SECURISATION D’UN COMMUTATEUR CISCO

Description du thème

|  |  |
| --- | --- |
| **Propriétés** | **Description** |
| **Intitulé long** | Sécuriser un commutateur Cisco Catalyst 2960 contre diverses attaques |
| **Formation(s) concernée(s)** | BTS Services Informatiques aux Organisations |
| **Matière(s)** | Bloc 3 SISR – Cybersécurité des services informatiques |
| **Présentation** | Ce support lié au bloc 3 cybersécurité spécialité SISR a pour but d’appliquer les préconisations de sécurité concernant la configuration d’un commutateur (ici de la marque Cisco modèle Catalyst 2960). A partir de la mission D, l’apprenant va simuler des attaques sur son infrastructure et apprendre à les parer/freiner par l’intermédiaire d’un commutateur. |
| **Compétences** | * Installer et configurer des éléments d’infrastructure (Bloc 2 SISR)
* Installer et configurer des éléments nécessaires pour assurer la continuité des services (Bloc 2 SISR)
* Tester l’intégration et l’acceptation d’une solution d’infrastructure (Bloc 2 SISR)
* Administrer sur site et à distance des éléments d’une infrastructure (Bloc 2 SISR)
* Prendre en compte la sécurité dans un projet de mise en en œuvre d’une solution d’infrastructure (Bloc 3 SISR)
* Mettre en œuvre et vérifier la conformité d’une infrastructure à un référentiel, une norme ou un standard de sécurité (Bloc 3 SISR)
* Prévenir les attaques (Bloc 3 SISR)
* Analyser les incidents de sécurité, proposer et mettre en œuvre des contre-mesures (Bloc 3 SISR)
 |
| **Prérequis** | VLAN, maitrise du CLI IOS Cisco, configuration de base d’un commutateur Cisco, principes d’attaques par saturation d’une table MAC, attaques DHCP par famine ou usurpation du serveur |
| **Outils** | Logiciels PuTTY et Tftpd64, distribution Kali (macof et yersinia) |
| **Mots-clés** | Attaques, commutateur, Kali, IOS, sécurisation, port security |
| **Durée** | 4 à 7 heures |
| **Auteur.e(s)** | Laurent Perrin avec les précieux conseils et les nombreuses relectures de Valérie Martinez et Quentin Demoulière |
| **Version** | v .0 |
| **Date de publication** | 19 décembre 2024 |

Dernières révisions

Ce tableau contient les modifications apportées au document après sa publication uniquement.

|  |  |  |
| --- | --- | --- |
| **Date** | **Auteur.e** | **Description** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

CONTEXTE

Votre responsable souhaite que vous effectuiez des tests sur un commutateur de la marque Cisco, la référence exacte est **Catalyst C2960-24TT-L** *(ou équivalent).*

Dans un compte-rendu d’activité vous indiquerez le contenu de votre plateforme (Noms des équipements, @MAC, @IP, VLAN, …). Ce document reprendra toutes les lignes de commandes tapées ainsi que leur rôle détaillé, cela sera fait en référence pour chaque mission demandée ci-après, il servira de document de référence à votre responsable … et à vous.

*« Les commutateurs sont des équipements réseau très répandus au sein des systèmes d’information. Ils distribuent une grande partie des données qui y transitent. S’ils ne doivent pas être considérés comme des équipements de sécurité, leur rôle est souvent trop négligé dans la mise en place des mesures de sécurisation du SI. Étant donnés leur positionnement et leur rôle dans le SI de l’entité (entreprise, administration, association, etc.), à la fois physiquement proche des utilisateurs pour certains et véhiculant beaucoup d’informations, ils ont potentiellement un impact important sur la sécurité et le fonctionnement du SI (déni de service, écoute du trafic réseau, intrusion dans le SI, etc.). Il convient donc de veiller à les sécuriser du mieux possible afin de renforcer leur robustesse face à des actions malveillantes (venant du SI interne ou de l’extérieur) ou à des erreurs de configuration.*

*…*

*Comme mentionné en préambule, les commutateurs sont des équipements de transit pour une quantité importante d’informations. Il convient donc de porter une attention toute particulière à leur niveau de robustesse face à des attaques venant du réseau. Ces équipements n’ont pas tous le même rôle dans un SI. Afin de bien appréhender les menaces auxquelles ceux-ci sont exposés, il est utile de distinguer les différents types de commutateurs d’un SI selon trois catégories :*

*– les* ***commutateurs de desserte ou d’accès*** *: ce sont les équipements directement reliés aux prises réseau auxquelles se connectent les terminaux du SI (postes bureautique, téléphones IP, etc.) ;*

*– les* ***commutateurs de distribution*** *: ils regroupent le trafic venant des commutateurs de desserte afin de transmettre les données vers les équipements du cœur de réseau comme les commutateurs de cœur de réseau ou les routeurs ;*

*– les* ***commutateurs de cœur de réseau*** *: ils sont directement reliés aux serveurs, aux commutateurs de distribution ou aux routeurs. Ils sont situés généralement au cœur du réseau ou à l’intérieur des centres de données.*

*Ces trois types se différencient principalement par leur contexte d’utilisation, leurs caractéristiques techniques en matière de capacité de traitement et de débit, les types de ports (Ethernet, fibre, etc.)*

*et leur nombre, etc.*

*Le schéma ci-dessous représente un exemple de répartition de ces différents types de commutateurs au sein d’un SI :*



*Figure 1 – Différents types de commutateurs au sein d’un SI*

*… » Extraits de la note technique de l’ANSSI intitulée « Recommandation pour la sécurisation d’un commutateur de desserte ».*

PLATEFORME NECESSAIRE

**Au niveau matériel et logiciel**

2 ordinateurs fixes + 1 ordinateur portable SISR (portable pour bien simuler l’attaquant mobile 😉)

1 commutateur Cisco Catalyst 2960

Le logiciel TFTPD64

Le logiciel PuTTY ou équivalent

1 DVD Kali, ou 1 clef USB Kali créée par Etcher par exemple ou une machine virtuelle Kali en mode bridge

Pour information, un mémo CLI IOS Cisco et un mémo utilitaire YERSINIA se trouvent en fin de ce support

**Au niveau référence et préconisation de configuration**

La note technique de l’ANSSI intitulée « Recommandation pour la sécurisation d’un commutateur de desserte » servira de guide tout au long de la sécurisation de l’équipement. Chaque extrait de cette note sera encadré et abrégé par la suite par *NT ANSSI.*

MISSION A : existant du commutateur (RAPPEL)

Pour la suite de ce TP, nous avons un commutateur réinitialisé et ne possédant aucun VLAN sauf ceux présents après réinitialisation.

Qu’est-ce qui vous indique que ce commutateur a été réinitialisé et ne contient pas de fichier startup-config ?

**Votre réponse :**

MISSION B : CONFIGURATION DE VLAN

*NT ANSSI : « Comme tout équipement réseau déployé dans un SI, l’administration des commutateurs doit se faire en respectant un certain nombre de recommandations de sécurité détaillées dans la note technique [Admin SI] de l’ANSSI relative à l’administration sécurisée des SI.*

***Réseau d’administration out-of-band***

*Pour des questions de sécurité, il est conseillé de mettre en place un réseau dédié aux flux d’administration des équipements du SI (hors terminaux), distinct des réseaux de données utilisés par les services métier.*

***Port physique dédié***

*Il est préférable d’utiliser un port physique dédié à l’administration d’un commutateur lorsque cela est possible afin de ne pas mélanger les flux de gestion et les flux métier. Cette pratique paraît d’autant plus aisée à réaliser que les commutateurs disposent en général d’un nombre important de*

*ports physiques.*

*…*

***Réseau dédié***

*Afin de procéder à une séparation entre le réseau d’administration du commutateur et les autres réseaux, plusieurs techniques peuvent être mises en œuvre. La méthode idéale consiste à utiliser un réseau physique dédié. Cependant, si cela n’est pas possible, l’utilisation d’un VLAN dédié à l’administration peut être une solution acceptable, mais elle dégrade le niveau de sécurité en comparaison de la première solution.*

*Préconisation : Mettre en place une séparation physique entre les réseaux d’administration et les réseaux métier.*

*Préconisation : Au minimum, prévoir un cloisonnement logique utilisant des VLAN pour appliquer cette séparation.*

*…*

***Limitation de l’accès à l’interface d’administration***

*Il est possible d’attribuer plusieurs adresses IP à un commutateur. Néanmoins, ceci n’est pas nécessaire et peut causer des problèmes de sécurité, comme par exemple exposer l’interface d’administration du commutateur aux postes bureautiques. Il faut donc veiller à ne configurer qu’une seule adresse IP répondant aux seuls besoins d’administration de l’équipement, réduisant ainsi sa surface d’attaque.*

*Préconisation : Un commutateur ne doit disposer que d’une seule adresse IP dédiée à son administration.*

*…*

***Configuration des VLAN***

*Un commutateur gère l’attribution des VLAN par port ; ces ports peuvent être configurés dans l’un des deux modes suivants :*

*– mode access : le port est directement connecté à un terminal (poste bureautique, imprimante, téléphone IP, etc.). Les trames Ethernet en provenance ou à destination de ces équipements ne sont pas marquées sur ce type de port ;*

*– mode trunk : le port est utilisé pour interconnecter le commutateur à tout autre équipement compatible avec la norme 802.1Q. Les trames Ethernet en provenance ou à destination de ces équipements sont marquées sur ce type de port à l’exception du VLAN natif qui n’est généralement pas marqué, notamment car certains équipements ne le supportent pas.*

*Chacun de ces deux modes a des particularités de configuration.*

***Ports en mode access***

*Par défaut, certains commutateurs basculent automatiquement un port du mode access au mode trunk lorsqu’un port en mode trunk est détecté de l’autre côté du câble. Même si cette fonction peut*

*paraître utile, elle nuit à la sécurité du réseau. En effet, une attaque consistant à faire passer l’attaquant pour un commutateur (Switch Spoofing) en simulant un port en mode trunk peut permettre à celui-ci de capter tout le trafic passant par le commutateur. Le fait de forcer les ports à être en mode access protège le commutateur contre l’attaque du Switch Spoofing.*

*…*

***VLAN par défaut et VLAN natif***

*Ces deux VLAN sont particuliers, il est indispensable de bien comprendre leur rôle afin d’appréhender les risques associés à leur mauvaise configuration :*

*– le VLAN par défaut est celui dans lequel les interfaces sont placées par défaut tant qu’elles n’ont été attribuées à aucun VLAN. En configuration par défaut, c’est généralement le VLAN 1 ;*

*– le VLAN natif est utilisé par les commutateurs pour s’échanger des informations nécessaires au fonctionnement de certains services qu’ils offrent dont STP, CDP et VTP. Ce VLAN a pour particularité de circuler non marqué (au sens 802.1Q) sur les liens trunk. Ainsi, toute trame Ethernet entrante non marquée sur un port trunk du commutateur sera automatiquement associée par celui-ci au VLAN natif.*

*Une mauvaise configuration du VLAN natif sur les commutateurs peut avoir plusieurs impacts sur*

*la sécurité du SI :*

*– en configuration par défaut de l’équipement, les ports non configurés sont associés au VLAN par défaut (VLAN 1). Or ce VLAN est également, en configuration par défaut, le VLAN natif.*

*Ainsi, le terminal se connectant à l’un de ces ports à accès à tout le trafic circulant sur le VLAN natif et peut donc attaquer en disponibilité certains services utilisant le VLAN natif et in fine perturber le fonctionnement du commutateur ;*

*– si des commutateurs d’un même domaine de diffusion sont configurés avec comme VLAN natif des numéros de VLAN différents, un phénomène de saut de VLAN peut se produire de manière permanente au niveau d’un port trunk ;*

*– si un attaquant connecté à un port trunk du commutateur envoie une trame marquée deux fois avec comme premier marquage visible le numéro du VLAN natif et comme second marquage le VLAN de destination du paquet, un saut de VLAN peut se produire. Cependant, si cette attaque réussit, seul un sens de communication fonctionne, il n’y a pas de retour.*

*Ces particularités impliquent de mettre en œuvre les recommandations énoncées ci-dessous :*

*Préconisation : Le VLAN par défaut ne doit jamais être utilisé.*

*Préconisation : Le VLAN natif :*

*– doit être configuré afin d’être différent du VLAN par défaut ;*

*– ne doit être attribué à aucun port en mode access (il ne doit pas être utilisé pour faire circuler du trafic métier ou d’administration ;*

*– doit être le même sur tous les commutateurs du même domaine de diffusion (et de préférence dans tout le système d’information par principe d’homogénéité) afin d’éviter les comportements inadéquats.»*

Vous allez devoir suivre les bonnes pratiques préconisées par Cisco (et par l’ANSSI) en créant un **VLAN d’administration** de l’infrastructure différent du VLAN par défaut (id VLAN 1).

Le VLAN 99 qui portera le nom de « **ADMINISTRATIONINFRA** ». Le **VLAN 99** appartiendra au réseau IP **192.168.99.0/24**, vous affecterez un peu plus tard dans ce support la première adresse IP à votre commutateur (plus précisément à son VLAN 99).

Les ports **1 à 6** appartiendront à ce nouveau **VLAN d’administration de l’infrastructure réseau**

Pourquoi ne pas utiliser le VLAN 1 comme VLAN d’administration de l’infrastructure ?

**Votre réponse :**

**Vos commandes CLI**(pour créer le VLAN 99, affecter les ports demandés dans ce VLAN et vérifier le résultat) :

Pour la suite, vos branchements PC fixes / commutateur devront permettre à vos deux PC de communiquer entre eux via le VLAN 50 de données que nous nommerons « **PRODUCTION**». Vous affecterez **la dixième et la onzième adresse IP affectable du réseau du VLAN 50 à vos deux PC fixes pour la suite en sachant que le réseau IP concerné sera le 192.168.50.0/24**. Les ports Fa0/7 à Fa0/12 seront affectés à ce VLAN de production. Vérifier que la communication entre vos deux PC fonctionne bien correctement au sein de ce VLAN de production.

**Vos commande CLI :**

MISSION C : SECURISATION DU COMMUTATEUR AU NIVEAU DE SON ADMINISTRATION

*NT ANSSI : «****Ethernet (VTY - ligne virtuelle) :*** *Les lignes virtuelles sont généralement utilisées pour accéder à distance aux commutateurs en SSH. Le protocole Telnet est encore utilisé sur les équipements obsolètes, mais pour des raisons de sécurité détaillées plus loin, il est à proscrire dès qu’un commutateur supporte SSH.*

***SSH :*** *SSH est un protocole sécurisé d’accès à distance à l’interface en ligne de commande l’équipements. C’est un protocole éprouvé d’administration à distance des équipements. Il existe deux versions du protocole, à savoir les versions 1 et 2. Seule la version 2 est recommandée, la version 1 étant sujette à une faille protocolaire connue et facilement exploitable par une personne malveillante.*

*Préconisation : Utiliser le protocole SSH en version 2 pour l’administration à distance des commutateurs.*

*…*

***Telnet*** *est un protocole non sécurisé permettant l’accès à distance à des équipements. Étant donné que toutes les informations sont envoyées en clair sur le réseau, notamment le mot de passe de l’administrateur (sauf si Telnet est couplé à d’autres mécanismes de sécurité), ce protocole est à proscrire sur les matériels supportant des protocoles d’administration sécurisés comme SSH.*

*Préconisation : Ne pas utiliser le protocole Telnet pour l’administration à distance des commutateurs lorsque des protocoles plus sécurisés sont supportés par l’équipement.*

*Préconisation : Si Telnet doit être utilisé du fait de l’absence de protocoles sécurisés, mettre en place les moyens adéquats de sécurisation du réseau sur lequel vont transiter ces flux.*

*…*

*La fonctionnalité de chiffrement des mots de passe contenus dans le fichier de configuration du commutateur permet de les masquer aux personnes indiscrètes.*

*Pour les commutateurs Cisco, cette fonctionnalité ne concerne pas la commande username (utilisée*

*pour créer des comptes locaux) si l’attribut secret est utilisé (qui offre une meilleure robustesse : Le mot de passe étant haché, il est toujours possible pour un attaquant de tenter de retrouver le mot de passe en procédant à une attaque par dictionnaire), mais s’applique aux autres secrets stockés (par exemple RADIUS ou TACACS+) dans le fichier de configuration. Cependant, étant donné que cette fonction utilise un chiffrement faible, elle ne protège pas efficacement les mots de passe contre des personnes malintentionnées qui possèderaient ces fichiers et souhaiteraient retrouver les mots de passe contenus. En effet, le chiffrement est facilement réversible et de nombreux outils disponibles sur Internet permettent de déchiffrer ces mots de passe quasi instantanément.*

*Pour les commutateurs HP, le mécanisme équivalent consiste à masquer les mots de passe lors de*

*leur affichage sur l’écran de l’administrateur ainsi que dans le fichier de configuration du commutateur.*

*Préconisation : Activer le chiffrement des mots de passe contenus dans le fichier de configuration.»*

Est-ce que votre commutateur accepte la prise en charge des fonctionnalités de cryptographie (chiffrement) ? Expliquez votre raisonnement (lire ressources).

**Votre réponse :**

Est-ce que votre commutateur prend en charge les versions 1 et 2 du protocole SSH par défaut ?

*Si vous voyez apparaitre version « 1.99 », cela signifie que les versions 1 et 2 sont prises en charge sur l’équipement*

**Votre réponse :**

Votre responsable vous demande d’effectuer les étapes suivantes pour sécuriser et autoriser la prise en main à distance sur ce commutateur via ssh version 2.

- Nommer le commutateur de la même manière que ce qui est écrit sur son étiquette en façade.

**Vos commandes CLI :**

- Effacer la paire de clefs RSA existantes (au cas où)

**Vos commandes CLI :**

- Configurer le domaine (**domainehsh.coop**), ce domaine va apparaitre

**Vos commandes CLI :**

- Générer une **paire de clefs RSA**. (Longueur de **2048 bits**)

La génération prendra moins d’une minute.

**Vos commandes CLI :**

- Configurer l’authentification utilisateur avec les couples suivants :

admin1/password1

**Vos commandes CLI :**

- Configurer toutes les lignes vty pour du ssh uniquement et une authentification locale

**Vos commandes CLI :**

- Activer uniquement la version 2 du protocole SSH et vérifier cette prise en compte.

**Vos commandes CLI :**

Avant de poursuivre, installer le client PuTTY version Windows 64 bits (gratuit) mis à votre disposition par l’enseignant sur un des PC en pensant également à le connecter au VLAN d’administration de l’infrastructure et en lui affectant temporairement l’adresse IP 192.168.**99**.10/24.

Il faudra également affecter l’adresse IP 192.168.99.1/24 à l’interface VLAN 99 du commutateur de manière à ce qu’il soit joignable via le réseau.

**Vos commandes CLI :**

Essayez de vous connecter à votre commutateur via PuTTY **en utilisant Telnet**, quel port TCP est utilisé par le commutateur lorsque vous tentez la connexion depuis PuTTY ?

**Constat de votre test :**

Essayez de vous connecter à votre commutateur via PuTTY **en utilisant ssh** et le compte **admin1**, quel port TCP est utilisé par le commutateur lorsque vous tentez une connexion SSH par défaut depuis PuTTY ? Essayer ensuite de taper la commande « **enable** », que se passe-t-il ? Pourquoi ?

**Constat de votre test :**

Comment pourriez-vous faire pour que nous puissions passer en mode privilégié sur cet équipement tout en faisant une administration à distance via SSH ?

**Vos commandes CLI :**

Vérifier tout en restant connecté en ssh, par une commande CLI IOS, les connexions SSH actives

**Vos commandes CLI :**

*NT ANSSI : « De nombreux modèles de commutateur embarquent un serveur HTTP offrant aux administrateurs réseau la possibilité de configurer ces équipements via une interface web. Même si cette fonctionnalité permet de configurer un commutateur sans avoir recours à l’interface en ligne de commandes, cette dernière se révèle plus adaptée à une gestion industrialisée des parcs de commutateurs. De plus, la présence d’un serveur web augmente la surface d’attaque de l’équipement et peut nuire à ses performances, il est donc recommandé de le désactiver.*

*Préconisation : Désactiver le serveur web de gestion du commutateur, que ce soit en version sécurisée (HTTPS) ou non (HTTP). »*

Pour ce qui concerne cet équipement Cisco, nous n’utiliserons jamais le service web (ni http et ni https), il est donc judicieux de les désactiver si ce n’est pas déjà le cas.

**Vos commandes CLI :**

ATTENTION : Avant de poursuivre remettre la configuration IP de votre PC sans oublier de le rebrancher à son VLAN de production.



**ATTENTION :** EFFECTUER UN « *COPY RUN START »* OU UN « WRITE » AVANT DE POURSUIVRE

MISSION D : TEST INONDATION MAC ET CONFIGURATION D’ATTENUATION

Pour cette mission, vous allez utiliser les 2 ordinateurs fixes situés dans un VLAN 50 PRODUCTION et un troisième ordinateur (fixe ou portable), celui de l’attaquant qui utilisera la distribution Kali.

Ce troisième ordinateur utilisera la distribution Kali

* soit **sans installation** sur disque dur **UNIQUEMENT en version live** *(choix pris pour la suite du support)*
* soit une machine virtuelle disposant d’un système Kali installé de façon définitive configurée en mode bridge.

Votre responsable veut voir l’attaque par inondation MAC (**MAC flooding**) fonctionner et voir comment vous allez l’atténuer/la contrer en sécurisant le commutateur. Pour cela, vous procéderez par étape en prenant bien note des différentes manipulations que vous réaliserez (impressions d’écran des commandes et des résultats affichés à intégrer dans votre compte rendu d’activité).

Brancher le PC Kali sur le même VLAN que les deux autres PC (le 50) avant de poursuivre.



**ATTENTION,** **ne pas installer Kali** sur le disque dur du portable, utiliser seulement la version live. Pour cela, après avoir booté sur le support USB, au menu de démarrage de Kali choisir le premier choix nommé « **Live system (amd64)** », c’est celui par défaut

Le démarrage de l’OS est un peu long, mais vous devriez voir apparaitre des icônes et un bureau graphique.

Informations utiles pour la suite :

* Le clavier par défaut sur Kali est en QWERTY, pour le passer en Azerty français, il faut taper la commande ***setxkbmap fr (au clavier qwerty : setxkb,qp fr)***
* Le **compte root de Kali** a pour mot de passe **kali (**avec le clavier qwerty : **kqli)**
* **Wireshark** est déjà présent dans Kali. Un filtre sur le bon protocole pourra être utile (quel est le protocole du ping ?), penser à sélectionner **eth0** avant de lancer une capture sinon le logiciel ne voudra rien capturer.
* **macof** est un utilitaire permettant, entre autres, de créer une attaque de type **inondation MAC**, la commande simpliste **macof -i eth0** permet de lancer l’attaque (avec **sudo**).

*NT ANSSI : «****Sécurisation des ports***

*Dans une entité, les commutateurs de desserte sont la principale porte d’entrée du SI depuis l’intérieur. Les prises réseau disséminées dans les locaux sont en effet directement connectées à ces commutateurs et le personnel, voire les visiteurs, y ont physiquement accès. Leur sécurisation joue donc un rôle essentiel dans le contrôle d’accès au SI de l’entité. Parmi les bonnes pratiques de contrôle d’accès, la plus efficace pour se protéger contre les intrusions est de désactiver tous les ports des commutateurs qui ne sont pas censés être utilisés. Ainsi, en prenant l’exemple des prises réseau des bureaux vacants, celles-ci ne pourront pas être utilisées par des personnes malveillantes.*

*Préconisation : Désactiver les ports inutilisés sur les commutateurs.*

*…*

*les deux solutions sont en partie redondantes et doivent donc être utilisées de façon exclusive, tout en privilégiant 802.1X.*

*Préconisation : Sécuriser l’accès aux ports des commutateurs en utilisant 802.1X.*

*Préconisation : S’il n’est pas possible de mettre en place 802.1X, utiliser port security.*

*…*

*Port security permet de limiter le nombre d’adresses MAC connectées à une même interface d’accès»*

Ce support n’abordera pas la mise en place du 802.1X, la solution choisie sera donc celle du port security.

**Etape 1 :** Vérifiez que dans un fonctionnement normal du commutateur, un échange unicast (ping par exemple) du PC1 au PC2 ne peut pas être capturé par le portable du « pirate » (distribution Kali). Vous utiliserez également la commande IOS ***show mac address-table count*** (vous expliquerez le résultat). Dans le compte-rendu d’activité destiné à votre responsable, vous expliquerez bien pourquoi le pirate ne peut pas capturer le trafic allant du PC1 au PC2 en expliquant clairement le fonctionnement d’un commutateur.

**Votre réponse :**

**Etape 2 :** Lancer l’attaque de type inondation MAC et vérifier son bon fonctionnement en regardant l’état du compteur de la table MAC du commutateur. Effectuer une capture de trames depuis le portable Kali et démontrer par une sauvegarde de la capture que le portable Kali peut désormais capturer un flux unicast prévu uniquement entre le PC 1 et le PC2, cette capture sera déposée en annexe de votre compte rendu comme preuve.

**ATTENTION :** la capture de trames unicast ne peut fonctionner que si les adresses MAC des PC1 et PC2 ne sont pas déjà présents dans la table CAM au moment de l’attaque. Pour cela :

- débrancher les 2 PC du commutateur

- vider la table d’adresse MAC (CAM) du commutateur

- lancer l’attaque à l’aide de la commande **sudo** **macof -i eth0**

- brancher ensuite les 2 PC

- lancer Wireshark et une capture depuis Kali

- faire un ping du PC1 vers le PC2

- taper la commande **sh mac address-table count** pour constater le résultat de l’attaque sur le commutateur

- arrêter l’attaque

- Déduire la différence de fonctionnement du commutateur en analysant les captures du PC pirate

**Votre réponse :**

***Etape 3 :*** *Appeler votre enseignant pour faire un bilan.*

**Etape 4 :** Rédiger, dans un compte-rendu d’activité, une explication sur le fait que le portable Kali peut capturer un flux unicast issu de l’échange entre le PC1 et le PC2. Indiquer également le principe des attaques de type **MAC flooding**.

**Votre mail :**

**Etape 5 :** Effectuer une sécurisation du commutateur pour éviter que ce type d’attaque fonctionne à l’avenir sur les ports du VLAN 50. Limiter le nombre d’adresses MAC à 10 pour chaque port du VLAN 50. Une notification devra avoir lieu mais le port devra rester actif en ignorant les nouvelles adresses MAC. Les adresses MAC seront enregistrées de manière rémanente (permanente *sticky*).

**Etape 6 :** Refaire un test d’attaque sur un des ports fraîchement sécurisé. Après avoir constaté la sécurisation du port concerné, vérifier si le compteur reprend sa valeur initiale, expliquer la réponse et proposer une solution pour y remédier.

***Etape 7 :*** *Appeler l’enseignant pour faire un bilan.*

**Vos commandes CLI et vos tests de validation :**

MISSION E : TEST USURPATION DHCP ET CONFIGURATION D’ATTÉNUATION

**ATTENTION :** Avant de poursuivre, nous débrancherons puis rebrancherons notre commutateur sans faire de sauvegarde de cette précédente partie sécurisation des ports.

*NT ANSSI :* « ***DHCP snooping et IP Source Guard***

*Le protocole DHCP permet d’attribuer et de configurer dynamiquement les adresses IP (et d’autres*

*informations comme la passerelle par défaut, le serveur DNS, etc.) des terminaux se connectant au réseau. Le DHCP snooping et l’IP Source Guard sont des fonctionnalités qui protègent le commutateur contre diverses attaques portant sur ce protocole. En effet, le protocole présente, de par sa conception, des faiblesses utilisables par des attaquants pour perturber le trafic réseau ou usurper des adresses IP. La machine d’un attaquant se faisant passer pour un serveur DHCP ou encore générant du trafic en se faisant passer pour un autre terminal (IP spoofing) sont les deux méthodes d’attaque les plus courantes. Parmi les contre-mesures existantes, les plus éprouvées sont :*

*le DHCP snooping, consistant à :*

*– déclarer des ports de confiance identifiés comme les seuls par lesquels peuvent provenir des*

*baux DHCP,*

*– maintenir une table d’association DHCP au sein du commutateur (appelée table DHCP snooping) afin qu’il conserve en temps-réel l’état du bail DHCP de tous les terminaux qui lui sont connectés,*

*– limiter le nombre de requêtes DHCP par seconde sur une interface,*

*– l’IP Source Guard, consistant à vérifier la cohérence entre les adresses IP utilisées par les terminaux connectés au commutateur et les données contenues dans la table DHCP snooping, afin d’empêcher l’IP spoofing.*

*Préconisation : Activer les fonctions de DHCP snooping et d’IP Source Guard afin de pallier les faiblesses de sécurité du protocole DHCP. »*

Nous utiliserons le VLAN 50 pour faire les tests DHCP, nous utiliserons la plage de test suivante : **192.168.50.0/24**. Le PC1 en adressage statique gardera l’adresses IP **192.168.50.10/24**, il va se nommer **serveur DHCP** pour la suite. Le PC2 va passer en **client DHCP** (adressage IP dynamique)

Les connexions filaires seront les suivantes : le **PC 1** **serveur DHCP** sera sur le port **fa0/7** (VLAN 50), le PC2 **client DHCP** sur le port **fa0/9** (VLAN 50) et le portable **Kali** (ou la VM Kali) sera sur le **fa0/11** (VLAN 50).



Sur le poste **PC2 client DHCP**

* Passer la configuration IP en dynamique

Sur le poste **PC1 serveur DHCP**

Installer et lancer l’applicatif **TFTPD64** pour qu’il propose le **service DHCP** sur le PC nommé serveur DHCP. Vous mettrez l’autre PC Labo fixe en **client DHCP**.

Avant de poursuivre, vous devez trouver comment fonctionne TFTPD64 pour que :

* **Seul le service DHCP** sera activé sur l’applicatif
* La plage DHCP soit la suivante [**192.168.50.100 ; 192.168.50.119**]

Vous devriez obtenir les fenêtres suivantes :



Tester que le service DHCP fonctionne correctement.

Rappel : Un client DHCP peut relancer son processus de demande DHCP en tapant les commandes **ipconfig /release**, ensuite **ipconfig** pour vérifier la perte du paramétrage dynamique puis **ipconfig /renew** pour lancer une nouvelle demande de bail DHCP

Faire un test normal de distribution d’adresse IP du serveur DHCP au client DHCP sans lancer d’attaque. Vous devriez voir **une distribution d’adresse IP** comme l’indique la fenêtre ci-après sur votre serveur DHCP.



Supprimer depuis le serveur DHCP le bail distribué au client DHCP de manière à rendre la plage DHCP complètement libre, l’autre étant celui de Kali, il peut rester. Déconnecter temporairement le client DHCP.

À l’aide de l’utilitaire **yersinia** et de son mémo se trouvant à la fin de ce support, en premier choisir le protocole concerné par l’attaque souhaitée puis lancer une attaque DHCP (type **sending DISCOVER packet** dans le menu de l’utilitaire).

**Remarque** : sur la version Kali 2024.3 live, yersinia n’est pas installé par défaut. Il faudra donc connecter temporairement votre équipement Kali à un réseau avec DHCP et accès Internet. Vous pouvez utiliser la commande suivante pour installer yersinia :

*sudo apt-get update && sudo apt-get install yersinia*

Observer sur votre serveur DHCP, qu’en quelques secondes, les adresses IP disponibles dans la plage du serveur DHCP vont être épuisées. Essayer de rebrancher le client DHCP, il ne devrait plus pouvoir obtenir d’adresse IP du serveur DHCP (*famine DHCP*).

**Votre capture d’écran qui démontre la saturation du serveur DHCP :**

Supprimer, l’un après l’autre, les baux présents sur le serveur DHCP de manière à rendre la plage DHCP de nouveau complètement libre.

Expliquez, dans votre compte-rendu, l’attaque DHCP Starvation en fournissant une capture de trames significative permettant de représenter le fonctionnement de cette dernière.

Paramétrer votre commutateur pour que cette attaque ne puisse plus se reproduire avec autant d’ampleur, nous nous limiterons au VLAN 50 de production. D’après les recherches de votre responsable, la commande Cisco **ip dhcp snooping** peut vous aider dans cette tâche de sécurisation.

Sur les ports du vlan 50 (fa 0/7 - 12), configurer ces derniers pour que le nombre de demande d’adresses IP dynamiques soit limité à 3 (3 demandes sur une période d’une seconde)

**Votre proposition (à montrer pour validation à votre enseignant avant de poursuivre)**

Mettre en place votre configuration, tester sa sécurisation en relançant l’attaque de saturation du serveur DHCP et **intégrer vos impressions d’écran dans le compte-rendu d’activité**

**Vos commandes CLI :**

Nous allons à présent lutter contre l’autre attaque classique contre un service DHCP, celle qui utilise un serveur DHCP fictif/fantôme (***usurpation de DHCP***). Pour cela nous allons garder un seul serveur DHCP mais il sera officiel s’il est branché au port fa0/7 et non officiel s’il est sur un autre port du commutateur.

**Expliquez à votre enseignant** ce que vous allez taper comme commandes avant de vous lancer dans cette configuration … à moins que ce ne soit déjà fait.

**Votre proposition de commandes :**

Réinitialiser les paramétrages du commutateur puis redémarrer le pour vérifier que cela a bien été pris en compte.

MEMO CLI IOS CISCO

***# Création du VLAN 30 avec l’adresse IP 172.16.10.10 et le descriptif GESTION***

Switch(config)# interface vlan 30

Switch(config-if)# ip address 172.16.10.10

Switch(config-if)# name GESTION

***# Afficher les VLAN créés et leurs ports rattachés***

Switch# show vlan

***# Affecter les ports 3, 4 et 5 dans le VLAN 30***

Switch(config)# interface range fa0/3 - 5

Switch(config)# switchport mode access

Switch(config)# switchport access vlan 30

***# Afficher les versions logicielles du commutateur (boot loader et IOS)***

***# Si le nom de l’IOS contient « k9 », cela indique la prise en charge des fonctionnalités et des capacités de chiffrement.***

Switch# show version

***# Définir le port 24 comme trunk (802.1Q) en désactivant les négociations DTP et en mettant le VLAN 10 en VLAN natif***

Switch(config)# interface fa0/24

Switch(config-if)# switchport mode trunk

Switch(config-if)# switchport nonegotiate

Switch(config-if)# switchport trunk native vlan 10

Switch(config-if)# end

***# Afficher l’état du service SSH ainsi que les versions disponibles***

Switch> show ip ssh

***# Procédure pour obtenir une connexion distante sécurisée au commutateur via ssh. On s’appuiera sur une paire de clef RSA nommé ssh-rsa-keypair (de longueur 2048 bits)***

Switch(config)# hostname COMM69

COMM69(config)# crypto key zeroize rsa *//pour effacer la paire de clefs RSA existantes*

COMM69(config)# ip domain-name domaineentrep.fr

COMM69(config)# crypto key generate rsa

COMM69(config)# username fdidier [privilege 15] secret fgh#15dFR

*La valeur 15 indique le niveau de privilège maximum attribué à l’utilisateur (*[*pour en savoir plus*](https://learningnetwork.cisco.com/s/blogs/a0D3i000002eeWTEAY/cisco-ios-privilege-levels)*)*

COMM69(config)# line vty 0 15

COMM69(config-line)# transport input ssh

COMM69(config-line)# login local

**# Afficher les connexions SSH actives**

Switch> show ssh

***# Activer uniquement la version 2 du protocole SSH***

Switch(config)# ip ssh version 2

***# Imposer un mot de passe pour accéder au mode privilégié (enable), ce dernier sera stocké en******clair dans le fichier de configuration***

Switch(config)# enable password FGh25@dd?

***# Imposer un mot de passe pour accéder au mode privilégié (enable), ce dernier sera stocké******sous forme de hashage MD5 dans le fichier de configuration***

Switch(config)# enable secret FGh25@dd?

***#Afficher le statut du serveur web HTTP/HTTPS***

Switch> show ip http server status

***#Activer/désactiver le*** ***serveur web HTTP/HTTPS***

Switch(config)# [no] ip http server

Switch(config)# [no] ip http secure-server

***# Vider le cache (adresses MAC) du commutateur***

Switch# clear mac address-table dynamic

***# Limiter le nombre d’adresses MAC à 20 pour les ports 3, 4 et 5 du VLAN 30***

Switch(config)# interface range fa0/3 - 5

Switch(config-if-range)# switchport mode access

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

Switch(config-if-range)# switchport port-security violation restrict

Switch(config-if-range)# switchport port-security maximum 20

Switch(config-if-range)# switchport port-security mac-address sticky

***# Configurer le port 10 pour que le nombre de demande d’adresses IP dynamiques soit limité à 3 en une seconde***

Switch(config)# ip dhcp snooping

Switch(config)# ip dhcp snooping vlan 4

Switch(config)# interface fastethernet 0/10

Switch(config-if)# ip dhcp snooping limit rate 3

***# Autoriser le port lié au serveur DHCP***

Switch(config)# interface fastethernet 0/20

Switch(config-if)# ip dhcp snooping trust

***# Réactiver un port bloqué (si violation de type restrict)***

Switch(config-if)# shutdown

Switch(config-if)# no shutdown

MEMO UTILITAIRE YERSINIA

***Avant de lancer yersinia, passer votre fenêtre en pleine écran***

***# Lancement de la console texte interactive (l’option est un i majuscule)***

yersinia -I

**#Touches utiles pour utiliser yersinia**

g : pour choisir le protocole concerné par l’attaque souhaitée

x : pour lancer une attaque

l : pour lister les attaques en cours

K : pour arrêter les attaques en cours

