crypter tous les mots de passe configurés.

```
Access#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Access(config)#service password-encryption
Access(config)#
```

Figure 2.9: Chiffrement des mots de passe

2.4.2 Création et configuration des VLANs

Les commandes suivantes permettent de créer et nommer les VLANs appropriés :

```
Access#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Access(config)#vlan 2
Access(config-vlan)#name Gestion
Access(config-vlan)#vlan 3
Access(config-vlan)#name Commercial
Access(config-vlan)#vlan 4
Access(config-vlan)#name informatique
Access(config-vlan)#
```

Figure 2.10 : Création des VLANs

- **Attribution des interfaces du commutateur aux VLANs**

Les commandes suivantes sont utilisées pour assigner un port à un VLAN en mode Accès, où chaque port d'un commutateur est associé à un VLAN spécifique selon le tableau suivant :

VLANs	Interfaces
2	Fa0/3-Fa0/5
3	Fa0/6-Fa0/9
4	Fa0/13-Fa0/20

Tableau 2.2 : Attribution des interfaces aux VLANs

- **Configuration des liens Trunk et Accès**

Les liens trunk et les liens accès sont deux types de connexions utilisés dans les réseaux VLAN pour transporter le trafic entre les commutateurs et les appareils finaux.

Les liens trunk sont utilisés pour transporter le trafic de plusieurs VLANs entre les commutateurs en ajoutant des étiquettes VLAN aux trames, ce qui permet de distinguer les différents VLANs. Les liens trunk sont configurés avec la possibilité de transporter des trames de plusieurs VLANs, ce qui les rend idéaux pour connecter des commutateurs ensemble ou pour connecter un commutateur à un routeur prenant en charge le trunking.

Les liens accès sont utilisés pour connecter des appareils finaux tels que des ordinateurs ou des serveurs à un commutateur. Ils sont configurés pour transporter le trafic d'un seul VLAN en ajoutant une étiquette VLAN à chaque trame entrante, ce qui les rend adaptés à fournir un accès réseau aux appareils finaux et à les attribuer à un VLAN spécifique.

```
Access(config)#
Access(config)#int range fa0/3-5
Access(config-if-range)#switchport mode access
Access(config-if-range)#switchport access vlan 2
Access(config-if-range)#int range fa0/6-9
Access(config-if-range)#switchport mode access
Access(config-if-range)#switchport access vlan 3
Access(config-if-range)#int range fa0/13
Access(config-if-range)#int range fa0/13-20
Access(config-if-range)#switchport mode access
Access(config-if-range)#switchport access vlan 4
Access(config-if-range)#
```

Figure 2.11 : Configurations des ports accès

```
Access(config)#interface fa0/1
Access(config-if)#switchport mode trunk

Access(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
```

Figure 2.12 : Liaison Trunk entre switch Access et core2

```
Access(config)#interface fa0/2
Access(config-if)#switchport mode trunk

Access(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up
```

Figure 2.13: Liaison Trunk entre switch Access et core1

- **Configuration des interfaces VLANs**

Une adresse de l'interface vlan sera attribuée à chaque switch Cœur selon le tableau ci-dessous :

VLANs	Adresse IP VLANs (CORE1)	Adresse IP VLANs (CORE2)
2	192.168.2.2	192.168.2.3
3	192.168.3.2	192.168.3.3
4	192.168.4.2	192.168.4.3

Tableau 2.3 : Adresses des interfaces Vlan

```
CORE_1(config)#int vlan 2
CORE_1(config-if)#ip address 192.168.2.2 255.255.255.0
CORE_1(config-if)#
CORE_1(config-if)#int vlan 3
CORE_1(config-if)#
%LINK-5-CHANGED: Interface Vlan3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan3, changed state to up

CORE_1(config-if)#ip address 192.168.3.2 255.255.255.0
CORE_1(config-if)#
CORE_1(config-if)#int vlan 4
CORE_1(config-if)#
%LINK-5-CHANGED: Interface Vlan4, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan4, changed state to up

CORE_1(config-if)#ip address 192.168.4.2 255.255.255.0
```

Figure 2.14: Configuration des interfaces VLANs sur Core1

```
CORE_2(config)#int vlan 2
CORE_2(config-if)#
%LINK-5-CHANGED: Interface Vlan2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2, changed state to up

CORE_2(config-if)#ip address 192.168.2.3 255.255.255.0
CORE_2(config-if)#
CORE_2(config-if)#int vlan 3
CORE_2(config-if)#
%LINK-5-CHANGED: Interface Vlan3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan3, changed state to up

CORE_2(config-if)#ip address 193.168.3.3 255.255.255.0
CORE_2(config-if)#
CORE_2(config-if)#int vlan 4
CORE_2(config-if)#
%LINK-5-CHANGED: Interface Vlan4, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan4, changed state to up

CORE_2(config-if)#ip address 192.168.4.3 255.255.255.0
```

Figure 2.15 : Configuration des interfaces VLANs sur Core2

- La commande **ip routing** est utilisée sur les commutateurs Cisco pour activer le routage IP sur le commutateur. Lorsque cette commande est activée, le commutateur peut fonctionner comme un routeur Layer 3, capable de prendre des décisions de routage basées sur les adresses IP des paquets. Une fois le routage IP activé, le commutateur peut router le trafic entre différents VLANs configurés sur le commutateur ou entre les VLANs et les réseaux externes via des interfaces routées

2.4.3 Configuration de la haute disponibilité HSRP

Pour garantir une haute disponibilité et répartir la charge entre les deux commutateurs de Core, on va définir une priorité pour chaque commutateur dans le cadre du protocole HSRP (Hot Standby Router Protocol). Sur l'un des Switch core, les VLANs prioritaires sont

configurés par rapport aux VLANs secondaires, tandis que sur l'autre Switch core, les priorités des VLANs sont inversées comme le montre le tableau ci-dessous :

Switch	Priorité
Core 1	Vlan 2, Vlan 3
Core 2	Vlan 4

Tableau 2.4 : Répartition des VLANs sur les switches cœur

Vlans	Adresse ip virtuellede l'interface vlan Standby
2	192.168.2.1
3	192.168.3.1
4	192.168.4.1

Tableau 2.5 : Adresse ip virtuelle des interfaces VLANs

La commande **"standby preempt"** accorde la priorité au multiswitch dans le protocole Cisco HSRP (Hot Standby Router Protocol), ce qui lui permet de devenir actif immédiatement.

```
CORE_1(config)#int vlan 2
CORE_1(config-if)#standby 2 ip 192.168.2.1
CORE_1(config-if)#standby 2 priority 150
CORE_1(config-if)#standby 2 preemp
%HSRP-6-STATECHANGE: Vlan2 Grp 2 state Speak -> Standby

%HSRP-6-STATECHANGE: Vlan2 Grp 2 state Standby -> Active

CORE_1(config-if)#standby 2 preempt
CORE_1(config-if)#exit
CORE_1(config)#
CORE_1(config)#int vlan 3
CORE_1(config-if)#standby 3 ip 192.168.3.1
CORE_1(config-if)#standby 3 priority 150
CORE_1(config-if)#standby 3 preempt
CORE_1(config-if)#
%HSRP-6-STATECHANGE: Vlan3 Grp 3 state Speak -> Standby

%HSRP-6-STATECHANGE: Vlan3 Grp 3 state Standby -> Active

CORE_1(config-if)#exit
CORE_1(config)#
CORE_1(config)#int vlan 4
CORE_1(config-if)#standby 4 ip 192.168.4.1
```

```
CORE_2#CONF T
Enter configuration commands, one per line.  End with CNTL/Z.
CORE_2(config)#int vlan 4
CORE_2(config-if)#standby 4 ip 192.168.4.1
CORE_2(config-if)#standby priority 150
CORE_2(config-if)#standby preempt
CORE_2(config-if)#
%HSRP-6-STATECHANGE: Vlan4 Grp 4 state Speak -> Standby

%HSRP-6-STATECHANGE: Vlan4 Grp 4 state Standby -> Active
```

Figure 2.16 : Configuration de HSRP Core 1 et Core 2

2.4.4 Configuration de STP

La figure 2.17 illustre les commandes qui nous permettent de configurer le protocole STP, et d'affecter un root primaire ou secondaire à un vlan

Les commandes **root primary** et **root secondary** sont utilisées dans un réseau STP pour influencer le choix du commutateur racine. La commande **root primary** est utilisée pour configurer un commutateur afin qu'il devienne le commutateur racine. D'autre part, la commande **root secondary** est utilisée pour configurer un commutateur en tant que commutateur racine de secours, prêt à prendre la place du commutateur racine actuel en cas de défaillance. L'utilisation de ces commandes doit être soigneusement planifiée pour éviter les boucles de commutation et garantir la fiabilité du réseau.

```
Enter configuration commands, one per line.  End with CNTL/Z.
CORE_2(config)#spanning-tree mode rapid-pvst
CORE_2(config)#spanning-tree vlan
%HSRP-6-STATECHANGE: Vlan2 Grp 2 state Standby -> Active

%HSRP-6-STATECHANGE: Vlan3 Grp 3 state Standby -> Active

% Incomplete command.
CORE_2(config)#spanning-tree vlan 4 root primary
CORE_2(config)#spanning-tree vlan 2,3 root secondary
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
CORE_1(config)#spanning-tree mode rapid-pvst
CORE_1(config)#
%HSRP-6-STATECHANGE: Vlan4 Grp 4 state Standby -> Active

CORE_1(config)#spanning-tree vlan 2,3 root primary
CORE_1(config)#spanning-tree vlan 2,3 root secondary
%HSRP-6-STATECHANGE: Vlan4 Grp 4 state Speak -> Standby

CORE_1(config)#spanning-tree vlan 4 root secondary
```

Figure 2.17 : Configuration STP

2.4.5 Configuration DHCP

Le protocole DHCP simplifie la gestion et l'attribution des adresses IP en configurant automatiquement les paramètres réseau des clients, éliminant ainsi la nécessité de configurer manuellement chaque ordinateur client.

```
CORE_1>en
CORE_1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CORE_1(config)#ip dhcp pool vlan2
CORE_1(dhcp-config)#network 192.168.2.0 255.255.255.0
CORE_1(dhcp-config)#dns-server 1.1.1.1
CORE_1(dhcp-config)#default-router 192.168.2.1
CORE_1(dhcp-config)#domain-name rsx.com
CORE_1(dhcp-config)#exit
CORE_1(config)#ip dhcp excluded-address 192.168.2.1 192.168.2.11
```

Figure 2.18 : Commandes de configuration DHCP du vlan 2

Le protocole DHCP doit assigner des adresses IP dans la plage 192.168.0.0/24, tout en excluant certaines adresses spécifiques de cette plage.

Le résultat de la configuration est le suivant :

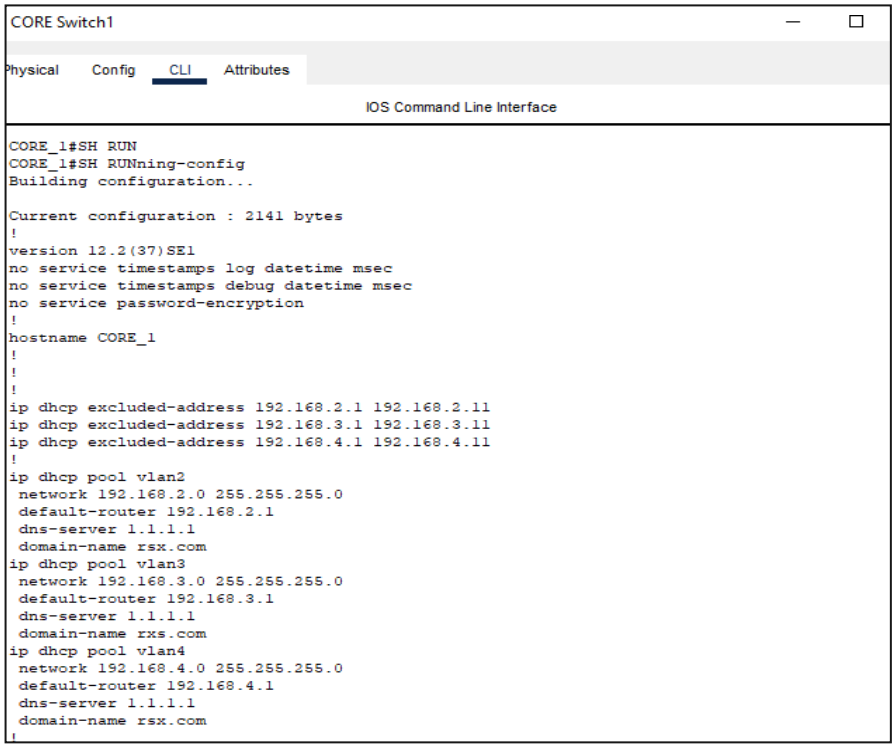

Figure 2.19 : Configuration DHCP sur Core 1

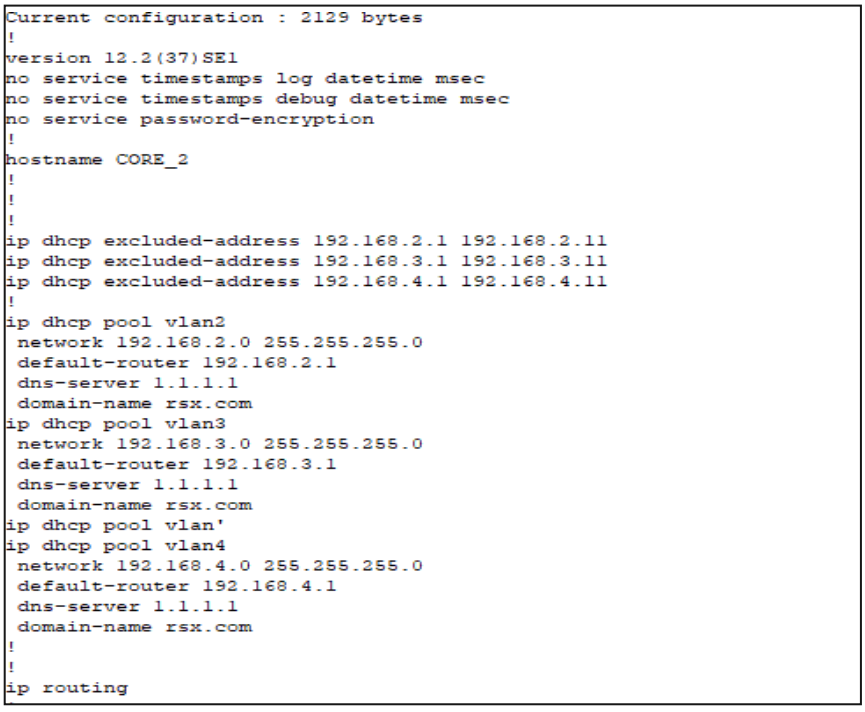

Figure 2.20 : Configuration DHCP sur Core 2

2.4.6 Configuration d'accès distant via Telnet

L'accès à distance aux commutateurs se fait par l'intermédiaire du protocole Telnet qui est utilisé sur les lignes VTY selon les commandes suivantes :

```
Access>EN
Access#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Access(config)#username stage password stage
Access(config)#line vty 0 15
Access(config-line)#login local
Access(config-line)#ex

Access(config-line)#exit
Access(config)#int vlan 2
Access(config-if)#ip address
Access(config-if)#ip address 192.168.2.4 255.255.255.0
Access(config-if)#NO SHUTDOWN
Access(config-if)#ex
Access(config)#



Access(config)#line vty 0 15
Access(config-line)#transport input telnet
Access(config-line)#
```

Figure 2.21: Configuration Telnet

2.5 Vérification et test de Réseau

2.5.1 Vérification des configurations VLANs

- Nous avons utilisé la commande « Show Vlan brief» à fin de prouver que les VLANs ont été créé et les interfaces du commutateur ont été associé.

```
Access#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig0/1, Gig0/2
2    Gestion                          active    Fa0/3, Fa0/4, Fa0/5
3    Commercial                       active    Fa0/6, Fa0/7, Fa0/8, Fa0/9
4    informatique                     active    Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
Access#
```

Figure 2.22: Configuration du réseau local virtuel

- La commande « show IP interface brief » permet d'afficher l'état des SVI.

```
CORE_2#
CORE_2#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/1        unassigned      YES unset  up                    up
FastEthernet0/2        unassigned      YES unset  up                    up
FastEthernet0/3        unassigned      YES unset  down                  down
FastEthernet0/4        unassigned      YES unset  down                  down
FastEthernet0/5        unassigned      YES unset  down                  down
FastEthernet0/6        unassigned      YES unset  down                  down
FastEthernet0/7        unassigned      YES unset  down                  down
FastEthernet0/8        unassigned      YES unset  down                  down
FastEthernet0/9        unassigned      YES unset  down                  down
FastEthernet0/10       unassigned      YES unset  down                  down
FastEthernet0/11       unassigned      YES unset  down                  down
FastEthernet0/12       unassigned      YES unset  down                  down
FastEthernet0/13       unassigned      YES unset  down                  down
FastEthernet0/14       unassigned      YES unset  down                  down
FastEthernet0/15       unassigned      YES unset  down                  down
FastEthernet0/16       unassigned      YES unset  down                  down
FastEthernet0/17       unassigned      YES unset  down                  down
FastEthernet0/18       unassigned      YES unset  down                  down
FastEthernet0/19       unassigned      YES unset  down                  down
FastEthernet0/20       unassigned      YES unset  down                  down
FastEthernet0/21       unassigned      YES unset  down                  down
FastEthernet0/22       unassigned      YES unset  down                  down
FastEthernet0/23       unassigned      YES unset  down                  down
FastEthernet0/24       unassigned      YES unset  down                  down
GigabitEthernet0/1     unassigned      YES unset  down                  down
GigabitEthernet0/2     unassigned      YES unset  down                  down
Vlan1                  unassigned      YES unset  administratively down down
Vlan2                  192.168.2.3     YES manual up                    up
Vlan3                  192.168.3.3     YES manual up                    up
Vlan4                  192.168.4.3     YES manual up                    up
```

Figure 2.23 : SVI sur core 2

```
CORE_1#SHOW IP INTERFACE BRIEF
Interface              IP-Address      OK? Method Status                Protocc
FastEthernet0/1        unassigned      YES unset  up                    up
FastEthernet0/2        unassigned      YES unset  up                    up
FastEthernet0/3        unassigned      YES unset  down                  down
FastEthernet0/4        unassigned      YES unset  down                  down
FastEthernet0/5        unassigned      YES unset  down                  down
FastEthernet0/6        unassigned      YES unset  down                  down
FastEthernet0/7        unassigned      YES unset  down                  down
FastEthernet0/8        unassigned      YES unset  down                  down
FastEthernet0/9        unassigned      YES unset  down                  down
FastEthernet0/10       unassigned      YES unset  down                  down
FastEthernet0/11       unassigned      YES unset  down                  down
FastEthernet0/12       unassigned      YES unset  down                  down
FastEthernet0/13       unassigned      YES unset  down                  down
FastEthernet0/14       unassigned      YES unset  down                  down
FastEthernet0/15       unassigned      YES unset  down                  down
FastEthernet0/16       unassigned      YES unset  down                  down
FastEthernet0/17       unassigned      YES unset  down                  down
FastEthernet0/18       unassigned      YES unset  down                  down
FastEthernet0/19       unassigned      YES unset  down                  down
FastEthernet0/20       unassigned      YES unset  down                  down
FastEthernet0/21       unassigned      YES unset  down                  down
FastEthernet0/22       unassigned      YES unset  down                  down
FastEthernet0/23       unassigned      YES unset  down                  down
FastEthernet0/24       unassigned      YES unset  down                  down
GigabitEthernet0/1     unassigned      YES unset  down                  down
GigabitEthernet0/2     unassigned      YES unset  down                  down
Vlan1                  unassigned      YES unset  administratively down down
Vlan2                  192.168.2.2     YES manual up                    up
Vlan3                  192.168.3.2     YES manual up                    up
Vlan4                  192.168.4.2     YES manual up                    up
```

Figure 2.24 : SVI sur core 1

2.5.2 Vérification de HSRP

La commande « show standby brief » est utilisé pour afficher le résumé des informations sur les groupes HSRP comme la montre les figures suivantes :

```
CORE_1>en
CORE_1#sh standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Vl2         2    100   Standby  192.168.2.3     local           192.168.2.1
Vl3         3    100   Standby  192.168.3.3     local           192.168.3.1
Vl4         4    150 P Active   local           192.168.4.3     192.168.4.1
CORE_1#
```

Figure 2.25: Etat HSRP sur core 1

```
CORE_2>en
CORE_2#sh standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Vl2         2    150 P Active   local           192.168.2.2     192.168.2.1
Vl3         3    150 P Active   local           192.168.3.2     192.168.3.1
Vl4         4    100   Standby  192.168.4.2     local           192.168.4.1
CORE_2#
```

Figure 2.26 : Etat HSRP sur core 2

2.5.3 Vérification du DHCP

A l'aide de la commande « show ip dhcp binding » qui permet d'afficher les adresses ip attribuées à chaque poste.

```
CORE_1#sh ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
192.168.2.11     0001.973E.0624           --                     Automatic
192.168.2.13     0001.C732.5ED2           --                     Automatic
192.168.3.11     00E0.F75C.40D7           --                     Automatic
192.168.3.12     0001.973E.0624           --                     Automatic
192.168.3.13     0004.9AD5.22B4           --                     Automatic
192.168.4.11     00D0.BA87.67B4           --                     Automatic
192.168.4.12     00E0.8FD5.0A70           --                     Automatic
CORE_1#
```

Figure 2.27 : Attribution des adresses IP

2.5.4 Vérification accès à distance Telnet

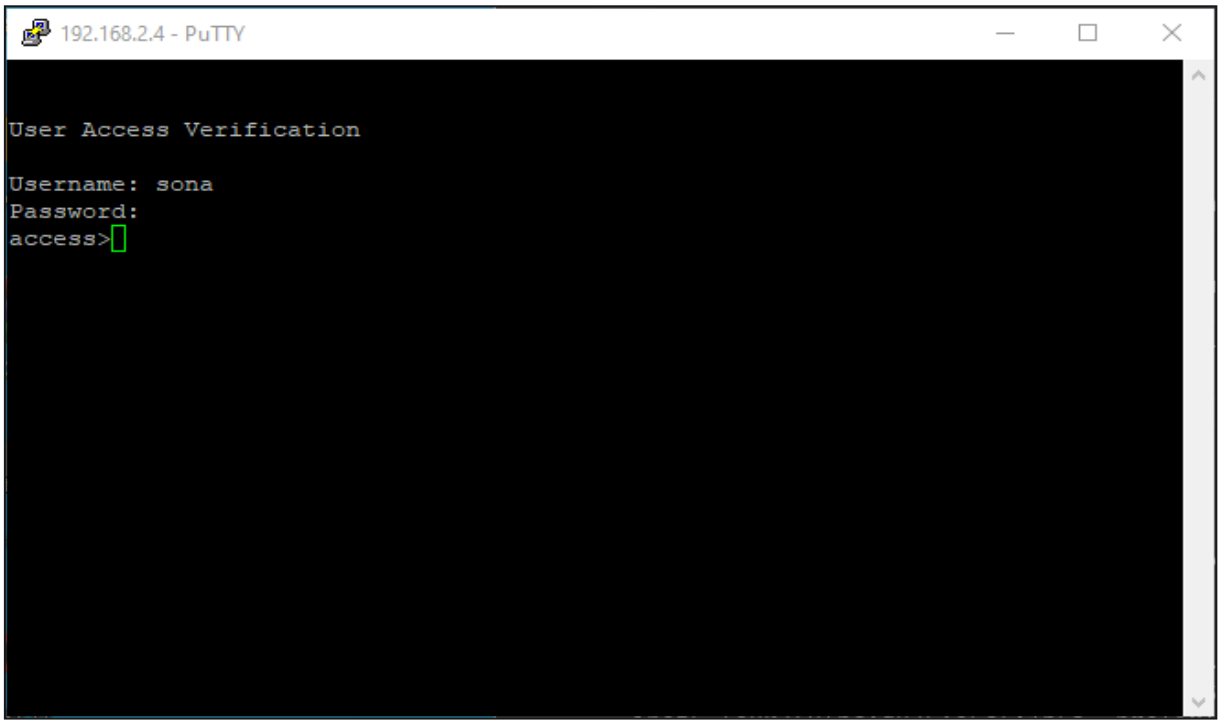

Figure 2.28 : Connexion à Telnet

2.5.5 Test de réseau

La commande « Ping » est utilisé pour vérifier la connectivité réseau entre deux périphériques en envoyant des paquets de test.

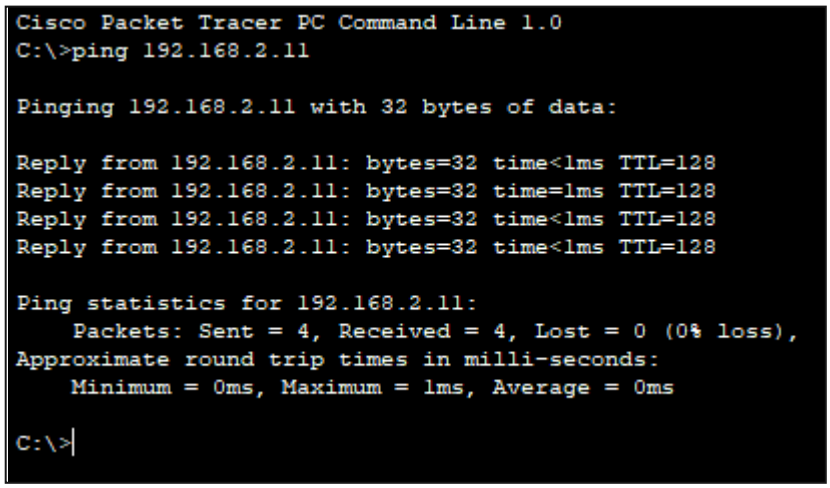

Figure 2.29: Test ping entre 2 postes du même Vlan

```
C:\>ping 192.168.3.11

Pinging 192.168.3.11 with 32 bytes of data:

Reply from 192.168.3.11: bytes=32 time<1ms TTL=127
Reply from 192.168.3.11: bytes=32 time=1ms TTL=127
Reply from 192.168.3.11: bytes=32 time<1ms TTL=127
Reply from 192.168.3.11: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.3.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

Figure 2.30: Test ping entre 2 postes de différent Vlan

2.6 Conclusion

Ce chapitre a traité des configurations de base des commutateurs Cisco, en particulier la configuration des VLAN, des ports et des protocoles de sécurité tels que HSRP. Ces configurations sont essentielles pour établir un réseau fonctionnel et sécurisé. Dans la prochaine partie, nous passerons à une étape critique en simulant des attaques sur le réseau que nous avons créé. Cela nous permettra d'évaluer l'efficacité de nos configurations et de mettre en lumière les vulnérabilités potentielles. La compréhension de ces concepts de base est cruciale pour la sécurité globale du réseau et nous fournira des informations précieuses pour améliorer notre stratégie de sécurité.

Chapitre 3 : les attaques réseaux du deuxième niveau

3.1 Introduction

La communication et les opérations modernes reposent sur les réseaux informatiques, qui connectent des millions de dispositifs et assurent un flux continu de données. Toutefois, ces réseaux sont fréquemment exposés à différentes formes d'attaques, notamment au niveau 2 du modèle OSI. Ce chapitre se concentre sur les attaques de niveau 2, telles que le MAC flooding, le VLAN hopping, et l'attaque STP. Nous explorerons les mécanismes de ces attaques, leurs conséquences sur les infrastructures réseau, et les vulnérabilités qu'elles exploitent. En comprenant ces menaces, nous serons en mesure de développer et de mettre en place des stratégies de défense afin de préserver les réseaux contre ces intrusions complexes.

3.2 Les attaques réseau du deuxième niveau

Les attaques de niveau 2 du modèle OSI se focalisent sur les vulnérabilités et les failles de sécurité dans la couche de liaison des données. Cette couche, aussi connu sous le nom de niveau 2, comprend les protocoles et les technologies employés pour la communication entre les nœuds d'un réseau local (LAN). Cette partie se penche sur quelques-unes des attaques les plus répandues au niveau de la couche 2 du modèle OSI, en expliquant comment elles opèrent et en détaillant leurs mécanismes de fonctionnement :

3.2.1 Schéma de Réseau et Localisation de l'Attaquant

Dans cette partie, nous exposons un schéma détaillé de notre réseau, créé à l'aide de Packet Tracer, qui illustre la topologie et les configurations des différents équipements. Ce schéma met en évidence la position de l'assaillant, identifié dans un VLAN spécifique, afin de démontrer que l'attaque est d'origine interne plutôt qu'externe. Cette représentation visuelle permet de mettre en évidence les points d'entrée de l'assaillant ainsi que les segments de réseau compromis, ce qui facilite la compréhension des mesures de défense et des stratégies de mitigation mises en place pour protéger l'infrastructure contre les menaces internes.

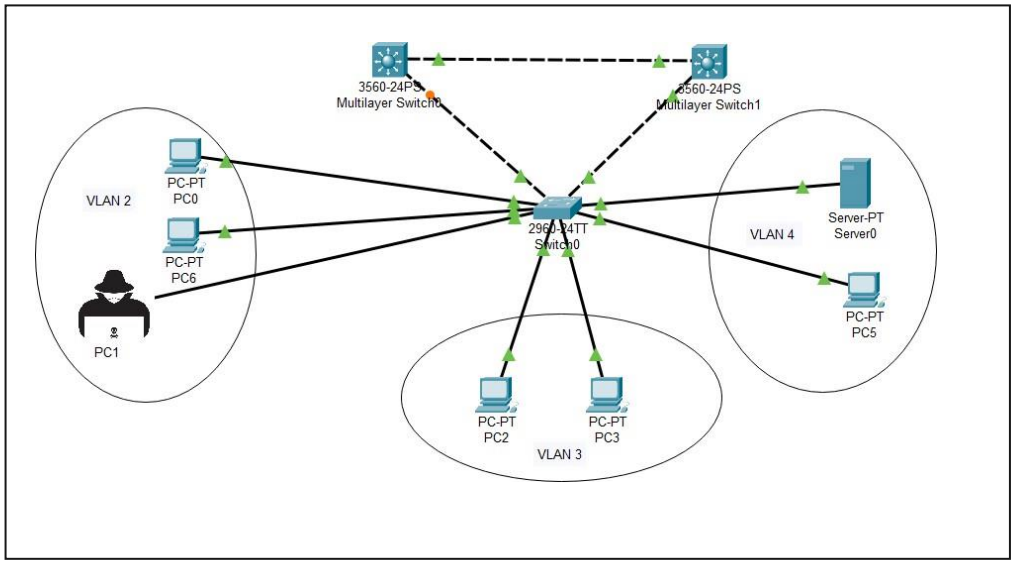

Figure 3.1 : Localisation de l'attaquant

3.3 Logiciels utilisés pour la simulation des attaques

3.3.1 PuTTY :

PuTTY est un logiciel libre open-source qui permet de se connecter à des serveurs distants en utilisant SSH, Telnet. Il est principalement employé dans les systèmes d'exploitation Windows, mais il existe des versions compatibles avec d'autres plateformes.

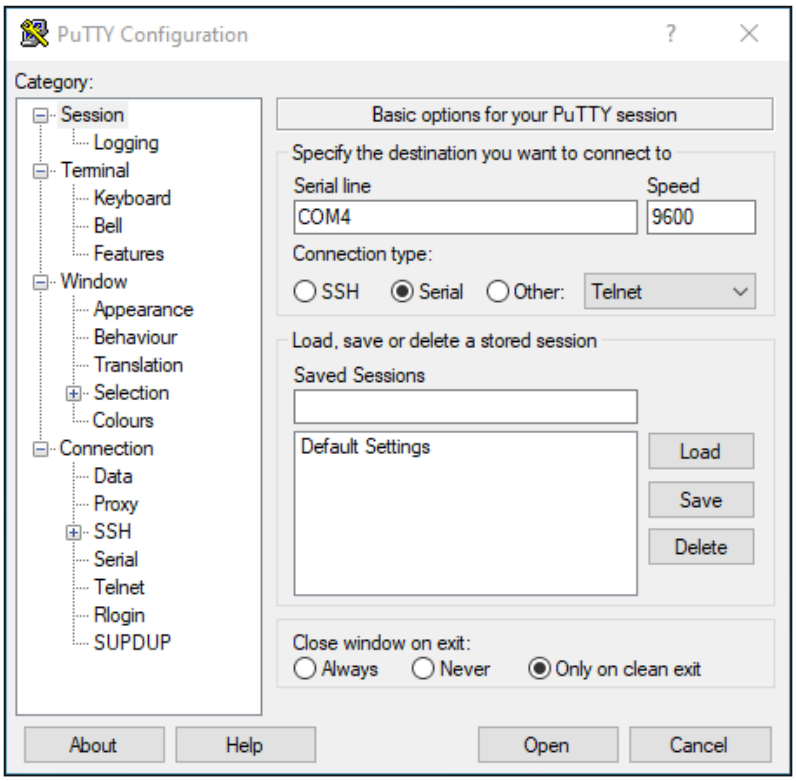

Figure 3.2: Configuration PuTTY

Dans notre partie, le logiciel PuTTY est utilisé pour se connecter aux commutateurs du réseau via un câble console.

3.3.2 Wireshark :

Wireshark est un logiciel open-source et gratuit d'analyse de réseau qui offre la possibilité de capturer, d'analyser et de diagnostiquer le trafic réseau en temps réel. Il est compatible avec de multiples protocoles de communication, propose une analyse approfondie des paquets capturés et possède une interface conviviale qui convient à la fois aux utilisateurs débutants et expérimentés. Il s'agit d'un instrument indispensable pour les experts en réseaux informatiques, les chercheurs en sécurité et les administrateurs système afin de saisir le fonctionnement du réseau, repérer les problèmes de performance et de sécurité, et améliorer les performances du réseau.

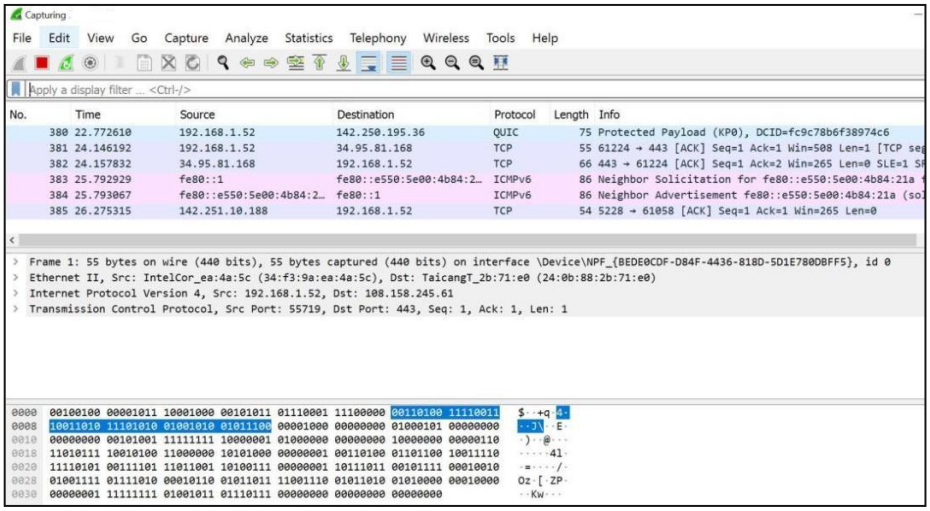

Figure 3.3 : Capture de WireShark

3.3.3 Kali Linux :

Kali Linux est une version de Linux qui se concentre sur la sécurité informatique et les tests de pénétration informatique Les outils de sécurité préinstallés dans Kali Linux couvrent divers aspects de la sécurité informatique, tels que les tests de pénétration, l'analyse de vulnérabilités, la forensique numérique et la sécurité informatique en général. Créée par Offensive Security et est largement employée par les experts en sécurité informatique, les chercheurs en sécurité et les spécialistes des tests d'intrusion.

Nous travaillons sur Kali Linux en utilisant VMware comme plateforme de virtualisation pour simuler des attaques réseau afin de tester la sécurité et la résilience de notre infrastructure informatique.

Figure 3.4 : Outils Kali Linux

- **Yersinia**

Yersinia est un modèle qui permet de réaliser des attaques de niveau 2. Son objectif est d'exploiter certaines faiblesses dans différents protocoles réseau. Il apparaît comme un Framework solide pour étudier et évaluer les réseaux et les systèmes mis en place. [24]

Dans ce modèle spécifique, les attaques pour les protocoles réseau suivants sont mises en place :

- Protocole Spanning Tree (STP).
- Protocole de découverte Cisco (CDP).
- Protocole de Trunk Dynamique (DTP).
- Protocole de Configuration Dynamique des Hôtes (DHCP).
- Protocole de Routage de Secours Actif (HSRP).
- 802.1q.
- 802.1x.
- Protocole de liaison entre commutateurs (ISL).
- Protocole de Trunk VLAN (VTP).

Yersinia est un outil d'attaque de couche 2 qui fait partie de la distribution Kali Linux.

Pour l'installer sur Kali linux on a utilisé la commande suivante :

« sudo apt-get install yersinia »

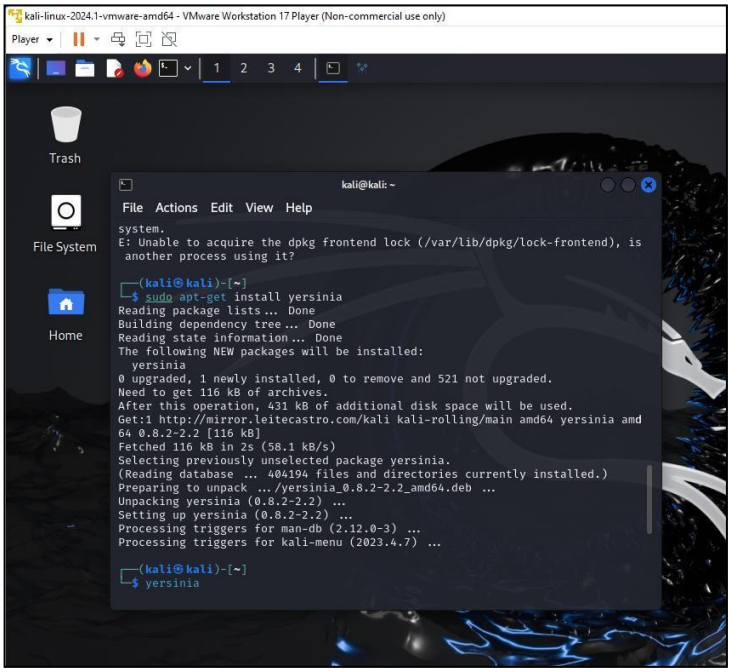

Figure 3.5: Installation Yersinia

3.4 Simulation des Scénarios d'Attaques sur le Réseau

3.4.1 Attaque par inondation de la table MAC (MAC flooding)

Dans les réseaux informatiques, le MAC flooding est une technique utilisée pour compromettre la sécurité des commutateurs réseau. En principe, le flux de données MAC submerge le commutateur réseau avec des paquets de données qui perturbent le flux de données habituel de l'expéditeur au destinataire, qui est partagé par les adresses MAC.

Les commutateurs conservent une table MAC (parfois connue sous le nom de table CAM) qui enregistre les adresses MAC individuelles du réseau pour les ports physiques du commutateur. Cela donne au commutateur la possibilité de rediriger les données vers le port physique où se trouve le destinataire, au lieu de les diffuser à tous les ports comme le ferait un concentrateur (hub). L'avantage de cette méthode est que les données sont acheminées exclusivement vers le segment réseau contenant l'ordinateur spécifiquement destinataire des données. [25]

Dans une attaque de type MAC flooding classique, l'attaquant envoie une multitude de trames Ethernet au commutateur, chacune avec une adresse MAC source distincte. L'objectif est de saturer la mémoire limitée du commutateur réservée à la table d'adresses MAC. Cela incite les commutateurs à se mettre en mode de défaillance ouverte (failopen), où ils agissent comme des concentrateurs, en diffusant les données à tous les ports. L'attaquant peut alors

utiliser un analyseur de paquets pour intercepter des données sensibles. Certains systèmes de commutation avancés, comme ceux offerts par Cisco, incluent des dispositifs de sécurité contre ce genre d'intervention. [26]

- **Table MAC du switch avant l'attaque :**

```
Switch#sh mac-
Switch#sh mac add
Switch#sh mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 All    0100.0ccc.cccc    STATIC      CPU
 All    0100.0ccc.cccd    STATIC      CPU
 All    0180.c200.0000    STATIC      CPU
 All    0180.c200.0001    STATIC      CPU
 All    0180.c200.0002    STATIC      CPU
 All    0180.c200.0003    STATIC      CPU
 All    0180.c200.0004    STATIC      CPU
 All    0180.c200.0005    STATIC      CPU
 All    0180.c200.0006    STATIC      CPU
 All    0180.c200.0007    STATIC      CPU
 All    0180.c200.0008    STATIC      CPU
 All    0180.c200.0009    STATIC      CPU
 All    0180.c200.000a    STATIC      CPU
 All    0180.c200.000b    STATIC      CPU
 All    0180.c200.000c    STATIC      CPU
 All    0180.c200.000d    STATIC      CPU
 All    0180.c200.000e    STATIC      CPU
 All    0180.c200.000f    STATIC      CPU
 All    0180.c200.0010    STATIC      CPU
 All    ffff.ffff.ffff    STATIC      CPU
   2    040e.3c22.7408    DYNAMIC     Gi0/3
Total Mac Addresses for this criterion: 21
Switch#
```

Figure 3.6: Mac-table avant l'attaque

Nous pouvons voir la taille de la table des adresses MAC semble être limitée à un certain nombre d'enregistrements.

- **Plan d'attaque :**

« Macof » (MAC address overflow) est un outil appartenant à la collection de « dsniff » sur Kali Linux, [27] il génère de paquets Ethernet contenant des adresses MAC source aléatoires à une vitesse très rapide, avec des milliers de paquets par seconde en moyenne.

Il s'agit de remplir la table d'adresses MAC du commutateur plus rapidement que sa capacité de gestion habituelle, ce qui peut entraîner des problèmes ou une mise en mode de défaillance ouverte (failopen) du commutateur.

L'attaque est lancée via la commande **« sudo macof –i eth0 »**

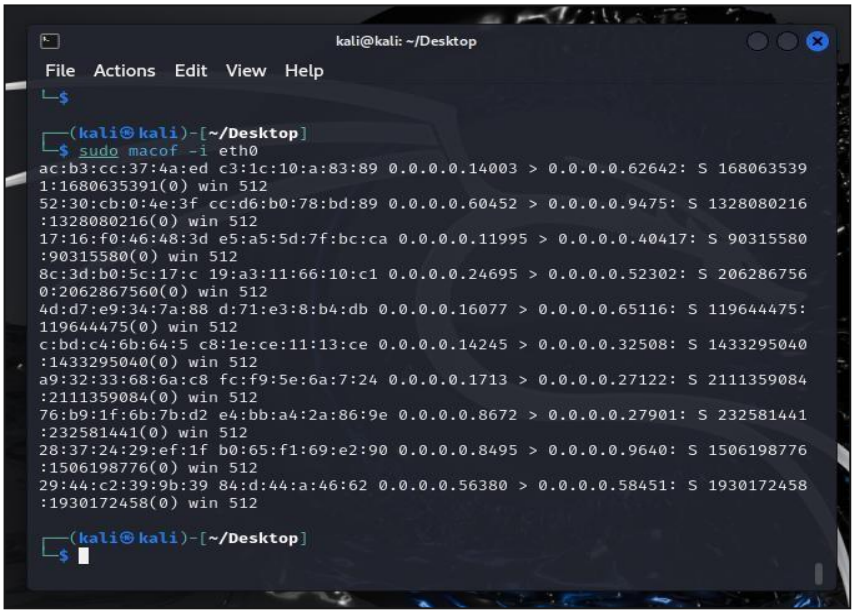

Figure 3.7: Lancement de l'attaque

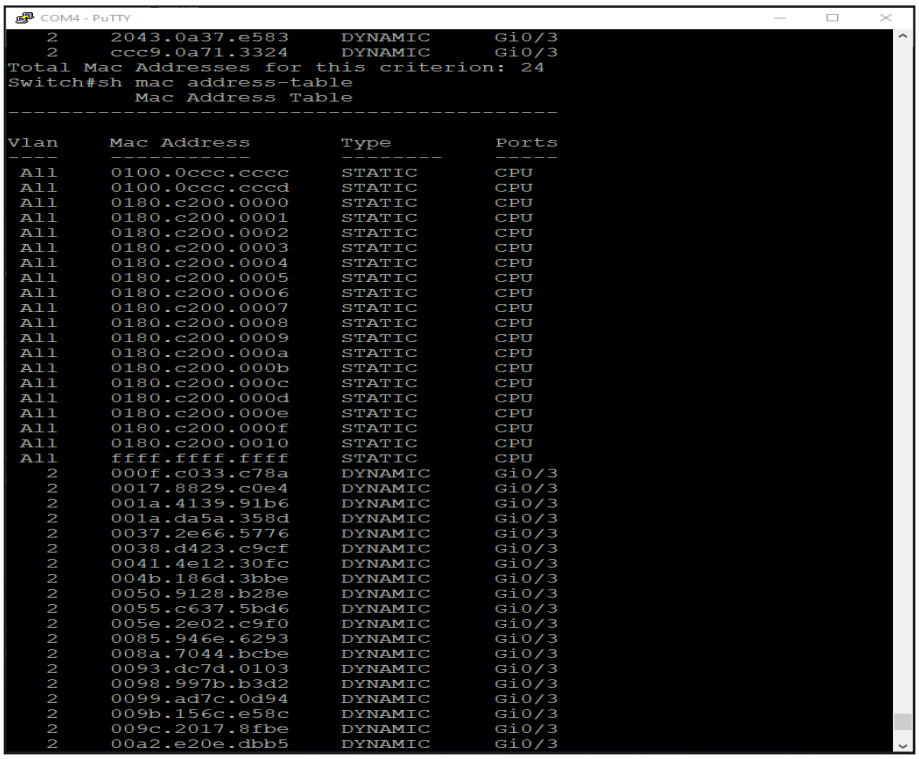

Figure 3.8: Mac-table après l'attaque

La table d'adresse MAC se remplit jusqu'à sa saturation, Cela va amener le commutateur à entrer en mode de défaillance ouverte (fail-open), et le commutateur va maintenant se comporter de la même manière qu'un concentrateur réseau. Il va transférer les données entrantes à tous les ports comme une diffusion générale.

3.4.2 Attaque par interception Telnet

Nous avons utilisé le logiciel « Wireshark » pour collecter et capturer le trafic Telnet, les paquets capturés peuvent être analysé en regardant les détails de chaque paquet.

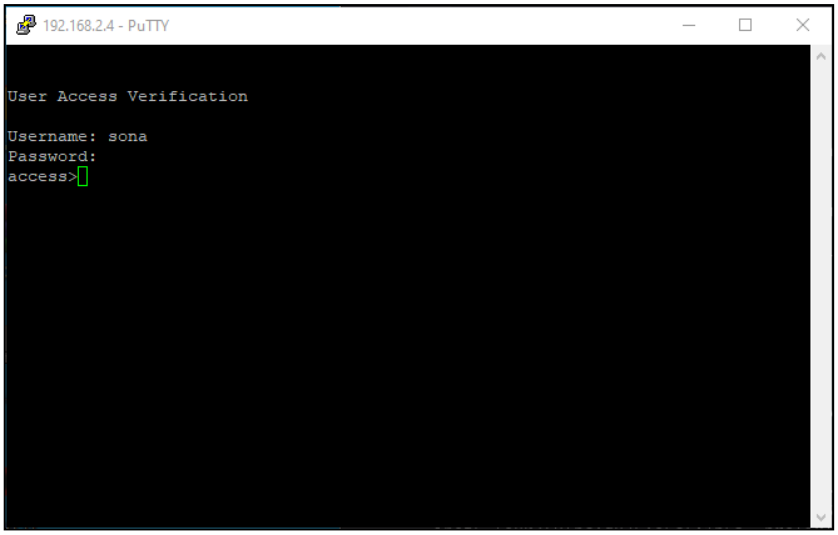

Figure 3.9: Avant attaque Telnet

En examinant les paquets Telnet, il est également possible de repérer des données confidentielles comme des identifiants d'authentification (noms d'utilisateur, mots de passe), des commandes système, et ainsi de suite.

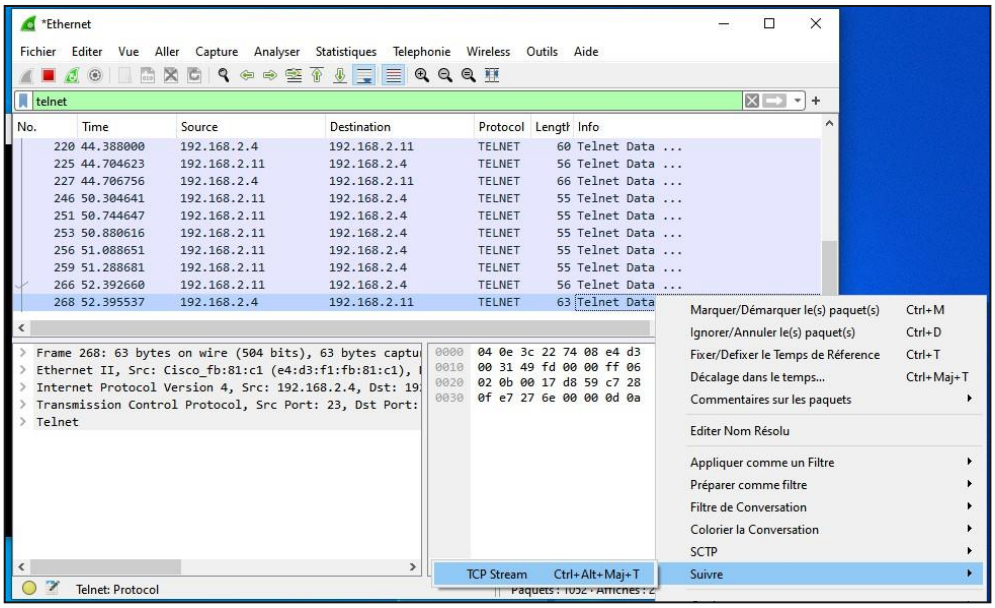

Figure 3.10: Activation du filtre Telnet sur Wireshark

Les informations la session Telnet sont affichées dans la fenêtre Follow TCP Stream. L'ensemble de la session est affiché en texte clair, incluant le mot de passe.

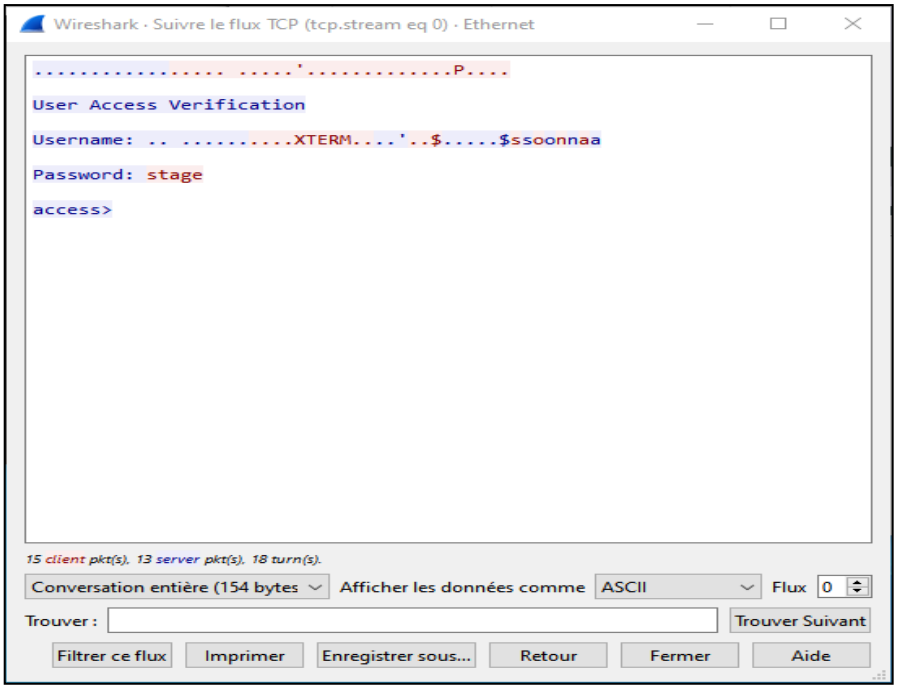

Figure 3.11: Résultat d'attaque Telnet

3.4.3 Attaque CDP Flooding

Cisco a développé le protocole Cisco Discovery Protocol (CDP), un protocole de couche 2 propriétaire. Un commutateur l'utilise pour repérer les périphériques adjacents. Toutefois, on a observé que lorsque le commutateur malveillant envoie des informations CDP incorrectes à son voisin, il est possible de lancer des attaques CDP.

Deux catégories d'attaques CDP existent. Le premier moyen est d'envoyer une quantité considérable de données CDP corrompues à une victime. Cela peut entraîner des problèmes tels que le plantage, le débordement ou même la réinitialisation de l'IOS du commutateur. Le deuxième moyen est d'envoyer un message CDP incorrect à une personne touchée. [28]

Nous utiliserons le modèle Yersinia pour la génération de l'attaque CDP flooding comme la montre la figure ci-dessous :

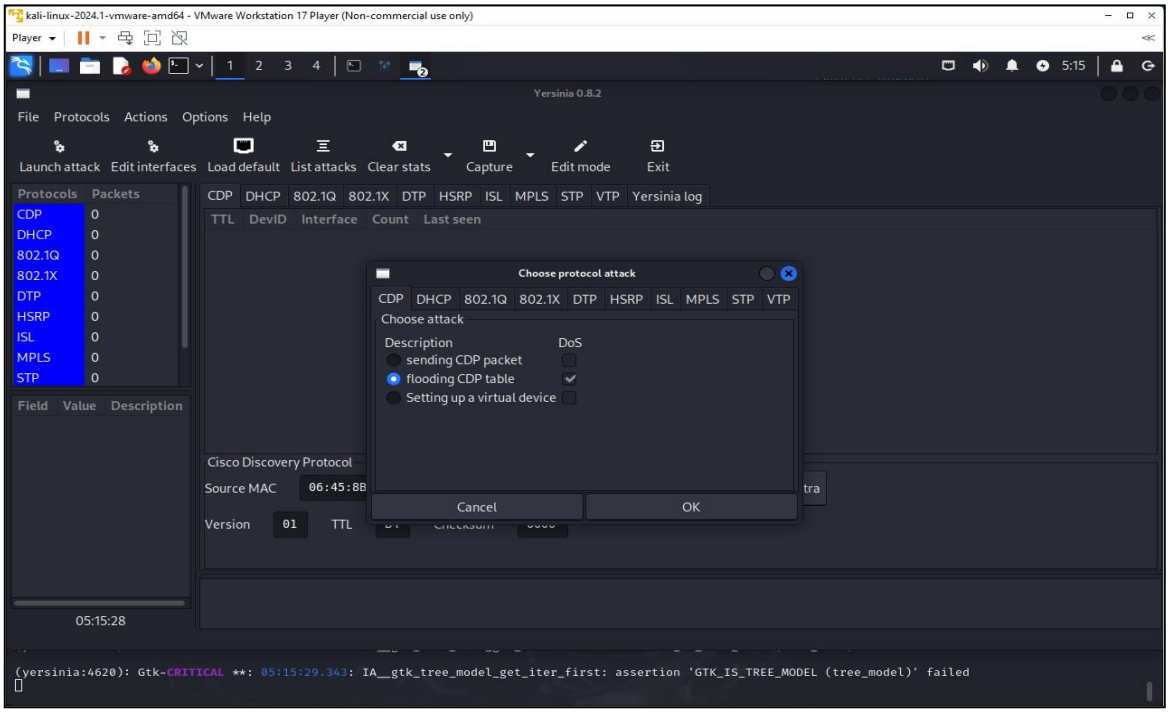

Figure 3.12: Attaque CDP flooding

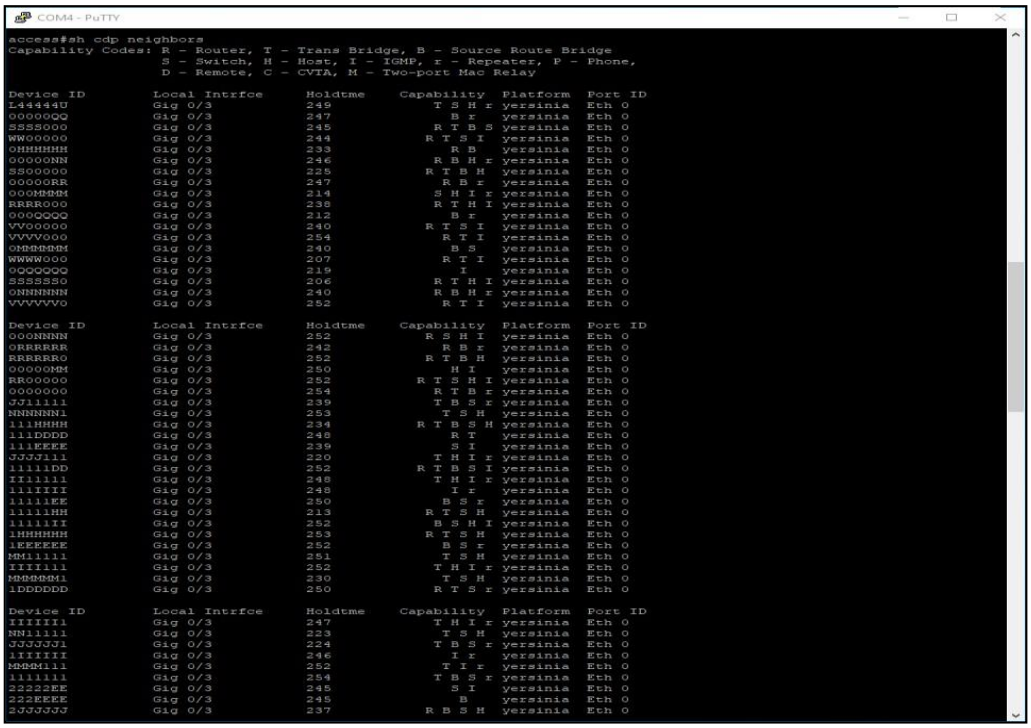

Figure 3.13: Résultat d'attaque CDP

Après l'exécution de la commande « show cdp neighbour » on remarque que la table cdp est saturée ce qui dépasse la capacité normale du dispositif à gérer ces informations. Ceci pourrait engendrer des difficultés de performance ou de fonctionnement du système.

3.4.4 Attaque par saut de vlan (VLAN hopping)

L'implémentation de VLAN dans un réseau moderne améliore les performances en réduisant la taille des domaines de collision et renforce la sécurité en isolant les flux de trafic de la couche 2 du modèle OSI. Cependant, il peut arriver dans certaines situations que le trafic d'autres VLAN soit visible ou que le changement de VLAN soit possible en raison de configurations réseau incomplètes établies par les administrateurs.

L'exploit de saut de VLAN est une technique de sécurité informatique qui vise à attirer les ressources en réseau sur un réseau virtuel (VLAN). Toutes les attaques par saut de VLAN reposent sur le principe fondamental selon lequel un hôte attaquant sur un VLAN peut accéder au trafic sur d'autres VLAN qui ne seraient normalement pas accessible. Deux techniques principales sont utilisées pour dépasser les VLAN : l'usurpation de commutateur (Spoofing) et le double marquage.

- **Attaque d'usurpation de commutateur (Spoofing)**

Les ports trunk, par défaut, sont accessibles à tous les VLAN et acheminent le trafic de plusieurs VLAN sur la même liaison physique, habituellement entre des commutateurs. Lors d'une attaque basique d'usurpation de commutateur, le pirate exploite le fait que la configuration par défaut du port du commutateur est dynamique automatique. Il met en place un système pour se présenter comme un commutateur.

Pour effectuer cette usurpation, il est nécessaire que le pirate puisse imiter 802.1Q et les messages DTP. Un pirate peut accéder à tous les VLAN autorisés sur le port trunk en faisant croire à un autre commutateur qu'il tente de former un trunk.

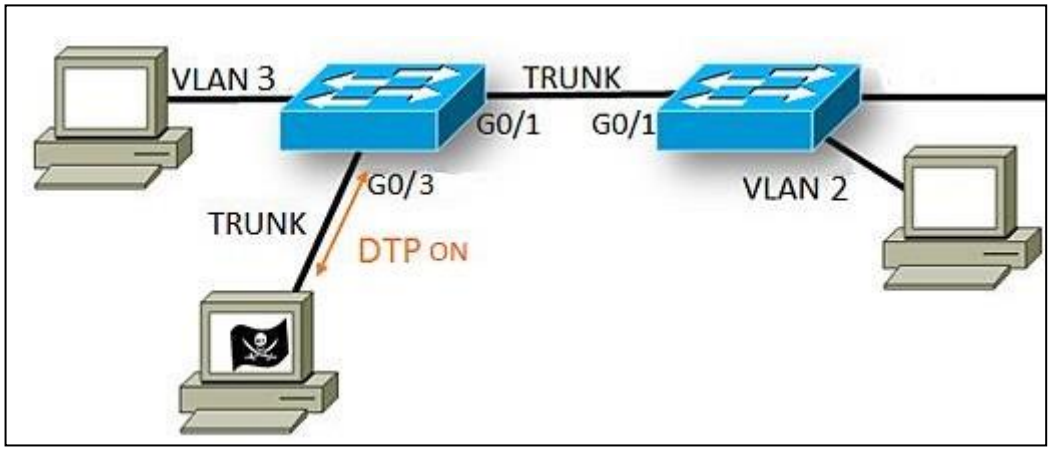

Figure 3.14: Attaque par usurpation de commutateur

- **Plan d'attaque**

La figure ci-dessous montre l'état du port G0/3 avant le lancement de l'attaque :

```
*Mar  1 02:07:57.765: %SYS-5-CONFIG_I: Configured from console by csh int g0/3 t
runk

Port        Mode             Encapsulation  Status        Native vlan
Gi0/3       auto             802.1q         not-trunking  1

Port        Vlans allowed on trunk
Gi0/3       2

Port        Vlans allowed and active in management domain
Gi0/3       2

Port        Vlans in spanning tree forwarding state and not pruned
Gi0/3       none
Access#
*Mar  1 02:08:18.711: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2, cha
nged state to up
```

Figure 3.15: statut du port G0/3 avant l'attaque

Lorsque le trunking est activé sur Yersinia, il est possible de simuler et de tester des attaques qui exploitent les vulnérabilités liées à la configuration des tronçons (trunks) du réseau.

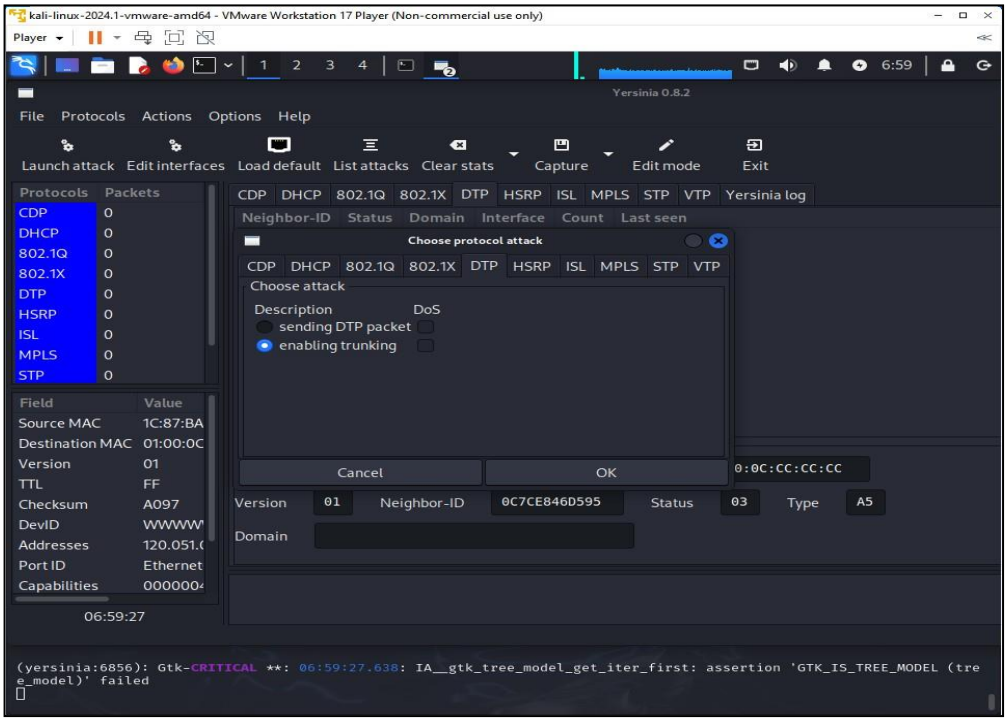

Figure 3.16: Génération d'attaque saut de vlan

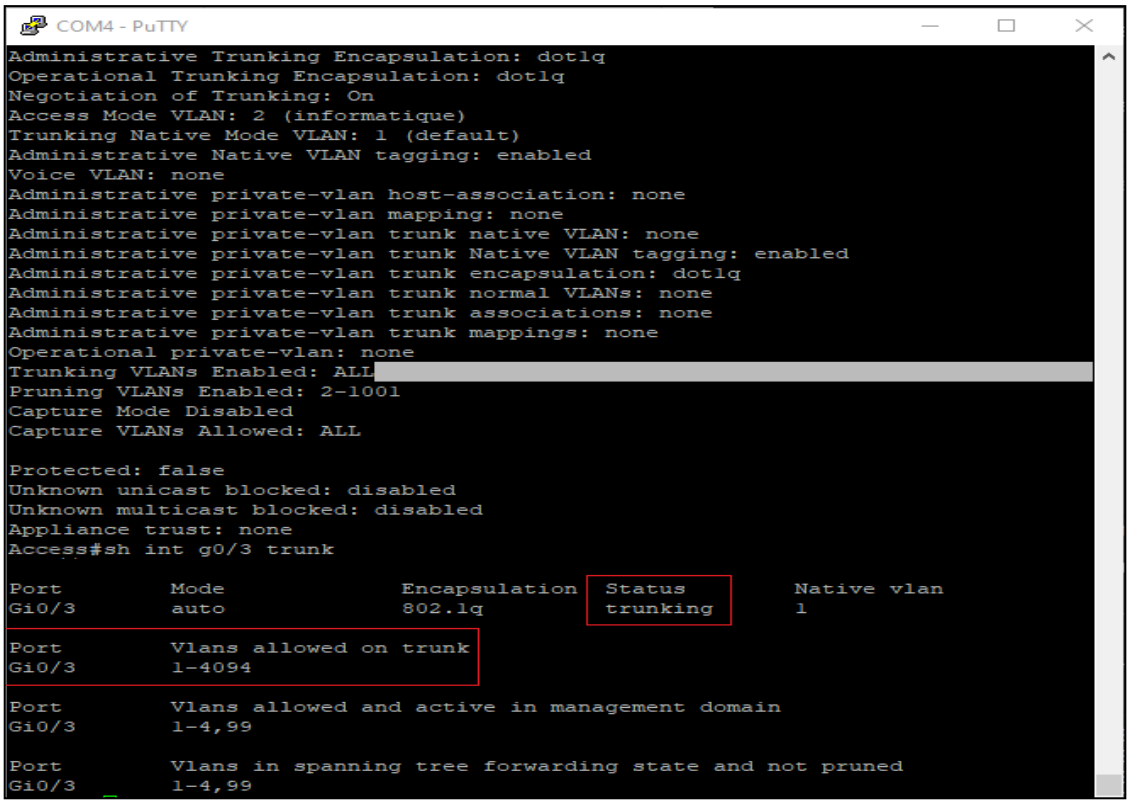

Figure 3.17: Statut du port G0/3 après l'attaque

Après l'attaque une agrégation trunk est activé, de plus le port G0/3 va directement recevoir le trafic de tous les VLAN et va également pouvoir accéder à tous les VLAN.

- **Attaque de double marquage**

L'attaque de double marquage est une technique de saut de VLAN où l'attaquant insère deux étiquettes VLAN dans une trame Ethernet. Dans ce type d'attaque, l'attaquant envoie une trame avec deux étiquettes VLAN (802.1Q). La première étiquette VLAN est retirée par le premier commutateur, et la trame est ensuite transmise à un autre VLAN.

3.4.5 Attaque DHCP par famine (DHCP Spoofing)

Le protocole Dynamic Host Control Protocol (DHCP) est utilisé par de nombreux appareils pour obtenir des configurations de réseau comme l'adresse IP, la passerelle, l'adresse du système de noms de domaine (DNS), etc. Cependant, la question de la sécurité n'a pas été étudiée de manière approfondie pendant la phase de conception. Ainsi, il présente plusieurs failles extrêmement lucratives pour de nombreux attaquants. Dans cette étude, nous examinons l'attaque DHCP par famine.

L'attaque de famine DHCP est une tentative d'attaquer les serveurs DHCP en créant des requêtes DHCP forgées dans le but d'épuiser toutes les adresses IP disponibles qui peuvent être attribuées par le serveur. Sous cette attaque, il est possible que les utilisateurs légitimes du réseau soient privés de leur service. [29]

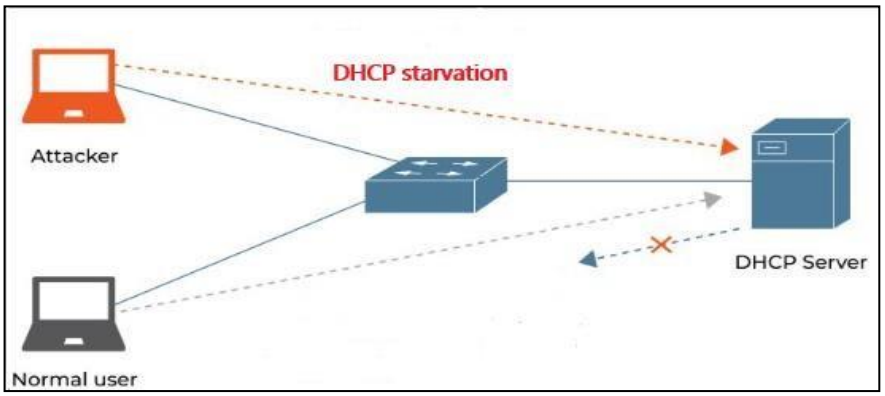

Figure 3.18: Attaque DHCP par famine

➢ Plan d'attaque

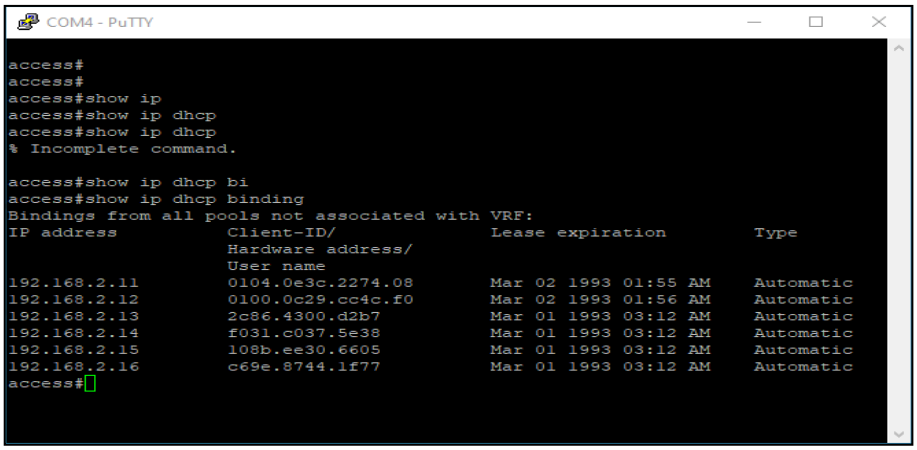

Figure 3.19: Avant l'attaque DHCP

Lors d'une attaque de famine DHCP, l'attaquant enverra un message de découverte au serveur DHCP avec une adresse MAC fausse afin de collecter toutes les adresses IP disponibles.

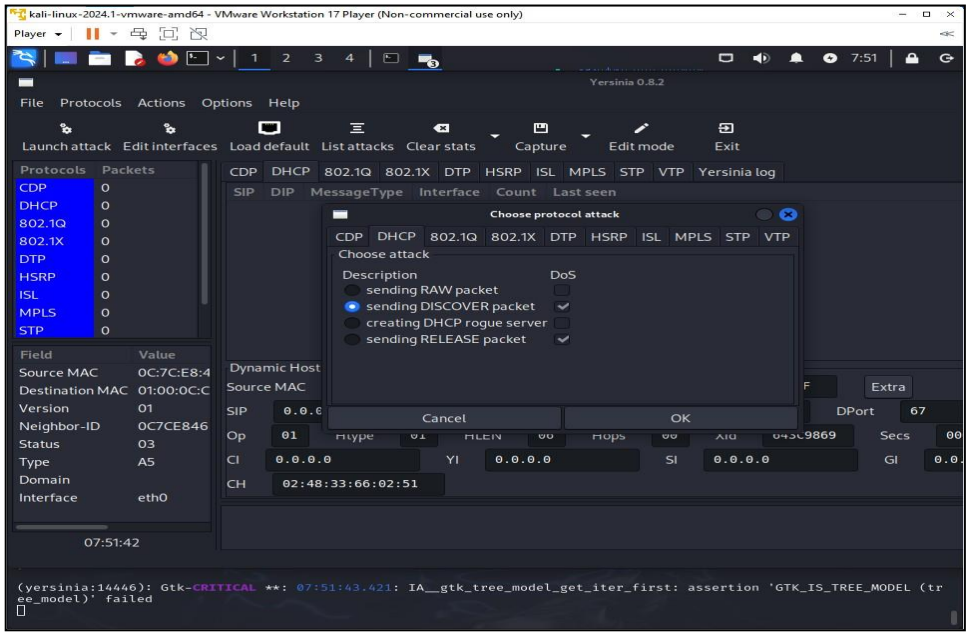

Figure 3.20: Envoi des messages de découverte DHCP

Une fois que l'attaquant a réalisé une attaque de famine, il va commencer à jouer le rôle d'un serveur DHCP et à louer de fausses adresses IP aux victimes.

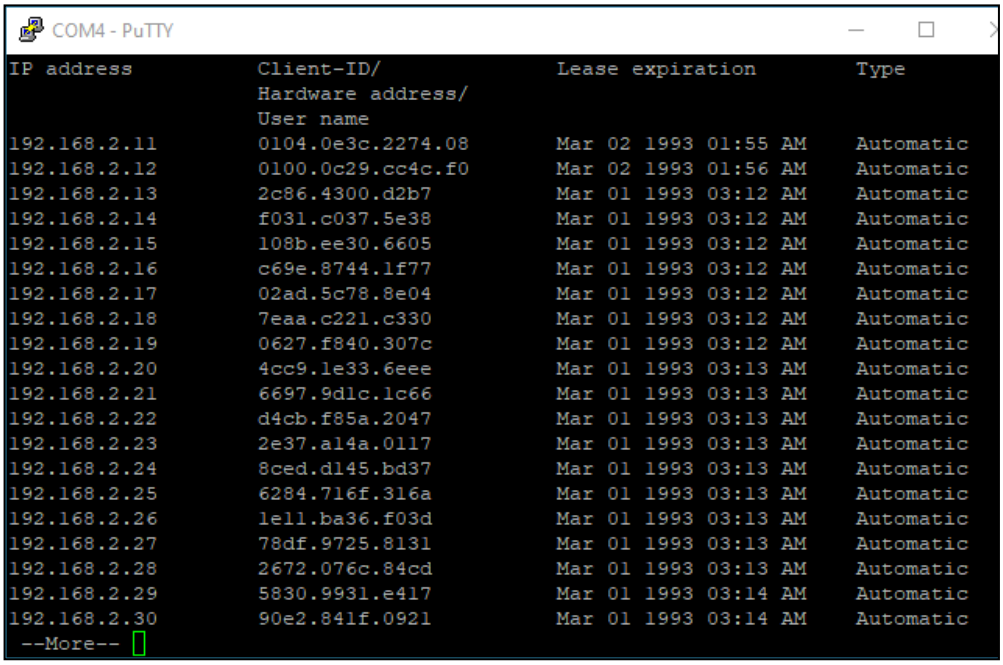

Figure 3.21: Résultat d'attaque DHCP

3.4.6 Attaque HSRP

Le protocole de routage HSRP (Hot Standby Routing Protocol) est utilisé dans les dispositifs CISCO afin de gérer les liens de secours. Le HSRP a pour objectif d'accroître la tolérance des pannes sur le réseau. Il comporte cependant une faille qui peut entraîner un déni de service ou la collecte de données par les attaquants. Nous vous expliquerons comment peut se produire une attaque HSRP dans la suite.

L'objectif de cette attaque est de faire de notre station d'attaque un commutateur actif HSRP, ce qui entraînera un déni de service ou la collecte de données sur le réseau. L'outil Yersinia, disponible sur la distribution Linux de KALI, sera utilisé de la manière suivante.

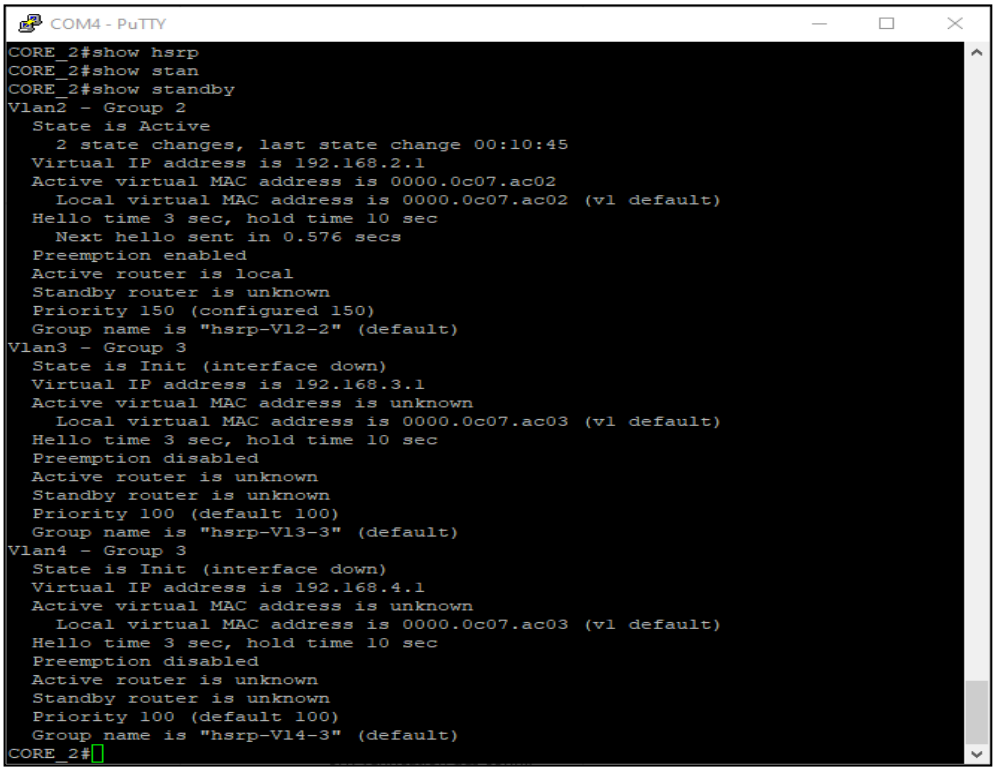

Figure 3.22: Avant attaque HSRP

Les messages HSRP envoyés par l'attaquant ont une priorité plus élevée ou un retard préempté inférieur à celui de leur routeur légitime. Cela entraîne la transformation du périphérique non autorisé en routeur ACTIVE du groupe HSRP ou dans notre cas un commutateur ACTIVE du groupe HSRP.

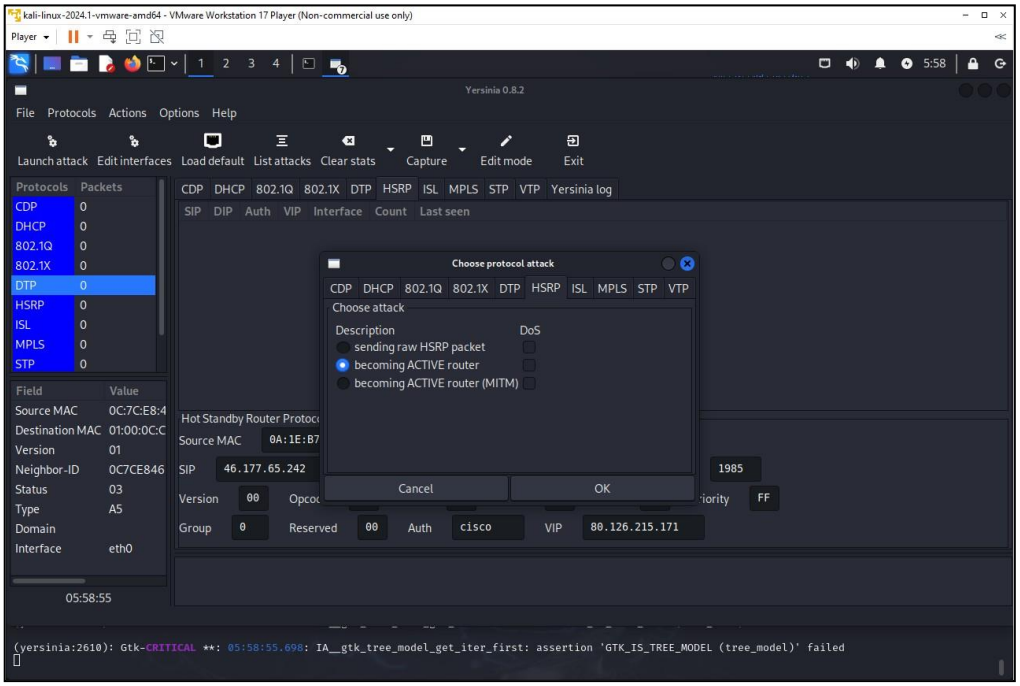

Figure 3.23: Début d'attaque HSRP

Après avoir exécuté l'attaque HSRP, On indique l'adresse IP source sous laquelle nous souhaitons la mettre en place. Il n'est pas essentiel d'appartenir au même sous-réseau.

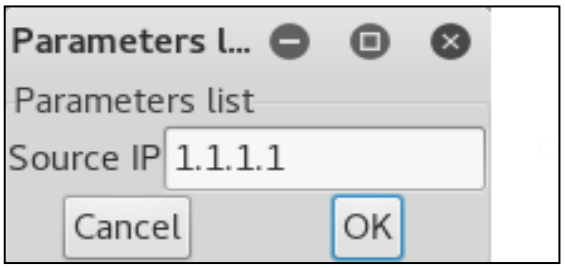

Figure 3.24: Adresse IP du routeur ACTIVE

Le résultat de l'attaque sera visible une fois que nous aurons saisi la commande « show standby brief ». Les deux commutateurs ont signalé que notre station d'attaque était un commutateur actif.

```
CORE_1#SH STANDBY BRIEF
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Vl2         2    100   Standby   1.1.1.1         local           192.168.2.1
Vl3         3    100   Standby   1.1.1.1         local           192.168.3.1
Vl4         4    150 P Active    1.1.1.1         192.168.4.3     192.168.4.1
CORE_1#
```

Figure 3.25: Résultat d'attaque sur core 1

```
CORE_2#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Vl2         2    150 P Active    1.1.1.1         192.168.2.2     192.168.2.1
Vl3         3    150 P Active    1.1.1.1         192.168.3.2     192.168.3.1
Vl4         4    100   Standby   1.1.1.1         local           192.168.4.1
CORE_2#
```

Figure 3.26: Résultat d'attaque sur core 2

3.4.7 Attaque Spanning-tree (STP)

Le protocole STP est utilisé dans les périphériques de commutation gérés qui appliquent plus d'un chemin à la connexion entre les commutateurs, il est essentiel pour la stabilité du réseau et la transmission de données efficace. Il offre des avantages tels que la redondance, la résilience, ainsi que la facilité de mise en œuvre et l'interopérabilité. Néanmoins, il est important de comprendre les risques liés à la sécurité ce qui nous mène à expliquer comment peut se produire une attaque STP dans la suite.

- **Plan d'attaque**

L'objectif de l'attaque STP (Spanning Tree Protocol) est d'influencer les processus de topologie réseau en envoyant des BPDUs (Bridge Protocol Data Units) simulés afin de prendre le contrôle du rôle du Root Bridge.

Le principe de fonctionnement de cette attaque est illustré dans la figure ci-dessous :

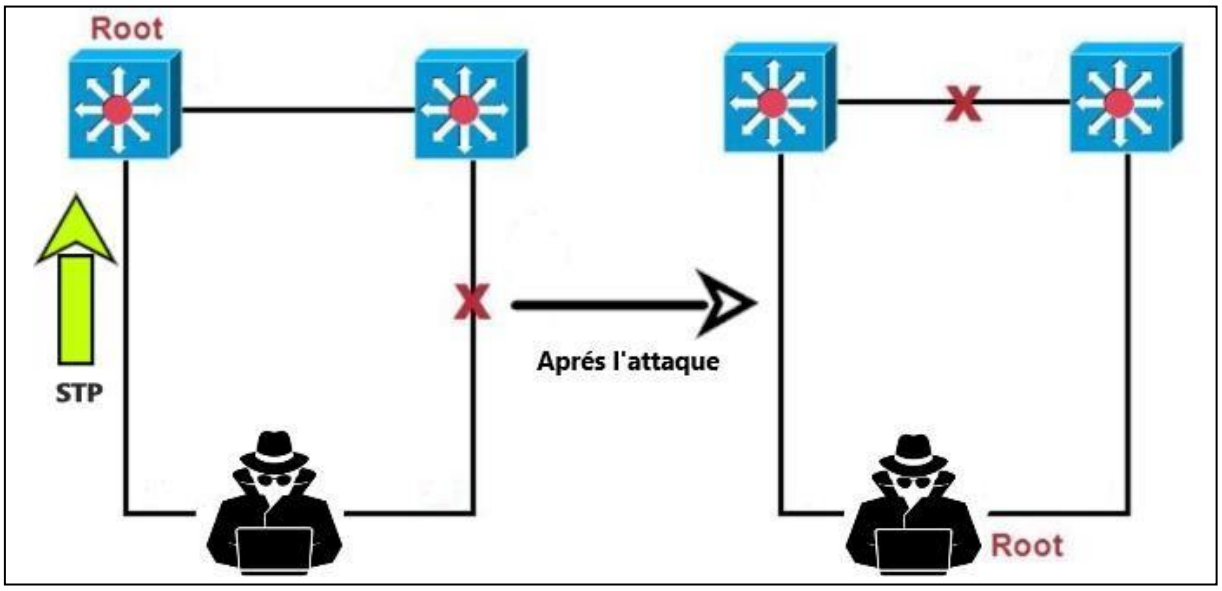

Figure 3.27: Principe attaque STP

Nous utilisons l'outil Yersinia pour envoyer des BPDUs falsifiés sur le réseau, ces BPDUs contiennent des informations de priorité et de coût de chemin supérieures à celles du root bridge actuel.

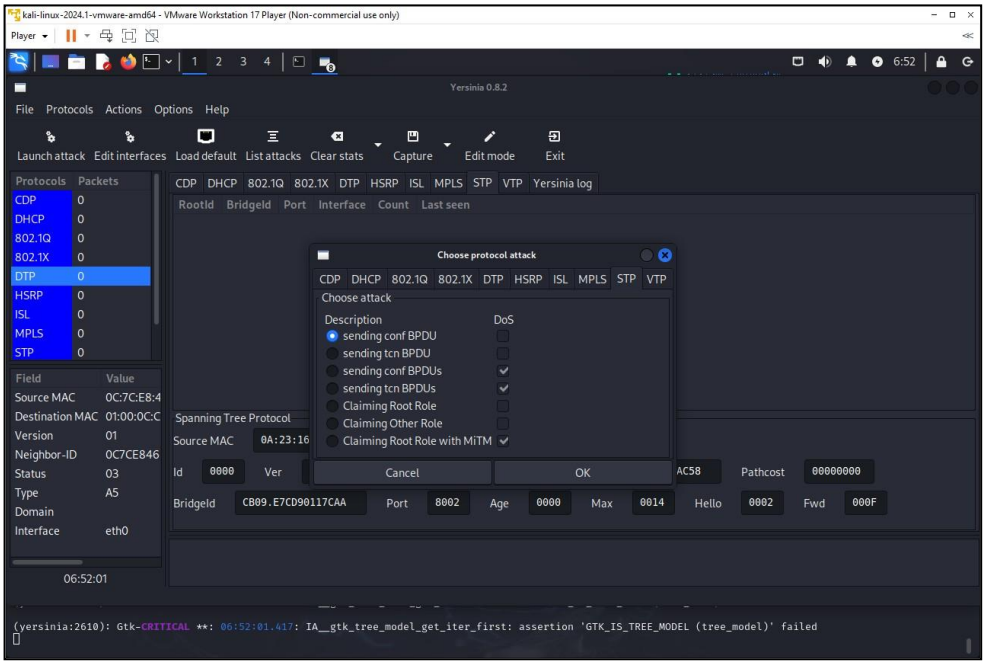

Figure 3.28: Attaque STP sur Yersinia

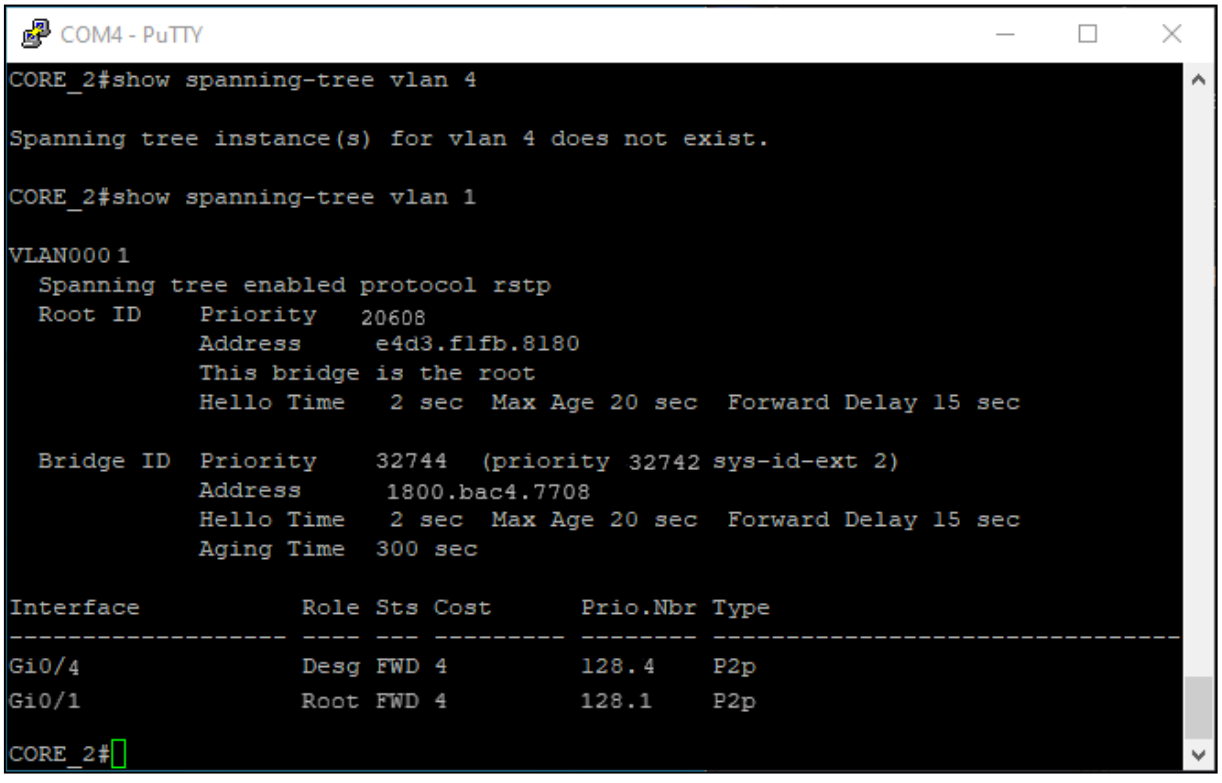

Figure 3.29: Avant attaque STP

L'attaque vise à réduire les niveaux de ressources de la CPU et à prendre les droits d'accès au pont de la racine en modifiant la valeur de l'adresse mac et en abaissant la valeur prioritaire sur STP.

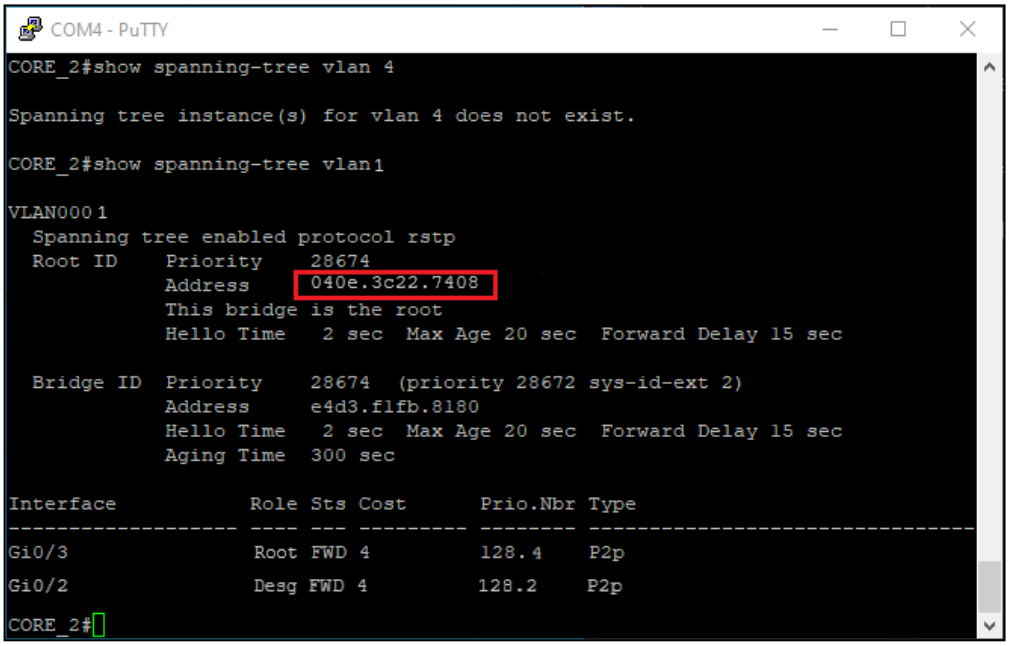

Figure 3.30: Après l'attaque STP

Le résultat de l'attaque est qu'il y a un changement dans ID Root et l'ID Bridge, qui est en constante évolution.

3.5 Conclusion

Ce chapitre examine différentes attaques réseau de niveau 2, en détaillant leur mécanisme, leurs conséquences potentielles et les failles qu'elles exploitent. En explorant des méthodes comme le MAC Flooding, le VLAN hopping et les attaques HSRP et STP, nous avons révélé combien un attaquant peut facilement compromettre l'intégrité et la sécurité d'un réseau si des mesures de protection adéquates ne sont pas mises en œuvre. L'importance cruciale de la sécurisation des réseaux au niveau 2 est mise en évidence par ces observations afin de prévenir les intrusions malveillantes et de protéger les informations confidentielles de l'entreprise. Donc, il est essentiel de renforcer les défenses réseau à ce stade afin d'assurer une infrastructure sécurisée et pérenne.

Chapitre 4 : Approches avancées pour la sécurisation des réseaux

4.1 Introduction

Dans ce chapitre, nous allons examiner un élément crucial de notre projet : la sécurisation du réseau que nous avons mis en place. Après avoir construit et configuré notre réseau, nous avons simulé divers types d'attaques pour évaluer sa résistance. En identifiant les vulnérabilités potentielles, nous pourrons mettre en place des solutions efficaces pour renforcer sa sécurité. Ce processus est essentiel pour assurer le bon fonctionnement et la sécurité de notre réseau dans des environnements réels.

4.2Les solutions de sécurité réseaux pour la prévention de chaque attaque réalisée :

4.2.1 Attaque par inondation de la table d'adresses MAC :

Après avoir utilisé la commande **macof** sur Kali Linux sur notre switch, notre table MAC a été saturée, entraînant la mise hors service du port en raison d'une surcharge. Pour remédier à cette situation, nous avons mis en place des solutions de sécurité des ports et d'authentification 802.1X.

- La sécurité des ports a été configurée pour limiter le nombre d'adresses MAC autorisées sur chaque port. Par exemple, nous pourrions autoriser uniquement une adresse MAC spécifique par port. Cela empêche les attaques de type MAC flooding, telles que celle provoquée par **macof**, en limitant le nombre d'adresses MAC pouvant être associées à un port.

```
Switch#conf  t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int g0/3
Switch(config-if)#switchport port-security ?
  aging         Port-security aging commands
  mac-address   Secure mac address
  maximum       Max secure addresses
  violation     Security violation mode
  <cr>

Switch(config-if)#switchport port-security
```

Figure 4.1 : Options port-security sur le switch

La commande **port security** sur un commutateur Cisco permet de configurer des fonctionnalités de sécurité pour limiter le nombre d'adresses MAC autorisées sur un port et de prendre des mesures en cas de violation de sécurité. Voici quelques options courantes de la commande **port security** :

1. **Switchport port-security maximum <valeur>** : Cette option définit le nombre maximal d'adresses MAC autorisées sur le port.

2. **Switchport port-security violation {shutdown | restrict | protect}** : Cette option spécifie l'action à prendre en cas de violation de sécurité.

- **Restrict** : Permet le trafic provenant de l'adresse MAC autorisée mais envoie une notification.
- **Protect** : Filtrer le trafic provenant de l'adresse MAC non autorisée sans notification.

3. **Switchport port-security mac-address <adresse MAC>** : Permet de spécifier manuellement une adresse MAC autorisée sur le port.

4. **Switchport port-security aging {time | type}** : Cette option configure la façon dont les adresses MAC sont retirées de la table de sécurité du port.

    - **Time** : Spécifie le temps en minutes avant qu'une adresse MAC non utilisée ne soit retirée.

    - **Type** : Configure le type d'expiration des adresses MAC (par exemple, **inactivity** pour l'expiration en fonction de l'inactivité).

```
Switch(config)#int g0/3
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 5
Switch(config-if)#sh
Switch(config-if)#shutdown
Switch(config-if)#no
*Mar  1 01:17:04.052: %LINEPROTO-5-UPDOWN: Line protocol on Interface
 Vlan2, changed state to down
Switch(config-if)#no
*Mar  1 01:17:06.040: %LINK-5-CHANGED: Interface GigabitEthernet0/3,
changed state to administratively down
*Mar  1 01:17:07.046: %LINEPROTO-5-UPDOWN: Line protocol on Interface
 GigabitEthernet0/3, changed state to down
Switch(config-if)#no sh
Switch(config-if)#no shutdown
Switch(config-if)#
*Mar  1 01:17:13.204: %LINK-3-UPDOWN: Interface GigabitEthernet0/3, c
hanged state to down
Switch(config-if)#
*Mar  1 01:17:21.878: %LINK-3-UPDOWN: Interface GigabitEthernet0/3, c
hanged state to up
*Mar  1 01:17:22.884: %LINEPROTO-5-UPDOWN: Line protocol on Interface
 GigabitEthernet0/3, changed state to up
Switch(config-if)#
```

Figure 4.2 : Configuration de la solution port-security

La figure 4.2 montre qu'on a configuré la sécurité des ports sur notre commutateur Cisco en utilisant la commande **switchport port-security maximum 5** pour limiter le nombre d'adresses MAC autorisées sur chaque port.

Après avoir configuré l'option **switchport port-security maximum 5** on a essayé de relancer une attaque avec kali linux et voici le résultat de l'attaque sur la table MAC de notre commutateur comme le montre la figure 4.3 ci-dessous. On remarque que on a 5 nouvelles adresses mac de l'interface ou l'attaque a été lancé g0/3 et cela n'a pas saturé notre switch.

```
Switch#sh mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 All    0100.0ccc.cccc    STATIC      CPU
 All    0100.0ccc.cccd    STATIC      CPU
 All    0180.c200.0000    STATIC      CPU
 All    0180.c200.0001    STATIC      CPU
 All    0180.c200.0002    STATIC      CPU
 All    0180.c200.0003    STATIC      CPU
 All    0180.c200.0004    STATIC      CPU
 All    0180.c200.0005    STATIC      CPU
 All    0180.c200.0006    STATIC      CPU
 All    0180.c200.0007    STATIC      CPU
 All    0180.c200.0008    STATIC      CPU
 All    0180.c200.0009    STATIC      CPU
 All    0180.c200.000a    STATIC      CPU
 All    0180.c200.000b    STATIC      CPU
 All    0180.c200.000c    STATIC      CPU
 All    0180.c200.000d    STATIC      CPU
 All    0180.c200.000e    STATIC      CPU
 All    0180.c200.000f    STATIC      CPU
 All    0180.c200.0010    STATIC      CPU
 All    ffff.ffff.ffff    STATIC      CPU
   2    000c.29cc.4cf0    DYNAMIC     Gi0/3
   2    040e.3c22.7408    DYNAMIC     Gi0/3
   2    1e7e.bc7d.6129    DYNAMIC     Gi0/3
   2    2ca4.9f49.b569    DYNAMIC     Gi0/3
   2    3808.4401.3154    DYNAMIC     Gi0/3
   2    ce2f.121e.1d43    DYNAMIC     Gi0/3
Total Mac Addresses for this criterion: 26
Switch#
```

Figure 4.3 : Tables des adresses mac après l'attaque

- L'authentification 802.1X est une mesure supplémentaire de sécurité qui exige que les appareils fournissent des informations d'identification avant d'être autorisés à accéder au réseau. Cela empêche les appareils non autorisés de se connecter même s'ils sont capables de générer du trafic réseau.

  En utilisant ces solutions en combinaison, nous renforçons la sécurité de notre réseau en empêchant les attaques de saturation de la table MAC et en limitant l'accès aux seuls appareils authentifiés.

4.2.2 Attaque par interception de trafic Telnet :

Au cours de la section précédente, nous avons employé l'outil Wireshark afin de saisir et d'analyser le flux de données réseau, ce qui nous a donné la possibilité de visualiser un mot de passe telnet en texte clair. À présent, nous allons mettre en place une solution plus sécurisée en configurant le service SSH (Secure Shell).

- SSH (Secure Shell) est un protocole de communication sécurisé qui permet d'accéder à distance à un système informatique via un réseau. Contrairement à d'autres protocoles tels que Telnet, qui transmettent les données y compris les mots de passe en texte clair, SSH utilise une connexion cryptée pour garantir la confidentialité et l'intégrité des données échangées entre le client et le serveur. En plus de cela, il offre des fonctionnalités avancées comme l'authentification par clé publique/privée, la gestion des identités et le transfert de fichiers sécurisé (SFTP). [30]

  Pour configurer SSH, voici les étapes générales :

```
access(config)#ip domain name sona.com
access(config)#username sona password stage
access(config)#ip ssh version 2
access(config)#crypto key generate rsa
The name for the keys will be: access.sona.com
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 4 seconds)
```

Figure 4.4 : Configuration SSH 1

```
access(config)#line vty 0 15
access(config-line)#tran
access(config-line)#transport in
access(config-line)#transport input s
access(config-line)#transport input ssh
access(config-line)#logi
access(config-line)#login loc
access(config-line)#login local
access(config-line)#
```

Figure 4.5 : Configuration SSH 2

Les figures 4.4 et 4.5 illustrent les étapes de configuration SSH sur un switch Cisco. La première étape consiste à créer un nom de domaine et à définir un nom d'utilisateur ainsi qu'un mot de passe. Ensuite, la clé RSA est générée pour le chiffrement des données. Après cela, le protocole SSH version 2 est activé pour renforcer la sécurité de la connexion. Enfin, le

transport SSH est activé sur les lignes virtuelles pour permettre les connexions SSH uniquement.

Une fois la configuration SSH terminée sur le switch, le trafic entre le client SSH et le serveur est chiffré. Cela signifie que même si un outil tel que Wireshark est utilisé pour capturer le trafic les données capturées apparaîtront comme des données chiffrées et ne pourront pas être lues en clair comme le montre la figure 4.8 ci-dessous. Le chiffrement utilisé par SSH rend extrêmement difficile pour un attaquant d'intercepter et de comprendre le contenu des communications entre le client et le serveur SSH.

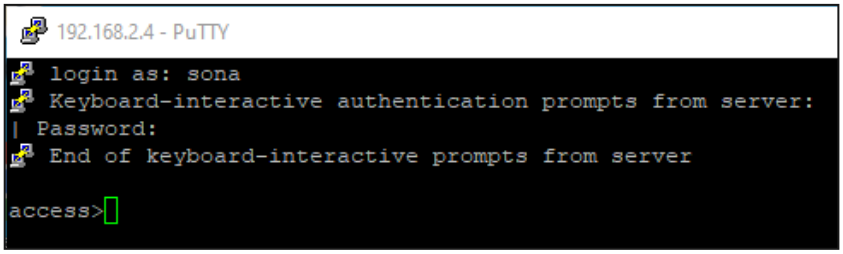

Figure 4.6 : Connexion SSH par le logiciel PuTTY

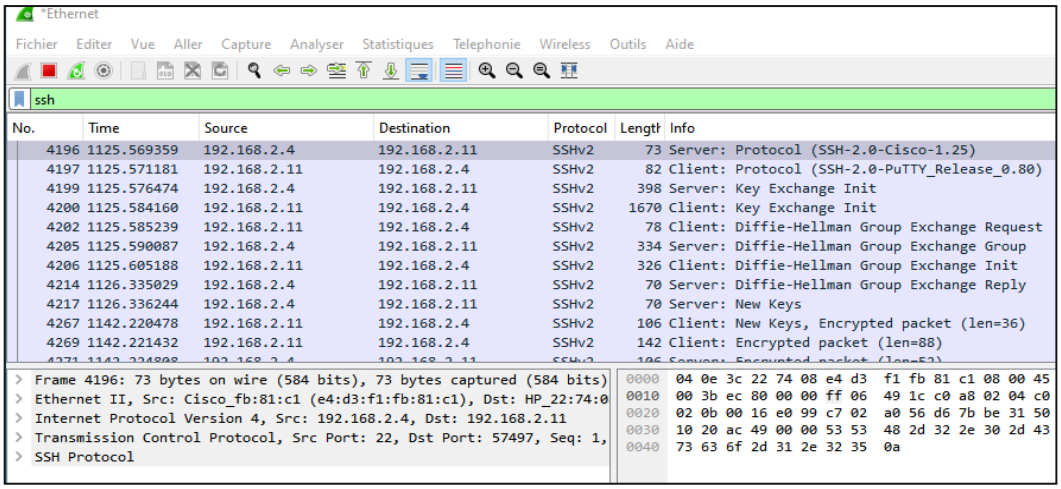

Figure 4.7 : Capture de Traffic SSH par WireShark

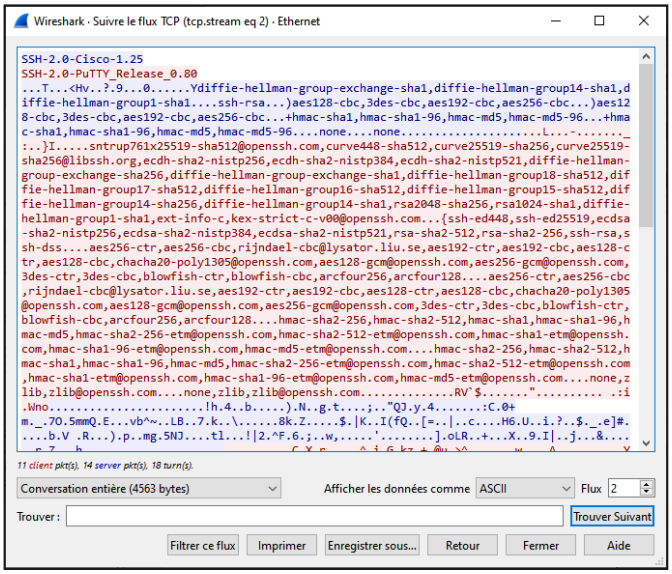

Figure 4.8 : Suivre le flux TCP par sur l'action de la connexion SSH avec WireShark

4.2.3 Attaque par inondation de la table CDP :

Dans la simulation précédente, une attaque a été menée pour saturer la table CDP (Cisco Discovery Protocol) d'un commutateur, entraînant la mise hors service du port. Pour éviter une telle attaque à l'avenir, plusieurs solutions peuvent être mises en œuvre :

- La première consiste à désactiver complètement le CDP sur les ports non utilisés ou sur l'ensemble du commutateur si son utilisation n'est pas nécessaire. Par exemple, sur un commutateur Cisco, la commande '**no cdp run**' désactive le CDP globalement.

```
Access(config)#no cdp run
Access(config)#end
Access#
%SYS-5-CONFIG_I: Configured from console by console

Access#show cdp
Access#show cdp n
Access#show cdp neighbors
% CDP is not enabled
Access#
```

Figure 4.9 : Désactiver le cdp sur le switch

Comme la montre la figure 4.9 la commande '**show cdp neighbors**' n'affiche plus les voisins disponibles.

- Il est également essentiel de surveiller régulièrement la table CDP pour détecter toute activité anormale. En cas de détection d'une saturation ou de toute autre anomalie, des mesures correctives doivent être prises immédiatement.

4.2.4 Attaque par saut de vlan

- **Attaque usurpation du commutateur**

Après une attaque d'usurpation de commutateur, il a été observé que l'interface G0/3 du switch a changé de mode dynamique auto à trunk. Ce changement peut entraîner plusieurs conséquences sur le fonctionnement du réseau. Tout d'abord, cela signifie que le port G0/3 est maintenant configuré en mode trunk, ce qui lui permet de transporter le trafic de plusieurs VLANs, en mode trunk, le port peut être vulnérable à d'autres attaques, telles que l'injection de trames malveillantes dans des VLANs auxquels l'attaquant n'est pas autorisé à accéder. Il est donc essentiel de reconfigurer les ports en mode accès et de configurer correctement les modes sur les deux extrémités de la connexion pour assurer une connectivité appropriée.

```
CORE_2(config-if-range)#switchport mode access
CORE_2(config-if-range)#switchport non
*Mar  1 02:00:32.942: %HSRP-5-STATECHANGE: Vlan2 Grp 2 state Standby -> Active
CORE_2(config-if-range)#switchport nonegotiate
CORE_2(config-if-range)#
```

Figure 4.10 : Configuration des interfaces en mode accès et désactivation du DTP

- La figure 4.10 montre que les ports du commutateur ont été configurés en mode accès et qu'ensuite l'option **switchport nonegotiate** a été utilisée.

  Cette commande est utilisée pour désactiver la négociation automatique des paramètres de trunking sur une interface de commutateur Cisco. Lorsque switchport nonegotiate est configuré sur une interface, le commutateur n'envoie pas les messages de négociation Dynamic Trunking Protocol (DTP) et ne répond pas aux messages DTP reçus. Cela garantit que l'interface reste en mode accès et empêche toute tentative d'un appareil connecté de forcer la configuration en mode trunk. Cela limite les interfaces à des modes prédéfinis et en évitant les configurations de trunking involontaires. Cependant, il est important de noter que switchport nonegotiate doit être configuré des deux côtés de la connexion pour garantir que les deux appareils sont en mode accès.

- **Attaque de double marquage**

- L'attaque de saut de VLAN par double marquage sur un commutateur Cisco permet à un individu malveillant de contourner les contrôles de sécurité basés sur les VLANs, lui accordant ainsi un accès non autorisé à des VLANs sensibles. En manipulant des trames Ethernet munies de deux étiquettes VLAN, l'assaillant peut acheminer du trafic

d'un VLAN à un autre, mettant ainsi en péril la confidentialité des données et potentiellement altérant la topologie du réseau.

L'utilisation du VLAN natif comme solution à l'attaque de saut de VLAN par double marquage est recommandée pour plusieurs raisons. Tout d'abord, en configurant un VLAN natif sur les liens trunk, les trames non étiquetées, telles que celles générées lors d'une attaque de double marquage, sont isolées dans ce VLAN. Cela empêche l'attaquant d'accéder à d'autres VLANs. De plus, la configuration du VLAN natif est relativement simple et largement prise en charge par les équipements réseau.

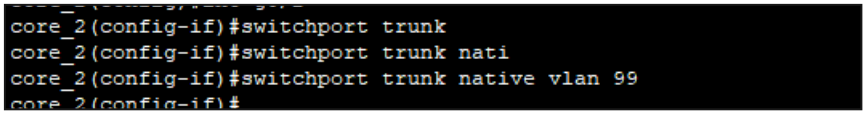

Figure 4.11 : Configuration vlan natif sur un port trunk

4.2.5 Attaque DHCP par famine

Après avoir simulé l'attaque DHCP, nous avons observé des changements dans la table des liaisons DHCP **(show ip DHCP binding).** Cette attaque peut entraîner l'attribution erronée d'adresses IP aux périphériques du réseau, voir l'indisponibilité de certains services réseau. Pour contrer cette attaque, une solution efficace consiste à mettre en place une surveillance active de la table des liaisons DHCP. Cela peut être réalisé en configurant des alertes pour détecter les changements suspects dans la table, tels que de limiter le nombre d'adresses IP disponibles pour les clients DHCP.

Pour mettre en place la surveillance active de la table des liaisons DHCP et limiter les risques associés à l'attaque DHCP, voici quelques configurations nécessaires :

- Le snooping DHCP est une fonction de sécurité qui agit comme un pare-feu entre les hôtes non fiables et les serveurs DHCP fiables. Il valide les messages DHCP et peut empêcher les attaques en filtrant les demandes illégitimes.
  En activant La commande IP DHCP snooping trust sur l'interface giga Ethernet 0/2 en la configure comme une interface de confiance pour le trafic DHCP.

```
access(config)#ip dhcp snooping
access(config)#ip dhcp snooping vlan 2
access(config)#int g0/2
access(config-if)#ip dhcp snooping trust
access(config-if)#ip dhcp snooping trust
```

Figure 4.12 : Activation du DHCP snooping

- La configuration des interfaces connectées aux utilisateurs finaux (non confiantes) avec une limite de taux pour les paquets DHCP.

La commande utilisée signifie que les ports configurés ne pourront traiter que 10 messages DHCP par seconde. Tout message supplémentaire au-delà de ce taux sera bloqué ou le port pourra être désactivé, selon les réglages du commutateur.

```
Enter configuration commands, one per line.  End with CNTL/Z.
access(config)#int range g0/3 - 0/24
access(config-if-range)#ip dhcp snooping limit rate 10
access(config-if-range)#
```

Figure 4.13 : Configuration des interfaces non confiantes

4.2.6 Attaque HSRP

Afin de sécuriser le protocole HSRP (Hot Standby Router Protocol) sur un switch Cisco et se prémunir contre les attaques potentielles initiées par des outils tels que Yersinia sur Kali Linux, il est possible de configurer l'authentification MD5. Bien que MD5 ne soit pas l'algorithme le plus sécurisé, il reste une option largement utilisée pour renforcer la sécurité des communications HSRP en empêchant les routeurs d'accepter des messages HSRP non authentifiés. [31]

- Nous avons configuré le protocole HSRP sur les interfaces vlan 2, 3 et 4 et maintenant on va rajouter le hachage MD5

```
CORE_1(config-if)#
CORE_1(config-if)#int vlan 2
CORE_1(config-if)#standby 2 authentication md5 key-string clesecreteclan2


CORE_1(config-if)#int vlan 3
CORE_1(config-if)#standby 3 authentication md5 key-string clesecreteclan3

CORE_1(config)#int vlan 4
CORE_1(config-if)#standby 4 authentication md5 key-string clesecretevlan4
```

Figure 4.14 : Configuration du hachage MD5 sur les interfaces vlan

4.2.7 Attaque STP

Dans cette partie, nous exposons les mesures visant à réduire les conséquences d'une attaque STP après avoir simulé une attaque à l'aide de Yersinia. Dans la section précédente, cette attaque a entraîné une modification de l'ID Root et de l'ID Bridge, perturbant ainsi la structure du réseau.

- **Activation de BPDU GUARD** : BPDU Guard désactive automatiquement les ports recevant des BPDUs non autorisés, empêchant ainsi les équipements malveillants d'altérer l'arbre de spanning tree.
- **Activation de PortFast sur les ports d'accès** PortFast permet aux ports de passer immédiatement à l'état de forwarding (dans cet état, le port du switch participe activement à l'acheminement des paquets. Il envoie et reçoit à la fois du trafic de gestion STP et du trafic de données normal) évitant ainsi les délais et réduisant la vulnérabilité aux attaques STP.

```
Access>EN
Access#CONF T
Enter configuration commands, one per line.  End with CNTL/Z.
Access(config)#int G0/3
Access(config-if)#spann
Access(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface  when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/1 but will only
have effect when the interface is in a non-trunking mode.
Access(config-if)#spanni
Access(config-if)#spanning-tree b
Access(config-if)#spanning-tree bpduguard enable
Access(config-if)#
```

Figure 4.15 : Configuration de la solution STP

- **Il est essentiel de** s'assurer que ces configurations ne sont pas appliquées aux ports trunk ou aux liaisons entre switches pour éviter des perturbations dans le fonctionnement du réseau.

4.3 Mise à Jour et Maintenance des Commutateurs Cisco

Dans notre entreprise, nous utilisons principalement des commutateurs Cisco pour notre infrastructure réseau. La mise à jour régulière de ces équipements est une pratique essentielle pour maintenir un niveau de sécurité élevé. Les mises à jour de firmware et de logiciels correctifs corrigent les vulnérabilités et améliorent les fonctionnalités de sécurité.

- **Vérification régulière des mises à jour disponibles** : Utilisation de l'interface Cisco pour rechercher les mises à jour de firmware.
- **Téléchargement et application des mises à jour** : Téléchargement des mises à jour à partir du site officiel de Cisco et application dans un environnement de test avant de les déployer en production.
- **Documentation** : Maintien de la documentation des versions de firmware utilisées et des mises à jour appliquées pour un suivi précis.

4.4 Conclusion

Ce chapitre a examiné plusieurs types d'attaques possibles sur un réseau et les solutions mises en place pour les prévenir. La mise en œuvre de ces solutions est essentielle pour maintenir un environnement réseau sécurisé et fonctionnel, capable de résister aux menaces internes et externes. En conclusion, une stratégie de sécurité bien définie et constamment mise à jour est indispensable pour protéger les ressources réseau et garantir leur disponibilité et intégrité

Conclusion générale :

Ce mémoire visait principalement à définir et à mettre en place une stratégie de sécurité pour un réseau de campus. Dans un premier temps, nous avons procédé à l'analyse des menaces et des vulnérabilités spécifiques aux réseaux de campus, puis nous avons formulé des solutions appropriées en utilisant des technologies de sécurité modernes.

Nos résultats montrent que la bonne configuration des switches peut considérablement améliorer la résilience et la sécurité d'un réseau de campus. Grâce à la simulation de différentes formes d'attaques et à l'expérimentation de diverses mesures de protection, nous avons pu confirmer l'efficacité de nos propositions et déterminer les meilleures pratiques à suivre.

Notre travail contribue à une meilleure compréhension des enjeux de sécurité dans les réseaux de campus et propose des solutions concrètes à travers des configurations réseau spécifiques pour renforcer leur protection. Il est crucial de continuer à évoluer et à adapter ces solutions face aux nouvelles menaces émergentes.

Les perspectives de ce mémoire offrent une base solide pour les futures recherches en documentant les menaces spécifiques aux réseaux de campus et les contremesures efficaces. Les résultats obtenus dans ce mémoire fournissent des points de comparaison pour évaluer l'efficacité d'autres configurations et solutions de sécurité. Les futurs chercheurs peuvent utiliser ces résultats comme référence pour développer et tester de nouvelles approches de sécurité. L'étude de technologies modernes et l'évaluation de leur efficacité dans des environnements de campus peuvent inspirer de nouvelles innovations. Les futurs mémoires peuvent explorer l'application de technologies émergentes, telles que l'IA et la blockchain, pour renforcer encore plus la sécurité des réseaux.

Bibliographie

[1] B. A. Forouzan, Data Communications and Networking (McGraw-Hill Forouzan Networking Series).

[2] «polaridad.es,» 2024. [En ligne]. Available: https://polaridad.es/fr/locaux-d%27ordinateurs-interconnect%C3%A9s-dans-une-zone-g%C3%A9ographique-limit%C3%A9e-toutes-les-informations-sur-le-r%C3%A9seau-local%2C-son-fonctionnement-et-ses-avantages/. Consulté le 14 mars 2024

[3] «Réseau de campus typique - Architecture et cycle de vie du réseau de campus,» HUAWEI, 2022. [En ligne]. Available: https://forum.huawei.com/enterprise/fr/R%C3%A9seau-de-campus-typique-Architecture-et-cycle-de-vie-du-r%C3%A9seau-de-campus/thread/667495280955768832-667481000260808704. Consulté le 16 mars 2024

[4] S. M. D. &. S. D. Halabi, Internet Routing Architectures, Cisco Press, 2002.

[5] «cisco goffinet,» cisco, [En ligne]. Available: https://cisco.goffinet.org/ccna/ethernet/principes-conception-lan-cisco/. Consulté le 30 mars 2024

[6] C. Systems, Campus LAN and Wireless LAN Design Guide.

[7] S. Halabi, Internet Routing Architectures., Cisco Press. .

[8] P. G. Casey (Expert en réseau d'accès, «fiber mall,» [En ligne]. Available: https://www.fibermall.com/fr/blog/core-distribution-and-assess-layer.htm.

[9] cisco, «netacad.com CCNA2 formation en ligne,» [En ligne]. Available: https://www.netacad.com/fr/courses/networking/ccna-switching-routing-wireless-essentials." support cours du formation ccna 2"

[10] «Cybersecurity Essentials "Formation en ligne",» [En ligne]. Available: https://www.netacad.com/courses/cybersecurity/cybersecurity-essentials. "support cours formation en ligne cisco"

[11] X. Z. Y. Y. Lianyu Zhang, «Survey on Modern VPN Technologies and Protocols,» *IEEE Communications Surveys & Tutorials, Vol. 23, No. 2, 2021*.

[12] O. S. A. O. Jazib Frahim, "Cisco ASA: All-in-One Next-Generation Firewall, IPS, and VPN Services".

[13] «Fortinet.com,» [En ligne]. Available: https://www.fortinet.com/fr/resources/cyberglossary/aaa-security. consulté le 12 avril

[14] D. &. D. B. Décary-Hétu, "Intrusion Prevention and Detection Systems.", 2014.

[15] «jedha,» [En ligne]. Available: https://www.jedha.co/blog/cybersecurite-quest-ce-que-la-triade-cia. consulté le 17 mars 2024

[16] A. Dubois, «Sécurité informatique et malwares: Défense contre les attaques de reconnaissance et les malwares,» Éditions ENI, 2018.

[17] J. M. e. al, "DDoS Attacks: Evolution, Detection, Prevention, Reaction, and Tolerance" par Jelena Mirkovic et al.

[18] M. Erbschloe, "Physical Security for IT", 2004.

[19] «CISCO.goffinet,» [En ligne]. Available: https://cisco.goffinet.org/ccna/disponibilite-lan/redondance-de-passerelle-host-standby-router-protocol-hsrp/. consulté le 15 avril 2024

[20] ccnp, «Networklab,» [En ligne]. Available: https://www.networklab.fr/spanning-tree-theorie/. consulté le 18 avril 2024

[21] J.-M. Seigneur, "Routage et Switching : Guide pratique", 2021.

[22] «Club tutoriel informatique,» [En ligne]. Available: https://clubtutoinformatique.blogspot.com/2012/09/service-dhcp-sous-linux.html. consulté le 18 avril 2024

[23] «ionos.fr,» [En ligne]. Available: https://www.ionos.fr/digitalguide/serveur/outils/telnet/. consulté le 24 avril 2024

[24] «Kali.org,» [En ligne]. Available: https://www.kali.org/tools/yersinia/. consulté le 10 avril 2024

[25] L. Bloch, Sécurité des réseaux : Attaques et contre-mesures, 2019.

[26] International Journal of Innovative Research in Computer and Communication Engineering Vol. 1, March 2013.

[27] «Monkey.org,» [En ligne]. Available: https://www.monkey.org/~dugsong/dsniff/. consulté le 13 avril 2024

[28] Proceedings of the International MultiConference of Engineers and Computer Scientists 2008 Vol II, Hong kong, March 2008.

[29] Biennial Symposium on Communications (BSC), Montreal, QC, Canada, August 2023.

[30] L. G. R. M. F. R. Pierre-Yves Bonnetain, SSH - Maitrisez le client OpenSSH, le serveur OpenSSH et SSH sous Windows, 2016.

[31] «CISCO,» cisco, 15 mai 2015. [En ligne]. Available: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp_fhrp/configuration/15-sy/fhp-15-sy-book/fhp-hsrp-md5.html. consulté le 24 mars 2024