

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITE SAAD DAHLAB-BLIDA1



Faculté des sciences

Département : informatique

Mémoire de fin d'étude

Pour l'obtention du Diplôme de :

Master système informatique et réseaux

Thème :

Implémentation d'une stratégie de sécurité dans un réseau de campus

Réalisé par :

- NIGHOUD YASSER
- BOUDJELLAL MOHAMED LOTFI

• **Encadre par :**

Mr.NIGHOUD ABDLEKADER

Mr. Mohamed Benyahia

Soutenu devant le jury composé par :

- Madame DJEDDAR AFRAH USDB Président
- Mr.OULED AISSI MOHAMED USDB Examineur

Année universitaire 2020/2021

REMERCIEMENTS

Nous tenons tout d'abord à remercier Dieu le tout puissant et miséricordieux, qui nous a donné la force et la patience d'accomplir ce Modeste travail.

En second lieu, nous tenons à remercier notre encadreur M. Abdelkader NIGHOUD pour avoir accepté de nous encadrer. Nous voudrions leurs témoigner notre gratitude de leurs patience, précieux conseil et aide et tous les conseils qu'ils nous ont prodigué durant toute la période du travail.

Nous adressons aussi nos sincères remerciements à tous les professeurs et enseignants du département de informatique de L'USDB pour la qualité de leur enseignement, qui nous ont enseigné et qui par leurs compétences nous ont soutenu dans la poursuite de nos études.

Nous voudrions leurs témoigner notre grande reconnaissance pour leurs contribution à notre formation, leurs effort et leurs conseils qui nous ont bien été utiles durant mes cinq années universitaires.

On n'oublie pas nos parents pour leur contribution, leur soutien et leur patience.

Enfin, on remercie tous ceux qui, de près ou de loin, ont contribué à la réalisation de ce travail.

nous tenons à adresser nos sincères remerciements et profonde gratitude à toute personne ayant aidé à l'aboutissement de ce travail.

DEDICACES

C'est avec profonde gratitude et sincères mots, que je remercie le bon Dieu, le tout puissant, de m'avoir donné la force pour survivre, ainsi que l'audace pour dépasser toutes les difficultés.

Je dédie ce modeste travail en signe de respect, reconnaissance et de Remerciement

A mes chers parents, qui m'ont aidé, de près et de loin. Particulièrement à ma mère, pour l'effort qu'elle a suscité en moi, de par sa rigueur.

Et je dédie ce travail à M. Abdelkader, qui nous a accompagnés et patiemment avec nous d'une manière qui ne nous a pas lésinés et qui nous a aidés à nous développer.

A mes chers frères , qui m'ont donné le courage. A tous mes amis.

A toute la famille NIGHOUD et KAHOUL. J'espère qu'un jour, je pourrai leur rendre un peu de ce qu'ils ont fait pour moi, que dieu leurs prête bonheur et longue vie.

« YASSER »

DEDICACES

En particulier à mes très chers parents qui ont toujours été là pour moi, et qui m'ont donné un magnifique modèle de labeur et de persévérance.

J'espère qu'ils trouveront dans ce travail toute ma reconnaissance et tout mon amour A toute la famille, pour leur soutien, sacrifice, patience, ainsi pour leurs conseils, que dieux les protèges et les entoure de bénédiction.

A tous mes amis, mes collègues, mon binôme YASSER et à tous ceux qui ont contribué de près ou de loin à réaliser ce travail.

« lotfi »

RESUME

Les systèmes d'information sont devenus des éléments critiques et indispensables au bon fonctionnement des entreprises en matière de services offerts comme le stockage, la gestion, et le transport des données qu'ils fournissent, d'où la nécessité de sécuriser de tels systèmes. Dans ce projet, nous nous intéressons à sécuriser le réseau LAN d'un campus au couche du périmètre de l'accès au réseau. On aura à explorer les différentes attaques utilisées par les hackers au couche deux du modèle OSI et mettre en œuvre une stratégie de sécurité basée sur les bonnes pratiques, afin de protéger cette couche en repoussant ces attaques qui peuvent nuire au bon fonctionnement du réseau, après mettre en œuvre la stratégie on va créer une application desktop qui va servir à optimiser et appliquer cette stratégie sur un commutateur .

Mots clé : LANs, Sécurité, couche 2, réseau, commutateur

ABSTRACT

Information systems have become critical and indispensable elements for the proper functioning of companies in terms of the services offered such as the storage, management, and transport of the data they provide, hence the need to secure such systems. In this project, we are interested in securing the LAN network of a campus at the level of the perimeter of access to the network. We will have to explore the different attacks used by hackers at layer two of the OSI model and implement a security strategy based on best practices as well as the latest research in the field, in order to protect this layer by repelling those attacks that can harm the proper functioning of the network, after implementing the strategy we will create a desktop application that will allow us to optimize and apply this strategy on a switch .

Key words: LANs, Security, Switches, Layer 2, network

ملخص

LISTE DES TABLEAUX

Tableau 2.1: tableau des vlans utilisés	14
Tableau 2.2 : commandes de la configuration initiale	18
Tableau 2.3: Commandes pour la création de vlan	18
Tableau 2.4: répartition des Vlan	20
Tableau 2.5 : Commandes utilisées pour un port interface.	21
Tableau 2.6 : les adresses des interfaces vlans	22
Tableau 2.7 : répartition des Vlans sur les switch Coeur via HSRP	22
Tableau 2.8 :explication de commandes HSRP	22
Tableau 2.9 : explication de commandes STP	23
Tableau 2.10 : Classification de menaces	29
Tableau 2.1 : expliqué les commande dhcp	67
Tableau 2.2 : explication de commandes du dynamic arp inspection	68
Tableau 2.3 : explication de commandes l'authentification HSRP	69
Tableau 2.4 :Explication de commandes STP	71
Tableau 4.5 : Explication de commandes du protocole 802.1X	75

LISTE DES FIGURES

Figure 1.1: Architecture du modèle ECNM.	03
Figure 1.2: Modèle hiérarchique d'un réseau de campus à 3 couches.	04
Figure 1.4: Triangle sécurité, fonctionnalité, utilisabilité.	09
Figure 2.1: architecture de réseaux	11
Figure 2.2: commutateurs utilisés	12
Figure 2.3: fibre optique	12
Figure 2.4: Cable console	13
Figure 2.5: Straight-through cable	13
Figure 2.6: desktop utilisé	14
Figure 2.7: reseau réalisé avec matériel réel	16
Figure 2.8.: configuration initiale	17
Figure 2.9.:Création du vlan	18
Figure 2.10:les vlans créés	18
Figure 2.11 : configuration d'interface	19
Figure 2.12 :Etapes de configuration d'un port trunk	20
Figure 2.13.: Interface de connexion entre switch access et coeur 1	20
Figure 2.14 : Interface de connexion entre switch access et coeur 2	20
Figure 2.15 : répartition des vlans entre les interfaces	20
Figure 2.12 :Etapes de configuration d'un port trunk	20
Figure 2.16 : Diviser les vlans sur les interfaces	20
Figure 2.17 : Configuration de default Gateway :	21
Figure 2.18 : Configuration des interface vlans	21
Figure 2.19 : étapes de Configuration HSRP	22
Figure 2.20 : étape de la configuration STP	23
Figure 2.21 : résultat des commandes STP	23
Figure 2.22 : étapes de Configuration dhcp pour le vlan 2	24
Figure 2.23 : configuration de DHCP switch core 1	24
Figure 2.24 : configuration de DHCP switch core 2	25
Figure 2.25 : Configuration de telnet	25
Figure 2.26 : tester le ping1	26
Figure 2.27 : tester le ping2	26
Figure 2.28 : tester le ping3	26
Figure 2.29 : tester le ping4	26
Figure 2.30 : connexion Telnet	27
Figure 2.31 : table mac	31
Figure 2.32 : table mac avant l'attaque	31
Figure 2.33 : lancement d'attaque	32
Figure 2.34 : résultat d'attaque	33
Figure 2.35 : whireshark résultat	33
Figure 2.36 : cdp avant l'attaque	34
Figure 2.37 : lancement d'attaque cdp	35
Figure 2.38 : résultat d'attaque cdp	36
Figure 3.39 : attaque vlanhopping	38
Figure 2.39 : activer trunking	38
Figure 2.41 : attaque stp	39

Figure 2.42 : avant l'attaque stp	39
Figure 2.43 : durant l'attaque stp	40
Figure 2.44 : résultat d'attaque stp	40
Figure 2.45: analyse avec whireshark	41
Figure 2.46: exemple d'attaque bpdu	42
Figure 2.47 : cpu avant l'attaque	42
Figure 2.48 : bpdu nombre avant l'attaque	43
Figure 2.49 : lancement d'attaque	43
Figure 2.50 : cpu après l'attaque	44
Figure 2.51 : résultat de nombre bpdu	45
Figure 2.52 : hsrp attaque	45
Figure 2.53: core1 avant l'attaque	46
Figure 2.54 : core2 avant l'attaque	46
Figure 2.55 : lancement d'attaque hsrp	47
Figure 2.56:devenir acite router	47
Figure 2.57 : choisir fake ip	47
Figure 2.58: whireshark analyse résultat	48
Figure 2.59 : address de hacker avant l'attaque	49
Figure 2.60 : address ip de système	50
Figure 2.61 : lancer l'attaque	50
Figure 2.62 : durant l'attaque	51
Figure 2.63 : whireshark analyse	51
Figure 2.64: résultat d'attaque dhcp	52
Figure 2.65 : avant l'attaque Telnet	53
Figure 2.66 : résultat d'attaque telnet	54
Figure 2.67 : préparation d'attaque	54
Figure 2.68 : étape pour établir l'attaque arp	55
Figure 2.69 : résultat d'attaque arp	56
Figure 2.70 : attaque mac flooding	59
Figure 2.71 : activer port security	59
Figure 2.72 : définir le nombre max de port	60
Figure 2.73 : défini le nombre max à 1	60
Figure 2.74 : résultat d'attaque mac	60
Figure 2.75: résultat d'attaque mac avec sticky	61
Table 2.76 : commande de security des ports	62
Figure 2.77 : configurer la port en mode nonnegotiate	63
Figure 2.78 : vlan 99 comme vlan	63
Figure 2.88 : résultat d'attaque vlanhopping après contremesure	63
Figure 2.89 : attaque dhcp	64
Figure 2.90 : configurer le dhcp snooping	65
Figure 2.91 : ip dhcp snooping	65
Figure 2.92 : limiter le rate à 3	65
Figure 2.93 : activer la surveillance DHCP par VLAN	66
Figure 2.94 : essayé une attaque	66
Figure 2.95: résultat d'attaque dhcp	66
Figure 2.96 : Dynamic ARP Inspection	68
Figure 2.97 : essaye une attaque	68
Figure 2.98 : Le switch détecter que il y'a une attack et l' arrêter	68
Figure 2.99 : configuration key chain	69
Figure 2.100 : stp exemple	70

Figure 2.101 : Configurer PortFast	70
Figure 2.102 : portfast activé	71
Figure 2.103 : Configuration BPDU Guard	71
Figure 2.104 : Exécutez la commande shutdown	72
Figure 2.105 : WHIRESHARK analyse	72
Figure 2.107 : vesrion ssh	73
Figure 2.108 : vérifier le support ssh	73
Figure 2.109: configurer le domaine name	73
Figure 2.110 : rsa configuration	73
Figure 2.111 : authentification configuration	74
Figure 2.112 : configurer vty	74
Figure 2.113 : activer ssh	74
Figure 2.114 : configuration du protocole 802.1X	74
Figure 3.1 : diagramme de cas d'utilisation	79
Figure 3.2 : diagramme séquence de Authentification	80
Figure 3.3 : diagramme séquence Configuration du commutateur	81
Figure 3.4 : diagramme séquence pour Consultation la liste	82
Figure 3-5 : Interface d'authentification	83
Figure 3-6 : Interface de sign-up	83
Figure 3-7 : choisir la couche	84
Figure 3-8 : Interface de sign-up	84
Figure 3-9 : choisir le nombre de switch et les inteface connecté	85
Figure 3-10 : creation de vlan	85
Figure 3-11 : configuration dhcp	86
Figure 3-12 : configuration hsrp	86
Figure 3-13 : configuration des interfaces	87
Figure 3-14 : distrubution des vlans	87

Notre travail :

Le développement technologique dans le domaine des réseaux a été rencontré par de nombreuses nouvelles techniques de piratage et d'infiltration de réseaux il est donc nécessaire de trouver des mécanismes pour se défendre contre ces attaques et parce que le système de défense dans les entreprises algériennes est faible notre objectif de ce projet est de créer une stratégie de défense contre les attaques de la deuxième couche du modèle osi.

Notre projet est divisé en deux parties où nous allons:

- Dans la première partie : nous allons créer une stratégie de défense en appliquant des attaques au deuxième niveau du modèle osi (attaque mac flooding, attaque dhcp, attaque hsrp, attaque telnet , plus d'attaque) sur de vrais appareils et un environnement de travail réel (vrai commutateur, vrai bureau) et nous défendrons contre ces attaques, donc dans la dernière partie, nous allons créer une stratégie de défense et le faire pour créer nos réseaux.
- dans la deuxième partie, nous créerons un logiciel qui automatisera le commutateur cisco en langage java qui aidera à augmenter la configuration du commutateur et aidera à minimiser le taux d'erreur, et à réduire le temps du travail, la meilleure partie est qu'il générera automatiquement les stratégies de défense.

Liste des symboles et des abréviations

- AAA : authentication, authorization, and accounting
- ACK : acknowledgment
- ACL : access control list
- AH : Authentication Header.
- AS : Autonomous System.
- ARP : Address Resolution Protocol
- CA : Certificate Authority.
- CAM : content-addressable memory
- CRL : certificate revocation list
- CDMA: Code Division Multiple Access.
- CPU : Central Processing Unit.
- DHCP : Dynamic Host Configuration Protocol
- DHCPv6 : Dynamic Host Configuration Protocol, version 6
- DNS : Domain Name Server
- DoS : denial of service
- ESW : Ethernet Switch
- FCFS : First Come First Served
- FCS : frame check sequence
- FEC : Fast EtherChannel
- FTP : File Transfer Protocol
- GNS 3 : Graphical Network Simulator 3.
- HA : High Availability
- HTTP : HyperText Transfer Protocol.
- HTTPS : HyperText Transfer Protocol Secure.
- HSRP : Hot Standby Router Protocol
- IEEE : Institute of Electrical and Electronics Engineers
- IP : Internet Protocole.
- IPS : IP Storage
- IPv6 : Internet Protocole version 6.
- IPv4 : Internet Protocole version 4.
- IPSec : Internet Protocol Security.

- IOS : Internet-work Operating System
- LAN : Local Area Network.
- L2 : Layer 2
- L2F : Layer 2 Forwarding
- LLC : logical link control
- MAC : Media Access Control
- NAT : Network Address Translation.
- NTP : Network Time Protocol
- NVRAM : nonvolatile RAM
- OFC : open fiber control
- OS : Operating System.
- RSRC : Resource
- RSVP : Resource Reservation Protocol
- RTT : round-trip time
- PA : port adapter
- SA : security association
- SA : Source-Active
- SBE : single-bit error
- SNMP : Simple Network Management Protocol
- SSL : Secure Socket Layer
- SSH : Secure Shell
- ToS : Type of Service
- TFTP : Trivial File Transfer Protocol
- ToS : Type of Service
- TP : Transport Protocol
- TR : Token Ring
- TVC : tag virtual circuits
- UA : unnumbered acknowledgement
- UPF : Undefined
- UDP : User Datagram Protocol
- VIP : Versatile Interface Processor
- VLAN : virtual LAN
- VTP : VLAN Trunk Protocol
- VT : virtual terminal
- WWW : World Wide Web
- XDR : eXternal Data Representation
- ZBT : zero bus turnaround

Sommaire

REMERCIEMENTS	
DEDICACES	
RESUME	
SUMMARY	
ملخص	
Liste des tableaux	
Liste des figures	
ABSTRACT	
Liste des symboles et des abréviations	
Sommaire	
Introduction Générale	01
CHAPITRE I : Sécurité des réseaux IP	
Introduction	02
Définition d'un réseau local	02
Conception hiérarchique du réseau	02
Réseau de campus	03
Définition	03
Couche d'accès	04
Couche de distribution	04
Couche cœur	04
La commutation dans les réseaux de campus	05
La sécurité des réseaux informatiques	05
Les objectifs principaux de la sécurité informatique	06
Les champs d'application de la sécurité	06
Approche de sécurité réseau	07
Mise en place d'une politique de sécurité	07
Stratégie de la sécurité	08
Triangle sécurité, fonctionnalité, utilisabilité	09
Résumé	09
Chapitre II Partie I :LES STRATEGIES DE SECURITE	
Introduction	10
Présentation du réseau réalisé	11
Equipements utilisés	12
Les protocoles Installés	14
VLANs	14
Spaning-tree :	15
CDP Cisco Discover Protocol	15
HSRP	15
DHCP	15
Agrégation des liens	15
Gestion d'accès aux équipements	15
Plan final de la configuration	16
Configuration initiale	16
Création de vlan	18

Configuration des interfaces	19
Configuration de la passerelle par défaut	20
Configuration des interfaces Vlan	20
Configuration HSRP	22
Configuration spanning tree STP	23
Configuration DHCP	23
Configuration d'accès distant aux switch via Telnet :	25
Tests de réseaux	26
Conclusion	27
Chapitre II Partie II : Etudier des attaques réseau de niveau II :	
Introduction	28
Classification des menaces	29
Attaque de niveau 2 du modèle OSI	30
Débordement de la table MAC	30
CDP FLOODING ATTACK	34
VLAN HOOPING	36
Attaque STP Spanning Tree Protocol	39
Attaque HSRP	44
ATTAQUE DHCP	48
Attaque distant aux équipement	52
Attaque ARP POISNING	54
avec ettercap suivre les étapes suivants	54
Conclusion	56
Chapitre II Partie III :Solutions de sécurité de niveau II	
Introduction	59
Atténuation des attaques de table d'adresses MAC	60
Atténuer les attaques VLAN	62
Atténuer les attaques DHCP	63
Exemple de configuration de l'espionnage DHCP	64
Atténuer les attaques d'ARP	67
Atténuer les attaques HSRP	68
Atténuer les attaques STP	69
Mise en oeuvre de la sécurité des ports :	71
Accès à distance sécurisé	72
Opération SSH	72
Configuration de SSH	73
Configuration du protocole 802.1X	74
Conclusion	76
Chapitre III : Automatisation sécurisé d'un switch	
Introduction	78
Étude conceptuelle	79
Diagramme des cas d'utilisation	80
Diagrammes de séquence	80
Authentification	80
Configuration du commutateur	81
Consultation la liste des configurations	82
Représentation des interfaces :Authentification	83
Nouvelle configuration	84
Conclusion	88
Bibliographie	89

INTRODUCTION GENERALE

Introduction Générale :

Après l'avènement du numérique, l'entreprise ne cesse jamais de s'agrandir et de se développer en termes d'évolution dans l'architecture des systèmes informatiques vers une plus grande distribution des fonctions. Aujourd'hui, les réseaux locaux constituent l'axe autour duquel s'organise l'ensemble des services informatiques.

La technologie actuelle permet d'accroître les volumes et les vitesses de transfert des données tout en diminuant les coûts. Les interconnexions de réseaux sont innombrables et pratiquement tous les réseaux se trouvent aujourd'hui imbriqués les uns dans les autres, cela a conduit au concept de réseau d'entreprise. Au le du temps, les entreprises et les organisations ouvrent leur système d'information à leurs partenaires ou leurs fournisseurs, les données vitales deviennent plus sensibles, ces systèmes peuvent être vulnérables soit à des attaques malveillantes ciblées soit à différentes types d'attaques non ciblées auxquels sont exposés les systèmes ouverts sur internet (virus, espionnage, rançongiciels, etc.).

Nous pouvons partir du constat que tout Système d'Information (SI) est vulnérable, la sécurité est maintenant un élément obligatoire de la conception de ces systèmes. Les protocoles de communication sont pénétrables, les logiciels et les équipements d'infrastructure qui le composent sont pour la plupart vulnérables.

Il est donc essentiel de connaître les ressources de l'entreprise à protéger et de maîtriser le contrôle d'accès et les droits des utilisateurs du système d'information.

Les équipes de sécurité au sein des organisations doivent mettre en oeuvre des nouvelles méthodes e caces et des améliorations des techniques utilisées pour sécuriser leurs ressources et assurer des niveaux de protection adéquats

pour que l'entreprise puisse mener ses activités.

Notre projet s'inscrit dans le cadre de l'élaboration d'un réseau de campus au sein de l'entreprise SONATRACH en mettant en oeuvre plusieurs mécanismes et procédures de sécurité de niveau 2 de la couche OSI.

CHAPITRE I : Sécurité des réseaux IP

1.1 Introduction

Avec l'avancement rapide et la dépendance totale de l'être humain avec les différentes technologies surtout dans le monde professionnel, les réseaux informatiques prennent une place de plus en plus importante dans l'activité des entreprises, par conséquent, ils connaissent une croissance exponentielle introduisant des nouvelles préoccupations en matière de sécurité. Les questions qui se posent sont : Qu'est-ce qu'un LAN? Quelle est sa structure ? Et comment élaborer une stratégie de sécurité ?

Dans ce chapitre, nous allons répondre à ces différentes questions en faisant une présentation générale des réseaux locaux, leurs différents concepts clés, ainsi que les aspects fondamentaux de la sécurité des réseaux.

1.2 Définition d'un réseau local

Un réseau local (en anglais LAN : local area network) est un moyen de communication permettant d'interconnecter des équipements informatiques et de partager des ressources (de calcul, de stockage, etc.) dans une zone géographique restreinte. Une norme commune très répandue pour les réseaux locaux câblés est le protocole Ethernet. Les autres technologies moins fréquentes et parfois obsolètes sont anneau à jeton et FDDI. La transmission de données est réalisée sur la base de câbles de cuivre ou via des câbles de fibre optique. Un LAN est conçu pour permettre un transfert rapide de grandes quantités de données. Selon la structure du réseau et du moyen de transmission utilisé, un débit de données de 10 à 1000 Mbit/s est courant. Les réseaux locaux permettent un échange d'informations confortable entre les différents périphériques qui sont connectés au réseau. [1]

Aujourd'hui, les réseaux locaux constituent l'épine dorsale de l'activité informatique et du système d'information de l'entreprise, du laboratoire, de l'atelier de production. [2]

1.3 Conception hiérarchique du réseau

Le modèle de réseau hiérarchique ECNM (Entreprise Cisco Network Model) a été l'un des premiers modèles de références recommandés par Cisco qui ont divisé le réseau en différents blocs afin d'obtenir un réseau simple, performant et facile à administrer. [3]

ECNM introduit la modularité en divisant le réseau en zones fonctionnelles qui facilitent la conception, et le dépannage. Dans une conception de couche modulaire, les composants de réseau peuvent être placés ou retirés du service avec peu ou pas d'impact sur le reste du réseau, ce qui facilite le dépannage, l'isolation des problèmes et la gestion du réseau. [4]

Comme illustré par la figure ci-dessous, l'architecture d'entreprise Cisco comprend les modules principaux suivants :

- ❖ Campus d'entreprise (Enterprise Campus).
- ❖ Périphérie d'entreprise (Enterprise Edge).
- ❖ Périphérie du fournisseur de service (Service Provider Edge).
- ❖ Réseau distant (Remote network).

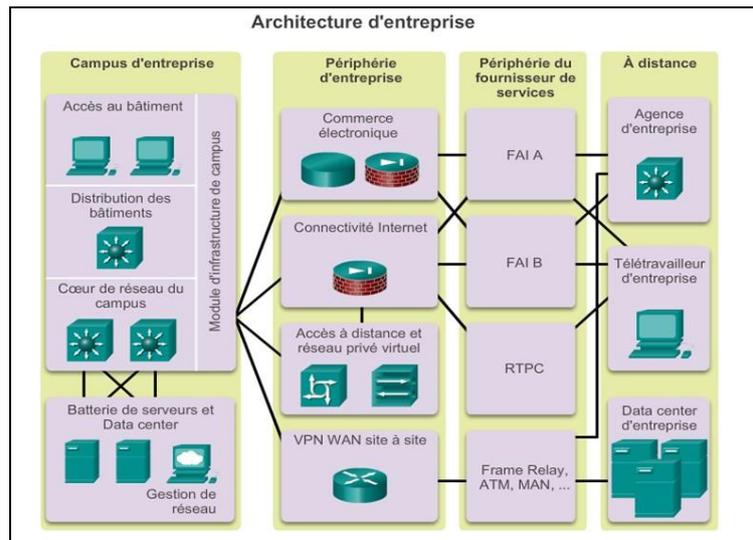


Figure 1.1: Architecture du modèle ECNM. [3]

1.4 Réseau de campus

1.4.1 Définition

Un réseau de campus est un réseau d'entreprise composé de nombreux LAN dans un ou plusieurs bâtiments, tous connectés et tous généralement dans la même zone géographique. Une entreprise typiquement est propriétaire de l'ensemble du réseau du campus et du câblage physique.

Une telle architecture est conçue pour répondre aux besoins des organisations qui vont d'un petit bâtiment ou d'un site éloigné à un grand bâtiment, multi emplacement. L'infrastructure des réseaux de campus peut être découpée en trois couches :

Accès, distribution et cœur, Chaque couche fournit des fonctionnalités et des capacités différentes au réseau. Le nombre de couches nécessaires dépend des caractéristiques du réseau site de déploiement. Par exemple, un site qui occupe un seul bâtiment pourrait nécessiter seulement les deux couches : accès et cour, tandis qu'un campus de bâtiments multiples nécessitera probablement les trois couches. [5]

La figure I.2 montre les trois couches d'un réseau de campus, où nous voyons

que la couche d'accès vient en premier, suivi de la couche de distribution et la couche cœur vient en dernier :

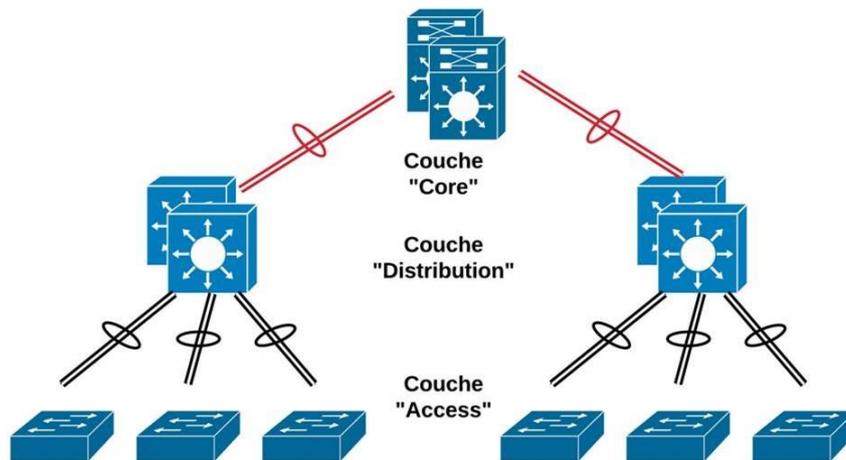


Figure 1.2: Modèle hiérarchique d'un réseau de campus à 3 couches.

1.4.2 Couche d'accès

La couche d'accès est la couche inférieure du modèle Cisco à 3 couches, et le point d'entrée du réseau, l'endroit où les dispositifs ou les extrémités de l'utilisateur final se connectent au réseau. Elle fournit une connectivité à bande passante élevée à l'aide de technologies d'accès filaires comme Gigabit Ethernet, et sans fil tel que 802.11n et 802.11ac.

Le module de couche d'accès contient des commutateurs de couche 2 pour assurer la densité de port requise. Il assure l'implémentation des réseaux locaux virtuels (VLAN) et des liens 'trunk' vers la couche de distribution du réseau.

1.4.3 Couche de distribution

La fonction principale de la couche de distribution est de regrouper les commutateurs de couche d'accès dans un bâtiment ou un campus donné. Cette couche peut inclure plusieurs rôles, y compris la mise en œuvre des fonctions suivantes : l'agrégation des liens, la redondance et l'équilibrage des charges, le routage entre les vlans, l'optimisation de routage IP en fournissant un résumé des routes vers le coeur, ainsi qu'un mécanisme de qualité de service QoS. [5][6]

Les commutateurs de distribution sont généralement des switches multiniveaux, et qui doivent être déployés par paires pour la redondance. Les paires de commutateurs de couches de distribution doivent être interconnectées les unes aux autres à l'aide d'un lien Couche 2 ou Couche 3.

1.4.4 Couche cœur

La couche de base est la couche principale du réseau et le point d'agrégation pour les réseaux multiples qui fournit l'évolutivité, la haute disponibilité et la convergence rapide au réseau. Cette couche donc doit être able, disponible, redondante et avoir un équilibrage de charge entre ses différentes liaisons. Parmi les principales caractéristiques de la couche coeur nous avons :

- Transport rapide.

- Haute fiabilité et disponibilité.
- faible latence et bonne gestion
- qualité de service (QoS).
- Tolérance aux pannes.

1.4.5 La commutation dans les réseaux de campus

Dans la terminologie des télécommunications, les commutateurs réseau améliorent l'évolutivité et la stabilité dans un réseau grâce à la création de canaux virtuels, il maintient une table qui associe l'adresse MAC locale pour acheminer le trafic réseau uniquement vers le port de destination où le MAC de destination est attaché. Cela réduit considérablement la taille du domaine de collision entre les appareils et permet aux appareils de transmettre et de recevoir des données en même temps. [7] Les commutateurs sont classés dans le LAN selon leur fonctionnement dans le modèle d'interconnexion de systèmes ouverts (OSI) comme nous décrivons dans la suite :

1. Commutateur niveau 2 : Un commutateur de niveau 2 fonctionne sur la couche de liaison de données, ce qui signifie que l'acheminement de trafic est basé sur les adresses MAC. Il prend en charge toujours des fonctions telles que la séparation des réseaux physiques en domaines de collision et de diffusion, ainsi l'élimination des boucles de commutation, mais ils sont concentrés que sur l'information recueillie dans la couche 2. [5][8]

Parmi les commutateurs de niveau 2 nous citons la série 2960 de Cisco qui est une nouvelle famille améliorée. Elle fournit des services avancés notamment :

Le contrôle d'admission au réseau (NAC), et une qualité de service.

2. Commutateur multi-niveau : Le commutateur multicouches (en anglais MLS : multilayer switch) est une technologie de commutation de routeur basée sur Ethernet qui opère la commutation de couche 3 conjointement aux routeurs existants. Désormais, en plus des fonctions traditionnelles de commutation d'un port à l'autre, les commutateurs multicouches sont capables d'effectuer des fonctions de niveau 3 et même de niveau 4 du modèle OSI. Parmi les commutateurs multi-couches nous citons la série 3650. Cette série permet un dépannage rapide, une sécurité avancée et un contrôle de la qualité de service (QoS) avec une très bonne résilience. Les fonctions de niveau 3 que peuvent exécuter par les MLS sont :

- Le routage inter-VLANs, en fonction des adresses IP.
- Le routage dynamique comme RIP, OSPF, BGP.
- Les protocoles VRRP (Virtual Router Redundancy Protocol), HSRP (Hot Standby Routing Protocol) et GLBP (Gateway Load Balancing Protocol) pour assurer la haute disponibilité.
- La gestion de listes de contrôle d'accès ou ACL (Access Control List). [9]

1.5 La sécurité des réseaux informatiques

1.5.1 Pourquoi sécuriser un réseau ?

Les réseaux de campus, comptent un grand nombre d'utilisateurs, y compris des employés, des entrepreneurs, des invités et des partenaires, qui sont extrêmement vulnérables aux

menaces à la sécurité, comme l'accès non autorisé au réseau, l'espionnage et la propagation de logiciels malveillants. Pour cette raison, une conception solide de la sécurité du réseau protège les extrémités de ces types de menaces est obligatoire. Les entreprises d'aujourd'hui doivent également se conformer à la politique de l'entreprise et aux lois sur la sécurité qui sont en place pour protéger les données et les garder privées.

1.5.2 Les objectifs principaux de la sécurité informatique

La sécurité réseau c'est un ensemble de règles et de configurations conçues pour assurer les cinq objectifs suivants : [10]

Confidentialité : c'est l'assurance que l'information n'est accessible qu'aux personnes ayant l'accès, et qu'elle ne sera pas divulguée en dehors d'un environnement spécifié.

Intégrité : c'est garantir que l'information n'a pas été altérée lors de son transit sur les différents éléments du réseau que ça soit de manière accidentelle ou intentionnel dans un but malveillant.

Disponibilité : est l'assurance que les ressources et données de l'entreprise sont disponibles pour les personnes autorisées en cas de besoin sans délai. Et donc, maintenir le bon fonctionnement du système de l'information.

Authentification : c'est le processus qui permet évidemment d'assurer l'authenticité, où il identifie l'utilisateur ou l'appareil pour accorder un accès, des privilèges et certaines règles et emplacements dans le réseau pour assurer que seules les personnes autorisées aient l'accès aux ressources.

Non répudiation : c'est l'assurance de l'information qui garantit la transmission et la réception d'informations entre l'expéditeur et le destinataire via différentes techniques telles que les signatures numériques et le cryptage.

1.5.3 Les champs d'application de la sécurité

Un environnement informatique et de télécommunication sécurisé implique la sécurisation de tous les éléments qui le compose, cela comprend :

La sécurité physique : soit la sécurité au niveau des infrastructures matérielles : salles sécurisées (accès sécurisé, contrôlé, et monitoré), adaptation à l'environnement (salle

climatisée), redondance de plusieurs sites, lieux ouverts au public, espaces communs de l'entreprise, postes de travail des personnels, etc.

La sécurité juridique : celle-ci est assurée par l'application des lois internes de l'entreprise, sensibilisation et accord des employés, lois du pays. La sécurité technique : c'est-à-dire la sécurité au niveau des données, notamment les données de l'entreprise, les applications ou encore les systèmes d'exploitation.

1.5.4 Approche de sécurité réseau

Pour considérer efficacement les besoins de sécurité d'une organisation, évaluer et choisir les nombreux produits et politiques pour renforcer la sécurité, le responsable de la sécurité a besoin de moyens systématiques de définition des exigences de sécurité et de caractérisation des approches qui satisfont le mieux possible ces exigences. Une approche possible est de considérer trois aspects de la sécurité de l'information :

Attaques de sécurité : une action qui compromet la sécurité de l'information possédée par une organisation.

Services de sécurité : un service qui améliore la sécurité des systèmes informatiques et des transferts d'information d'une organisation. Les services sont conçus pour contrer les attaques de sécurité, et ils utilisent un ou plusieurs mécanismes de sécurité.

Mécanismes de sécurité : un mécanisme est conçu pour détecter, prévenir ou rattraper une attaque de sécurité. Donc, l'équipe de sécurité se base essentiellement sur ces trois approches pour la mise en place d'une stratégie de sécurité solide et efficace dans n'importe quelle organisation. [11]

1.5.5 Mise en place d'une politique de sécurité

L'implémentation de mesures de sécurité doit répondre à des besoins de sécurité clairement identifiés à la suite d'une analyse des risques spécifiquement encourus par une organisation. Les besoins s'expriment en termes d'exigences de sécurité à satisfaire au travers d'une politique de sécurité. La politique de sécurité est donc l'ensemble des orientations suivies par une organisation à prendre au sens large en termes de sécurité :

- Désigner un responsable informatique, qui sera en charge de l'élaboration et de la mise en place de cette politique de sécurité.
- Précision des droits d'accès et d'administration aux différents utilisateurs.
- Contrôler et analyser la circulation des données avec des outils matériels et logiciels sur différents niveaux.
- Tenir à jour un registre de l'ensemble des éléments qui composent le système d'information. Ce registre est important lors des modifications des composants de la configuration informatique. En cas d'incident, il peut permettre aux équipes IT de trouver l'origine du problème.
- Effectuer une analyse des risques informatiques, au regard du préjudice possible et de la probabilité d'occurrence de l'incident.

- Déterminer les moyens nécessaires pour la réduction des risques et la prise en charge des incidents, qu'il s'agisse de moyens matériels ou humains.
- Rédiger une charte informatique, à l'attention des collaborateurs.
- Communiquer sur la politique de sécurité informatique auprès de l'ensemble de l'entreprise.

1.5.6 Stratégie de la sécurité

La sécurité informatique d'une entreprise doit s'appréhender d'une manière globale et stratégique. Cette gestion fournit à l'entreprise les concepts et la terminologie spécifique de façon à ce que le personnel puisse comprendre les objectifs de sécurité et les risques potentiels, suivre les procédures liées aux impératifs requis. De nombreuses organisations nationales et professionnelles recommandent des règles de bonne pratique pour améliorer la sécurité, ces règles sont :

-Effectuer une évaluation des risques : la connaissance de la valeur de ce que nous protégeons aidera à justifier les dépenses de sécurité. Créer une politique de sécurité qui décrit clairement les règles de l'entreprise,

Les tâches et les attentes. Mesures de sécurité physiques : restreignez l'accès aux équipements réseau, aux emplacements des serveurs, ainsi qu'à la suppression des incidents.

- Mesures de sécurité des ressources humaines : les employés doivent faire l'objet d'une recherche appropriée avec vérification de leurs antécédents.
- Effectuer et tester les sauvegardes : effectuez des sauvegardes régulières et testez la récupération des données à partir de ces dernières.
- Gérez les mises à jour : mettez régulièrement à jour les systèmes d'exploitation et les programmes des serveurs, clients et périphériques réseau.
- Utilisez les contrôles d'accès : configurez les rôles d'utilisateur et des niveaux de privilèges ainsi qu'une authentification forte.
- Testez régulièrement la réponse aux incidents : faites appel à une équipe de réponse aux incidents et testez des scénarios de réponse aux urgences.
- Mettre en œuvre un outil de surveillance, d'analyse et de gestion de réseau : choisissez une solution de surveillance de la sécurité qui s'intègre à d'autres technologies.
- Implémentez des dispositifs de sécurité réseau : utilisez des routeurs, des pare-feu et d'autres dispositifs de sécurité de nouvelle génération.
- Mettre en œuvre une solution complète de sécurité des points finaux :
- Utilisation d'un logiciel anti-malware et antivirus.
- Éduquer les utilisateurs et les employés aux procédures de sécurité.
- Cryptage de données : crypter toutes les données sensibles de l'entreprise, y compris les e-mails. [12]

1.5.7 Triangle sécurité, fonctionnalité, utilisabilité

Tout système sécurisé doit fournir une protection solide tout en offrant tous les services, et facilité l'utilisation de fonctionnalités du système. Le niveau de sécurité est une mesure de la force de la sécurité du système, de sa fonctionnalité et de son utilisabilité, la mise en œuvre d'un haut niveau de sécurité généralement un impact sur les deux autres facteurs. Le système devient moins convivial avec une diminution des performances, voir la qualité de service. Lors de déploiement d'une solution de sécurité dans un système, nous devons garder à l'esprit d'assurer la fonctionnalité et de la facilité d'utilisation. Ces trois composantes du triangle doivent être équilibrées. [13] Ce trio constitue un maillon important dans le domaine des réseaux comme le montre la figure ci-dessous, où si l'un d'entre eux est retiré, le réseau devient inefficace.

L'image suivant représente le triangle de sécurité :

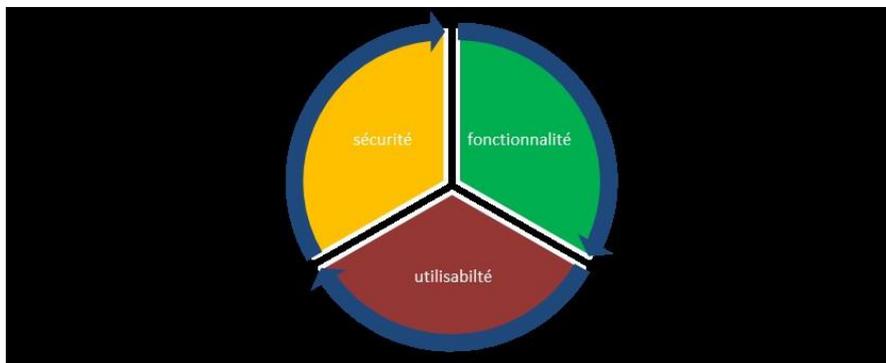


Figure 1.4: Triangle sécurité, fonctionnalité, utilisabilité.[13]

1.6 Conclusion

L'infrastructure de couche 2 est principalement composée de commutateurs d'Interconnexion Ethernet. La plupart des appareils des utilisateurs finaux, tels que Ordinateurs, imprimantes, téléphones IP, serveurs et autres. L'hôte est connecté au réseau via un commutateur d'accès de couche 2.

Par conséquent, ces commutateurs peuvent constituer une menace pour la sécurité de réseau, ils sont vulnérables aux attaques d'utilisateurs internes malveillants, la mise en place d'une politique de sécurité solide et efficace n'est pas facultatif mais une obligation. Dans le prochain chapitre, nous verrons les attaques les plus courantes et leur impact sur le réseau afin de mettre en œuvre les mécanismes nécessaires pour renforcer la sécurité.

Chapitre II - Partie I :

LES STRATEGIES DE SECURITE

Chapitre 2 :

Introduction

Notre travail commence par la réalisation d'un réseau LAN sans la prise en considération des aspects de la sécurité afin de tester ensuite les différentes attaques.

Nous allons présenter dans ce chapitre l'architecture du réseau réalisé, il est basé sur l'architecture d'un réseau d'entreprise à deux couches (Collapsed Network).

Pour cela, nous présentons les différents protocoles implémentés et le détail de la configuration implémentée dans chaque switch.

Le chapitre est divisé en trois parties, la première est consacrée à la conception, configuration et déploiement du réseau. Le troisième est réservée à l'application des diverses attaques qui peuvent cibler la couche 2 du modèle OSI.

II.1 Partie 1 : Présentation du réseau réalisé

Le réseau réalisé est schématisé par le schéma suivant

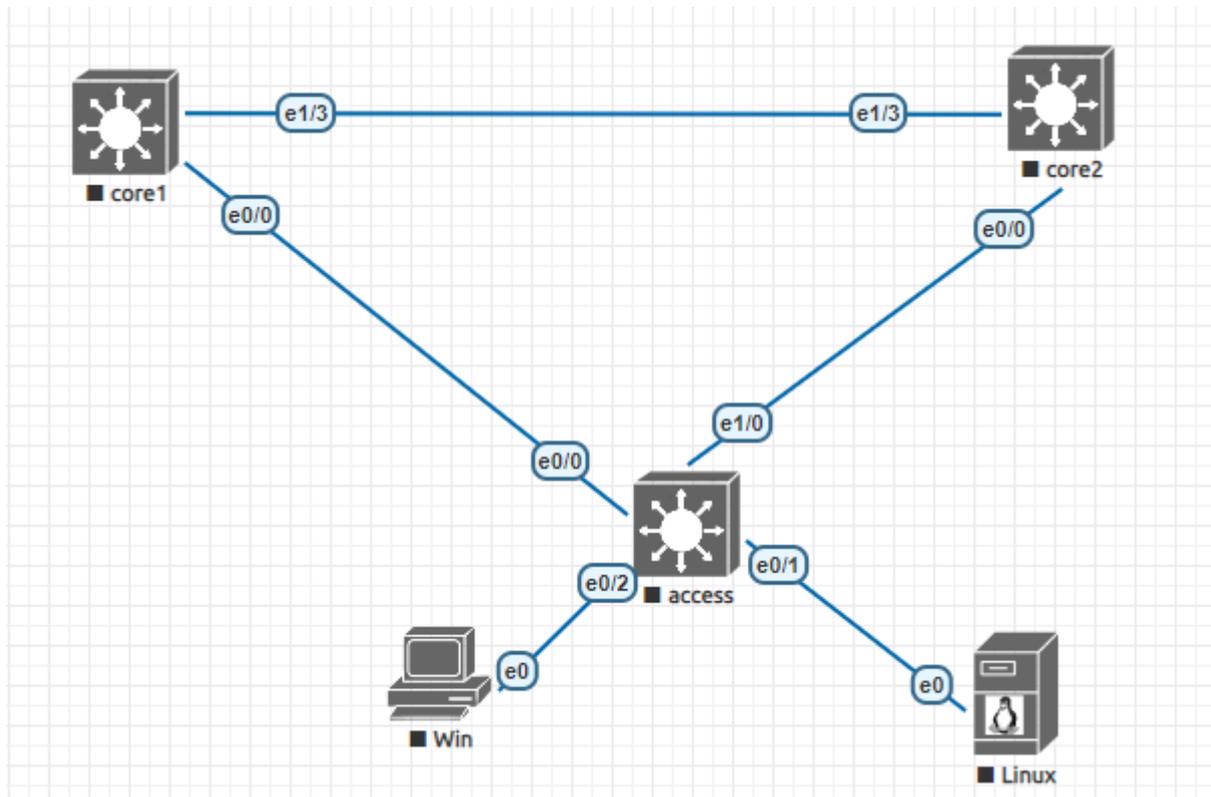


Figure 2.1: architecture de réseaux

Notre modèle d'entreprise est composé de :

Niveau cœur de réseau : Il est composé de deux commutateurs de niveau 3. Il assure les connexions avec le commutateur d'accès.

Niveau accès : Le niveau d'accès est composé d'un commutateur Cisco niveau 2, destiné à connecter les périphériques finaux.

Ces deux niveaux s'interconnectent entre eux selon certaines règles de conception Pour assurer la Haute Disponibilité de l'infrastructure, le routage entre les VLANs, la limitation des boucles . . . etc.

Entre les deux couches, on trouve un maillage partiel (le switch d'accès est connecté au deux switches coeur), Cela fournit une redondance forte pour le réseau, ainsi que la connectivité de la couche Access ne dépend d'aucun autre commutateur de même couche.

A. Equipements utilisés

1. **Commutateur niveau 3 (catalyst 3650)** : ils se trouvent au niveau de la couche d'accès et cœur . Nous allons l'exploiter comme la porte d'entrée au réseau, en implémentant plusieurs services et protocoles pour assurer le bon fonctionnement de ce dernier selon la couche la quelle est installée. [8]

L'image suivant représente un commutateurs utilisé :



Figure 2.2: commutateurs utilisés

2. **Fibre optique** : les interconnexions entre les switch est réalisée par des jarretières de la fibre optique.

L'image suivant représente fibre utilisé :

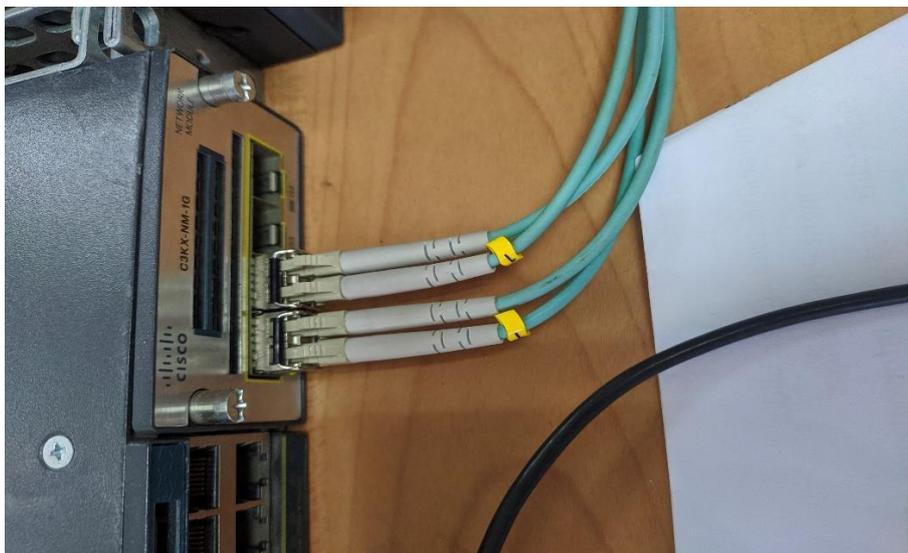


Figure 2.3: fibre optique

CHAPITRE II-Partie I : LES STRATEGIES DE SECURITE

3. **Cable console** : Il s'agit d'un câble utilisé pour la transmission de données informatiques. Il permet de connecter la console du switch au port série ou USB du Pc, il permet ainsi d'introduire la configuration initiale du switch avant de pouvoir accéder à ce dernier à travers le réseau.

L'image suivant représente un câble console utilisé :



Figure 2.4: Cable console

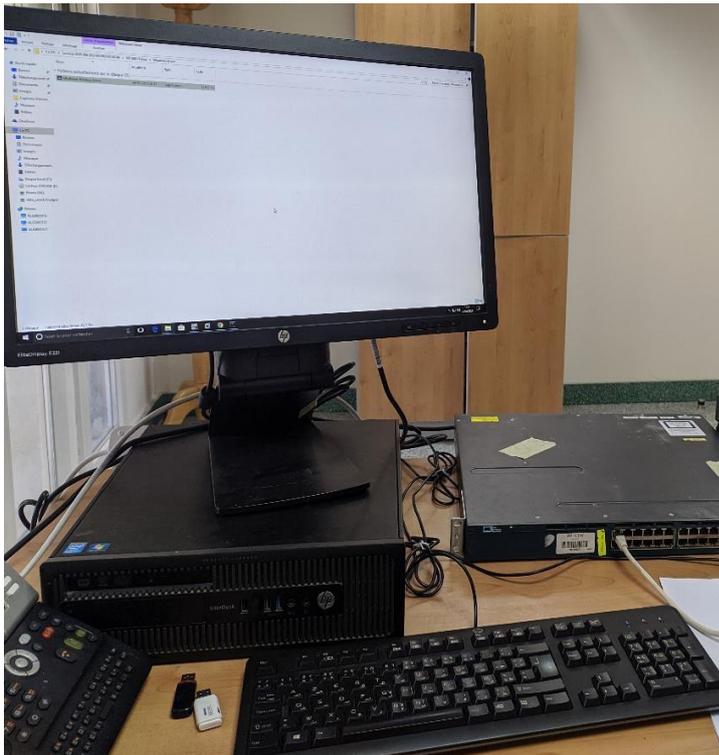
4. **Câble réseau RJ45** : Le câble réseau est utilisé pour connecter des ordinateurs et d'autres périphériques d'utilisateurs finaux (par exemple, des imprimantes) aux switches.

L'image suivant représente câble réseau RJ45 utilisé :



Figure 2.5: Straight-through cable

5. Micro ordinateur Pc :



Performance :

-8 GB ram

-1To Sata disque dur

-windows 10

-processeur i7

-carte graphique Intel HD intégrée

Figure 2.6: desktop utilisé

B. Les protocoles Installés

Le long de notre travail, nous allons exploiter plusieurs protocoles et technologies.

Dans cette partie, nous allons décrire le mode de fonctionnement du niveau

2 de réseau, ainsi que d'autres protocoles des couches supérieures nécessaires pour le bon fonctionnement de notre réseau (HSRP, DHCP), en décrivant la façon de les implémenter.

1. VLAN Trunking Protocol VTP

VLAN Trunking Protocol ou VTP est un protocole de niveau 2 utilisé pour configurer et administrer les VLAN sur les périphériques Cisco. [9]

Trois modes de configuration sont disponibles : serveur, client et transparent. Le mode serveur permet au switch en question de propager ces VLAN vers les clients VTP. Par contre, dans le mode transparent, les VLAN devront être créés sur chaque switch et aucune propagation n'est permise, par défaut le mode est serveur. [7]

2. VLANs

Nous avons segmenté notre réseau en VLANs afin de segmenter le réseau et limiter ainsi les domaines de broadcast et gérer les flux d'information. [7] Dans notre réseau campus, 04 VLANs ont été créés comme suit :

N° de VLAN	Nom de VLAN	Plage d'adressage	Masque
2	informatique	10.110.2.0	255.255.255.0
3	Commercial	10.110.3.0	255.255.255.0
4	production	10.110.4.0	255.255.255.0
5	Management	10.110.5.0	255.255.255.0

Tableau 2.1: tableau des vlans utilisés

- VLAN informatique : Ce vlan sera utilisé pour héberger les employeurs du service Informatique .
- VLAN commerciale : Il sera utilisé par les employeurs du service commerciale.
- VLAN production : ce vlan est destiné aux services de production .
- VLAN management : Ce vlan sera utilisé pour administrer les switch

3. Spanning-tree :

Le STP est un protocole crucial et fondamental dans tout réseau informatique. L'ensemble des switchs du réseau utilisent ce protocole qui permet d'éviter les boucles dans le réseau. [7] Dans notre cas on a utilisé la version Rapid-PVST (Rapid-Per Vlan Spanning-Tree) grâce aux avantages qu'il offre notamment : la vitesse de calcul et réponse au changement de la topologie.

Afin de répartir la charge des Vlan entre les deux switch cœur, la configuration de root primary et root secondary est importante. [6]

4. CDP Cisco Discover Protocol

Ce protocole sera activé sur les commutateurs d'accès et cœur de réseau pour des besoins de facilitation de l'administration et du troubleshooting, en plus cela permettra une meilleure intégration avec les solutions de téléphonie IP et Wireless. [3]

5. HSRP

C'est le protocole de redondance qu'il sera utilisé pour assurer une disponibilité accrue de la passerelle du réseau où l'adresse IP de la passerelle est configurée sur les deux commutateurs cœur (interfaces), une seule de ces deux interfaces sera active. Si l'interface active ne sera plus accessible, l'autre interface deviendra active.

La configuration du HSRP dépendra aussi du STP pour mieux exploiter les deux protocoles, dont le commutateur qui sera le primaire pour un VLAN, son interface va être active pour le même VLAN, et vice versa. [9]

6. DHCP

Afin de simplifier à l'administrateur la gestion et l'attribution des adresses IP, on utilise le protocole DHCP qui permet de configurer les paramètres réseaux client, au lieu de les configurer sur chaque ordinateur manuellement. [4]

7. Agrégation des liens

EtherChannel est une technologie d'agrégation de liens utilisés principalement sur les commutateurs de Cisco. Elle permet d'assembler plusieurs liens physiques Ethernet en un lien logique. [6]

Nous allons implémenter l'etherchannel entre les commutateurs cœur de réseau pour augmenter la vitesse et la tolérance aux pannes entre eux. Pour la configuration d'etherchannel, nous allons utiliser le protocole LACP qui est le protocole standard de l'agrégation des liens.

8. Gestion d'accès aux équipements :

Le protocole **Telnet** définit un protocole standard d'Internet qui autorise les communications entre un client et un serveur. Plus concrètement, ce protocole relie un système composé d'un

CHAPITRE II-Partie I : LES STRATEGIES DE SECURITE

clavier et d'un affichage à un interpréteur de commande. Dans notre cas il sera pour se connecter aux commutateurs à travers le réseau. [7]

C. Plan final de la configuration :

La mise en place d'un réseau campus qui répond aux exigences de l'entreprise nécessite un bon plan de travail. Ce dernier doit être simple, clair et facile à appliquer. Pour cela, nous allons deviser la configuration de notre réseau en trois niveaux où chacun complètera les autres.

Le premier niveau va être basé sur la configuration initiale pour tout réseau tel que la manipulation basique des protocoles notamment : STP, VTP, HSRP. etc. Quoique ce niveau est tellement simple et basique, il reste la base des réseaux informatiques, d'où la nécessiter de l'implémenter.

L'image suivant représente le réseaux utilisé :

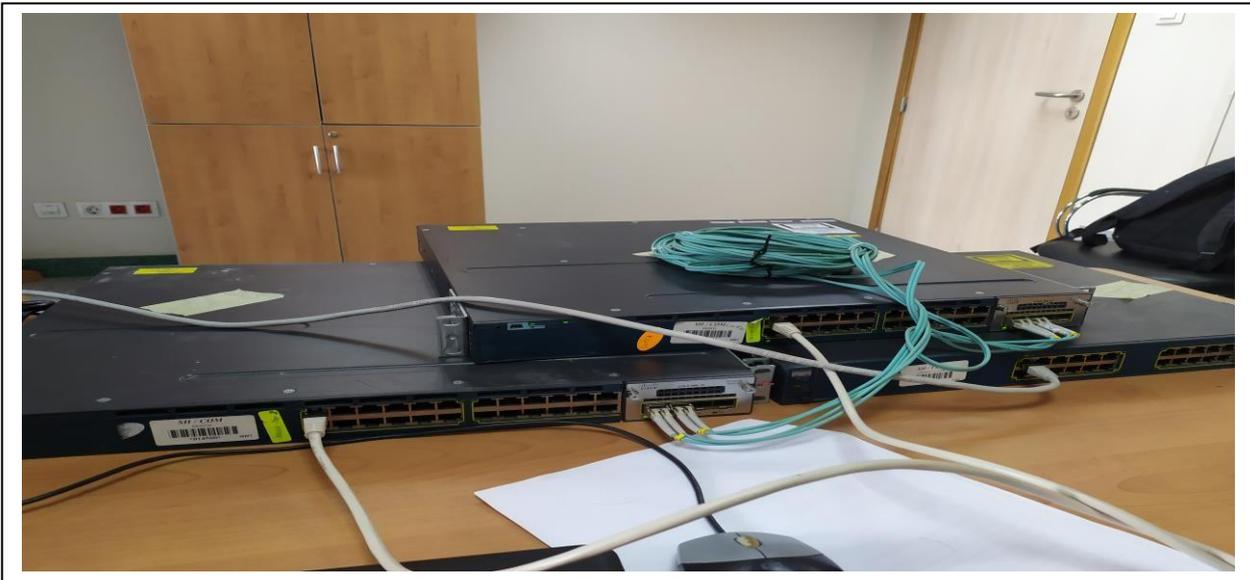


Figure 2.7:reseau réalisé avec matériel réel

1. **Configuration initiale** : Nous allons implémenter ici les premières configurations d'un réseau comme : le nom (hostname), mot de passe d'accès par console, Ces commandes sont les mêmes pour tous les switches comme présenter dans l'image suivant :

```

Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname access
access(config)#line console 0
access(config-line)#password cisco
access(config-line)#login
access(config-line)#logging synchronous
access(config-line)#exit
access(config)#ip domain-lookup
access(config)#enable secret cisco
access(config)#banner login -attention systeme securise
access(config)#banner login -attention systeme securise-
access(config)#banner login -attention systeme securise-?
LINE    <cr>

access(config)#banner login -attention systeme securise
Enter TEXT message. End with the character '-'.
banner login -attention systeme securise-
access(config)#service password-encryption

```

Figure 2.8.: configuration initiale

Le tableau suivant donne la signification de chaque commande utilisée.

Commande	Signification
Enable	Changer de mode, de celui d'exécution utilisateur à celui d'exécution privilégié.
Configure terminal	Passer du mode d'exécution privilégié à celui de configuration globale.
Hostname sw-core-1	Définir un nom d'hôte pour le périphérique, pour notre cas le nom est : sw-core-1.
Line console 0	Passer du mode de configuration globale au mode de configuration de ligne pour la console 0.
Passwordcisco	Définir cisco en tant que mot de passe pour la ligne de console 0 sur le switch.
Login	Définir la ligne de console pour exiger la saisie du mot de passe avant l'octroi de l'accès.
Loggingsynchronous	Forcer l'affichage de tous les messages d'état du routeur sur une nouvelle ligne
Exit	Passer du mode de configuration d'interface en mode de configuration globale.
No ipdomain-lookup	Désactiver la recherche DNS en mode console.
Enable secret cisco	Configurer 'cisco' comme mot de passe pour le passage en mode d'exécution privilégié.

CHAPITRE II-Partie I : LES STRATEGIES DE SECURITE

Banner login « personnel autorisé uniquement »	Configurer une bannière de connexion.
bannermotd « attention! Système sécurisé »	La bannière MOTD affiche tous les terminaux connectés à la connexion et permet de transmettre des messages destinés à tous les utilisateurs du réseau
Service password-encryption	Crypter tous les mots de passes d'un coup.

Tableau 2.2 : commandes de la configuration initiale

2. Création de vlan :

On va configurer suite à cette figure

création du Vlan 2

```
access(config)#vlan 2
access(config-vlan)#name informatique
```

Figure 2.9.:Création du vlan

Après la création on affiche les vlan

Les vlans :

```
vlan 2
  name informatique
!
vlan 3
  name commercial
!
vlan 4
  name production
!
vlan 5
  name managment
```

Figure 2.10:les vlans créés

Commandes pour la création de vlan

Commande	Sifnification
Vlan 10	créer le VLAN 10
name HR	Nommer le VLAN

Tableau 2.3: Commandes pour la création de vlan

Configuration des interfaces :

Les interfaces seront configurées selon leurs utilisation, une interface qui sert à interconnecter deux switch sera configurée en mode trunk qui permet de véhiculer tous les Vlan (l'interface Ethernet0/0 dans le schéma ci-dessous). Les interfaces d'accès du switch d'accès seront configurées en mode access en indiquant le vlan attribué (l'interface Ethernet0/1 dans le schéma ci-dessous)

Les images suivants présent les étapes pour configurer les interfaces :

```
interface Ethernet0/0
  switchport trunk encapsulation dot1q
  switchport mode trunk
  duplex auto
!
interface Ethernet0/1
  switchport access vlan 2
  switchport mode access
  duplex auto
!
interface Ethernet0/2
  switchport access vlan 2
  switchport mode access
  duplex auto
!
interface Ethernet0/3
  switchport access vlan 3
  switchport mode access
  duplex auto
!
interface Ethernet1/0
  switchport access vlan 3
  switchport trunk encapsulation dot1q
  switchport mode trunk
  duplex auto
!
interface Ethernet1/1
  switchport access vlan 3
  switchport mode access
  duplex auto
!
interface Ethernet1/2
  switchport access vlan 4
  switchport mode access
  duplex auto
!
interface Ethernet1/3
  switchport access vlan 4
  switchport mode access
  duplex auto
```

Figure 2.11 : configuration d'interface

CHAPITRE II-Partie I : LES STRATEGIES DE SECURITE

```
access(config)#int e0/0
access(config-if)#switchport mode trunk
access(config-if)#sw
*Sep 13 11:26:38.497: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to down
access(config-if)#switchport
*Sep 13 11:26:41.503: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to up
access(config-if)#switchport trunk encapsulation dot1q
access(config-if)#exit
```

Figure 2.12 : Etapes de configuration d'un port trunk

Interface e0/0 :

```
interface Ethernet0/0
switchport trunk encapsulation dot1q
switchport mode trunk
```

Figure 2.13.: Interface de connexion entre switch access et cœur 1 :

```
interface Ethernet1/0
switchport trunk encapsulation dot1q
switchport mode trunk
```

Figure 2.14 : Interface de connexion entre switch access et cœur 2

```
access(config-vlan)#int e0/2
access(config-if)#switchport mode access
access(config-if)#switchport access vlan 2
```

Figure 2.15 : répartition des vlans entre les interfaces

Vlan 2	Interface e0/1-interface e0/2
Vlan 3	Interface e0/3-interface e1/1
Vlan 4	Interface e1/2-interface e1/3

Tableau 2.4: répartition des Vlan

VLAN	Name	Status	Ports
1	default	active	
2	informatique	active	Et0/1, Et0/2
3	commercial	active	Et0/3, Et1/1
4	production	active	Et1/2, Et1/3
5	managment	active	

Figure 2.16 : Diviser les vlans sur les interfaces

Dans le tableau ci-dessous, est affiché les commandes avec leurs significations pour un port configuré en trunk.

CHAPITRE II-Partie I : LES STRATEGIES DE SECURITE

Commande	Signification
Intaerface range G0/0 -1, G1/0 -2	Sélectionner plusieurs interfaces à la fois.
Switchport trunk encapsulation dot1q	Définir les interfaces comme agrégation IEEE 802.1Q
Switchport mode trunk	Forcer la liaison reliant les switches à devenir une liaison agrégée.
Switch port nonegotiate	Désactiver la négociation et empêcher le port d'envoyer des messages DTP.
Switchporttrunk native vlan 99	Spécifier le VLAN 99 en tant que VLAN natif pour le trafic non étiqueté pour les agrégations IEEE 802.1Q.

Tableau 2.5 : Commandes utilisées pour un port interface.

Configuration de la passerelle par défaut

Une passerelle par défaut est définie dans le switch d'accès afin de l'administrer à travers le réseau via le Vlan 5 de Management.

L'image ci-dessous configurer la passerelle

```
access(config-if)#ip default-gateway 10.110.5.1
access(config)#ip route 0.0.0.0 0.0.0.0 10.110.5.1
access(config)#
```

Figure 2.17 : Configuration de default Gateway :

Configuration des interfaces Vlan

Chaque Vlan, a une interface vlan configurée au niveau des deux Cœur avec une adresse virtuelle gérée par le HSRP et configurée via la commande standby. Cette adresse sera l'adresse par défaut du vlan concerné. Une autre adresse de l'interface vlan sera attribuée à chaque switch Cœur selon le tableau ci-dessous .

Exemple de l'interface vlan 2 du cœur 1

```
core1(config)#int vlan 2
core1(config-if)#
*Sep 13 12:54:25.756: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2, cha
nged state to down
core1(config-if)#ip add 10.110.2.3 255.255.255.0
core1(config-if)#no sh
```

Figure 2.18 : Configuration des interface vlans

CHAPITRE II-Partie I : LES STRATEGIES DE SECURITE

numéro Vlan	Adresse ip de l'interface vlan dans le cœur 1	Adresse ip de l'interface vlan dans le cœur 2	Adresse ip virtuelle de l'interface vlan standby
2	10.110.2.3	10.110.2.2	10.110.2.1
3	10.110.3.3	10.110.3.2	10.110.3.1
4	10.110.4.3	10.110.4.2	10.110.4.1
5	10.110.5.3	10.110.5.2	10.110.5.1

Tableau 2.6 : les adresses des interfaces vlans

Configuration HSRP :

Afin de répartir la charge entre les deux switch cœur et assurer ainsi une haute disponibilité, on va assigner à chaque cœur une priorité dans le HSRP pour certains vlan afin de forcer le trafic des vlans en question à passer via ce dernier à l'aide de la commande *standby x priority* figure et tableau ci-dessous

```
access(config-if)#int vlan 2
access(config-if)#standby 2 ip 10.110.2.1
access(config-if)#standby 2 preiority
^
% Invalid input detected at '^' marker.

access(config-if)#standby 2 preiority
*Sep 13 12:57:03.083: %HSRP-5-STATECHANGE: Vlan2 Grp 2 state Standby -> Active
access(config-if)#standby 2 priority 150
access(config-if)#standby 2 preempt
```

Figure 2.19 : étapes de Configuration HSRP

Les priorités assignées sont comme suit

switch	priority
Core 1	2,3
Core 2	4,5

Tableau 2.7 : répartition des Vlans sur les switch Cœur via HSRP

La liste des commandes utilisées est la suivante

Commande	Signification
Ip address 10.110.2.1 255.255.255.0	Configurer l'adresse IP et le masque de l'interface.
No shutdown	Activer l'interface.
Standby 2 ip 10.110.2.3	Configurer une adresse IP virtuelle pour le HSRP.
Standby 2 priority 150	Configurer la priorité de l'HSRP (facultatif).
Standby 2 preempt	Configurer la préemption HSRP (facultatif).
Ip helper-address 10.110.40.254	relayer les demandes DHCP vers votre serveur DHCP.

Tableau 2.8 :explication de commandes HSRP

CHAPITRE II-Partie I : LES STRATEGIES DE SECURITE

Configuration spanning tree STP :

Afin de garder la cohérence de partage de trafic via HSRP, les vlan sont priorisés au niveau du STP de la même façon via la commande **spanning-tree vlan x,y root primary (secondary)** figure et tableau ci-dessous.

```
core1(config)#spanning-tree vlan 2,3 root primary
core1(config)#spanning-tree vlan 4,5 root secondary
```

Figure 2.20 : étape de la configuration STP

Commande	Signification
Spanning-tree mode rapid-pvst	active la version rapid-pvst du protocol STP.
Spanning-tree vlan 2,3 root primary	designer le commutateur sw-core-1 comme un root primaire pour les VLANs 2,3
Spanning-tree vlan 4,5 root secondary	designer le commutateur sw-core-1 comme un root secondaire pour les VLANs 4 5

Explication de commandes du STP.

Tableau 2.9 : explication de commandes STP

Résultat : via la commande show run

```
spanning-tree mode pvst
spanning-tree extend system-id
spanning-tree vlan 2-3 priority 24576
spanning-tree vlan 4-5 priority 28672
```

Figure 2.21 : résultat des commandes STP

Configuration DHCP :

Chaque switch Cœur est configuré comme serveur DHCP pour les clients finaux du réseau (end point).

Dans la figure ci-dessous, un exemple de configuration pour le vlan2, pour chaque vlan on créé un pool DHCP avec la commande **ip dhcp pool vlan x** et on associé:

- Le réseau à attribuer via la commande **network** pour le vlan 2 c'est 10.110.2.0/24
- La passerelle par défaut via la commande **default-router**
- Le serveur DNS via la commande **dns-server**

```
(config)#ip dhcp pool vlan10
(dhcp-config)#network 10.110.2.0 255.255.255.0
(dhcp-config)#dns-server 1.1.1.1
(dhcp-config)#default-router 10.110.2.1
(dhcp-config)#domain-name stage.com
      ^
valid input detected at '^' marker.
(dhcp-config)#domain-name stage.com
(dhcp-config)#exit
(config)#ip dhcp excluded-address 10.110.2.1 10.110.2.12
```

Figure 2.22 : étapes de Configuration dhcp pour le vlan 2

La commande *ip dhcp excluded-address* est utilisée pour réserver des adresses ip afin de les attribuer statiquement, dans l'exemple en-dessus les adresses de 10.110.2.1 jusqu'à 10.110.2.12 sont réservées.

A la fin de configuration du DHCP on a :

Pour le Core 1 figure suivant :

```
ip dhcp excluded-address 10.110.2.1 10.110.2.12
ip dhcp excluded-address 10.110.3.1 10.110.3.12
ip dhcp excluded-address 10.110.2.1 10.110.2.20
ip dhcp excluded-address 10.110.3.1 10.110.3.20
ip dhcp excluded-address 10.110.4.1 10.110.4.20
ip dhcp excluded-address 10.110.5.1 10.110.5.20
!
ip dhcp pool VLAN2
 network 10.110.2.0 255.255.255.0
 dns-server 1.1.1.1
 default-router 10.110.2.1
 domain-name stage.com
!
ip dhcp pool vlan3
 network 10.110.3.0 255.255.255.0
 dns-server 1.1.1.1
 default-router 10.110.3.1
 domain-name stage.com
!
ip dhcp pool vlan4
 network 10.110.4.0 255.255.255.0
 dns-server 1.1.1.1
 default-router 10.110.4.1
 domain-name stage.com
!
ip dhcp pool vlan5
 network 10.110.5.0 255.255.255.0
 default-router 10.110.5.1
 domain-name stage.com
```

Figure 2.23 : configuration de DHCP switch core 1

CHAPITRE II-Partie I : LES STRATEGIES DE SECURITE

Pour le core2 la figure ci-dessus

```
ip dhcp excluded-address 10.110.2.20 10.110.2.254
ip dhcp excluded-address 10.110.2.20 10.110.2.250
ip dhcp excluded-address 10.110.2.32 10.110.2.250
ip dhcp excluded-address 10.110.2.33 10.110.2.250
ip dhcp excluded-address 10.110.3.33
ip dhcp excluded-address 10.110.3.34 10.110.3.254
ip dhcp excluded-address 10.110.2.33 10.110.2.254
ip dhcp excluded-address 10.110.4.33 10.110.4.254
ip dhcp excluded-address 10.110.5.33 10.110.5.254
!
ip dhcp pool vlan3
 network 10.110.3.0 255.255.255.0
 default-router 10.110.3.1
 dns-server 1.1.1.1
 domain-name stage.com
!
ip dhcp pool vlan2
 network 10.110.2.0 255.255.255.0
 default-router 10.110.2.1
 dns-server 1.1.1.1
 domain-name stage.com
!
ip dhcp pool vlan4
 network 10.110.4.0 255.255.255.0
 dns-server 1.1.1.1
 domain-name stage.com
 default-router 10.110.4.1
!
ip dhcp pool vlan5
 network 10.110.5.0 255.255.255.0
 default-router 10.110.5.1
```

Figure 2.24 : configuration de DHCP switch core 2

Configuration d'accès distant aux switch via Telnet :

Le protocole telnet est utilisé dans les lignes virtuelle vty afin d'accéder au switch à distance les commandes utilisées sont

Line vty 0 4 : les lignes virtuelles de 0 à 4 donc 05 connexions simultanées

Transport input telnet : définition de telnet comme protocole d'accès

Password xxxxxx : définit le mot de passe

```
core1(config)#line vty 0 4
core1(config-line)#
*Sep 13 14:18:41.889: %IP-4-DUPADDR: Duplicate address 10.110.3.1 on Vlan3, sourced by 0000.0c07.ac02
core1(config-line)#
*Sep 13 14:19:12.385: %IP-4-DUPADDR: Duplicate address 10.110.3.1 on Vlan3, sourced by 0000.0c07.ac02
core1(config-line)#
*Sep 13 14:19:42.385: %IP-4-DUPADDR: Duplicate address 10.110.3.1 on Vlan3, sourced by 0000.0c07.ac02
core1(config-line)#transport
*Sep 13 14:20:12.389: %IP-4-DUPADDR: Duplicate address 10.110.3.1 on Vlan3, sourced by 0000.0c07.ac02
core1(config-line)#transport input telnet
^
% Invalid input detected at '^' marker.
core1(config-line)#transport input tel
*Sep 13 14:20:42.389: %IP-4-DUPADDR: Duplicate address 10.110.3.1 on Vlan3, sourced by 0000.0c07.ac02
core1(config-line)#transport input telnet
core1(config-line)#password stage
*Sep 13 14:21:12.886: %IP-4-DUPADDR: Duplicate address 10.110.3.1 on Vlan3, sourced by 0000.0c07.ac02
core1(config-line)#password stage
core1(config-line)#login
core1(config-line)#
*Sep 13 14:21:42.888: %IP-4-DUPADDR: Duplicate address 10.110.3.1 on Vlan3, sourced by 0000.0c07.ac02
core1(config-line)#exit
```

Figure 2.25 : Configuration de telnet

CHAPITRE II-Partie I : LES STRATEGIES DE SECURITE

Tests de réseaux :

Ainsi la configuration de base de notre réseau est terminée, afin de vérifier le bon fonctionnement de notre réseau, on a effectué les tests suivants

La communication entre core 1 et Access switch :

```
core1#ping 10.110.5.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.110.5.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Figure 2.26 : tester le ping1

La communication entre core 2 et switch Access :

```
core2#ping 10.110.5.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.110.5.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Figure 2.27 : tester le ping2

La communication entre core 1 et core 2 :

```
core1#ping 10.110.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.110.2.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/3 ms
```

Figure 2.28 : tester le ping3

La communication entre le switch Access et le core 1 :

```
access#ping 10.110.2.1
Type escape sequet.
Sending 5, 100-byte ICMP Echos to 10.110.2.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/3 ms
```

Figure 2.29 : tester le ping4

CHAPITRE II-Partie I : LES STRATEGIES DE SECURITE

Teste d'accès distant au switch core 1 via Telnet :

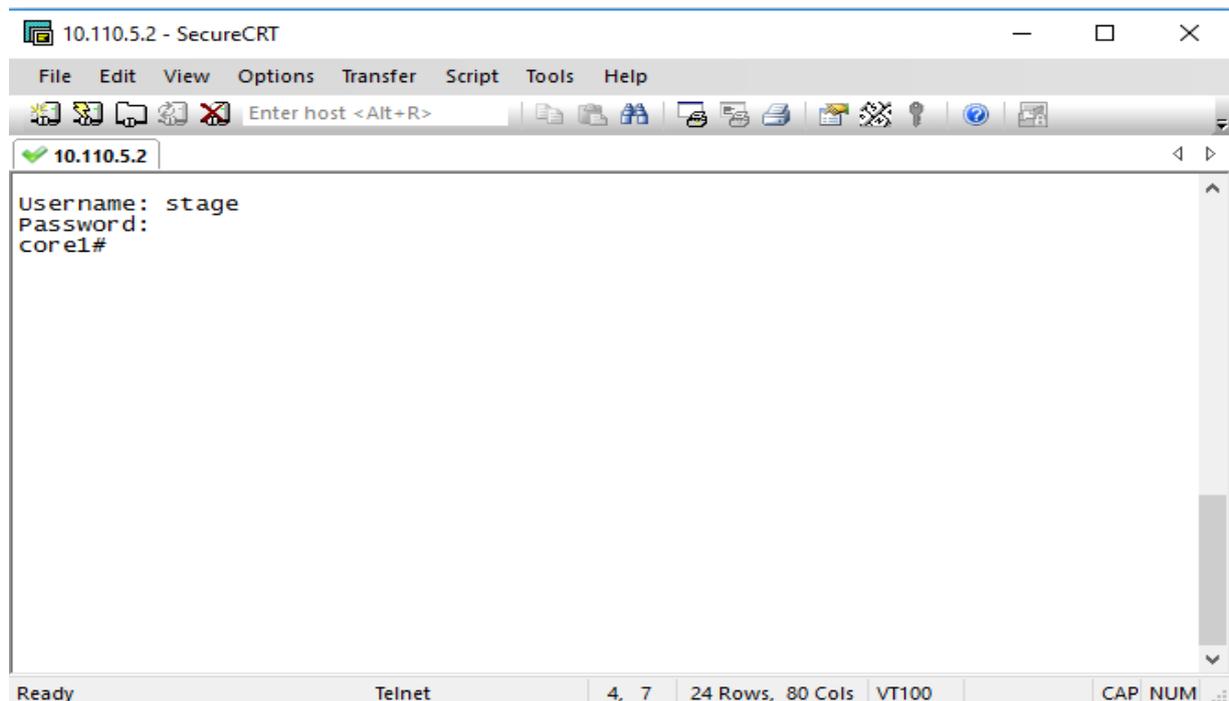


Figure 2.30 : connexion Telnet

Conclusion :

Dans cette partie, on a réalisé un réseau LAN basé sur l'architecture du réseau campus à deux couches (Collapsed Network). Tous les protocoles nécessaires au bon fonctionnement ont été implémentés. Les tests de vérification étaient concluants.

Aucune mesure de sécurité n'est implémentée dans notre architecture, dans la prochaine partie on va démontrer les vulnérabilités de cette implémentation, en lançant différentes attaques qui exploitent les failles de sécurité du niveau 2 .

Chapitre II - Partie II :
Etudier des attaques réseau de niveau II

Partie 2 :

Etudier des attaques réseau de niveau II :

1 Introduction :

La sécurité de l'information est le point le plus critique du processus de déploiement Réseau, car il est soumis à de nombreux types d'attaques et de menaces, utilisant Pour diverses raisons, il existe diverses vulnérabilités dans le réseau mal intentionné. Par conséquent, un audit de sécurité informatique est requis Définir une stratégie de sécurité efficace, y compris l'entreprise qu'ils utilisent Aujourd'hui, traitez-le comme un avantage concurrentiel et un nouveau défi qui doit être réalisé. Dans ce chapitre, nous allons détailler ces attaques à partir du niveau 2 du modèle. OSI, leurs principes de fonctionnement et leur impact sur le réseau. Mettre en œuvre des contre-mesures et des stratégies solides pour assurer notre Le réseau d'entreprise fermera cette partie.

2 Classification des menaces :

Le réseau est définitivement confronté à des menaces de sécurité, et ces Les menaces peuvent se manifester sous diverses formes. Les attaques contre ces Les vulnérabilités peuvent être très diverses et très dangereuses. Il existe différentes manières de classer n'importe quelle menace système. Nous pouvons les classer selon les dégâts occasionnés et le degré de dégâts Les compétences requises pour effectuer l'attaque, et peut-être même la motivation Derrière l'attaque. Au début, les menaces de sécurité étaient essentiellement divisées en trois catégories Les principales catégories sont décrites dans le tableau ci-dessous : [10]

Menaces naturelles	Menaces physiques	Menaces humaines
- Inondations.	-Pertes ou dommages des ressources.	-Hackers.
-Tremblements de terre.	-Intrusions physiques.	-Social Engineering.
-Catastrophes naturelles.	-Sabotage et espionnage	-Manque de conscience.

Tableau 2.10 : Classification de menaces

Par la suite, en général, les attaques sont classées par ce qu'elles font réellement. Sur la base de cette philosophie, la plupart des attaques peuvent être classées dans l'une des trois grandes classes : [14]

- **Intrusion** : cette catégorie comprend les attaques visant à violer la sécurité et à obtenir un accès non autorisé à un système. Ce groupe d'attaques comprend toute tentative d'obtenir un accès non autorisé à un système. C'est généralement ce que font les pirates.

- **Blocage** : cette catégorie comprend les attaques conçues pour empêcher l'accès légitime à un système. Les attaques de blocage sont souvent appelées attaques par déni de service (DoS). Dans ces types d'attaques, le but n'est pas de pénétrer réellement dans le système mais simplement d'empêcher les utilisateurs légitimes d'y accéder.
- **Malware** : l'installation de logiciels malveillants sur un système. Un logiciel malveillant est un terme générique désignant un logiciel à des fins malveillantes. Il comprend les attaques de virus, les chevaux de Troie et les logiciels espions.

3 Attaque de niveau 2 du modèle OSI :

Un grand nombre de menaces courantes doivent être prises en compte lors de la sécurisation d'un réseau, mais un domaine souvent négligé est la sécurité du LAN. Lorsque les gens pensent à la sécurité, ils pensent souvent spéciquement aux couches au-dessus de la couche 2, mais il n'y a aucune raison de limiter un plan de sécurité à ces couches supérieures, surtout que plus de 70% des attaques proviennent de l'interne. [10] Un bon plan de sécurité doit prendre en compte toutes les couches, de la couche 1 à la couche 7. Cette partie examine certaines attaques de couche 2 les plus courantes ainsi que leurs principes de fonctionnement : [11]

3.1 Débordement de la table CAM :

Mac flooding attack se produit lorsque l'attaquant essaie d'envoyer un grand nombre d'adresses MAC invalides à la table MAC. Il inonde la table source avec les adresses MAC invalides. Une fois que la table MAC atteint la limite assignée de la table MAC, elle commence à supprimer les adresses MAC valides. C'est une des caractéristiques de la table MAC, elle supprime l'adresse précédente au fur et à mesure que de nouvelles adresses s'y ajoutent.

Maintenant, toutes les adresses MAC valides ont été supprimées. Le commutateur se comportera désormais comme le concentrateur du réseau. Si les utilisateurs connectés au même réseau tentent d'accéder au Web, ils reçoivent une diffusion ou une inondation sur tout le réseau.

Lorsque deux utilisateurs valides tentent de se connecter, leurs données seront transmises à tous les ports comme la diffusion. Ceci est également connu sous le nom d'attaque par inondation de table MAC. Une fois cela fait, tous les utilisateurs valides ne feront pas d'entrée. Ils vont travailler en fonction de la diffusion.

Dans de tels scénarios, les attaquants font partie d'un réseau. Il enverra des packs de données malveillants à la machine de l'utilisateur. Cela permettra à l'attaquant de pouvoir voler des données sensibles de la machine de l'utilisateur. Cela permettra également à l'attaquant d'obtenir toutes les données de communication aller-retour. Cela permet à une attaque par inondation MAC de réussir. [15]

Déroulement de l'attaque

Attack Scenario :

1. Installation de l'outil DSNIFF :

Vous pouvez effectuer une attaque par inondation MAC avec un outil appelé Macof . C'est la partie de Dsniff qui peut être installée avec cette commande sur kali Linux

```
# yum install dsniff
```

Figure 3.1 : installation de dsniff

2. Verification de la table Mac du switch avant l'attaque :

```
access#sh mac address-table dynamic
      Mac Address Table
-----
Vlan    Mac Address      Type              Ports
-----
1       e4d3.f1fb.8181   DYNAMIC          Gi0/23
2       0000.0c07.ac02   DYNAMIC          Gi0/23
2       000c.294b.5389   DYNAMIC          Gi0/1
2       a0d3.c134.7698   DYNAMIC          Gi0/1
2       acf2.c502.62c1   DYNAMIC          Gi0/23
2       e4d3.f1fb.8181   DYNAMIC          Gi0/23
2       e4d3.f1fb.81c1   DYNAMIC          Gi0/23
3       0000.0c07.ac03   DYNAMIC          Gi0/23
3       acf2.c502.62c2   DYNAMIC          Gi0/23
3       e4d3.f1fb.8181   DYNAMIC          Gi0/23
4       0000.0c07.ac04   DYNAMIC          Gi0/24
4       acf2.c502.6281   DYNAMIC          Gi0/24
4       e4d3.f1fb.81c3   DYNAMIC          Gi0/24
5       0000.0c07.ac05   DYNAMIC          Gi0/24
5       acf2.c502.6281   DYNAMIC          Gi0/24
5       e4d3.f1fb.81c4   DYNAMIC          Gi0/24
Total Mac Addresses for this criterion: 16
```

Figure 2.32 : table mac avant l'attaque

On Remarque que la table est de taille limitée aux enregistrements des adresses Mac des différents Vlan.

3.lancement de l'attaque MAC address flooding

Lancer l'utilitaire **macof** : via la commande `macof -i eth0` à partir de Kali linux, dont est l'interface avec la quelle Kali est connectée au réseau .

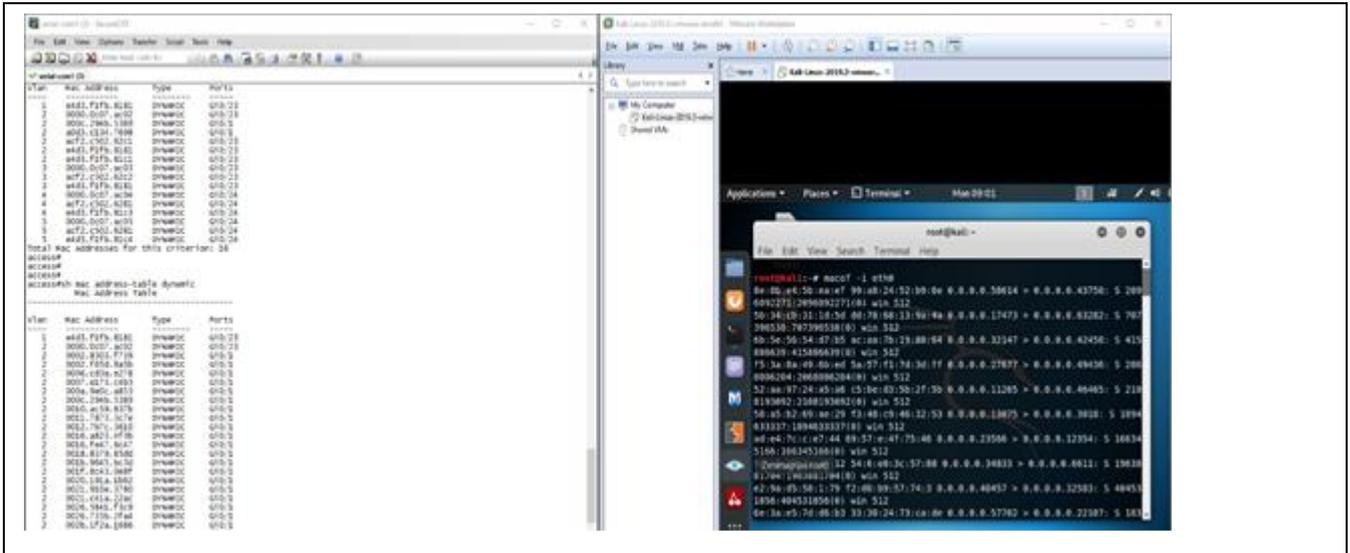


Figure 2.33 : lancement d'attaque

Macof génère entre 10000 et 15000 paquets par seconde. Chaque paquet est envoyé avec une adresse IP source et destination aléatoire. L'adresse MAC source et destination est également différente pour chaque frame Ethernet.

Le processus d'apprentissage de l'adresse MAC dure plus de 2 secondes et le commutateur s'en plaint. Dans la sortie ci-dessous, l'utilisation du processeur est affichée immédiatement après la fin de l'attaque cryptés, donc si quelqu'un les capture, l'attaquant peut obtenir ces informations.

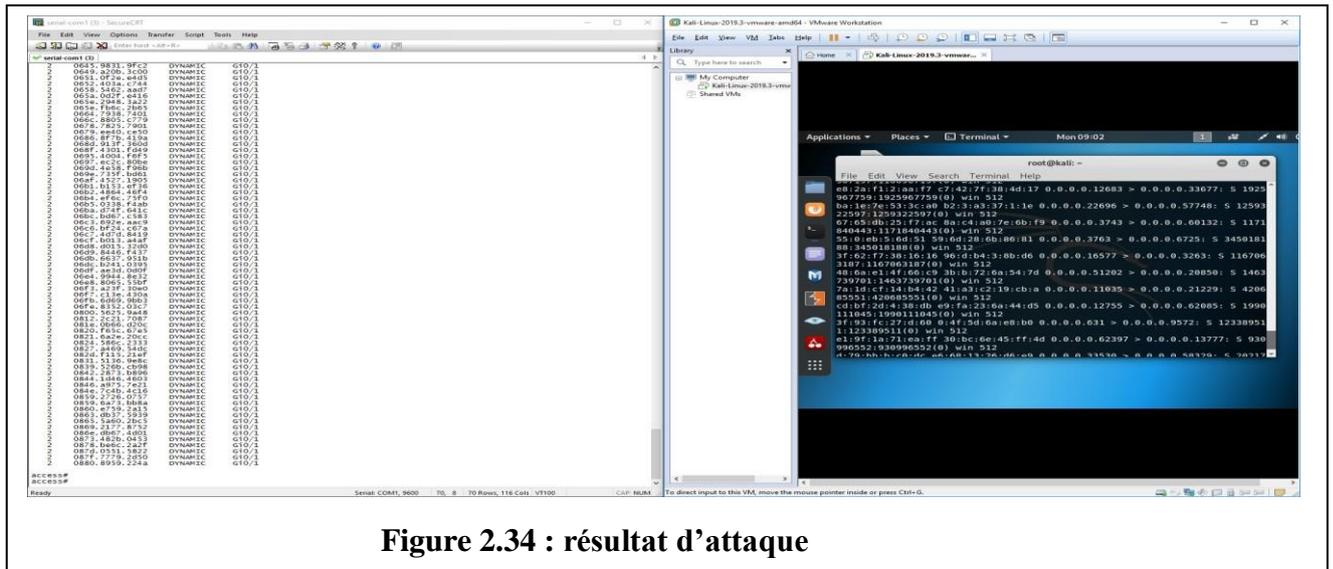
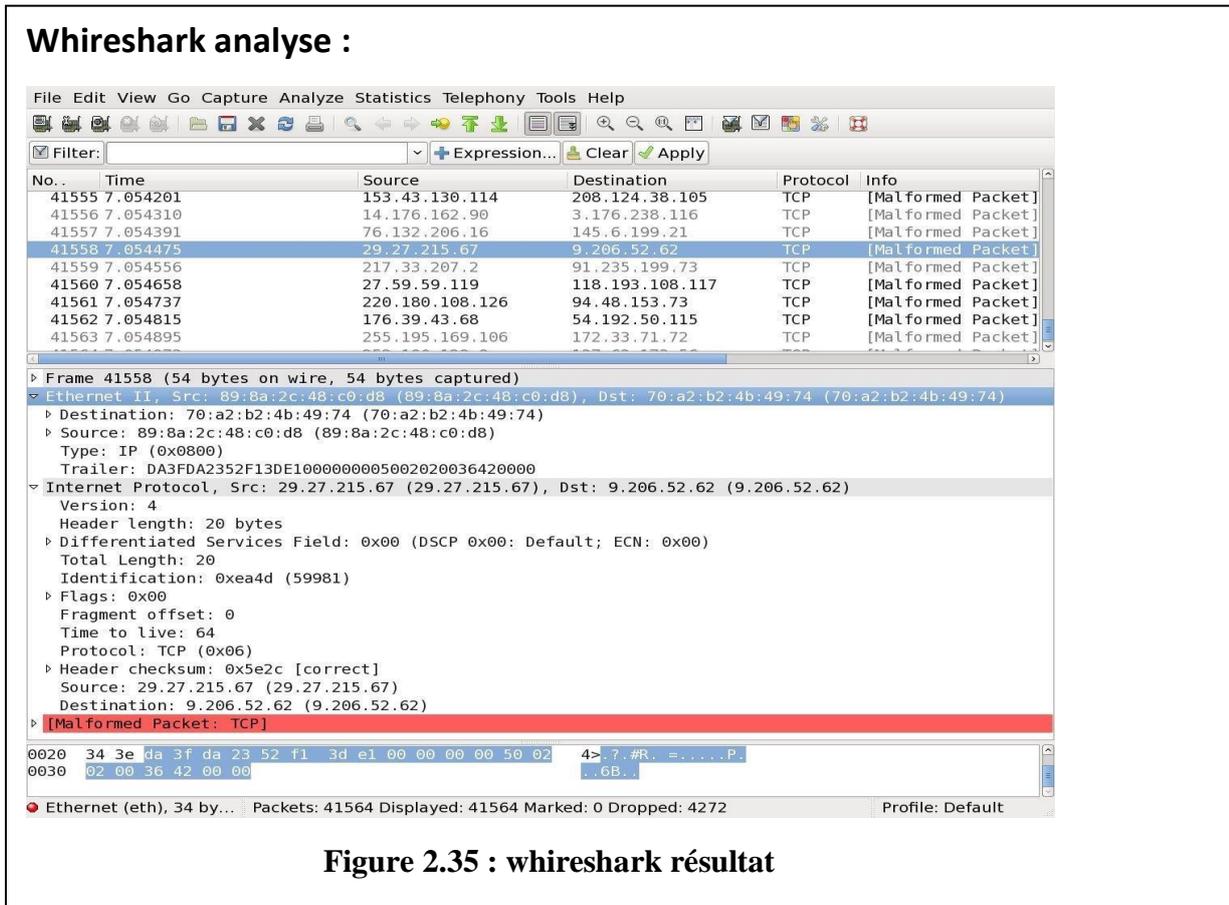


Figure 2.34 : résultat d'attaque



Sur Wireshark, on capte les paquets envoyés pas Kali comme paquets Tcp mal formé Malformed paket TCP

3.2 CDP FLOODING ATTACK :

L'inondation CDP est une attaque DoS utilisant la vulnérabilité du protocole CDP, qui est activé par défaut sur la plupart des appareils Cisco. Une fois l'attaque lancée, le processeur de l'appareil cible est saturé à 100 %, ce qui l'empêche de fonctionner normalement. [21]

Le protocole CDP est propriétaire Cisco permet de détecter automatiquement d'autres périphériques CDP

Les diffusions CDP ne sont ni chiffrées, ni authentifiées. Par conséquent, un acteur de menace peut compromettre l'infrastructure de réseau en envoyant de fausses trames CDP contenant de fausses informations aux périphériques Cisco connectés.

- Pour désactiver CDP globalement sur un périphérique, utilisez la commande du mode de configuration globale **no cdp run** . Pour activer CDP globalement, utilisez la commande de configuration globale **cdp run** .
- Pour désactiver CDP sur un port, utilisez la commande de configuration d'interface **no cdp enable** .
- Pour activer CDP sur un port, utilisez la commande de configuration d'interface **cdp enable** .

Remarque: Le protocole LLDP (Link Layer Discovery Protocol) est également vulnérable aux attaques de reconnaissance. configurez **no lldp run** pour désactiver LLDP globalement. Pour désactiver LLDP sur l'interface, configurez **no lldp transmit** et **no lldp receive**.

```
Username: stage
Password:
access#show cdp ?
  entry      Information for specific neighbor entry
  interface  CDP interface status and configuration
  neighbors  CDP neighbor entries
  traffic    CDP statistics
  |         Output modifiers
  <cr>

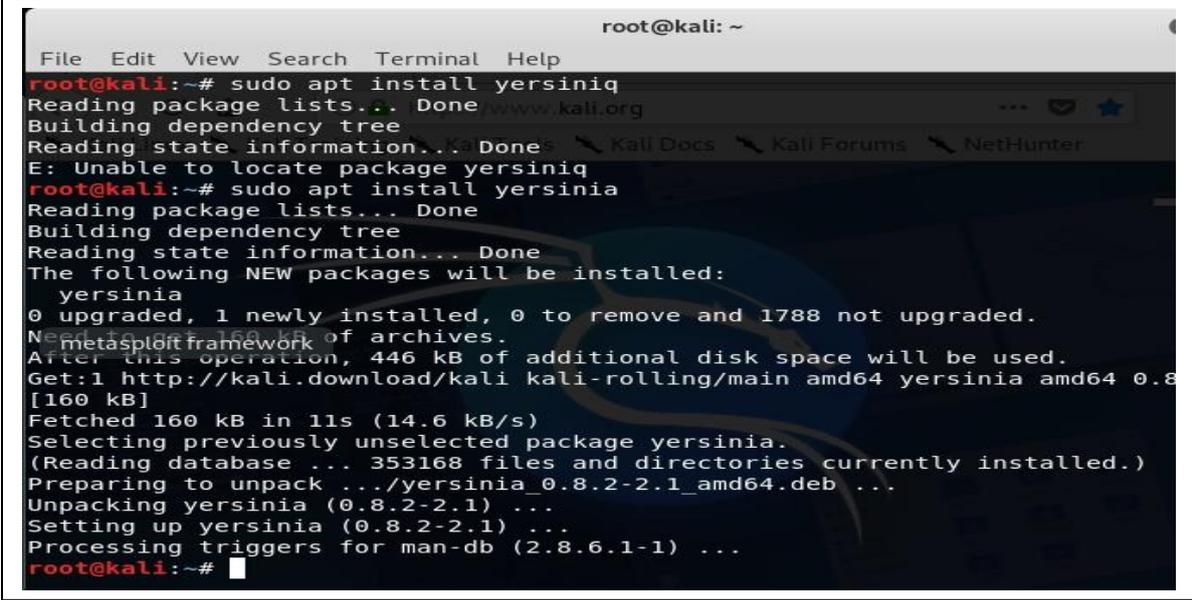
access#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone

Device ID           Local Intrfce   Holdtme    Capability   Platform   Port ID
core1.test.com      Gig 0/23       164        R S I       WS-C3560X-Gig 0/1
core2.test2.com     Gig 0/24       152        R S I       WS-C3560X-Gig 0/1
```

Figure 2.36 : cdp avant l'attaque

- Lancement du CDP flooding

Nous utiliserons l'outil Yersinia situé sur la distribution Linux KALI ainsi que les autres tutoriels sur les tests d'intrusion et le piratage éthique.



```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# sudo apt install yersiniq
Reading package lists... Done www.kali.org
Building dependency tree
Reading state information... Done
E: Unable to locate package yersiniq
root@kali:~# sudo apt install yersinia
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  yersinia
0 upgraded, 1 newly installed, 0 to remove and 1788 not upgraded.
Need to get 160 kB of archives.
After this operation, 446 kB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 yersinia amd64 0.8.2-2.1 [160 kB]
Fetched 160 kB in 11s (14.6 kB/s)
Selecting previously unselected package yersinia.
(Reading database ... 353168 files and directories currently installed.)
Preparing to unpack ../yersinia_0.8.2-2.1_amd64.deb ...
Unpacking yersinia (0.8.2-2.1) ...
Setting up yersinia (0.8.2-2.1) ...
Processing triggers for man-db (2.8.6.1-1) ...
root@kali:~#
```

Figure 2.37 : lancement d'attaque cdp

4. durant l'attaque :

Nous pouvons geler le système d'exploitation exécuté sur le commutateur, ce qui empêche efficacement quiconque de gérer le commutateur à distance. Nous pouvons également verrouiller le processeur, ce qui fait que le commutateur commence à réduire le trafic réseau. Mais ce n'est pas la seule chose qu'une inondation CDP fait.

Cela signifie qu'un attaquant pourrait lancer un analyseur de protocole tel que Wireshark et commencer à renifler et à collecter des données sensibles sur votre réseau. Pourquoi? Parce que normalement, un commutateur ne transfère que des trames directement au MAC de destination, de sorte qu'un utilisateur capturant des trames sur le port de commutation 2 ne verra que des trames sur le port de commutation 2. Mais lorsque la table d'adresses MAC se remplit, le commutateur commence à transférer des trames sur tous les ports, ce qui le rend vraiment facile pour un intrus pour voir des choses qu'il ne devrait pas voir. [17]

Lorsque la table d'adresses MAC déborde, le commutateur commence à supprimer des trames.

Résultat d'attaque :

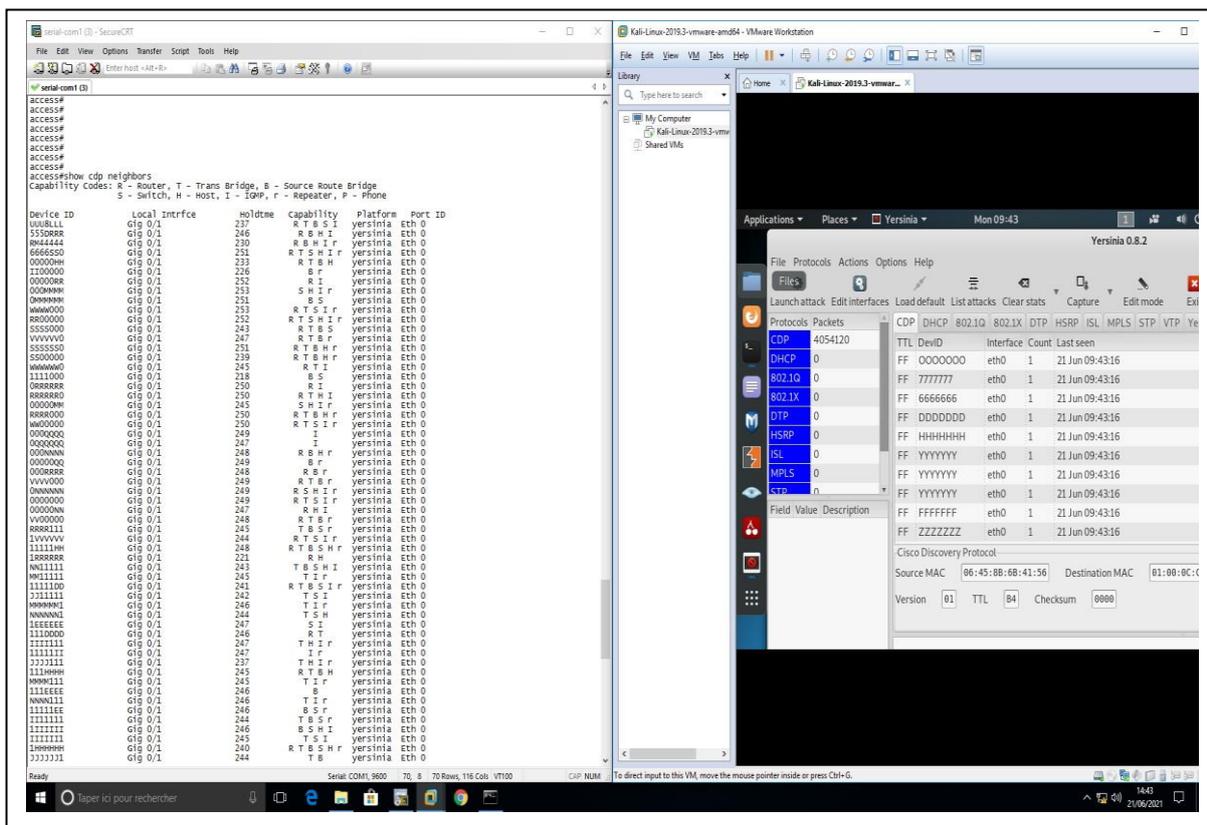


Figure 2.38 : résultat d'attaque cdp

Nous pouvons ainsi saturer le switch, ce qui empêche efficacement quiconque de gérer le commutateur à distance. Nous pouvons également verrouiller le processeur, ce qui fait que le commutateur commence à réduire le trafic réseau est le Dos est ainsi réalisé.

3.3VLAN HOOPING :

VLAN :

. Un réseau local virtuel (VLAN) est utilisé pour partager le réseau physique tout en créant des segmentations virtuelles pour diviser des groupes spécifiques. Par exemple, un hôte sur le VLAN 1 est séparé de tout hôte sur le VLAN 2. Tous les paquets envoyés entre les VLAN doivent passer par un routeur ou d'autres périphériques de couche 3. La sécurité est l'une des nombreuses raisons pour lesquelles les administrateurs réseau configurent les VLAN. Cependant, avec un exploit connu sous le nom de « VLAN Hopping », un attaquant est capable de contourner ces implémentations de sécurité.

Saut de VLAN :

Ce type d'exploit permet à un attaquant de contourner toutes les restrictions de couche 2 conçues pour diviser les hôtes. Avec une configuration appropriée du port de commutation, un attaquant devrait passer par un routeur et tout autre périphérique de couche 3 pour accéder à sa cible. Cependant, de nombreux réseaux ont une mauvaise implémentation du VLAN ou des erreurs de configuration qui permettront aux attaquants d'effectuer cet exploit. Je vais passer en revue les deux principales méthodes de saut de VLAN, connues sous le nom de « spoofing commuté » et de « double balisage ». Je discuterai ensuite des techniques d'atténuation[15]

Réseau commuté

Il est crucial que nous comprenions le fonctionnement des commutateurs si nous souhaitons trouver et exploiter leurs vulnérabilités. Nous n'exploitons pas nécessairement l'appareil lui-même, mais plutôt les protocoles et les configurations qui expliquent leur fonctionnement.

Sur un commutateur, un port est soit configuré en tant que port d'accès, soit en tant que port de jonction. Un port d'accès est généralement utilisé lors de la connexion d'un hôte à un commutateur. Avec la mise en œuvre des VLAN, chaque port d'accès est affecté à un seul VLAN. Un port de jonction est utilisé lors de la connexion de deux commutateurs ou d'un commutateur et d'un routeur ensemble. Les ports de jonction permettent le trafic de plusieurs VLAN. Un port de jonction peut être configuré manuellement ou créé dynamiquement à l'aide du protocole DTP (Dynamic Trunking Protocol).

DTP est un protocole propriétaire de Cisco où une utilisation est d'établir dynamiquement une liaison de jonction entre deux commutateurs.

Attaque de VLAN par usurpation commutée

Un attaquant agit comme un commutateur afin de tromper un commutateur légitime en créant un lien de jonction entre eux. Comme mentionné précédemment, les paquets de n'importe quel VLAN sont autorisés à passer par une liaison de jonction. Une fois la liaison de jonction établie, l'attaquant a alors accès au trafic de n'importe quel VLAN. Cet exploit n'est réussi que lorsque le commutateur légitime est configuré pour négocier une jonction. Cela se produit lorsqu'une interface est configurée avec le mode "dynamique souhaitable", "dynamique automatique" ou "tronc". Si l'un de ces modes est configuré sur le commutateur cible, l'attaquant peut alors générer un message DTP à partir de son ordinateur et un lien de jonction peut être formé.

Double marquage

Le double marquage se produit lorsqu'un attaquant ajoute et modifie des balises sur une trame Ethernet pour permettre l'envoi de paquets via n'importe quel VLAN. Cette attaque tire parti du nombre de commutateurs qui traitent les balises. La plupart des commutateurs suppriment uniquement la balise externe et transmettent la trame à tous les ports VLAN natifs. Cela dit, cet exploit n'est réussi que si l'attaquant appartient au VLAN natif de la liaison de jonction. Autre point important, cette attaque est strictement à sens unique car il est impossible d'encapsuler le paquet de retour.

Exploit de saut de VLAN

Les attaques par saut de VLAN peuvent être lancées par :

- I. L'usurpation du message DTP de l'hôte attaquant fait passer le commutateur en mode relais. À partir de là, l'attaquant peut envoyer du trafic étiqueté avec le VLAN cible et le commutateur transmet le paquet à la destination.

nous pouvons exécuter l'outil (yersinia) et choisir la DTP, puis lancer une attaque:

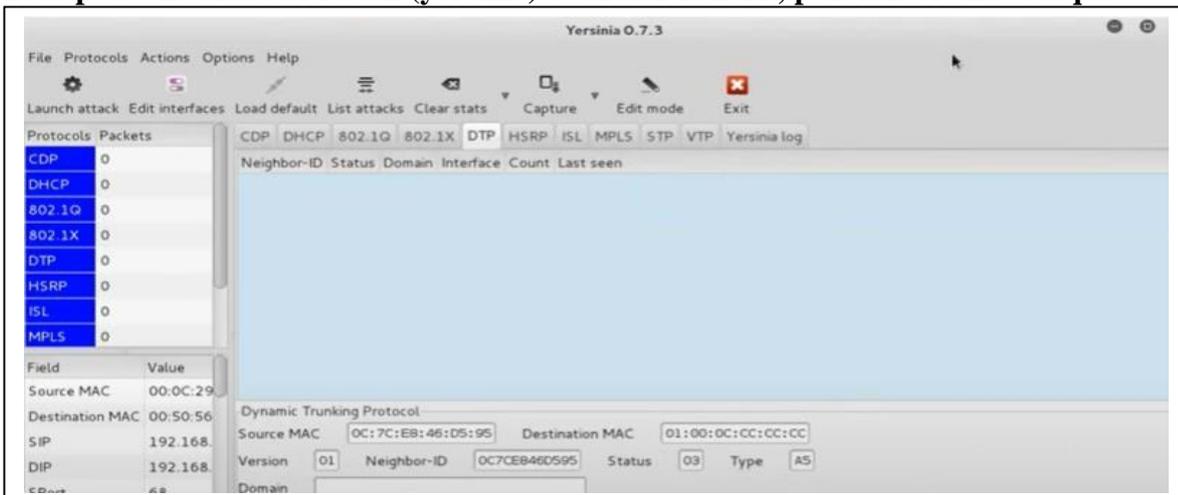


Figure 3.9 : attaque vlanhopping

Choisissez ensuite "enabling trunking" et cliquez sur OK:

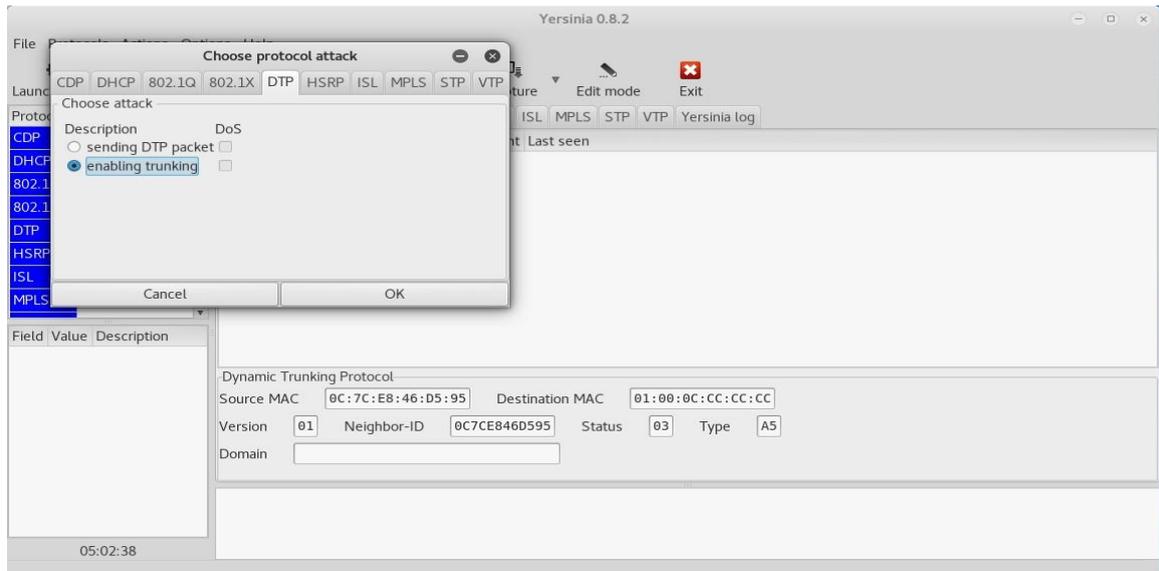


Figure 2.39 : activer trunking

Nous pouvons voir que l'interface (E0 / 0) est définie sur le tronc ce qui signifie que nous pouvons sauter d'autres

VLAN	Name	Status	Ports
1	default	active	Et0/1, Et0/2, Et0/3, Et1/0, Et1/1, Et1/2, Et1/3, Et2/0, Et2/1, Et2/2, Et2/3, Et3/0, Et3/1, Et3/2, Et3/3
10	VLAN0010	active	Et0/0
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

Figure 2.40 : résultat d'attaque vlan hopping

3.4 Attaque STP Spanning Tree Protocol :

STP est l'un des principaux protocoles que l'on retrouve au niveau 2. Il Permet d'éviter les boucles dans un réseau, mais aussi de profiter des topologies Redondantes, sans risque de créer des boucles. Sans STP, les réseaux locaux de Couche 2 cesseraient tout simplement de fonctionner, car les boucles créées au Sein du réseau inonderaient les commutateurs de Traffic. Le fonctionnement et la Configuration optimisés de STP garantissent que le LAN reste stable et que le Traffic emprunte le chemin le plus optimisé à travers le réseau. Si un attaquant avait un accès à l'un des ports de commutation qui peuvent devenir des ports truck, il peut introduire un commutateur non autorisé dans le réseau. [14]

Nous savons que les commutateurs Cisco ont tous les ports en mode dynamique auto par défaut, cela signifie que si les ports sont toujours dans ce mode, l'attaquant

Peut connecter le commutateur escroc dans le réseau, et il va négocier La liaison truck avec le commutateur de l'entreprise. À ce moment, il a la possibilité de former une autre connexion avec les autres commutateurs de cette société, puis il va être capable de manipuler la priorité de l'arborescence des commutateurs non autorisés. S'il configure son commutateur escroc avec une priorité inférieure à tout autre commutateur de l'entreprise, il deviendra le pont racine et tout le trafic traversera ce commutateur. Cela lui donne la possibilité de renifler tout le trafic dans l'entreprise. [15]

Le principe de fonctionnement de cette attaque est illustré dans la figure

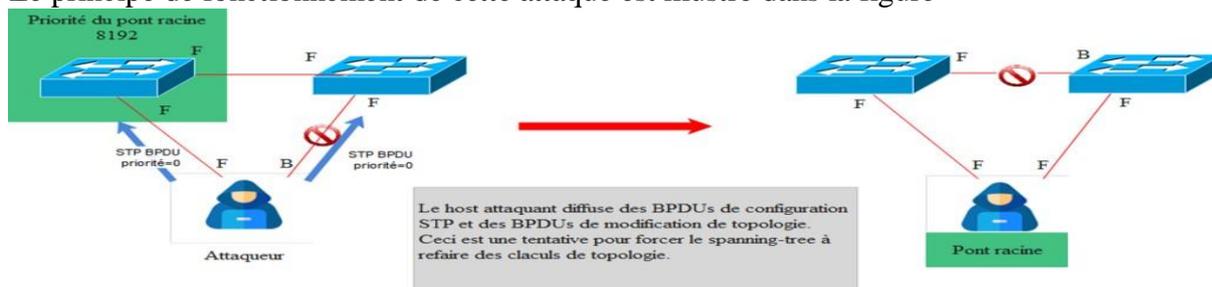


Figure 2.41 : attaque stp

Avant l'attaque :

On vérifie le protocole STP pour le vlan 1

```
access#show spanning-tree vlan 1
```

```
VLAN0001
Spanning tree enabled protocol ieee
Root ID    Priority    24577
           Address    e4d3.f1fb.8180
           Cost        4
           Port        23 (GigabitEthernet0/23)
           Hello Time  2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID  Priority    32769 (priority 32768 sys-id-ext 1)
           Address    0018.bac8.4700
           Hello Time  2 sec Max Age 20 sec Forward Delay 15 sec
           Aging Time 300
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Gi0/23	Root	FWD	4	128.23	P2p
Gi0/24	Altn	BLK	4	128.24	P2p

Figure 2.42 : avant l'attaque stp

L'ID de Root a l'adresse mac est e4d3.f1fb.8180L'attaque est réalisée à l'aide de YERSINIA figure ci-dessous

Whireshark analyse :

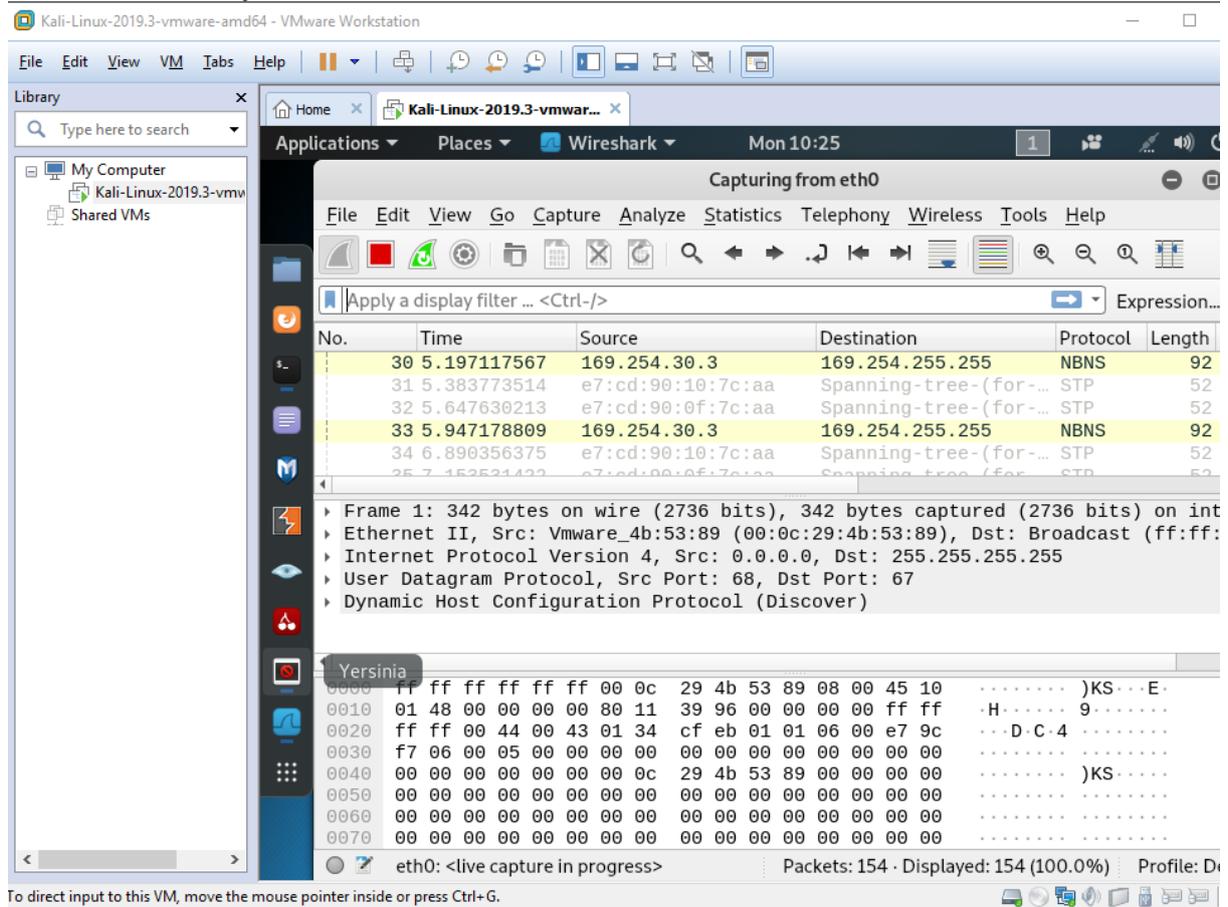


Figure 2.45: analyse avec whireshark

3.5– Attaque saturation processeur via BPDU

Cette attaque se base sur l’envoi massive de datagramme multicast (consommateur de processeur distant) à destination du Switch. L’intérêt est de changer le mode de fonctionnement du Switch afin qu’il travail en HUB. Cela est possible car certain Switch, à l’approche de la saturation processeur, préfère basculer en mode HUB afin de préserver une priorité sur l’exploitation.

Cela dépend du constructeur, de l’équipement et de la version, mais les conséquences peuvent être multiple comme par exemple :

- Buffer over flow du Switch (cette conséquence n’est plus réaliste de nos jours)
- Impossibilité au Switch de commuter la plus part des trames

Bpdu number :

```

access#show spanning-tree interface g0/3 detail
Port 3 (GigabitEthernet0/3) of VLAN0001 is forwarding
Port path cost 4, Port priority 128, Port Identifier 128.3.
Designated root has priority 24577, address e4d3.flfb.8180
Designated bridge has priority 32769, address 0018.bac8.4700
Designated port id is 128.3, designated path cost 4
Timers: message age 0, forward delay 0, hold 0
Number of transitions to forwarding state: 1
Link type is point-to-point by default
Bpdu filter is enabled internally
BPDU: sent 1746, received 0

Port 3 (GigabitEthernet0/3) of VLAN0002 is forwarding
Port path cost 4, Port priority 128, Port Identifier 128.3.
Designated root has priority 24578, address e4d3.flfb.8180
Designated bridge has priority 32770, address 0018.bac8.4700
Designated port id is 128.3, designated path cost 4
Timers: message age 0, forward delay 0, hold 0
Number of transitions to forwarding state: 1
Link type is point-to-point by default
Bpdu filter is enabled internally
BPDU: sent 878, received 0
    
```

Figure 2.48 : bpdv nombre avant l'attaque

Durant l'attaque :

l'attaque est réalisée par YERSINIA, comme indiqué dans la figure ci-dessous

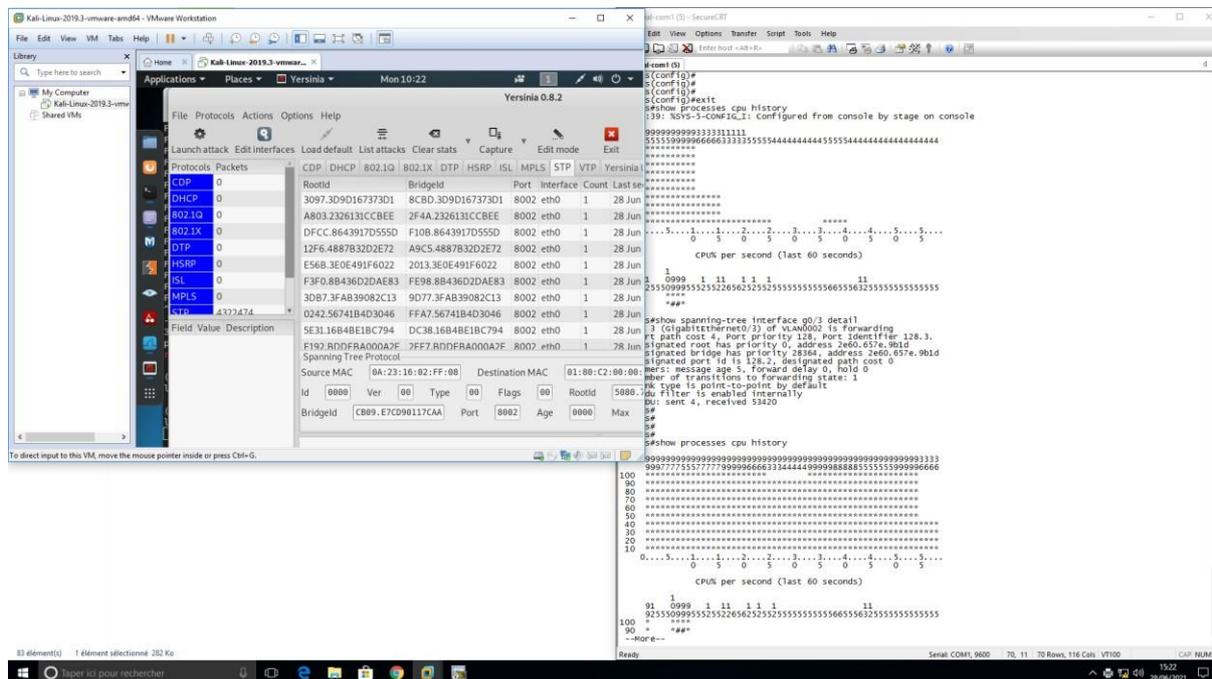


Figure 2.49 : lancement d'attaque

3.7 Attaque HSRP _ Host Standby Routing Protocol _ :

HSRP (Hot Standby Router Protocol) est un protocole propriétaire de Cisco qui assure la redondance du réseau en cas de défaillance du routeur de passerelle par défaut. C'est l'un des protocoles les plus courants, cependant, il contient une vulnérabilité qui pourrait amener un attaquant à refuser le service ou à capturer des données. Nous vous montrerons comment se produisent les attaques HSRP et comment protéger votre réseau contre les attaques.[14]

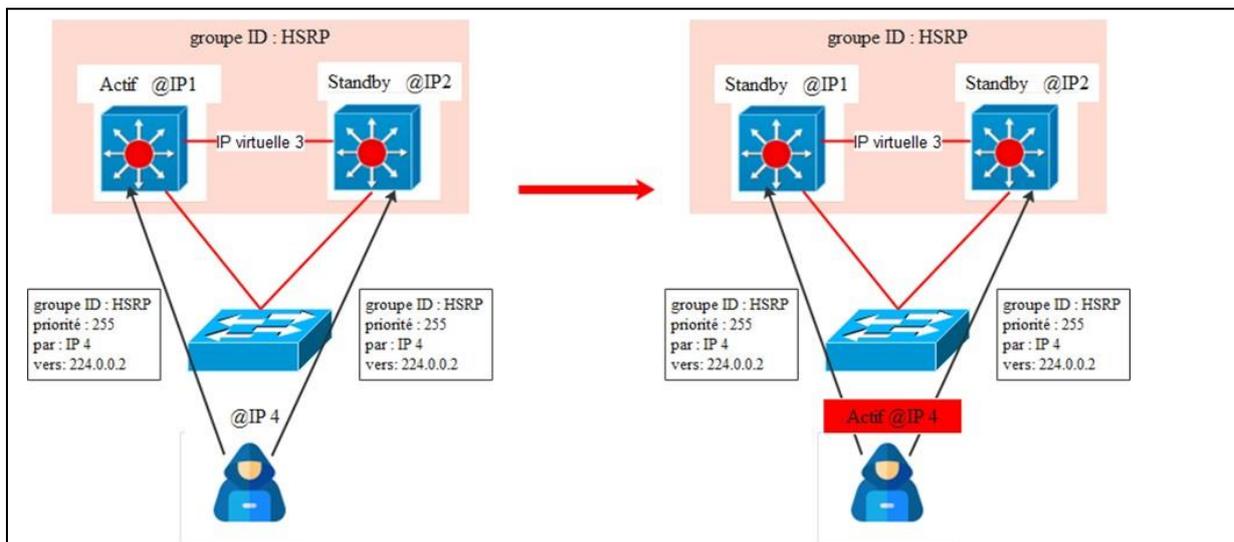


Figure 2.52 : hsrp attaque

Le but de cette attaque est de faire jouer à notre station d'attaque le rôle d'un routeur HSRP actif, ce qui va provoquer un déni de service, ou nous pouvons capturer des données sur le réseau. Nous utiliserons l'outil Yersinia situé dans la distribution Linux KALI et d'autres tutoriels de tests d'intrusion et de piratage éthique. Nous pouvons exécuter Yersinia des manières suivante

Avant l'attaque :

Core1:

```
int vlan 2
ip address 10.110.2.2 255.255.255.0
standby 2 ip 10.110.2.1
standby 2 priority 150
standby 2 preempt
```

core2:

```
int vlan2
ip address 10.110.2.3 255.255.255.0
```

core1:

```
▣ Frame 14: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface eth0, id 0
▣ Ethernet II, Src: All-HSRP-routers_01 (00:00:0c:07:ac:01), Dst: IPv4mcast_02 (01:00:5e:00:00:02)
▣ Internet Protocol Version 4, Src: 10.11010.2, Dst: 224.0.0.2
▣ User Datagram Protocol, Src Port: 1985, Dst Port: 1985
▣ Cisco Hot Standby Router Protocol
  Version: 0
  Op Code: Hello (0)
  State: Active (16)
  Hellotime: Default (3)
  Holdtime: Default (10)
  Priority: 150
  Group: 1
  Reserved: 0
  Authentication Data: Default (cisco)
  Virtual IP Address: 10.0.0.1
```

Figure 2.53: core1 avant l'attaque

Core2:

```
▣ Frame 14: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface eth0, id 0
▣ Ethernet II, Src: All-HSRP-routers_01 (00:00:0c:07:ac:01), Dst: IPv4mcast_02 (01:00:5e:00:00:02)
▣ Internet Protocol Version 4, Src: 10.11010.3, Dst: 224.0.0.2
▣ User Datagram Protocol, Src Port: 1985, Dst Port: 1985
▣ Cisco Hot Standby Router Protocol
  Version: 0
  Op Code: Hello (0)
  State: Active (16)
  Hellotime: Default (3)
  Holdtime: Default (10)
  Priority: 100
  Group: 1
  Reserved: 0
  Authentication Data: Default (cisco)
  Virtual IP Address: 10.0.0.1
```

Figure 2.54 : core2 avant l'attaque

Vulnérabilité

Si vous vous arrêtez et réfléchissez aux opérations de base de HSRP, vous serez en mesure de reconnaître sa faiblesse. Essentiellement, tout périphérique compatible HSRP peut annoncer une valeur de haute priorité et prendre le relais en tant que switch actif.

L'appareil peut être un routeur légitime ou un acteur malveillant qui souhaite émettre un déni de service (DoS) ou une attaque par intercepteur (MITM). En tant que professionnels du réseau, nous sommes chargés d'assurer la fiabilité du réseau et de protéger les équipements du réseau contre les attaques.

Exploitation

Maintenant que vous connaissez les opérations de base et la vulnérabilité de HSRP, vous pouvez appliquer ces connaissances pour exploiter sa faiblesse. Il existe deux outils logiciels open source que vous pouvez utiliser pour effectuer une attaque DoS : Scapy et Yersinia. Avec l'aide de ces outils, attaquer HSRP permet à tout le monde de le faire facilement.

Durant l'attaque :

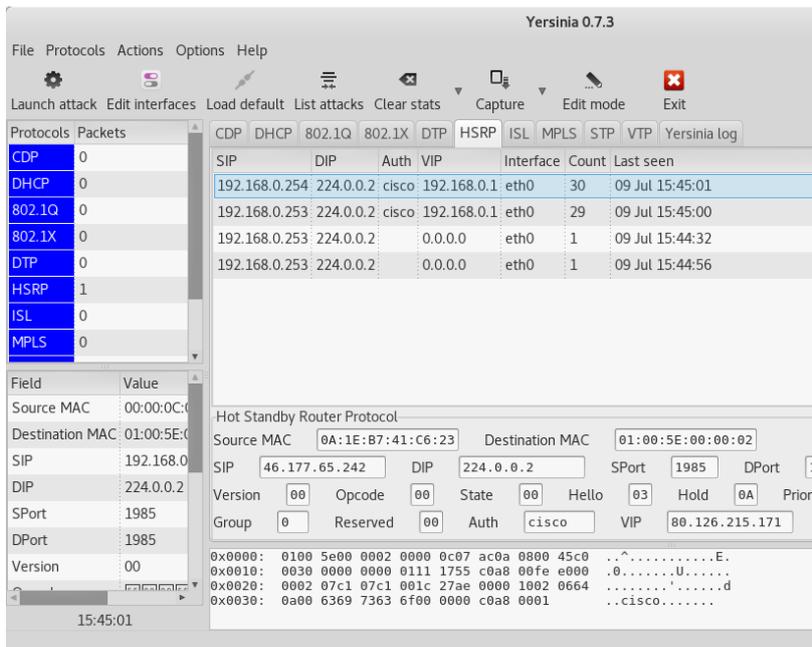


Figure 2.55 : lancement d'attaque hsrp

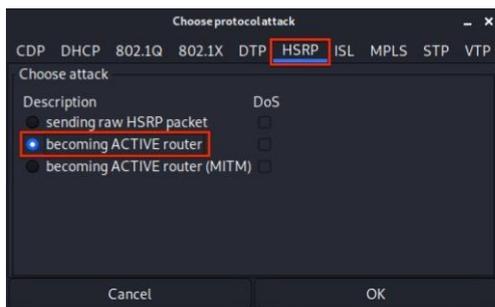


Figure 2.56:devenir acite router

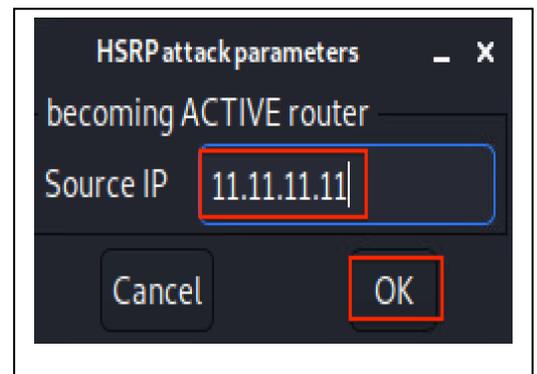
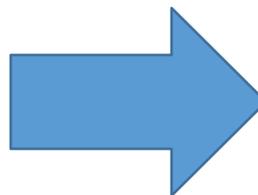


Figure 2.57 : choisir fake ip

Résultat de l'attaque :

Comme vous pouvez le voir, le message HSRP envoyé par l'outil Yersinia. Le logiciel a envoyé un message de succès au lieu d'un. Techniquement, Quoi qu'il en soit, le logiciel à lancé avec succès l'attaque et à repris le rôle du switch actif.

No.	Time	Source	Destination	Protocol	Info
5	5.304571416	10.0.0.2	224.0.0.2	HSRP	Hello (state Active)
6	6.850224884	10.0.0.3	224.0.0.2	HSRP	Hello (state Standby)
7	7.234020900	11.11.11.11	224.0.0.2	HSRP	Coup (state Speak)
8	7.242049964	10.0.0.2	224.0.0.2	HSRP	Advertise (state Passive)
9	7.244661114	10.0.0.3	224.0.0.2	HSRP	Advertise (state Passive)
10	7.249332276	10.0.0.2	224.0.0.2	HSRP	Hello (state Speak)
11	9.721062865	10.0.0.2	224.0.0.2	HSRP	Hello (state Speak)
12	10.237996221	11.11.11.11	224.0.0.2	HSRP	Hello (state Active)
13	12.204312712	10.0.0.2	224.0.0.2	HSRP	Hello (state Speak)
14	14.241404534	11.11.11.11	224.0.0.2	HSRP	Hello (state Active)
15	14.619823260	10.0.0.2	224.0.0.2	HSRP	Hello (state Speak)
16	17.320510198	10.0.0.2	224.0.0.2	HSRP	Hello (state Speak)
17	17.641252769	10.0.0.2	224.0.0.2	HSRP	Hello (state Standby)
18	18.245130878	11.11.11.11	224.0.0.2	HSRP	Hello (state Active)
19	20.347917874	10.0.0.2	224.0.0.2	HSRP	Hello (state Standby)
20	22.249228546	11.11.11.11	224.0.0.2	HSRP	Hello (state Active)
21	22.960870916	10.0.0.2	224.0.0.2	HSRP	Hello (state Standby)
22	25.488301181	10.0.0.2	224.0.0.2	HSRP	Hello (state Standby)
23	26.253323262	11.11.11.11	224.0.0.2	HSRP	Hello (state Active)
24	28.291601102	10.0.0.2	224.0.0.2	HSRP	Hello (state Standby)
25	30.257564510	11.11.11.11	224.0.0.2	HSRP	Hello (state Active)
26	31.187239137	10.0.0.2	224.0.0.2	HSRP	Hello (state Standby)
27	32.321951979	10.0.0.2	224.0.0.2	HSRP	Advertise (state Passive)

```

# Frame 7: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface eth0, id 0
# Ethernet II, Src: 50:00:00:02:00:00 (50:00:00:02:00:00), Dst: IPv4mcast_02 (01:00:5e:00:00:02)
# Internet Protocol Version 4, Src: 11.11.11.11, Dst: 224.0.0.2
# User Datagram Protocol, Src Port: 1985, Dst Port: 1985
# Cisco Hot Standby Router Protocol
  Version: 0
  Op Code: Coup (1)
  State: Speak (4)
  HelloTime: Default (3)
  HoldTime: Default (10)
  Priority: 255
  Group: 1
  Reserved: 0
  Authentication Data: Default (cisco)
  Virtual IP Address: 10.0.0.1
    
```

Figure 2.58: whireshark analyse résultat

3.8 ATTAQUE DHCP :

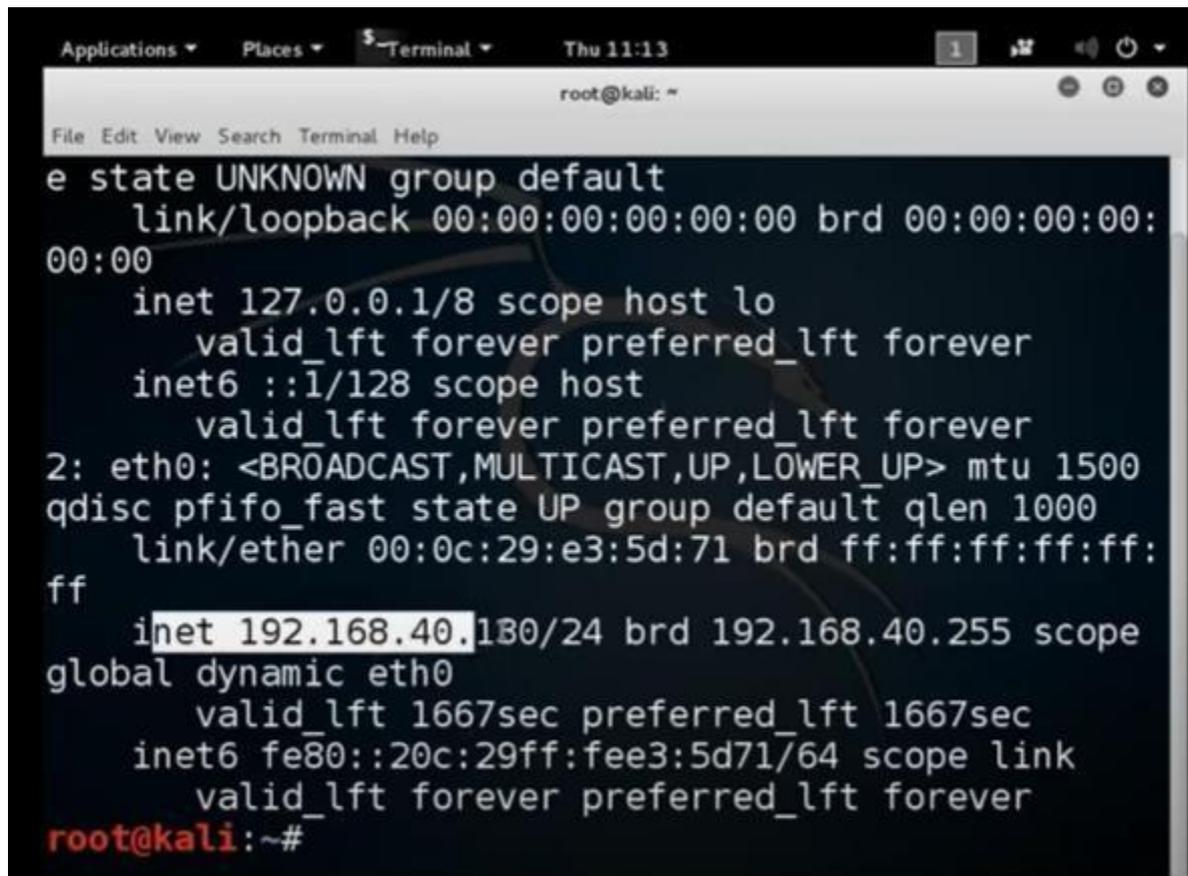
Attaque DHCP Spoofing :

Dans une attaque de famine DHCP, le client envoie un grand nombre de messages DHCP Discover avec de fausses adresses MAC, de sorte que le pool DHCP est rempli et que le serveur ne peut pas fournir de services pour les clients valides. Après avoir effectué une attaque de famine, l'attaquant peut configurer un serveur DHCP malveillant et commencer à utiliser de fausses adresses IP pour fournir des services à la machine de la victime. De cette façon, un attaquant peut effectuer une attaque de type man-in-the-middle, capturer les demandes des clients et les transmettre au serveur et recevoir les réponses du serveur et les envoyer au client.[15]

Pour atténuer ces attaques, la surveillance DHCP est utilisée. Dans la surveillance DHCP, les ports de confiance sont autorisés à envoyer des offres DHCP et des messages DHCP ACK. Pour les ports non approuvés, la demande de message DHCP doit être vérifiée. Les ports non approuvés ne sont pas autorisés à envoyer des messages tels que des offres DHCP.

La table DHCP Snooping est utilisée pour identifier les messages de port non approuvés ou filtrés. Toutes les demandes des ports non approuvés seront interceptées par le commutateur et toutes les réponses des ports non approuvés seront rejetées.

Avant connecter avec l'interface :



```
Applications ▾ Places ▾ $ Terminal ▾ Thu 11:13 1 [M] [V] [P]
root@kali: ~
File Edit View Search Terminal Help
e state UNKNOWN group default
  link/loopback 00:00:00:00:00:00 brd 00:00:00:00:
00:00
  inet 127.0.0.1/8 scope host lo
    valid_lft forever preferred_lft forever
  inet6 ::1/128 scope host
    valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500
qdisc pfifo_fast state UP group default qlen 1000
  link/ether 00:0c:29:e3:5d:71 brd ff:ff:ff:ff:ff:
ff
  inet 192.168.40.130/24 brd 192.168.40.255 scope
global dynamic eth0
    valid_lft 1667sec preferred_lft 1667sec
  inet6 fe80::20c:29ff:fee3:5d71/64 scope link
    valid_lft forever preferred_lft forever
root@kali:~#
```

Figure 2.59 : address de hacker avant l'attaque

1.Vérifiez si le service fonctionne bien en vérifiant l'adresse IP du système connecté au switch.

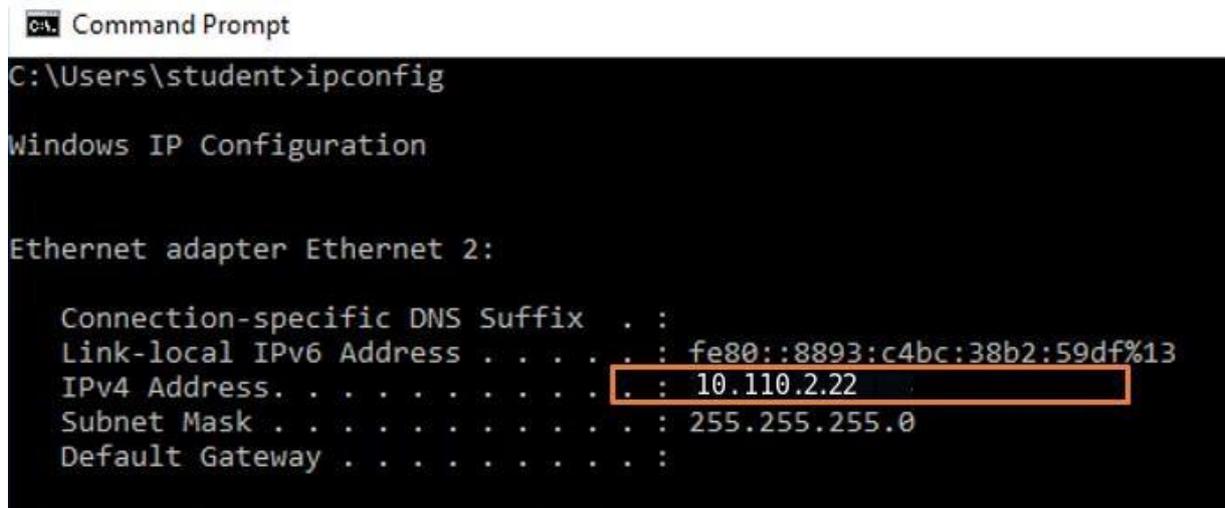


Figure 2.60 : address ip de système

Durant l’attaque :

Dans une attaque de famine DHCP, l'attaquant enverra un message de découverte DHCP avec une adresse MAC falsifiée et obtiendra toutes les adresses IP disponibles. Après avoir effectué une attaque de famine, l'attaquant va maintenant commencer à louer de fausses adresses IP aux victimes comme un serveur DHCP.

Avec Yersinia -G :

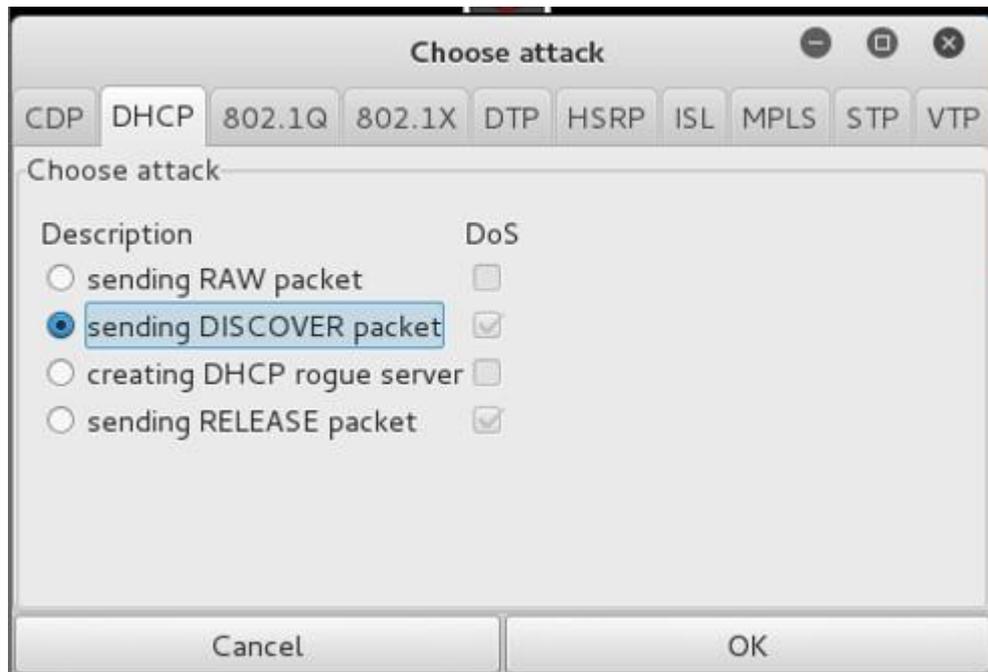


Figure 2.61 : lancer l’attaque

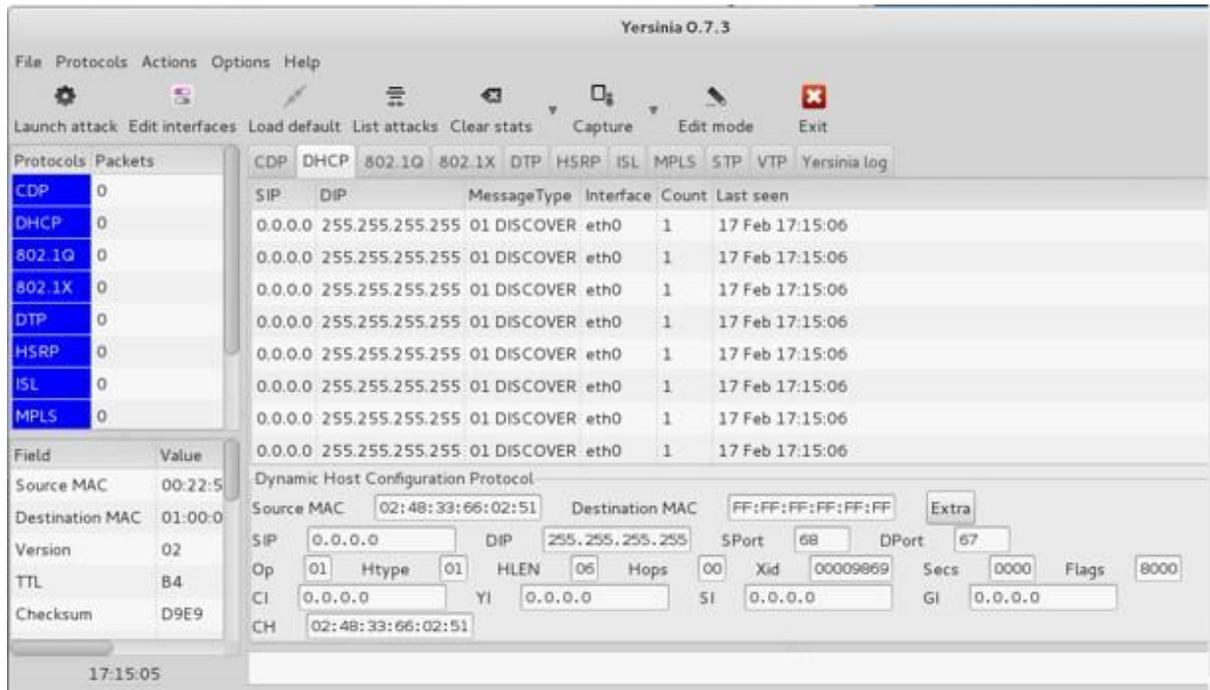


Figure 2.62 : durant l'attaque

Wireshark :

Au niveau de Wireshark on capte les DHCP Discover envoyer au serveur DHCP

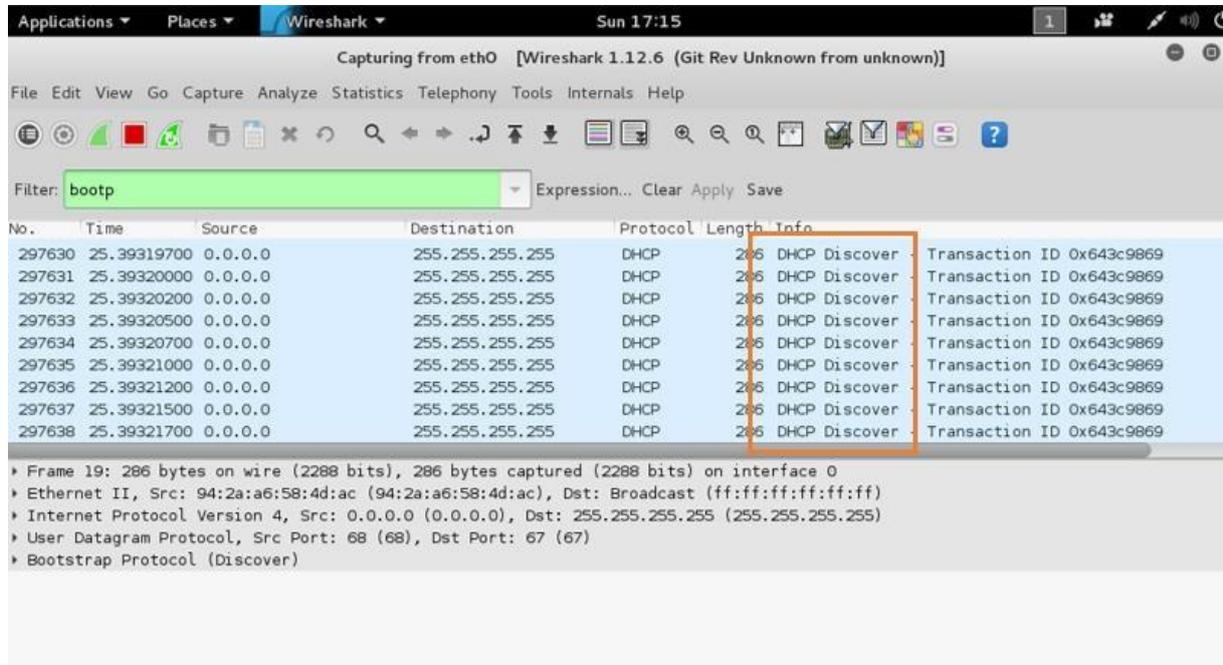


Figure 2.63 : wireshark analyse

Les résultats de l'attaque :

Le nombre de bases de données DHCP Snooping n'est pas verrouillé et les requêtes sont nombreuses :

```
Router#show ip dhcp binding
% The DHCP database could not be locked. Please retry the command later.
Router#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/
                   Hardware address/
                   User name
10.110.2.3          01ec.b1d7.40d7.e8      Infinite      Automatic
10.110.2.4          01ec.b1d7.3a7d.82      Infinite      Automatic
10.110.2.5          000c.29ed.2076         Infinite      Automatic
10.110.2.6          942a.a658.4dac         Sep 21 2002 06:29 PM Automatic
10.110.2.7          661f.be65.04a1         Sep 21 2002 06:29 PM Automatic
10.110.2.8          1ad2.331a.3afd         Sep 21 2002 06:29 PM Automatic
10.110.2.9          5649.7d61.3ae5         Sep 21 2002 06:29 PM Automatic
10.110.2.10         1c4f.d024.9087         Sep 21 2002 06:29 PM Automatic
10.110.2.11         b819.c57d.9d9c         Sep 21 2002 06:29 PM Automatic
10.110.2.12         7610.7538.5a3b         Sep 21 2002 06:29 PM Automatic
10.110.2.13         1ad9.a162.3a35         Sep 21 2002 06:29 PM Automatic
10.110.2.14         b0b4.e403.d1bb         Sep 21 2002 06:29 PM Automatic
10.110.2.15         ea76.752a.51b0         Sep 21 2002 06:29 PM Automatic
10.110.2.16         eac6.9c1a.9480         Sep 21 2002 06:29 PM Automatic
10.110.2.17         92de.a912.26a8         Sep 21 2002 06:29 PM Automatic
10.110.2.18         2455.ec09.d04f         Sep 21 2002 06:29 PM Automatic
10.110.2.19         5495.4c4c.4515         Sep 21 2002 06:29 PM Automatic
10.110.2.20         1876.7074.8caa         Sep 21 2002 06:30 PM Automatic
10.110.2.21         5c88.6a57.3409         Sep 21 2002 06:30 PM Automatic
10.110.2.22         bec2.581f.2601         Sep 21 2002 06:30 PM Automatic
10.110.2.23         225d.7043.e087         Sep 21 2002 06:30 PM Automatic
10.110.2.24         68ce.a632.568c         Sep 21 2002 06:30 PM Automatic
10.110.2.25         0286.693b.95e2         Sep 21 2002 06:30 PM Automatic
```

Figure 2.64: résultat d'attaque dhcp

Le switch peut ainsi distribuer toutes les adresses de pool et se saturer si les paquets DHCP DISCOVER continuent à affluer .

3.9 Attaque distant aux équipements :**Telnet définition :**

Telnet, développé en 1969, est un protocole qui fournit une interface de ligne de commande pour la communication avec un périphérique ou un serveur distant, parfois utilisé pour la gestion à distance mais aussi pour la configuration initiale du périphérique comme le matériel réseau. Telnet signifie Teletype Network, mais il peut aussi être utilisé comme verbe ; « to telnet » consiste à établir une connexion en utilisant le protocole Telnet.

Attaque Telnet :

Avant de pouvoir attaqué, vous devez télécharger un utilitaire pour renifler les paquets sur votre réseau. on s'appuiera sur un utilitaire gratuit nommé Wireshark car il fait le travail admirablement et est pris en charge sur un certain nombre de plates-formes. Une partie de la configuration de Wireshark installera également WinPcap, [19]

Parce qu'il a été développé avant l'adaptation grand public d'Internet, Telnet n'utilise à lui seul aucune forme de cryptage, ce qui le rend obsolète en termes de sécurité moderne. Il a été largement chevauché par le protocole Secure Shell (SSH) (qui a ses propres considérations de sécurité autour de l'accès à distance), au moins sur l'Internet public, mais pour les cas où Telnet est toujours utilisé, il existe quelques méthodes pour sécuriser vos communications .

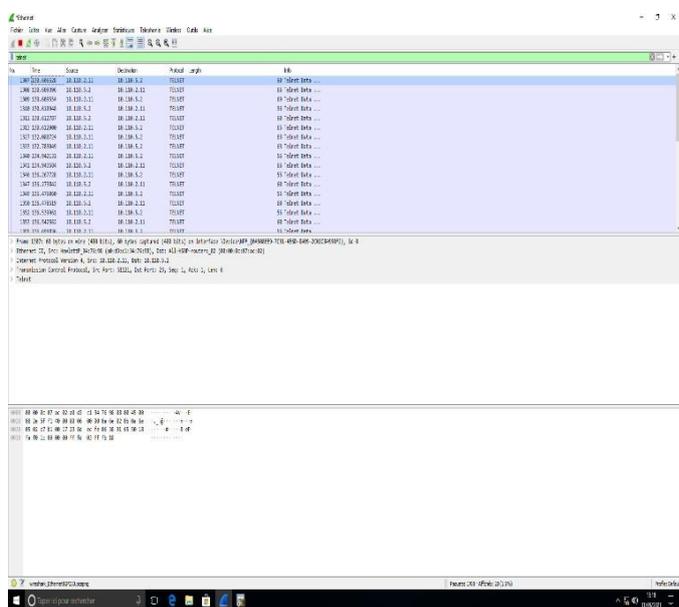


Figure 2.65 : avant l'attaque telnet

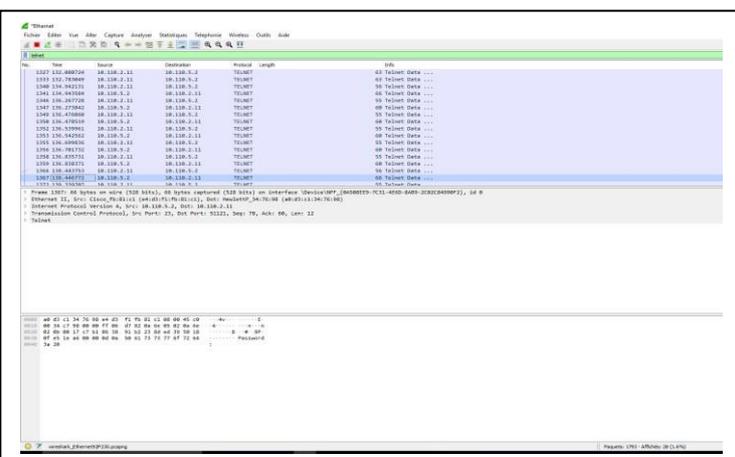
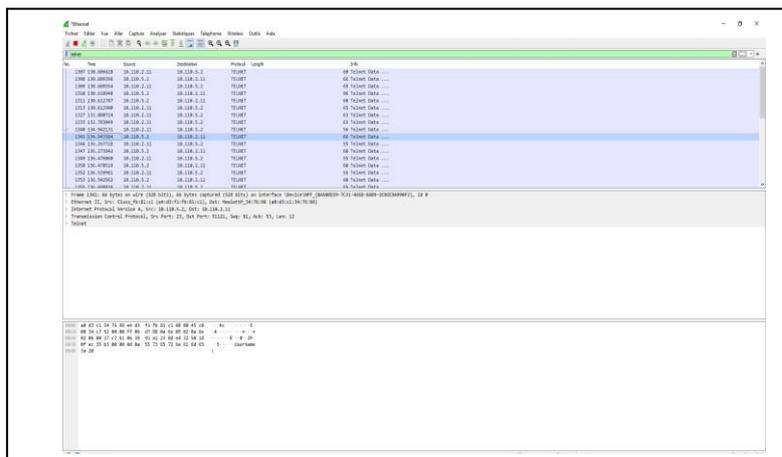


Figure 2.66 : résultat d'attaque telnet

Après l'attaque

Afin de l'attaque le hacker peut avoir le nom d'utilisateur et mot de passe et peut suivre la transformations des donnée , et tous les activités d'utilisateur.

3.10Attaque ARP POISNING :

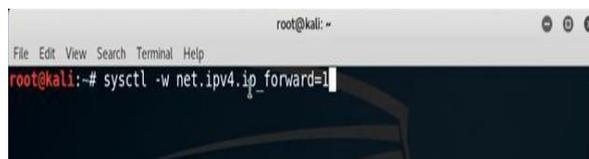
Afin d'éviter que cette mystification ne soit découverte, le trafic intercepté est transmis au système initialement(ARP spoofing : attaques du réseau interne - IONOS, n.d.) ciblé. Puis le pirate est devenu l'homme du milieu. Si le paquet de données intercepté n'est pas transmis, mais rejeté, cela s'appelle une attaque par déni de service. L'usurpation d'identité ARP s'applique aux environnements LAN et WLAN. Même l'utilisation d'un accès WiFi protégé (WPA) pour crypter les réseaux sans fil n'offre pas une protection adéquate. Pour communiquer dans le réseau IPv4 local, tous les appareils connectés doivent résoudre(ARP spoofing : attaques du réseau interne - IONOS, n.d.) l'adresse MAC, et cela ne peut être fait que via ARP. [15]

Afin d'éviter que cette mystification ne soit découverte, le trafic intercepté est transmis au système initialement ciblé. Puis le pirate est devenu l'homme du milieu. Si le paquet de données intercepté n'est pas transmis, mais rejeté, cela s'appelle une attaque par déni de service. L'usurpation d'identité ARP s'applique aux environnements LAN et WLAN. Même l'utilisation d'un accès WiFi protégé (WPA) pour crypter les réseaux sans fil n'offre pas une protection adéquate. Pour communiquer dans le réseau IPv4 local, tous les appareils connectés doivent résoudre l'adresse MAC, et cela ne peut être fait que via ARP.

Scénario d'attaque :

1-Changer la valeur de ip forward = 1

Pour que l'access de flow entre le switch et le client



2- choisir la victime :

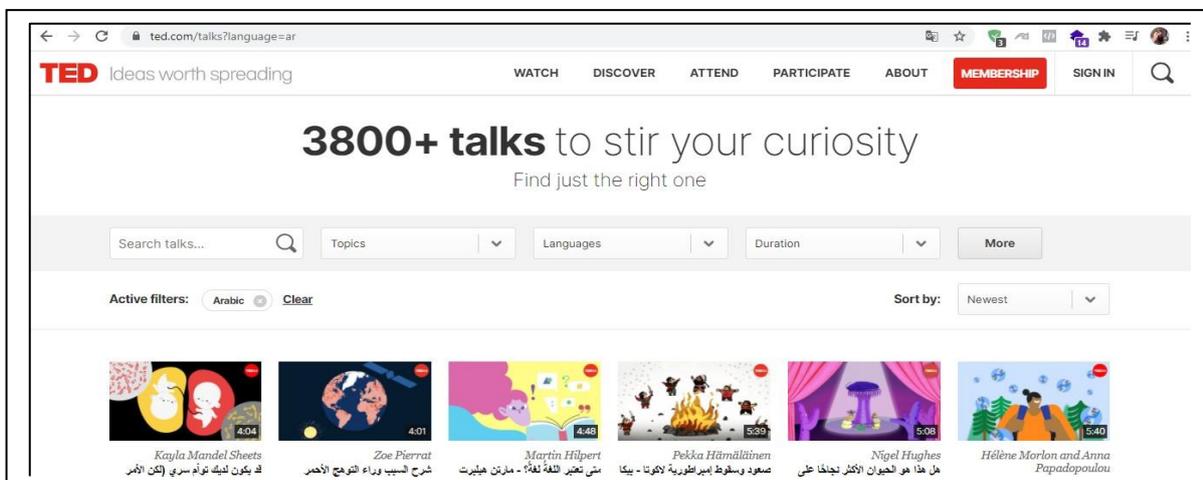


Figure 2.67 : préparation d'attaque

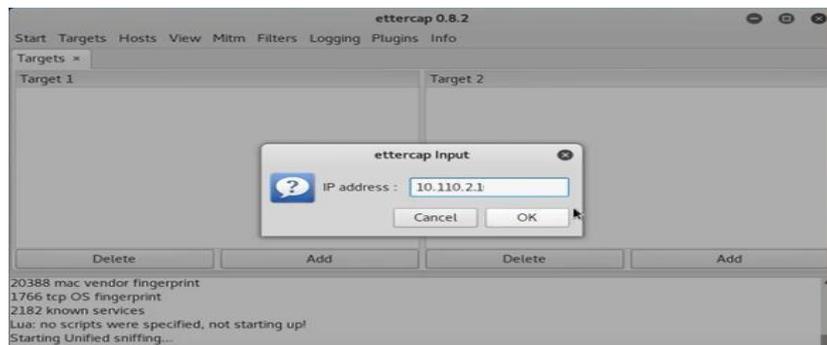
3- avec ettercap suivre les étapes suivantes :

Lorsque vous être connecter physiquement avec le réseaux utiliser bridge sniffing



4- choisir votre victime :

4.1-choisir default-gateway comme premier victime :



4.2-choisir l'address de victime comme 2 éme :

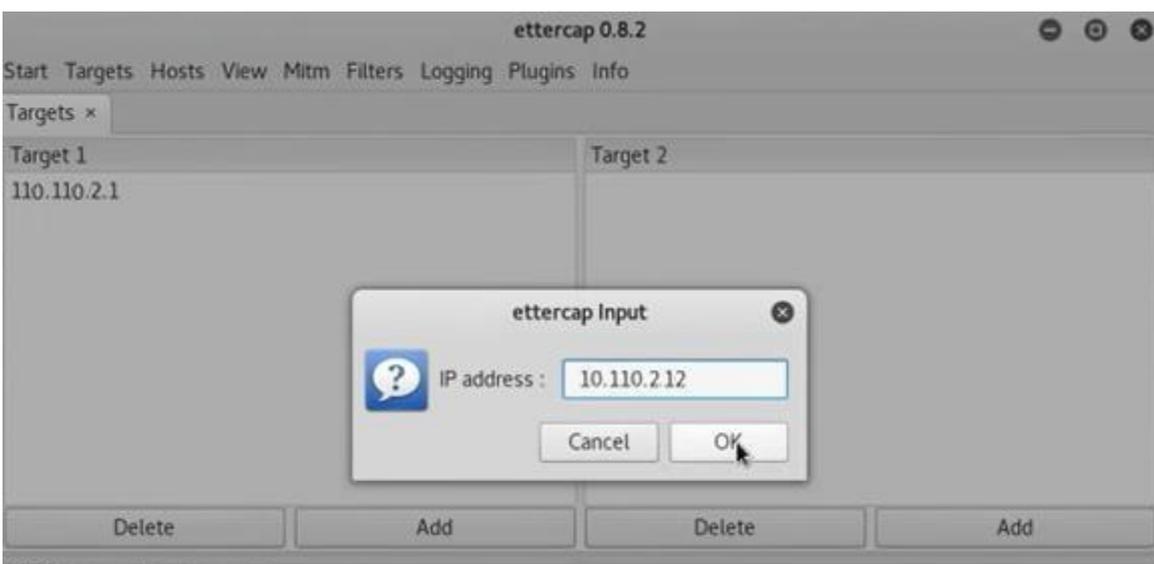


Figure 2.68 : étape pour établir l'attaque arp

On va utiliser tcpdump pour sniffer les informations :

```
root@kali:~# tcpdump -i eth0 -n port 80 and host 10.110.2.12
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
```

Résultat de l'attaque on le Traffic de victime :

```
7, ack 425, win 172, length 706: HTTP: HTTP/1.1 200 OK
16:53:22.394696 IP 216.58.223.110.80 > 192.168.1.102.49258: Flags [P.], seq 1:70
7, ack 425, win 172, length 706: HTTP: HTTP/1.1 200 OK
16:53:22.394937 IP 192.168.1.102.49257 > 216.58.223.110.80: Flags [.], ack 707,
win 255, options [nop,nop,sack 1 {1:707}], length 0
16:53:22.395084 IP 192.168.1.102.49258 > 216.58.223.110.80: Flags [.], ack 707,
win 255, options [nop,nop,sack 1 {1:707}], length 0
16:53:22.401389 IP 192.168.1.102.49248 > 93.184.220.29.80: Flags [.], ack 1577,
win 260, length 0
16:53:22.403194 IP 192.168.1.102.49257 > 216.58.223.110.80: Flags [.], ack 707,
win 255, options [nop,nop,sack 1 {1:707}], length 0
16:53:22.403506 IP 192.168.1.102.49258 > 216.58.223.110.80: Flags [.], ack 707,
win 255, options [nop,nop,sack 1 {1:707}], length 0
16:53:22.405565 IP 192.168.1.102.49248 > 93.184.220.29.80: Flags [.], ack 1577,
win 260, length 0
16:53:22.467008 IP 93.184.220.29.80 > 192.168.1.102.49248: Flags [P.], seq 789:1
577, ack 857, win 290, length 788: HTTP: HTTP/1.1 200 OK
16:53:22.474753 IP 93.184.220.29.80 > 192.168.1.102.49248: Flags [P.], seq 789:1
577, ack 857, win 290, length 788: HTTP: HTTP/1.1 200 OK
16:53:22.475060 IP 192.168.1.102.49248 > 93.184.220.29.80: Flags [.], ack 1577,
win 260, options [nop,nop,sack 1 {789:1577}], length 0
16:53:22.482611 IP 192.168.1.102.49248 > 93.184.220.29.80: Flags [.], ack 1577,
win 260, options [nop,nop,sack 1 {789:1577}], length 0
```

Figure 2.69 : résultat d'attaque arp

4.3-on va exécuter l'attaque de Mitm)man in the middle) :



Conclusion :

Dans cette partie, nous avons appliqué des attaques sur des commutateur réelle et identifié ces attaques avec une définition détaillée de chacune et leurs résultats sur commutateur et nous sommes assurés qu'il existe plusieurs façons de pirater les appareils et arrivé à des informations importantes de l'entreprise et cette complaisance peut entraîner de graves conséquences, nous devons donc les protéger dans la partie suivante Pour obtenir une stratégie de défense.

Chapitre II Partie III :
Solutions de sécurité de niveau II

Introduction :

Afin de protéger tout réseau, une certaine terminologie doit être suivie pour promouvoir et accélérer le processus de sécurité. Dans cette partie, nous allons présenter en détail une stratégie basée sur plusieurs mécanismes qui aident à améliorer et renforcer la sécurité du réseau.

2.1 Atténuation des attaques de table d'adresses MAC :

Le moyen le plus simple et le plus efficace d'empêcher les attaques par saturation des tables d'adresses MAC est d'activer la sécurité des ports.

La sécurité des ports limite le nombre d'adresses MAC autorisées sur un port.

Il permet à l'administrateur Configurer manuellement l'adresse MAC Port ou autoriser le commutateur Apprendre un nombre dynamiquement Adresse MAC limitée. [14]

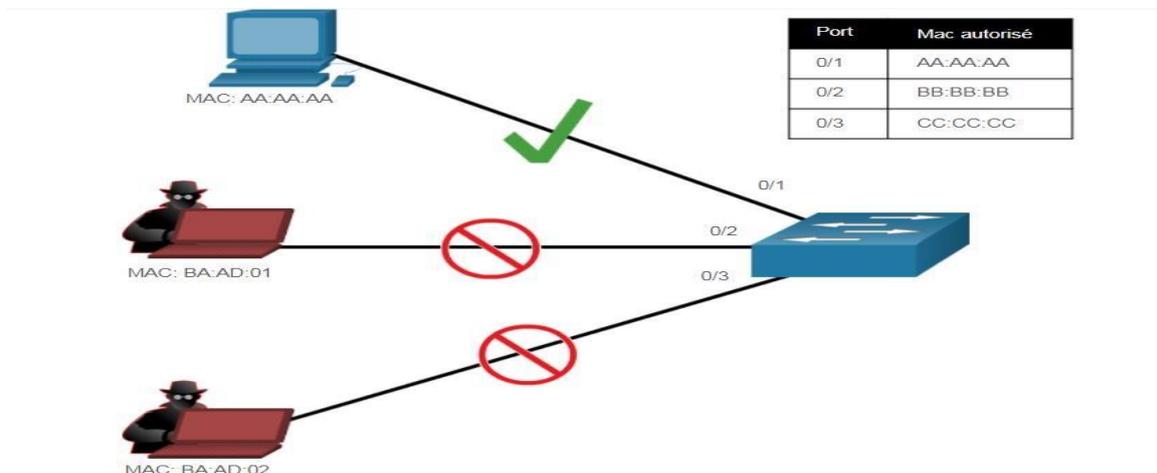


Figure 2.70 : attaque mac flooding

La sécurité des ports ne peut être configurée que sur des ports d'accès.

La sécurité des ports est activée sur les ports concernés par la commande

```

serial-com1 (3)
access(config-if)#switchport port-se
access(config-if)#switchport port-security
access(config-if)#switchport port-security max
    
```

Figure 2.71 : activer port sécurité

switchport port-security , en cas de violation du nombre maximum d'adresses MAC est de 1 dans notre cas , le port entrera par erreur dans l'état désactivé.

Pour définir le nombre maximal d'adresses MAC autorisées sur un port, utilisez la commande suivante

```
access(config-if)#switchport port-security maximum
```

Figure 2.72 : définir le nombre max de port

```
access(config-if)#switchport port-security maximum 1
```

La valeur de sécurité du port par défaut est 1. Le nombre maximum d'adresses MAC sécurisées configurables dépend de Commutateur et IOS.

Figure 2.73 : défini le nombre max à 1

Après l'application de la mesure de sécurité, on essaye une attaque le message est affiché security violation occurred

On essaye une attaque :

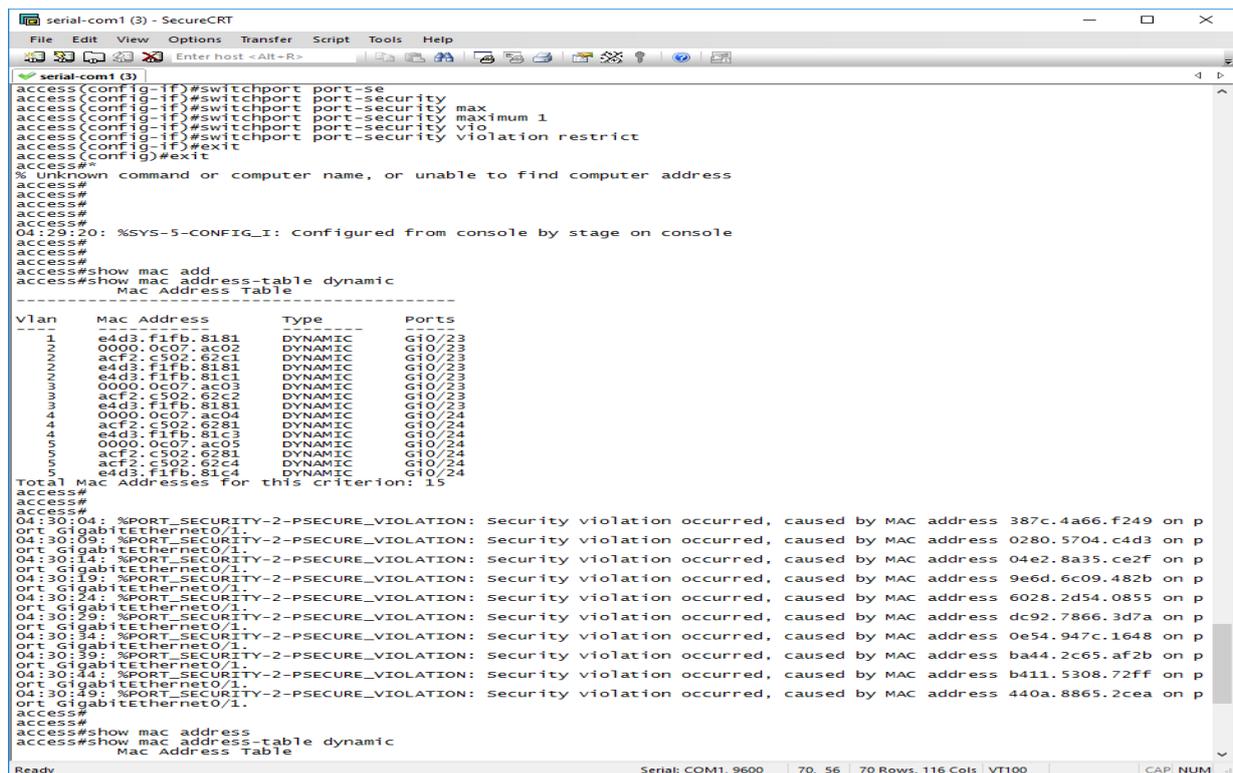


Figure 2.74 : résultat d'attaque mac

- Le commutateur est configuré pour apprendre l'adresse MAC sur le port sécurisé de trois manières :

1. Configuration manuelle :

L'administrateur configure manuellement une ou plusieurs adresses MAC statiques pour chaque adresse MAC sécurisée sur le port :

2. Apprentissage dynamique :

Lorsque la commande `switchport port-security` est exécutée, le MAC source actuel du périphérique connecté au port sera automatiquement protégé, mais il ne sera pas ajouté à la configuration en cours. Si le commutateur redémarre, le port devra réapprendre l'adresse MAC de l'appareil.

3. Apprentissage dynamique – Sticky :

L'administrateur peut utiliser la commande suivante pour permettre au commutateur d'apprendre dynamiquement l'adresse MAC et de la « coller » dans la configuration en cours : [20]

```
access(config-if)#switchport port-security mac-address sticky
```

Conservez la configuration actuelle et l'apprentissage dynamique de l'adresse MAC sera stocké dans la NVRAM.

On essaye une attaque après activer mode sticky

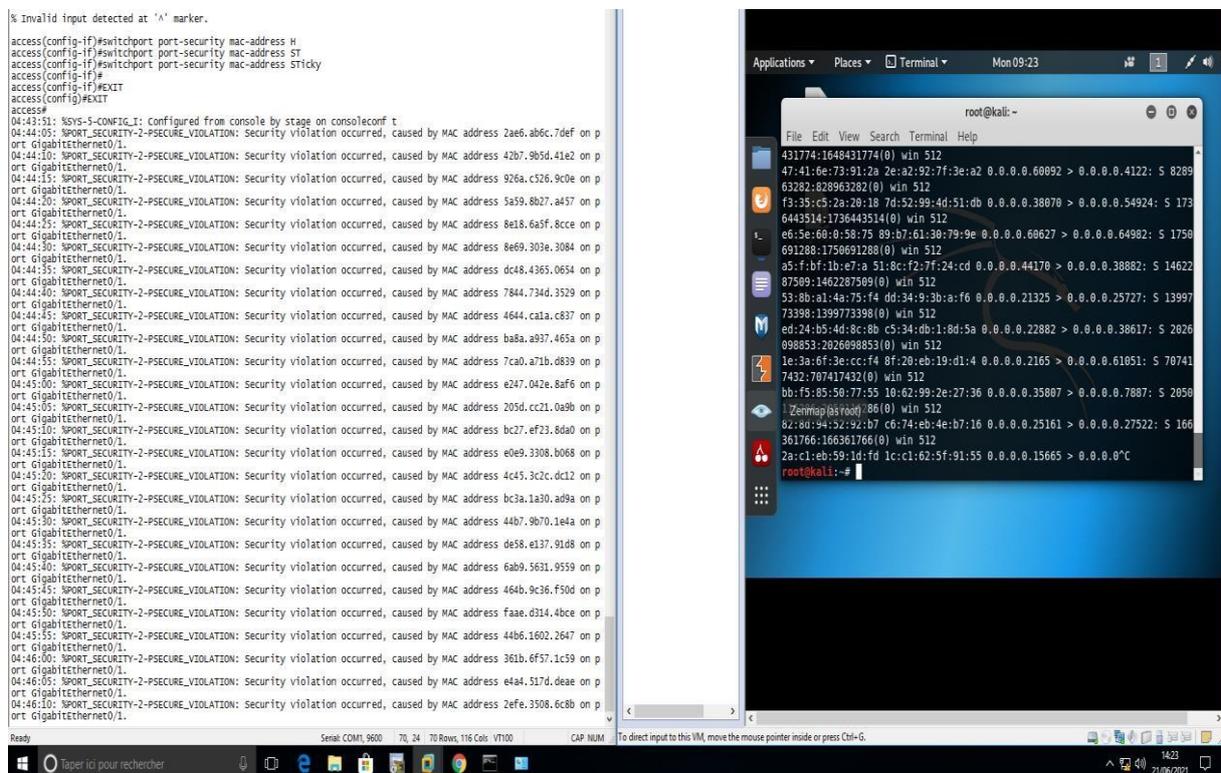


Figure 2.75: résultat d'attaque mac avec sticky

Commande	Signification
Switchport host	Cette commande fait trois choses (met le port en mode «access », activer le mode « portfast », désactiver la fonction de « etherchannel »).
Switchport port-security maximum 3	Définir le nombre maximal d'adresses sécurisées à 3.
Switchport port-security	Activer la sécurité des ports sur l'interface.
Switchport port-security mac-address sticky	Activer l'apprentissage rémanent.
Switchport port-security violation restrict	définir l'action à entreprendre lorsqu'une violation de sécurité est détectée.
Ip verify source	activer IP source guard pour ajouter un niveau de sécurité plus élevé au port souhaité en empêchant l'usurpation d'adresse IP.
errdisable recovery cause security-violation	activer le mode « recovery » pour la sécurité des ports.
errdisable recovery interval 60	configurer le minuteur de récupération a 60 second.

Table 2.76 : commande de security des ports

2.2 Atténuer les attaques VLAN :

Utilisez les étapes suivantes pour atténuer les attaques de saut de VLAN :

Étape 1 : utilisez la commande de configuration de l'interface d'accès en mode switchport pour désactiver la négociation DTP (jointure automatique) sur les ports non tronqués.

Étape 2 : Désactivez les ports inutilisés et placez-les dans le VLAN inutilisé.

Étape 3 : utilisez la commande switchport mode trunk pour activer manuellement la liaison de jonction sur le port de jonction.

Étape 4 : utilisez la commande switchport nonegotiate pour désactiver la négociation de relais automatique (DTP) sur le port de jonction.

Étape 5 : utilisez la commande switchport trunk native vlan vlan_number pour définir le VLAN natif sur un VLAN autre que le VLAN 1.

Les Étapes pour atténuer les attaques par sauts de VLAN

Par exemple, supposons ce qui suit :

Les ports FastEthernet 0/1 à fa0/16 sont des ports d'accès actifs

Les ports FastEthernet 0/17 à 0/20 sont actuellement inutilisés

Les ports FastEthernet 0/21 à 0/24 sont des ports de jonction.

Vous pouvez réduire le saut de VLAN en implémentant la configuration suivante.

```

access(config)#int range fa0/1-24
access(config-if-range)#
access(config-if-range)#
access(config-if-range)#swi
access(config-if-range)#switchport mode
access(config-if-range)#switchport mode acc
access(config-if-range)#switchport mode access
access(config-if-range)#
access(config-if-range)#
access(config-if-range)#swi
access(config-if-range)#switchport no
access(config-if-range)#switchport nonegotiate
access(config-if-range)#exit
access(config)#
access(config)#
access(config)#
access(config)#vla
access(config)#vlan 99
access(config-vlan)#exit
    
```

Figure 2.77 : configurer la port en mode nonegotiate

```

access(config)#int range fa0/1-24
access(config-if-range)#swi
access(config-if-range)#switchport acc
access(config-if-range)#switchport access vl
access(config-if-range)#switchport access vlan 99
    
```

Figure 2.78 : vlan 99 comme vlan

On essaye une attaque :

The screenshot shows the Yersinia 0.7.3 interface. On the left, a 'Protocols' list shows DTP with 23 packets. The main table displays DTP neighbors:

Neighbor-ID	Status	Domain	Interface	Count	Last seen
0012D981FB02	03 ACCESS/DESIRABLE		eth0	3	05 Feb 21:33:03
0C7CE846D595	03 ACCESS/DESIRABLE		eth0	10	05 Feb 21:36:43
0012D981FB02	83 TRUNK/DESIRABLE		eth0	6	05 Feb 21:34:38
0C7CE846D595	83 TRUNK/DESIRABLE		eth0	3	05 Feb 21:34:39
0012D981FB02	02 ACCESS/OFF		eth0	1	05 Feb 21:34:54

Below the table, the 'Dynamic Trunking Protocol' configuration is visible:

- Source MAC: 0C:7C:E8:46:D5:95
- Destination MAC: 01:00:0C:CC:CC:CC
- Version: 01
- Neighbor-ID: 0C7CE846D595
- Status: 03
- Type: A5

Figure 2.88 : résultat d'attaque vlanshopping après contremesure

On remarque que status a changer et le trunk ne passe pas dans le switch :

2.3 Atténuer les attaques DHCP :

L'objectif d'une attaque de pénurie DHCP est de créer un déni de service (DoS) pour connecter les clients.

Les attaques de pénurie de ressources DHCP reposent sur des outils d'attaque tels que Gobbler.

N'oubliez pas que vous pouvez atténuer efficacement les attaques de failles DHCP en utilisant la sécurité des ports, car Gobbler utilise une adresse MAC source unique pour chaque requête DHCP envoyée.

Cependant, l'atténuation des attaques d'usurpation DHCP nécessite plus de protection. Gobbler peut être configuré pour utiliser l'adresse MAC de l'interface réelle comme adresse Ethernet source, mais spécifiez une adresse Ethernet différente dans la charge utile DHCP. Cela invalidera la sécurité du port car l'adresse MAC source est légale. [24]

Vous pouvez atténuer les attaques d'usurpation DHCP en utilisant la surveillance DHCP sur les ports de confiance.

La surveillance DHCP ne dépend pas de l'adresse MAC source.

Au lieu de cela, la surveillance DHCP détermine si le message DHCP provient d'une source approuvée configurée ou d'une source non approuvée. Administrativement.

Filtrez ensuite les messages DHCP et limitez la fiabilité du trafic DHCP provenant de sources non fiables.

Les appareils sous contrôle de gestion (par exemple, les commutateurs, les routeurs et les serveurs) sont des sources fiables.

Tout appareil placé en dehors du pare-feu ou en dehors du réseau est une source non fiable. De plus, tous les ports d'accès sont généralement considérés comme des sources peu fiables.

La figure montre des exemples de ports approuvés et non approuvés. [14]

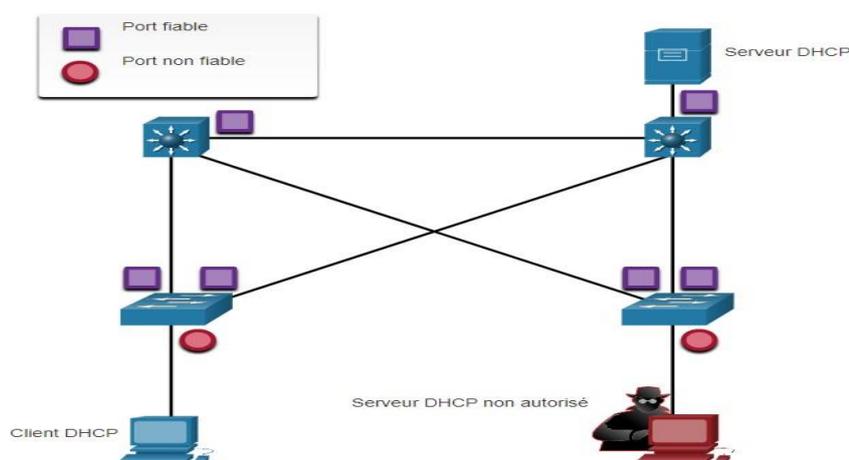


Figure 2.89 : attaque dhcp

Notez que lorsque la surveillance DHCP est activée, le serveur DHCP malveillant sera situé sur un port non approuvé.

Par défaut, toutes les interfaces sont considérées comme non fiables.

Les interfaces de confiance sont généralement des liens relais et des ports directement connectés à des serveurs DHCP légitimes ; ces interfaces doivent être explicitement configurées comme étant de confiance.

Créez une table DHCP qui inclut l'adresse MAC source du périphérique sur le port non approuvé et l'adresse IP attribuée au périphérique par le serveur DHCP.

L'adresse MAC et l'adresse IP sont liées ensemble, cette table est donc appelée table de liaison d'espionnage DHCP.

Exemple de configuration de l'espionnage DHCP:

Utilisez les étapes suivantes pour activer la surveillance DHCP :

Étape 1 Utilisez la commande de configuration globale `ip dhcp snooping` pour activer la surveillance DHCP.

```
(config)#ip dhcp sn
(config)#ip dhcp snooping
```

Figure 2.90 : configurer le dhcp snooping

Étape 2 : Sur le port de confiance, utilisez la commande `ip dhcp snooping trust` pour configurer l'interface

```
(config)#int e0/1
(config-if)#
(config-if)#
(config-if)#ip dhcp sn
(config-if)#ip dhcp snooping tr
(config-if)#ip dhcp snooping trust
```

Figure 2.91 : ip dhcp snooping

Étape 3 : Utilisez la commande de configuration de l'interface `ip dhcp snooping limit rate` pour limiter le nombre de messages de découverte DHCP qu'un port non approuvé peut recevoir par seconde.

```
(config)# int e0/0
(config-if)#ip dhcp snooping limit rate 3
```

Figure 2.92 : limiter le rate à 3

Étape 4 : Utilisez la commande de configuration globale `ip dhcp snooping vlan` pour activer la surveillance DHCP par VLAN ou par plage de VLAN.

```
(config)#ip dhcp sn
(config)#ip dhcp snooping
(config)#ip dhcp snooping vlan 1
(config)#
```

Figure 2.93 : activer la surveillance DHCP par VLAN

Essaye une attaque après la contre mesure :

```
root@kali:~# systemctl restart smbd
root@kali:~# dhclient
```

Figure 2.94 : essayé une attaque

On essaye de prendre une adresse d'après le serveur dhcp mais aucun réponse ,
 Quand on utilise whireshark on Remarque que on a aucun réponse dhcp :

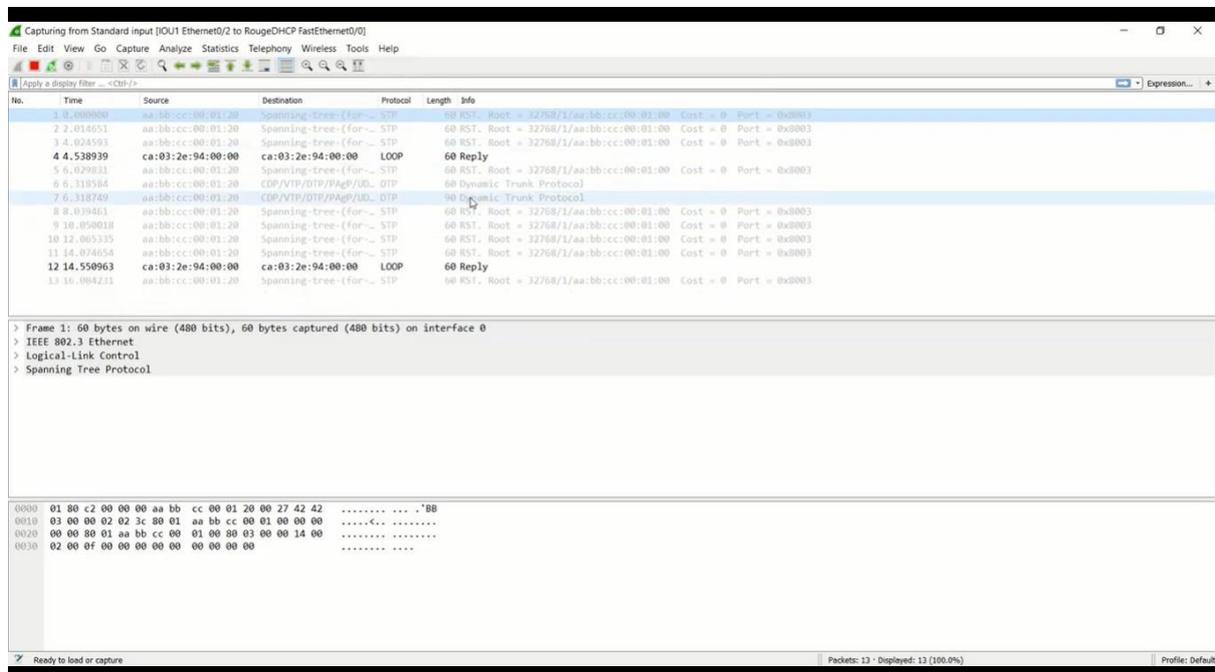


Figure 2.95: résultat d'attaque dhcp

Commande	Signification
Ip dhcp snooping	Activer DHCP-snooping globalement.
Ip dhcp snooping verify mac-address	Activer la vérification d'adresse MAC de DHCP-snooping.
Ip dhcp snooping vlan 10,20,30,40,50	Activer DHCP-snooping sur plusieurs VLANs.
Ip dhcp snooping trust	Configurer l'interface comme approuvée.
Ip dhcp snooping limit rate 4	Configurer la limitation du débit des paquets DHCP.

Tableau 2.1 : expliqué les commande dhcp

2.4 Atténuer les attaques d’ARP :

Dans une attaque typique ARP , un acteur menaçant peut envoyer une réponse ARP non sollicitée à d'autres hôtes du sous-réseau, qui contient l'adresse MAC de l'acteur menaçant et l'adresse IP de la passerelle par défaut. [25]

Afin d'éviter l'usurpation ARP et l'empoisonnement ARP qui en résulte, le commutateur doit s'assurer que seules les demandes et les réponses Transféré efficacement.

La vérification dynamique ARP nécessite une surveillance DHCP et aide à prévenir les attaques ARP Pour réduire le risque de tromperie ARP et d'empoisonnement ARP, veuillez suivre ces directives de mise en œuvre du DAI

- Activer l'espionnage DHCP globalement.
- Activer la surveillance DHCP sur le VLAN sélectionné.
- Activer l'inspection ARP dynamique sur le VLAN sélectionné.
- Configurer des interfaces de confiance à l'aide de la surveillance DHCP ; inspection ARP .

Il est généralement recommandé de configurer tous les ports de commutateur d'accès comme non approuvés et tous les ports de liaison montante connectés à d'autres commutateurs comme approuvés.

Configuration de « Dynamic ARP Inspection » : le commutateur ira vérifier l'ensemble des paquets ARP sur les interfaces non approuvées.

Tout de même l'inspection dynamique de l'ARP autorise tous les paquets ARP sur des interfaces de confiance, en mettant les ports du réseau comme ports trustés. [25] [19]

```
access(config)#ip arp inspection vlan 2,3,4,5
access(config)#interface range G0/0-1
access(config-if-range)#ip arp inspection trust
access(config-if-range)#exit
```

Figure 2.96 : Dynamic ARP Inspection

On essaye une attaque :

```
root@kali:~# nmap -F 10.110.10.1/24
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2021-09-18 12:24 EDT
Failed to resolve "".
Note: Host seems down. If it is really up, but blocking our ping probes,
Nmap done: 1 IP address (0 hosts up) scanned in 10.60 seconds
```

Figure 2.97 : essaye une attaque

L'attaque ne pas pas et le ping est bloqué

Le switch détecter que il y'a une attack et l' arrêter :

```
16:23:57.029: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Et0/2, vlan 1.([000c.29e3.5d71/0000.0000.0000/10.0.0.0/16:23:56 UTC Thu Apr 18 2019])
16:23:58.029: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Et0/2, vlan 1.([000c.29e3.5d71/0000.0000.0000/10.0.0.0/16:23:57 UTC Thu Apr 18 2019])
fig-if)#
16:24:02.043: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Et0/2, vlan 1.([000c.29e3.5d71/0000.0000.0000/10.0.0.1/16:24:01 UTC Thu Apr 18 2019])
16:24:03.044: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Et0/2, vlan 1.([000c.29e3.5d71/0000.0000.0000/10.0.0.1/16:24:02 UTC Thu Apr 18 2019])
fig-if)#
16:24:04.053: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Et0/2, vlan 1.([000c.29e3.5d71/0000.0000.0000/10.0.0.1/16:24:03 UTC Thu Apr 18 2019])
```

Figure 2.98 : Le switch détecter que il y'a une attack et l'arrêter

Commande	signification
Ip arp inspection vlan 10,20,30,40,50	Activer arp-inspection sur plusieurs VLANs.
Ip arp inspection trust	Configurer l'interface comme approuvée pour le fonctionnement de arp-inspection.

Tableau 2.2 : explication de commandes du dynamic arp inspection

Atténuer les attaques HSRP :

Configuration de l'authentification de HSRP : pour mieux sécuriser notre HSRP nous allons mettre en place un mot de passe, cependant ce dernier reste en clair et cela donne la possibilité à des attaquants d'envoyer des paquets en multicast 224.0.0.2 en UDP sur le port 1985 aux routeurs afin de difuser de fausses informations et avec le bon mot de passe qui peut être

facilement capturé. Nous allons maintenant chercher à hasher ce mot de passe afin de ne pas le diffuser en clair, ce qui montre dans la figure : [19]

```
access(config)#key chain HSRP
access(config-keychain)#key 1
access(config-keychain-key)#key-string cisco
access(config-keychain-key)#exit
access(config-keychain)#exit
access(config)#int vlan 10
access(config-if)#standby 10 authentication md5 key-chain HSRP
```

Figure 2.99 : configuration key chain

Commande	Signification
Key chain HSRP	Activer l'authentification, identifier un groupe de clés d'authentification, et entrer au mode de configuration (key-chain).
Key 1	Identifier une clé d'authentification sur key-chain et entrer au mode de configuration (key-chain key).
Key-string cisco	Spécifier la clé d'authentification.
Standby 10 authentication md5 key-chain HSRP	Configurer l'authentification MD5 key-chain pour l'authentification HSRP.

Tableau 2.3 : explication de commandes l'authentification HSRP

Atténuer les attaques STP :

PortFast et protection BPDU :

N'oubliez pas que les attaquants du réseau peuvent manipuler le protocole 3 pour attaquer en usurpant le pont racine et en modifiant la topologie du réseau.

Utilisez PortFast et Bridge Protocol Data Unit (BPDU) Garde :

PortFast - L'objectif de la fonction PortFast est de minimiser le temps d'attente du port d'accès avant que le spanning tree ne converge. Elle ne doit être utilisée que pour le port d'accès. PortFast ne doit pas être configuré uniquement sur le port connecté au terminal. [20]

BPDU Guard-une Erreur BPDU Guard Le port qui reçoit les BPDU est immédiatement désactivé. Comme 2. BPDU Guard ne doit pas être configuré uniquement sur le port connecté au terminal.

Le port d'accès de S1 dans la figure doit être configuré comme PortFast et BPDU Guard

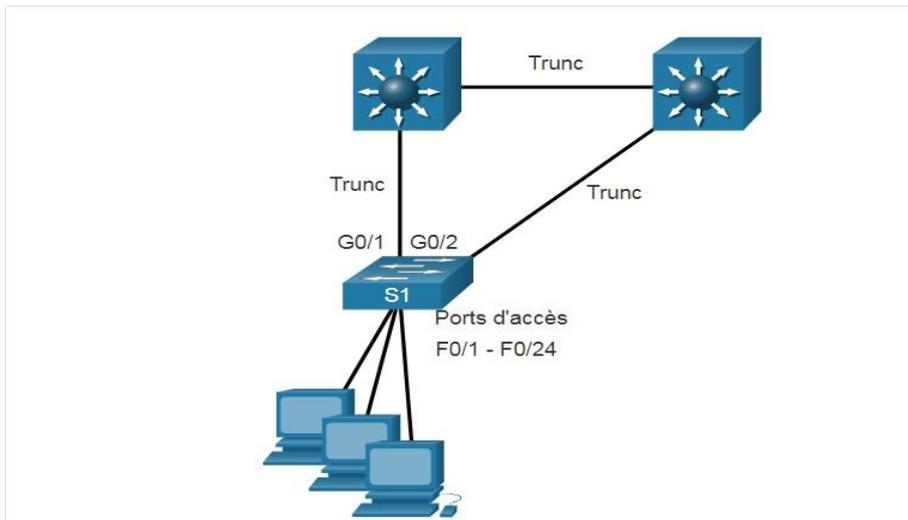


Figure 2.100 : stp example

Configurer PortFast :

PortFast Contournez la situation d'écoute et d'apprentissage STP pour limiter le temps que le port d'accès doit attendre pour que STP converge.

```
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#int e0/1
Switch(config-if)#switchport mode access
Switch(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 Ethernet0/1 but will only
have effect when the interface is in a non-trunking mode.
Switch(config-if)#exit
Switch(config)#spanning -tree portfast default
^
% Invalid input detected at '^' marker.

Switch(config)#spanning-tree portfast default
%Warning: this command enables portfast by default on all interfaces. You
should now disable portfast explicitly on switched ports leading to hubs,
switches and bridges as they may create temporary bridging loops.
```

Figure 2.101 : Configurer PortFast

Pour vérifier si PortFast est globalement activé, vous pouvez utiliser la commande `show running-config | begin span` ou la commande `show spanning-tree summary`.

```
spanning-tree mode pvst
spanning-tree portfast default
spanning-tree extend system-id
```

Figure 2.102 : portfast activé

2.5 Configuration BPDU Guard :

Même si PortFast est activé, l'interface écoutera toujours les BPDU. Les BPDU inattendues peuvent être accidentelles ou faire partie d'une tentative non autorisée d'ajouter un commutateur au réseau. [20]

Si un BPDU est reçu sur un port d'accès avec BPDU Guard activé, le port sera placé par erreur dans l'état désactivé. Cela signifie que le port a été arrêté et doit être réactivé manuellement ou automatiquement restauré via la commande globale errdisable recovery cause psecure_violation.

```
Switch(config)#int e0/1
Switch(config-if)#spanning-tree bpduguard enable
Switch(config-if)#exit
Switch(config)#spanning-tree portfast bpduguard default
Switch(config)#end
Switch#
*Sep 21 13:12:32.434: %SYS-5-CONFIG_I: Configured from console by consoles
Switch#sh spanning-tree summary
Switch is in pvst mode
Root bridge for: VLAN0001
Extended system ID      is enabled
Portfast Default        is enabled
PortFast BPDU Guard Default is enabled
Portfast BPDU Filter Default is disabled
Loopguard Default       is disabled
EtherChannel misconfig guard is enabled
Configured Pathcost method used is short
UplinkFast              is disabled
BackboneFast            is disabled
```

Figure 2.103 : Configuration BPDU Guard

Commande	Signification
Spanning-tree portfast	Activer le mode portfast.
Spanning-tree bpduguard enable	Active la fonction bpduguard.

Tableau 2.4 :Explication de commandes STP

2.6 Mise en œuvre de la sécurité des ports :

De nombreuses administrateurs méthodes simples utilisées pour aider à protéger le réseau contre les accès non autorisés consistent à désactiver tous les ports inutilisés sur le commutateur.

Par exemple, si le switch dispose de 24 ports, et si trois connexions 2 sont utilisées, il est recommandé de désactiver les 21 ports inutilisés. [20]

Exécutez la commande shutdown pour chaque port inutilisé.

Si vous devez réactiver un port ultérieurement, vous pouvez l'activer en exécutant la commande #no shutdown.

Pour configurer le port gamma, utilisez la commande interface range.

Par exemple, pour fermer les ports Fa0 / 8 à Fa0 / 24 sur S1, vous devez utiliser la commande suivante.

```
Switch(config)#int range e0/1-3
Switch(config-if-range)#shutdown
Switch(config-if-range)#
*Sep 21 13:18:55.783: %LINK-5-CHANGED: Interface Ethernet0/1, changed state to administratively down
*Sep 21 13:18:55.784: %LINK-5-CHANGED: Interface Ethernet0/2, changed state to administratively down
*Sep 21 13:18:55.795: %LINK-5-CHANGED: Interface Ethernet0/3, changed state to administratively down
*Sep 21 13:18:56.789: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1, changed state to down
*Sep 21 13:18:56.789: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/2, changed state to down
Switch(config-if-range)#
*Sep 21 13:18:56.796: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/3, changed state to down
```

Figure 2.104 : Exécutez la commande shutdown

2.6 Accès à distance sécurisé :

1. Opération SSH :

-Secure Shell (SSH) est un protocole sécurisé qui utilise le port TCP 22. Il fournit une connexion de gestion sécurisée (cryptée) à un appareil distant. SSH doit remplacer Telnet pour les connexions de gestion. [25]

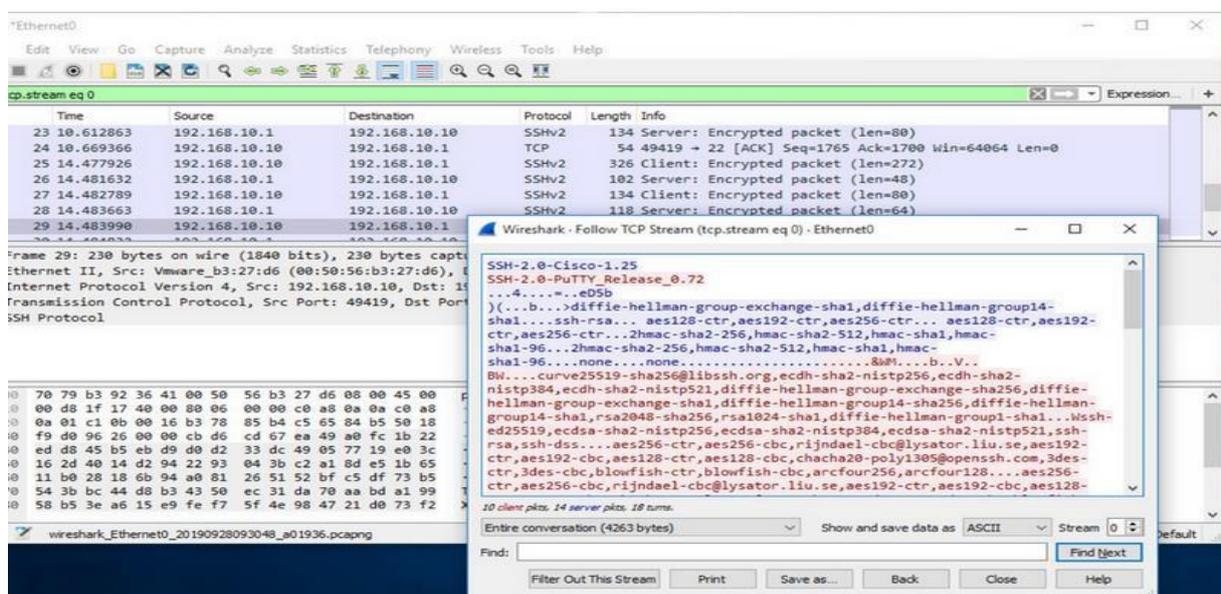


Figure 2.105 : WHIRESHARK analyse

Vérifiez que le commutateur prend en charge SSH :

-Pour activer le SSH sur un commutateur Catalyst 2960, le commutateur doit utiliser une version du logiciel IOS comprenant des fonctions et des capacités cryptographiques (cryptées). Utilisez la commande `show version` du commutateur pour voir quel IOS le commutateur est en cours d'exécution. Un nom de fichier IOS qui inclut la combinaison "k9" prend en charge les fonctions et capacités cryptographiques (chiffrées). L'exemple montre le résultat de la commande `show version`. [25]

```
S1# show version
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE7, RELEASE SOFTWARE (fc1)
```

Figure 2.107 : version ssh**Configuration de SSH :****Étape 1****Vérifier le support SSH.**

Utilisez la commande `show ip ssh` pour vérifier que le commutateur supporte SSH. Si le commutateur n'exécute pas un IOS qui prend en charge les fonctions cryptographiques, cette commande n'est pas reconnue.

```
S1# show ip ssh
```

Figure 2.108 : vérifier le support ssh**Étape 2****Configurer le domaine IP.**

Configurez le nom de domaine IP du réseau à l'aide de la commande de mode de configuration globale `ip domain-name domain-name`. Dans la figure, la valeur `domain-name` est `cisco.com`.

```
S1(config)# ip domain-name cisco.com
```

Figure 2.109: configurer le domaine name**Étape 3****Générer des paires de clés RSA.**

```
S1(config)# crypto key generate rsa
How many bits in the modulus [512]: 1024
```

Figure 2.110 : rsa configuration

Étape 4

Configurer l'authentification des utilisateurs.

Le serveur SSH peut authentifier les utilisateurs localement ou à l'aide d'un serveur d'authentification. Pour utiliser la méthode d'authentification locale, créez une paire de nom d'utilisateur et de mot de passe à l'aide de la commande de configuration globale `username username secret password`. Dans cet exemple, l'utilisateur admin se voit attribuer le mot de passe ccna.

```
S1(config)# nom d'utilisateur admin secret ccna
```

Figure 2.111 : authentification configuration

Étape 5

Configurer les lignes de vty.

```
S1(config)# line vty 0 15
S1(config-line)# transport input ssh
S1(config-line)# login local
S1(config-line)# exit
```

Figure 2.112 : configurer vty

Étape 6

Activer SSH version 2.

```
S1(config)# ip ssh version 2
```

Figure 2.113 : activer ssh

2. Configuration du protocole 802.1X : on sait que le protocole 802.1X contrôle l'accès à des réseaux locaux, et pour l'appliquer il faut l'activer sur tous les équipements du réseau qui ont besoin d'être sécurisé (commutateurs, équipement terminal), et pour cela nous allons suivre la configuration montrée dans la figure suivante :

```
access(config)#AAA new-model
access(config)#AAA authentication dot1x default group radius
access(config)#AAA authorization network default group radius
access(config)#AAA accounting dot1x default start-stop group radius
access(config)#Radius server AD
access(config-radius-server)#Address ipv4 10.110.5.13
access(config-radius-server)#Key cisco
access(config-radius-server)#exit
access(config)#Dot1x system-auth-control
access(config)#interface range G1/0- 3
access(config-if-range)#Authentication host-mode multi-auth
access(config-if-range)#Authentication port-control auto
access(config-if-range)#Dot1x pae authenticator
access(config-if-range)#exit
```

Figure 2.114 : configuration du protocole 802.1X

Commande	Signification
AAA new-model	Activer l'AAA
AAA authentication dot1x default group radius	Configurer AAA pour qu'il utilise RADIUS lors de l'authentification 802.1x
AAA authorization network default group radius	configurer AAA pour qu'il utilise RADIUS lors de l'autorisation 802.1x
AAA accounting dot1x default start-stop group radius	configurer AAA pour qu'il utilise RADIUS lors de la comptabilité 802.1x
Radius server AD	Donner un nom au serveur radius
Address ipv4 192.168.40.253	Configuration de l'IP du serveur Radius.
Key cisco	Définir la clef utilisée lors de l'authentification entre le commutateur et le serveur radius.
Dot1x system-auth-control	Activer le service d'authentification 802.1x sur le commutateur.
Authentication host-mode multi-auth	Autoriser un client sur le VLAN vocal et plusieurs clients authentifiés sur le VLAN de données.
Authentication port-control auto	Afficher des informations des interfaces.
Dot1x pae authenticator	Définit le type d'entité d'accès au port (PAE).

Tableau 4.5 : Explication de commandes du protocole 802.1X

Conclusion :

Dans ce chapitre on a présenté une configuration basique d'un réseau campus, ensuite on a montré la fragilité de cette dernière face aux différentes attaques ciblant la couche 2 de ce dernier en exploitant les vulnérabilités de protocoles. A la fin du chapitre on a défini une stratégie de sécurisation de la couche 2 en se basant sur les bonnes pratiques dans le domaine et les recommandation des constructeurs.

Chapitre III : Automatisation sécurisé d'un switch

Introduction :

L'un des objectifs d'un ingénieur réseau est de trouver des solutions aux problèmes rencontrés quotidiennement ou d'essayer de développer le système pour cette raison, nous vous proposons une application qui fonctionne pour faciliter et automatiser le changement de paramètres en suivant la stratégie précédemment étudiée dans la première partie car nous avons remarqué que le processus de préparation se fait par un processus constant et que du temps est perdu pour écrire des commandes et recréer plusieurs fois les mêmes commandes. Et afin d'appliquer automatiquement la stratégie précédente.

C'est pourquoi tout ce que l'administrateur fera est d'internaliser les paramètres et une stratégie sera formée de manière automatisée.

Étude conceptuelle :

▪ Diagramme des cas d'utilisation :

La figure ci-dessous représente le diagramme des cas d'utilisations qui décrit les utilisations requises par notre application :

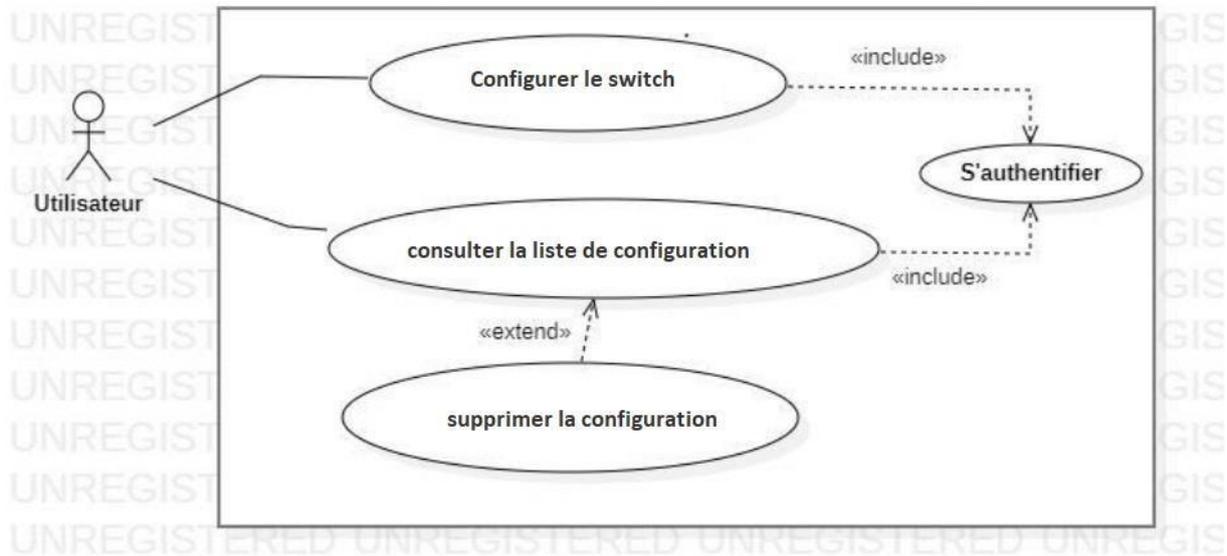


Figure 3.1 : diagramme de cas d'utilisation

Diagrammes de séquence :

Un diagramme de séquence est un diagramme interactif montrant comment les opérations sont effectuées

❖ **Authentification :**

Lorsqu'un utilisateur souhaite accéder à notre application, il sera obligé de vérifier son identité en entrant son nom d'utilisateur et son mot de passe avant d'y accéder. Après être entré dans le système, il enverra une demande au serveur pour traiter les informations envoyées. Si les informations sont correctes, l'utilisateur accédera à sa session, sinon un message d'erreur s'affichera et l'utilisateur sera renvoyé à la page d'authentification.

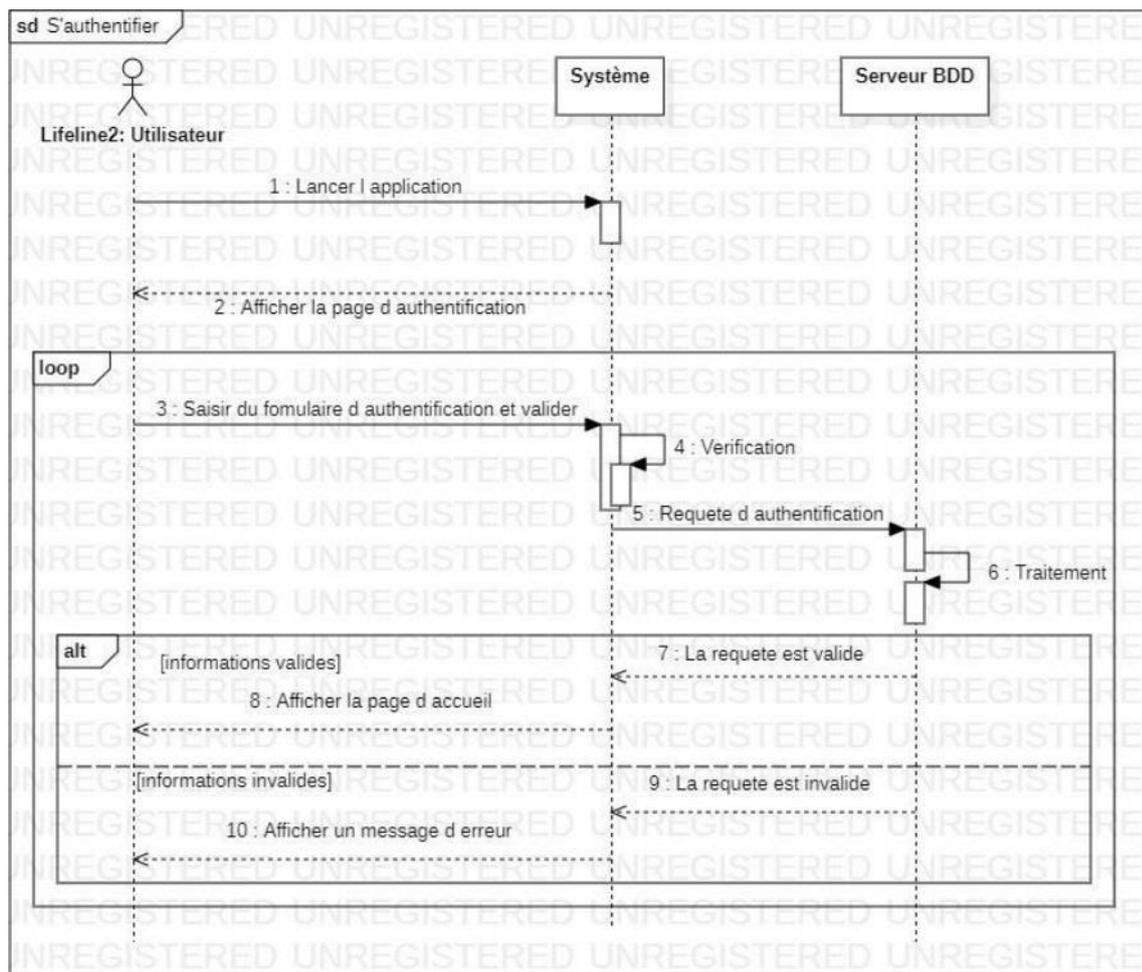


Figure 3.2 : diagramme séquence de Authentification

Configuration du commutateur :

Pour faire une nouvelle configuration, l'utilisateur doit saisir les configuration de commutateur d'après c'est besoins : vlan , dhcp , stp , telnet , hsrp ,hostname, configuration des interfaces

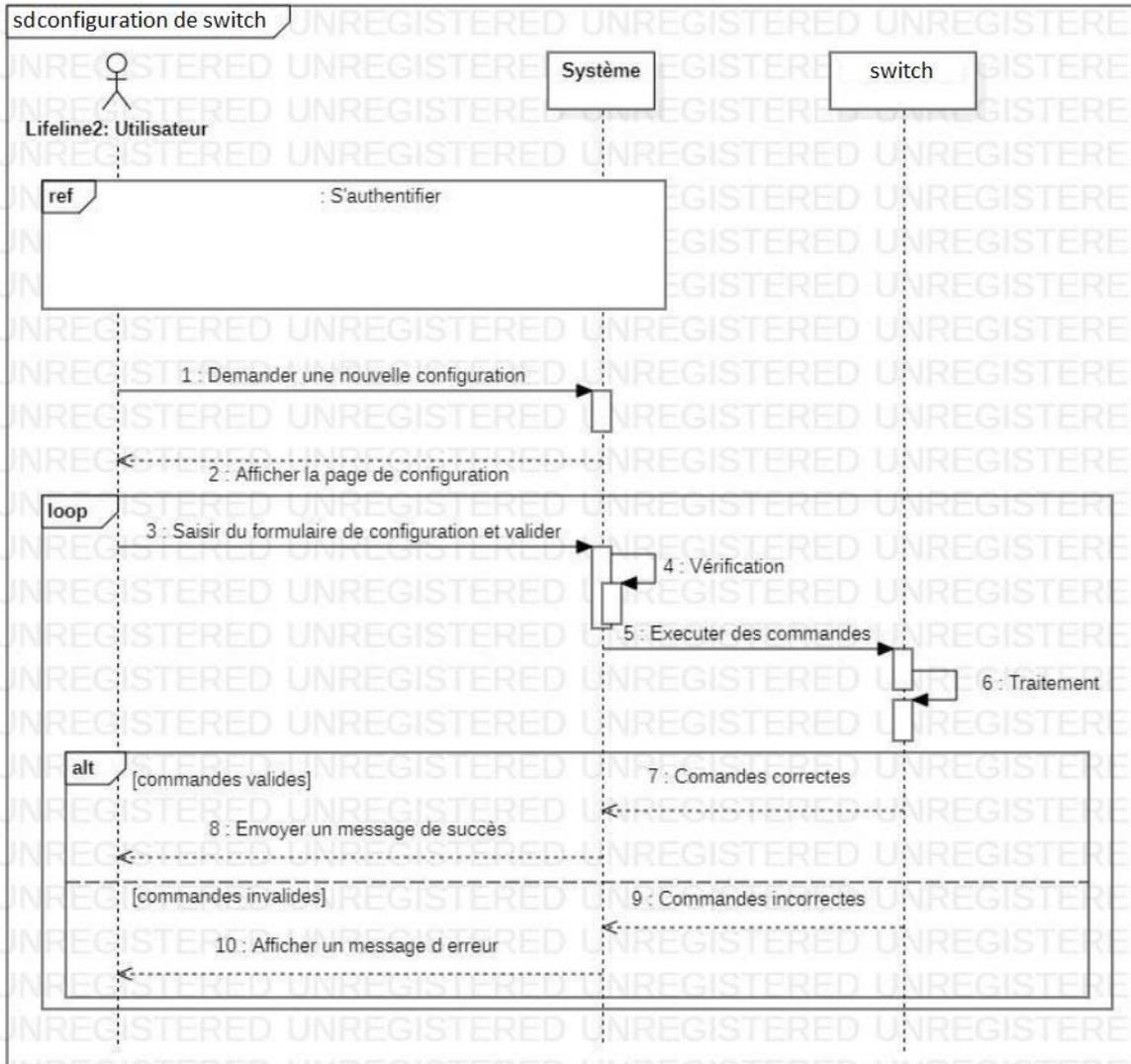


Figure 3.3 : diagramme séquence Configuration du commutateur

Consultation la liste des configurations :

L'utilisateur peut consulter la liste de ses configurations. Par option il peut supprimer une configuration.

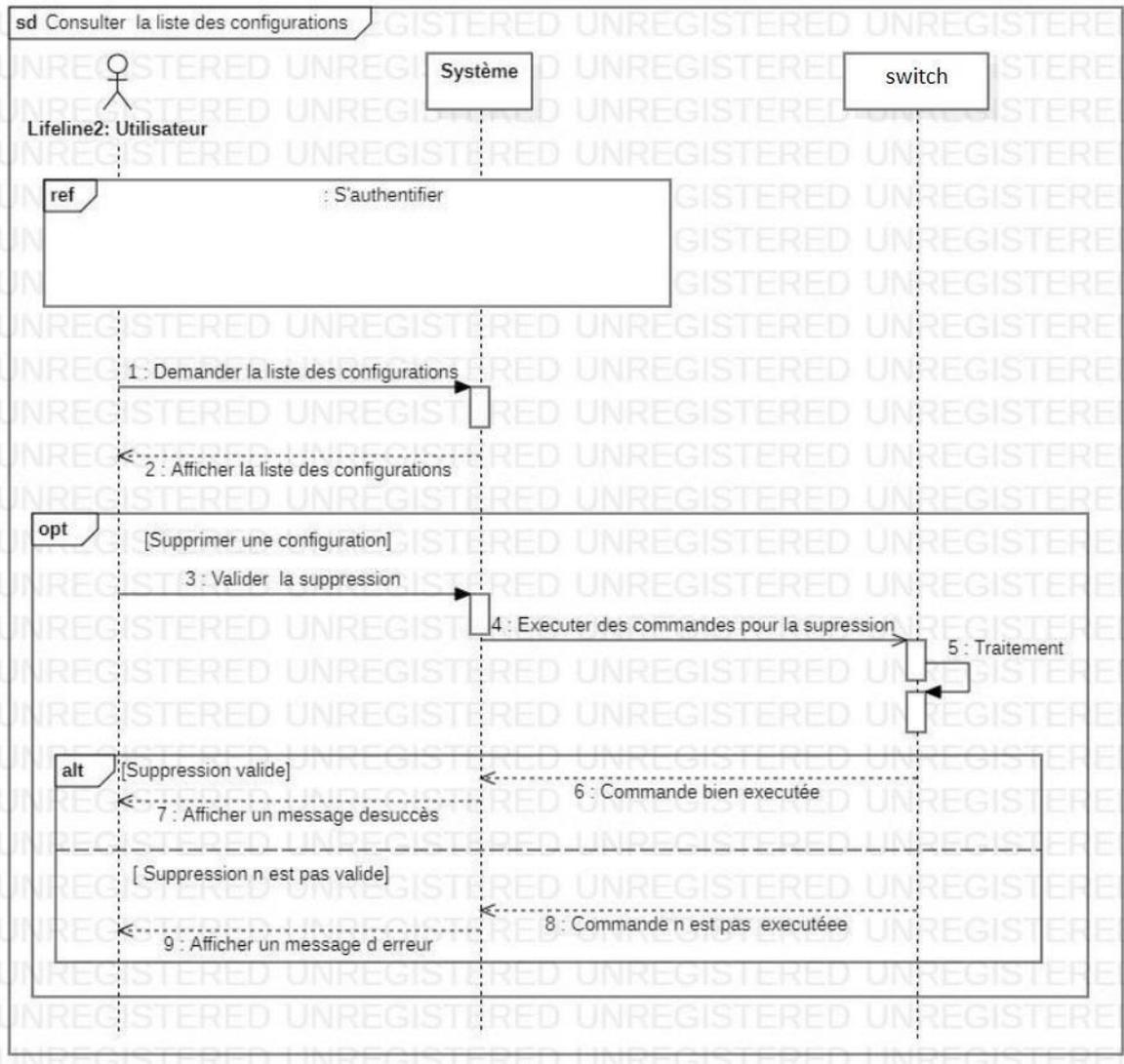


Figure 3.4 : diagramme séquence pour Consultation la liste

Représentation des interfaces :

Authentification :



Figure 3-5 : Interface d'authentification

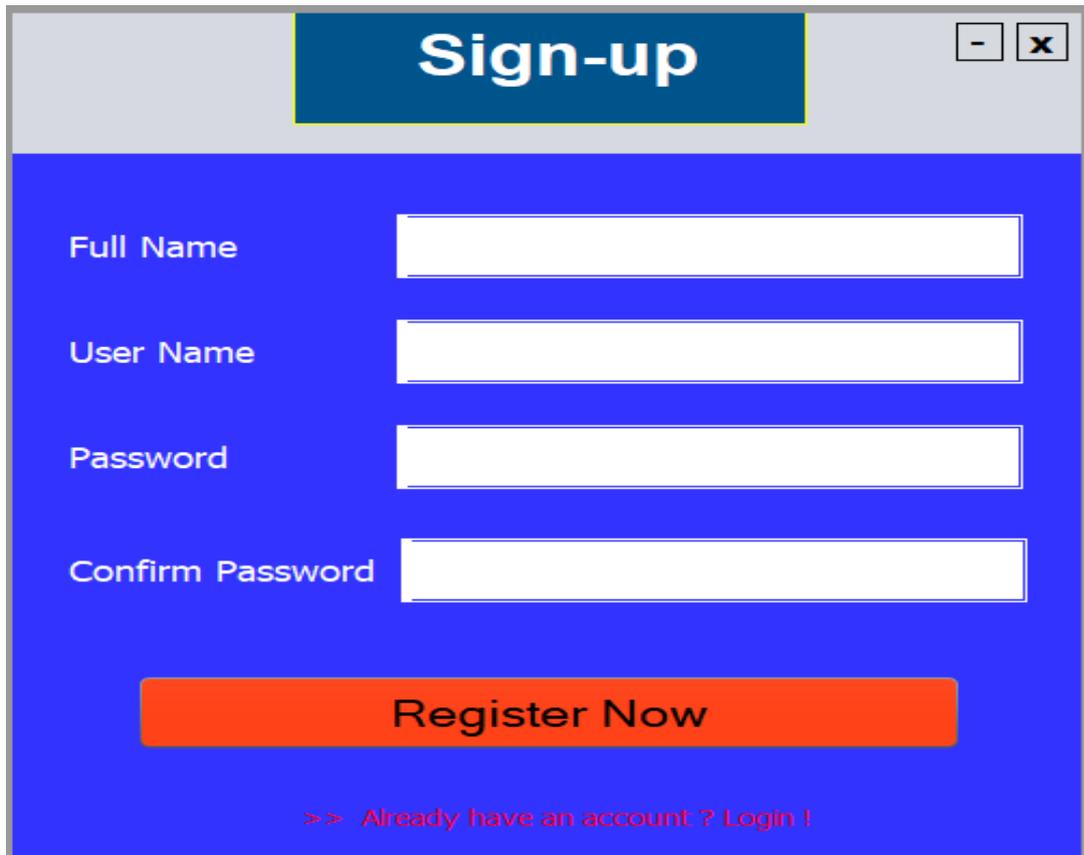


Figure 3-6 : Interface de sign-up

▪ Nouvelle configuration :

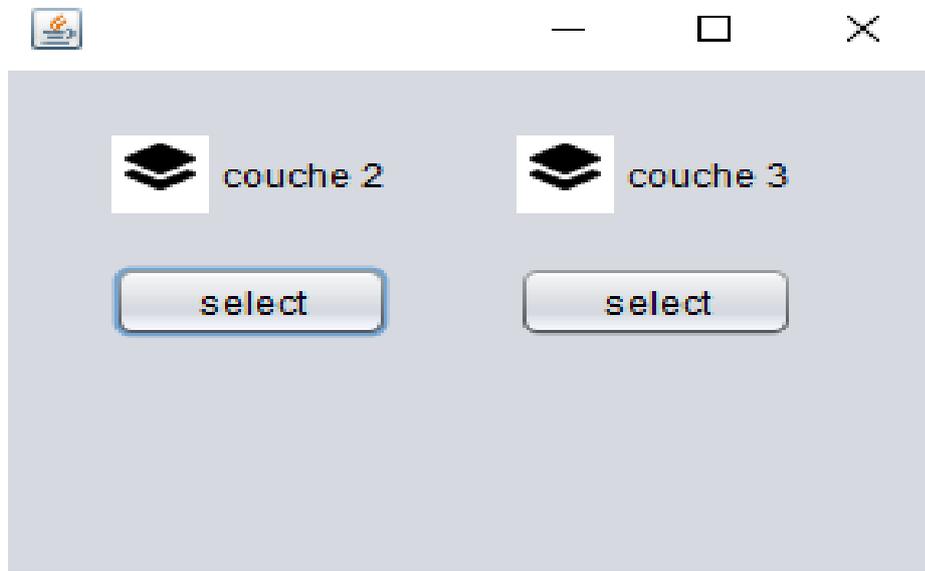


Figure 3-7 : choisir la couche

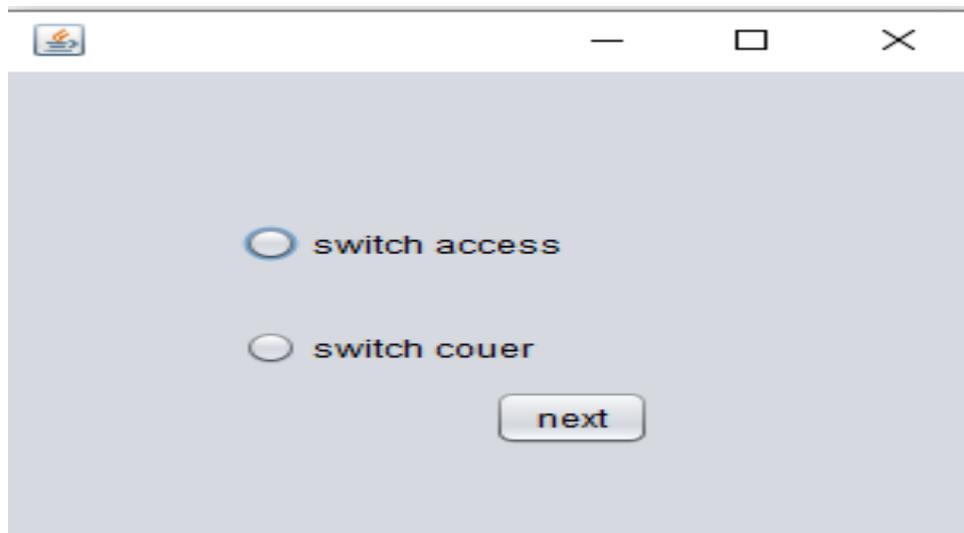


Figure 3-8 : Interface de sign-up

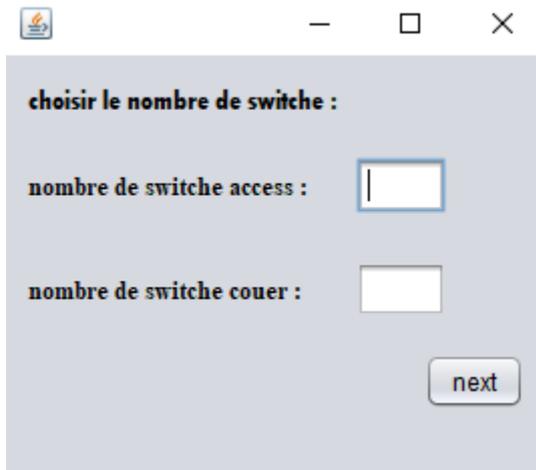


Figure 3-9 : choisir le nombre de switch



Figure 3-10 : creation de vlan



Figure 3-11 : configuration dhcp

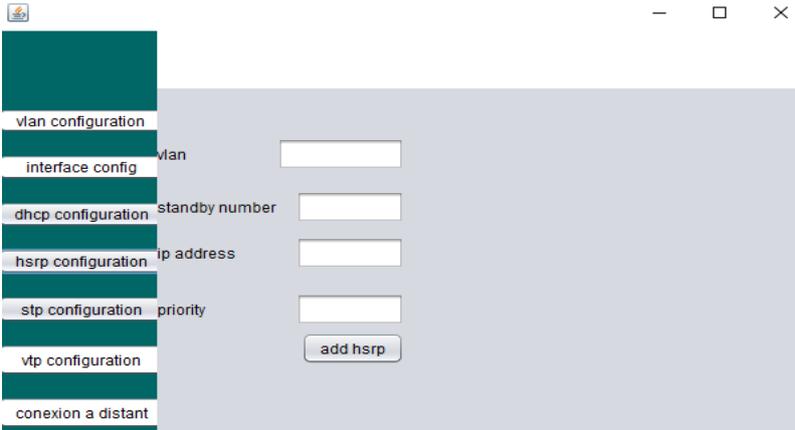


Figure 3-12 : configuration hsrp



Figure 3-13 : configuration des interfaces

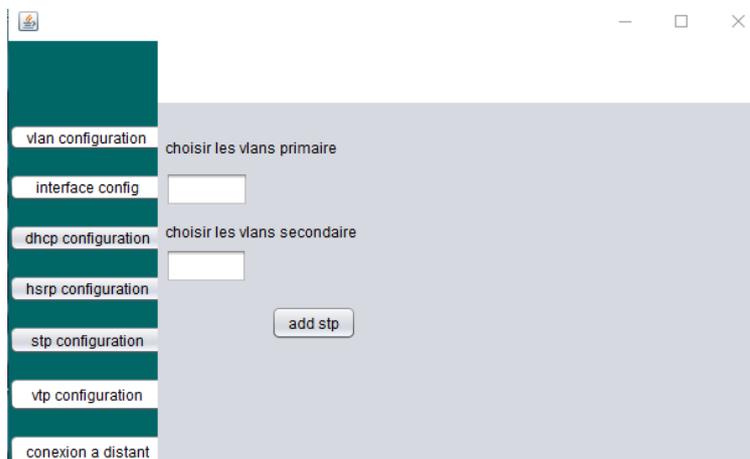


Figure 3-14 : configuration stp

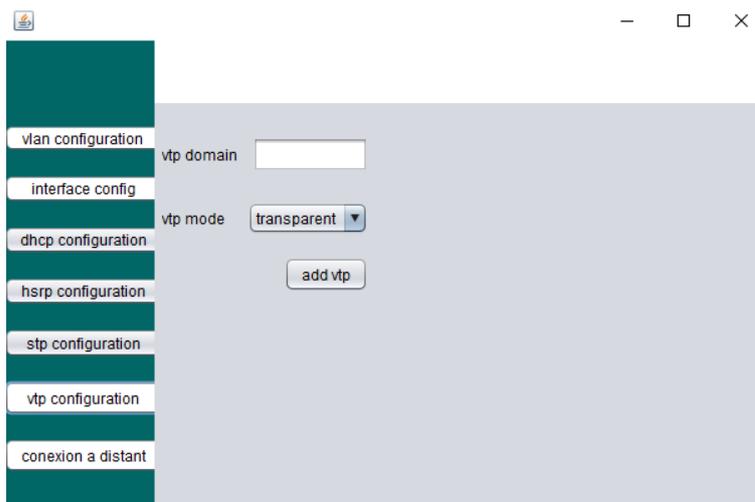


Figure 3-14 : configuration vtp

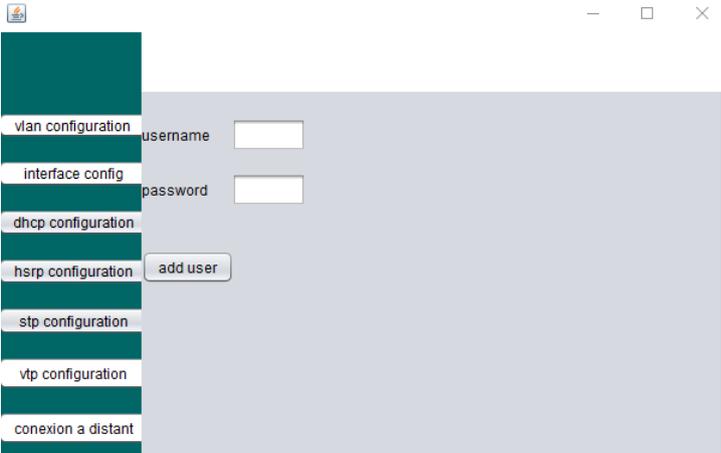


Figure 3-14 : configuration a distant

Conclusion :

Dans ce chapitre, nous avons abordé une description de l'application,

L'application proposée la configuration automatisé d'un switch avec une stratégie contre les attaques de couche 2.

Conclusion générale :

Le réseau est devenu l'épine dorsale qui supporte la transformation digitale de l'entreprise. Sa conception impacte directement la performance des nouveaux usages et des services mis à disposition des collaborateurs et des clients d'une organisation.

La sécurité de cette partie de l'infrastructure de communication est particulièrement délaissée en terme de sécurité et d'audit au profit de l'historique pare-feu.

Dans ce travail on a essayé d'attirer l'attention sur cette question, afin de prendre conscience de l'ampleur des menaces sur le réseau local et à envisager les contre-mesures disponibles et les bonnes pratiques particulièrement sur le matériel Cisco Systems.

La première partie a été consacrée à la conception et la réalisation d'un réseau campus avec ces différentes couches, ensuite on a montré les failles existantes dans la couche 2 et comment sont exploitées par les hackers afin d'attaquer cette partie de l'infrastructure.

Dans la deuxième partie on a présenté comment mettre en place les mesures de sécurité afin de contourner les attaques. Essentiellement la mesure de type Port-Security qui vise à limiter le nombre d'adresses MAC qui peuvent se connecter à un port de commutateur, mais aussi les sécurité Deep ARP Inspection (DAI), DHCP Snooping et autres.

Une stratégie de sécurisation de la couche 2 a été ensuite élaborée, afin de faciliter la tâche aux administrateurs réseaux et de sécurité en mettant à leur profit les étapes à suivre afin d'implémenter cette dernière.

A la fin, on a développé une application qui permet d'automatiser la configuration sécurisée basée sur la stratégie précédente d'un réseau campus. En limitant au maximum l'intervention des administrateurs afin de réduire la surface d'attaque liée à l'erreur humaine.

On espère que notre travail servira comme un guide pour la conception, la configuration et le déploiement d'un réseau campus sécurisé. Et que notre application sera l'outil essentiel pour le réaliser.

Notre travail ouvrira la porte à d'autres projet dans ce domaine, qui est un peu délaissé. Des améliorations peuvent être réalisées sur notre application en l'orientant vers le SDN et les dernières technologies dans le domaine.

Bibliographie

- [1] Architecture des réseaux, danièle dromard et dominique seret ,collection Synthex ,2009, Pearson Education, France.
- [2] Réseaux locaux, par Gerardo RUBINO et Laurent TOUTAIN. Ecole Nationale Supérieure des Télécommunications de Bretagne - Campus de Rennes.
Site web : http://www.resoo.org/docs/reseaux/reseaux_locaux.pdf
- [3] Cisco Networking Academy Connecting Networks Companion Guide : Hierarchical Network Design, By Cisco Networking Academy. Sample Chapter
is provided courtesy of Cisco Press. Date : May 9, 2014. Site web :<https://www.ciscopress.com/articles/article.asp?p=2202410&seqNum=6>
- [4] CCDA200-301 Officialcert guide ANTHONY BRUNO, STEVE JORDAN.
- [5] CCNP and CCIE Enterprise Core ENCOR (350-401) Official Cert Guide,by Brad Edgeworth, Ramiro Garza Rios, David Hucaby,JasonGooley. PartVII : Architecture
- [6] Campus LAN and WirelessLAN Design Guide, January 2018
- [7] Les reseaux, edition EYROLLES,2008.
- [8] Site web : <https://www.sciencedirect.com/topics/computer-science/layer-2-switch>.
- [9] Site web : [9 https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/HA_campus_DG/](https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/HA_campus_DG/).
- [10] Sécurité informatique et réseaux, Solange Ghernaouti, 4ème édition,dunod.
- [11] Introduction à la sécurité informatique, Laurent Poinot, UMR 7030 - Université Paris 13 - Institut Galilée.
- [12] Introduction to cybersecurity 0420 (formation gratuite proposé par cisco)Site web : <https://373583482.netacad.com/courses/1014521>. Date d'inscription: 20/04/2020.
- [13] CEH v10 : EC-Council Certified Ethical Hacker Complete Training Guide with Practice Labs. Document release date : 14/05/2018. Chapitre 1 : introduction to ethical hacking. Site web : <https://www.ethicalhackx.com/cehv10-download/>
- [14] ICSA |CNSS Certified Network Security Specialist (formation gratuite) Site web : <https://www.icsi.co.uk/courses/take/icsi-cnss-certified-networksecurity-specialist-covid-19/texts/11570276-introduction>
- [15] CEH v10 : EC-Council Certified Ethical Hacker Complete Training Guide with Practice Labs. Document release date : 14/05/2018. Chapitre 8 : Snifing. Site web : <https://www.ethicalhackx.com/ceh-v10-download/>.
- [16] <https://www.cisco.com/c/en/us/td/docs/iosxml/ios/snmp/configuration/xr-16/snmp-xr-16-book/nm-snmp-cfgsnmp-support.html>.