Institut Universitaire de Technologie,
Aix-Marseille Université

RAPPORT DE STAGE de fin de deuxième année
Bachelor Universitaire de Technologie
Spécialité Réseaux et Télécommunications
parcours cybersécurité

Expérience Professionnelle en Réseaux et Cybersécurité

Ethan AMEVET

REGION SUD

Responsable entreprise : Emmanuelle ROME

Responsable académique : Rabah IGUERNAISSI

2023

Table des matières

1 Introduction

J'ai effectué un stage de 10 semaines au sein des équipes de la direction des systèmes d'informations de la Région SUD. Les deux équipes sont composés d'un total d'une douzaine d'agents responsables de la sécurité et de la maintenance du parc informatique.

L'objectif de mon stage était de découvrir le monde professionnel et d'acquérir des compétences techniques et de savoir-être en réseaux et en cybersécurité. Mon travail comprenait la création et le déploiement d'un projet de gestionnaire de mots de passe ainsi que de diverses missions initiatiques dans ces domaines.

Ce rapport présente d'abord le projet de gestionnaire de mots de passe, puis les missions réalisées dans les domaines du réseau et de la cybersécurité, et se termine par une réflexion personnelle sur cette expérience. Se trouvent dans l'annexe des informations complémentaire afin de afin de fournir des détails techniques et contextuels supplémentaires.

1.1 Présentation de la Région SUD

La Région Provence-Alpes-Côte d'Azur

Erigée en collectivité territoriale par la loi de décentralisation de 1982, la Région Provence-Alpes-Côte d'Azur est une des 13 régions françaises métropolitaines (avec la collectivité territoriale unique de Corse).
Le périmètre géographique de la Région correspond à celui des 6 départements suivant : Bouches-du-Rhône, Var, Alpes-Maritimes, Vaucluse, Alpes de Haute-Provence et Hautes-Alpes.

Le budget de la Région s'élève à 3,2 milliards d'euros (budget primitif 2024), dont 1,0 milliard de dépenses d'investissement.

Comme les autres régions françaises, la Région Provence-Alpes-Côte d'Azur exerce les compétences qui lui ont été transférées par la loi, en matière de transports collectifs (transport régional de voyageurs, transports interurbains et scolaires), d'enseignement secondaire (fonctionnement, équipement et construction des lycées), de formation professionnelle et de formations sanitaires et sociales, d'aides aux entreprises, d'aménagement du territoire et de gestion des fonds européens.
La Région intervient également aux côtés de l'Etat dans le cadre du contrat de plan, et développe des politiques dites « volontaristes » en matière de culture, de sport, de recherche, d'aides aux communes, de santé, de sécurité, etc.

L'exécutif de la Région est représenté par le Président du Conseil régional. Le Président prépare et exécute les délibérations de l'assemblée régionale (123 élus régionaux) et de la commission permanente, gère le patrimoine, saisit le Conseil économique, social et environnemental régional, dirige l'administration régionale.
Renaud Muselier est le Président de la Région Provence-Alpes-Côte d'Azur. Il a été réélu le 2 juillet 2021, pour un nouveau mandat de six ans à la tête de l'exécutif régional.

Les services de la Région.

L'administration régionale est organisée en 9 directions générales adjointes, correspondant aux grandes compétences de la Région.

Le siège de la Région est situé à Marseille, où sont localisés environ 2000 agents dans plusieurs bâtiments. La Région a également une antenne dans chaque département (les « Maisons de la Région »).

Relèvent également de la Région les 183 lycées régionaux. Dans ces lycées, le personnel hors personnel éducatif et administratif (cad. les agents d'entretien et de restauration principalement, soit environ 4000 agents) dépend du Conseil régional.

La direction des systèmes d'information - DSI

Rattachée à la direction générale adjointe « Ressources », la DSI est composée de 3 services :

- Le service applications et données (SAD), qui a pour mission l'installation, le développement la maintenance des applications, de l'intranet et des sites collaboratifs, et qui vient en aide aux utilisateurs du progiciel finances « Astre » et effectue la formation de ces derniers.

- Le service postes de travail et support (SPTS - 18 personnes) qui a pour mission la configuration, le déploiement et la maintenance des postes de travail, y compris des photocopieurs, vient en aide aux utilisateurs et effectue la formation de ces derniers aux logiciels bureautiques. Je n'ai pas travaillé avec eux directement mais leurs rôles ont été cruciaux dans beaucoup de mes missions.

- Le service Architecture technique (SART), qui a pour mission la mise à disposition de ressources de traitement automatisé de l'information ainsi que la communication des postes de travail et terminaux vers ces ressources. Il est composé d'une unité exploitation qui gère les traitements d'exploitation, les salles informatiques, les imprimantes réseau et l'organisation des visioconférences, d'une unité systèmes en charge de gérer et superviser les serveurs et les applications hébergés, les baies de stockage, la messagerie et les bases de données et une unité réseaux, téléphonie et sécurité qui intervient sur les éléments de communication, gère les comptes utilisateurs et l'accès aux ressources du SI, l'autocom et les logiciels de sécurité.

La Région est également chargée des équipements et réseaux informatiques des 183 lycées régionaux répartis sur tout le territoire. Cette mission est confiée à la direction de l'éducation et de la vie des lycées (DEVL), plus particulièrement au service « Numérique éducatif ».

1.2 Le cadre du travail

Ma tutrice de stage était ROME Emmanuelle, elle travaille au service architecture technique. Le chef de ce service (et par extension le mien) est JACQUIER Dominique. Celui-ci gère principalement les effectifs de son service et veille à l'application des décisions du directeur. Son supérieur, le directeur ANIGO Gregory, prend les décisions, gère le budget et gère l'ensemble des effectifs de sa direction. Il y a de nombreux services au sein de la région. Ils sont très variés et sont tous sous la responsabilité de Raphaëlle SIMEONI, la directrice générale des services. Son supérieur est le président Renaud MUSELIER. L'organisation est assez dense, je présente une version plus complète dans l'annexe.

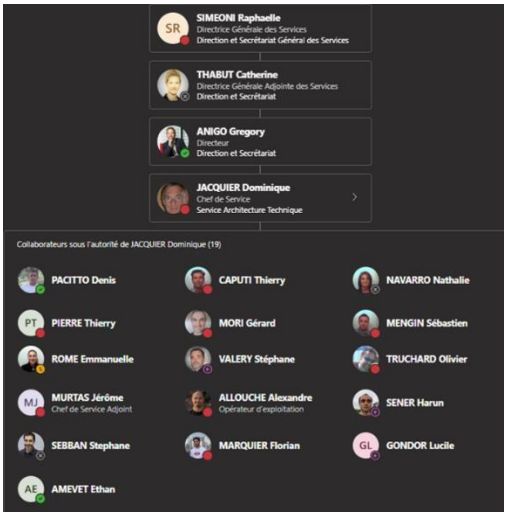
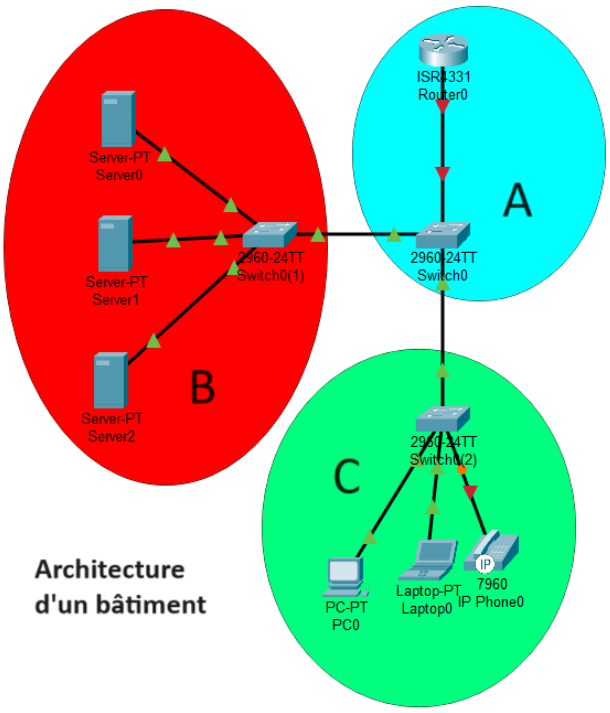


Figure 1 : Organigramme de mon service

1.3 Présentation du réseau et des technologies utilisées

Voici schéma du réseau que j'ai fait à l'aide du logiciel Packet Tracer. Il est important de connaitre l'architecture du réseau et son fonctionnement afin de mener à bien les futures opérations



A Marseille, la région SUD comprend 3 bâtiments (HDR pour Hôtel de région, Azur et Alpes). Chaque bâtiment à la même architecture. J'ai passé mon stage dans l'hôtel de région ; L'architecture a été définit à l'aide des recommandations de l'ANSII*. C'est pourquoi par exemple ils utilisent de pare-feu de marques différentes
J'ai rédigé une explication qui traite des technologies déployées et du fonctionnement général de cette architecture de ce réseau en annexe.

La Région attends d'un stagiaire qu'il soit autonome, curieux, et à l'écoute. Il fallait aussi des connaissances et des compétences techniques dans leur domaines. Je devais être capable de paramétrer des Switch, faire de l'administration système, de comprendre le fonctionnement d'un data center et d'un réseau informatique. Je n'avais jamais eu d'expérience professionnel dans un milieu similaire, je savais que je devais acquérir rapidement des compétences de savoir-être. Malgré ça, j'étais dans les attendus techniques à l'aide de ma formation, je me sentais prêt à débuter ce stage.

2 Le projet gestionnaire de mots de passe

2.1 Présentation du projet

2.1.1 Introduction

Chaque agent doit avoir accès à différents outils et bases de données plus ou moins sensible.

La première mesure de sécurité est de limiter les accès par des mots de passe générés aléatoirement qui change régulièrement. Les mots de passe sont distribués aux fonctionnaires habilités depuis un gestionnaire tiers.

Cependant, les exigences ont évolué et le gestionnaire actuellement utilisé ne réponds plus aux attentes actuelles. Il a des lacunes en sécurité et en ergonomie, on aura l'occasion de les étudier par la suite. Il m'a été demandé de mettre en place un nouveau service de gestionnaire de mots de passe pour les services de réseaux et cybersécurité, avec la possibilité de l'étendre à la Région SUD.

Ce projet m'a été présenté lors de ma première semaine, et constitue une partie importante de mon stage. Au fil de cette section je vais vous présenter chronologiquement son avancement. C'est-à-dire traiter des problèmes que j'ai rencontré, les solutions que j'ai apportées enfin conclure sur ce que j'ai produit et ce que j'en ai tiré.

Tout d'abord, je voici la première étape que j'ai entreprise après avoir pris connaissance du sujet : l'élaboration d'un cahier des charges précis.

2.1.2 Cahier des charges

Les projets tutorés auxquels j'ai participé dans le cadre de mon BUT (Bachelor Universitaire Technologique) m'ont inculqué l'importance primordiale de rédiger un cahier des charges. Un cahier des charges bien réalisé permet de s'assurer d'être en accord avec l'attendu, de se focaliser sur l'essentiel et d'estimer les besoins et les délais nécessaires. Voici la liste des exigences et des contraintes à respecter.

(Les points d'exclamations représentent les exigences qui n'étaient pas attendues sur l'ancienne solution)

Application open-source !	Une application open source est un logiciel dont le code source est accessible publiquement, permettant aux utilisateurs de l'étudier, de le modifier et de le distribuer librement selon les termes de la licence associée.
NAS local (network attached stockage)	Les mots de passes sont centralisés sur un serveur local, ce qui permet à plusieurs utilisateurs de stocker et de partager des fichiers sur un réseau TCP/IP.
Déployable à l'échelle d'une entreprise	Ce service doit être capable de prendre en charge simultanément une dizaine d'agents (l'ensemble des employés du département de réseaux et de cybersécurité), puis potentiellement plusieurs centaines si cette solution est adoptée.
Déployer l'application en ligne !	On doit pouvoir s'y connecter depuis un navigateur à l'aide d'une URL sur Internet.
Compte utilisateur unique !	Chaque agent doit disposer d'un compte personnel dédié, ce qui facilite la gestion de leurs activités individuelles et permet de surveiller l'utilisation des mots de passe. Pour l'instant, chaque service a un compte unique distribué à l'ensembles de ses membres.
Authentification à double facteur	Idéalement à l'aide de leur smartphone professionnel, les agents doivent confirmer leur identité à l'aide d'une deuxième authentification.
Contrôle d'accès !	Chaque agent doit pouvoir créer un compte en utilisant son adresse mèl professionnelle, limitée au domaine spécifique de l'organisation (« ...@maregionsud.fr »), tout en restreignant l'accès aux adresses provenant de domaines externes tels que « @gmail.com » par exemple.

Support de la langue française	L'application doit supporter la langue française. Par exemple, les mails envoyés où les messages d'erreur doivent être en français par défaut, ou du moins personnalisables afin de les traduire manuellement.

2.1.3 Choix de la solution

Il existe de nombreux gestionnaires de mots de passe open source. Après avoir évalué les principaux candidats, plusieurs raisons m'ont conduit à choisir Vaultwarden. Vaultwarden est un gestionnaire open-source, codé en Rust, basé sur l'application payante Bitwarden. Voici les raisons ;

Extensions et adaptabilité : Vaultwarden supporte gratuitement les extensions et les fonctionnalités supplémentaires de Bitwarden, tels que l'authentification à double facteur ou la synchronisation avec un cloud.

Reference : Lors de mes recherches, j'ai découvert un post LinkedIn de la SITIV intitulé « Le SITIV déploie Vaultwarden ». Ce post détaille leurs besoins, qui sont similaires aux miens.

Recommandation : Un de mes collègue de travail m'a recommandé cette solution qu'il connaissait.

Son fonctionnement est le suivant ; l'admin de l'organisation peut inviter des membres et leurs donner différents droits pour les coffres qu'il décide. Chaque coffre regroupe différents mots de passes, textes ou des fichiers textuels de différentes natures. Il peut y avoir une infinités de coffres et d'utilisateurs. La gestion de l'organisation est réputée pour être ergonomique et très flexible, permettant une grande variété de manipulations adaptées à toutes sortes de situations.

2.1.4 Besoins

Pour déployer le gestionnaire de mots de passe, j'ai besoin d'une machine virtuelle (VM) qui peut supporter l'application Docker. J'aurai également besoin d'avoir accès à différentes outils informatiques pour publier l'application.

Ma VM est une machine Linux qui a comme adresse IP 192.168.85.5. J'ai besoin d'un **logiciel d'accès**. Celui que le service cybersécurité utilise est Bitvise. Je le télécharge et l'utilise de la façon suivante (figure 2) :

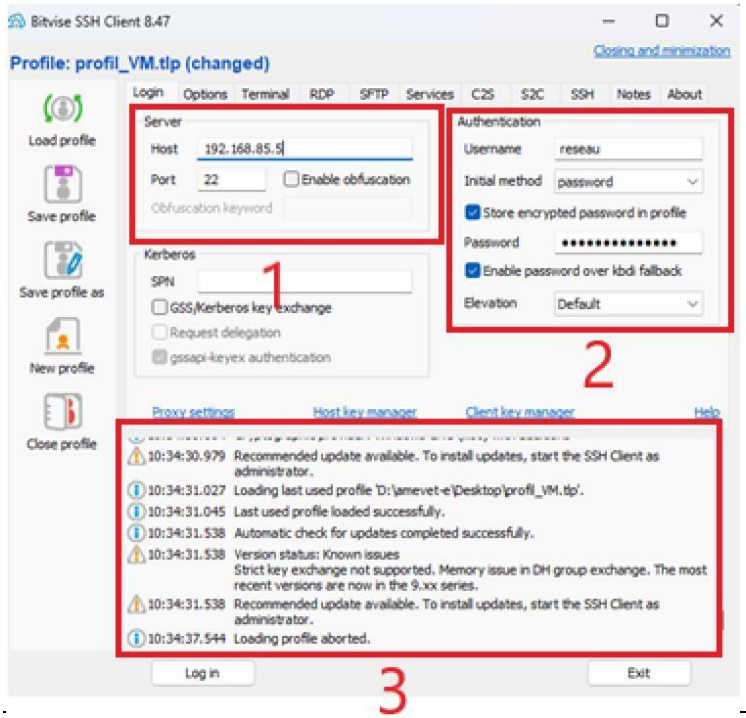


Figure 2 : Capture d'écran de l'interface de Bitvise

1- Je rentre l'adresse et le port de connexion
2- Je rentre l'utilisateur avec lequel me connecter, et je choisis mon élévation de privilège (mes droits)
3- Affichage des logs

2.2 Docker

J'ai commencé ce projet par déployer l'application Docker sur ma VM. Docker est une plateforme de conteneurisation.

Figure 3 : Logo de Docker

2.2.1 Étapes de Déploiement

Installation des paquets

Pour installer Docker sur la VM, j'ai exécuté les commandes suivantes :

```
apt update && apt full-upgrade -y
```

```
apt install docker.io -y
```

Ces commandes mettent à jour le système, installent Docker-.

Pour installer le serveur web Apache2, j'ai utilisé la commande :

```
apt install apache2 -y
```

Docker Compose permet de gérer des applications multi-conteneurs. Pour l'installer :

```
apt install docker-compose -y
```

Création de l'Arborescence de Répertoires

Pour organiser les fichiers Docker, j'ai créé l'arborescence suivante :

```
mkdir /srv/docker
mkdir /srv/docker/portainer
cd /srv/docker/portainer
nano docker-compose.yaml
```

Le fichier `docker-compose.yaml` permet de définir les services et leur configuration.

Déploiement de la Stack

Le fichier `docker-compose.yaml` permet de décrire comment lancer et organiser plusieurs conteneurs Docker pour une application. On peut l'activer à l'aide de la commande :

```
docker-compose up -d
```

L'option `-d` lance les conteneurs en arrière-plan.

Explication détaillée des informations de ce fichier (figure 4) :
Version : Utilise Docker Compose version 3.3.
Nom du conteneur : portainer.
Ports : Expose les ports 9443 et 9000.
Volumes : C'est le chemin sur l'hôte (votre machine) où les données seront stockées de manière persistante. Monte /var/run/docker.sock et un volume nommé data.

Redémarrage : Redémarre toujours en cas de panne.

Image : Utilise portainer/portainer-ce:latest disponible sur le Docker Hub (service cloud collaboratif).

```yaml
version: '3.3'
services:
    portainer-ce:
        container_name: portainer
        ports:
            - 9443:9443
            - 9000:9000
        volumes:
            - /var/run/docker.sock:/var/run/docker.sock
            - data:/data
        restart: always
        image: portainer/portainer-ce:latest

volumes:
  data:
```

Figure 4 : Capture d'écran du fichier docker-compose.yaml

Création et Construction de l'Image Docker

Pour créer une image Docker personnalisée (un nouveau modèle de conteneur), je commence par écrire un fichier `Dockerfile` :

```
Dockerfile

FROM httpd:latest
COPY ./mywebapp /usr/local/apache2/htdocs/
```

Puis, pour construire l'image :

```
docker build -t mywebapp .
```

Cette commande construit une nouvelle image Docker en utilisant les instructions spécifiées dans le Dockerfile présent dans le répertoire actuel. L'option `-t` permet de donner un nom à cette nouvelle image, ici "mywebapp".

.

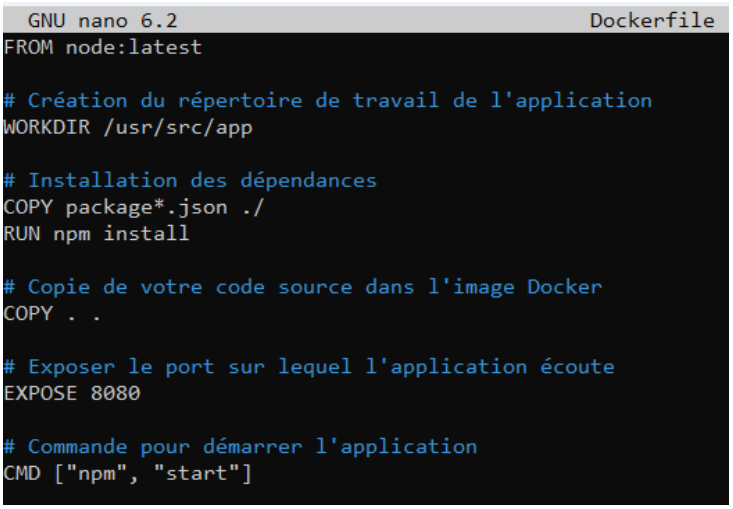


Figure 5 : Capture d'écran du fichier Dockerfile (avec commentaires)

FROM node:latest # Utilise la dernière image Node.js officielle

Pour exécuter l'image Docker construite :

```
docker run -d -p 8080:80 3b823240cfe8
```

À la suite de la construction de l'image Docker, j'ai lancé le conteneur en utilisant la commande "docker run". Cette commande permet de récupérer l'image mywebapp pour crée un conteneur. L'option -p 8080:80 mappe le port 80 du conteneur au port 8080 de l'hôte. Ainsi, l'application hébergée dans le conteneur est accessible depuis le port 8080 de l'hôte.
3b823240cfe8 est l'id de l'image mywebapp.

Pour autoriser le trafic HTTP (port 80) :

```
firewall-cmd --docker --add-service=http
systemctl status firewalld
```

Pour ajouter l'autorisation du trafic ICMP :

```
firewall-cmd --zone=docker --add-protocol=icmp --permanent
```

Installation des Certificats SSL

Pour activer HTTPS et sécuriser les communications :

```
openssl req -new -x509 -days 365 -nodes -out /etc/ssl/certs/mailserver.crt -
keyout /etc/ssl/private/mailserver.key
a2enmod ssl
```

Commandes utiles

Pour lister les images Docker et obtenir leur ID :

```
docker images
```

```
root@vaultwarden:/home/reseau# docker images
REPOSITORY                TAG       IMAGE ID       CREATED          SIZE
portainer                 latest    0667f4875843   5 weeks ago      294MB
vaultwarden/server        latest    739990a8e475   2 months ago     201MB
mywebapp                  latest    3b823240cfe8   2 months ago     278MB
root@vaultwarden:/home/reseau#
```

Figure 6 : Liste des images Docker que j'ai crée

Pour s'assurer que Docker fonctionne correctement :

```
systemctl status docker
```

```
root@vaultwarden:/home/reseau# systemctl status docker
● docker.service - Docker Application Container Engine
     Loaded: loaded (/lib/systemd/system/docker.service; enabled; vendor preset: enabled)
     Active: active (running) since Fri 2024-05-17 06:41:04 CEST; 2 weeks 4 days ago
TriggeredBy: ● docker.socket
       Docs: https://docs.docker.com
   Main PID: 1352 (dockerd)
      Tasks: 37
     Memory: 107.9M
        CPU: 17min 17.057s
     CGroup: /system.slice/docker.service
             ├─1352 /usr/bin/dockerd -H fd:// --containerd=/run/containerd/containerd.sock
             ├─1776 /usr/bin/docker-proxy -proto tcp -host-ip 0.0.0.0 -host-port 8000 -container-ip
             ├─1788 /usr/bin/docker-proxy -proto tcp -host-ip 0.0.0.0 -host-port 9443 -container-ip
             └─1802 /usr/bin/docker-proxy -proto tcp -host-ip 0.0.0.0 -host-port 9000 -container-ip
```

Figure 7 : On peut voir différentes informations utiles, notamment si le docker est actif

Pour voir les conteneurs qui tournent :

```
docker ps
```

```
root@vaultwarden:/home/reseau# docker ps
CONTAINER ID   IMAGE                          COMMAND        CREATED       STATUS                 PORTS
        NAMES
b6b20cecef8e   vaultwarden/server:latest       "/start.sh"    4 weeks ago   Up 2 weeks (healthy)   3012/tcp, 0.0.0.0:8000->80/tcp
        vaultwarden-test
5ac160e9f149   portainer/portainer-ce:latest   "/portainer"   6 weeks ago   Up 2 weeks             0.0.0.0:9000->9000/tcp, 8000/tcp, 0.0.0.0:9443->94
43/tcp   portainer
root@vaultwarden:/home/reseau#
```

Figure 8 : On peut voir les deux conteneurs que j'ai crée

2.2.2 Prise en main de Portainer

Portainer est une interface de gestion pour Docker. J'ai accès à Portainer via :

```
http://192.168.85.5:9000/
```

Le stack que j'ai créé depuis la VM est « Limited ». Je n'ai pas tous les droits car je l'ai crée en dehors du Portainer. J'en crée un nouveau depuis ce client léger, « vaultwarden_test » (son nom est trompeur, il m'a servit de test mais c'est également lui qui sera utile tout au long du projet).

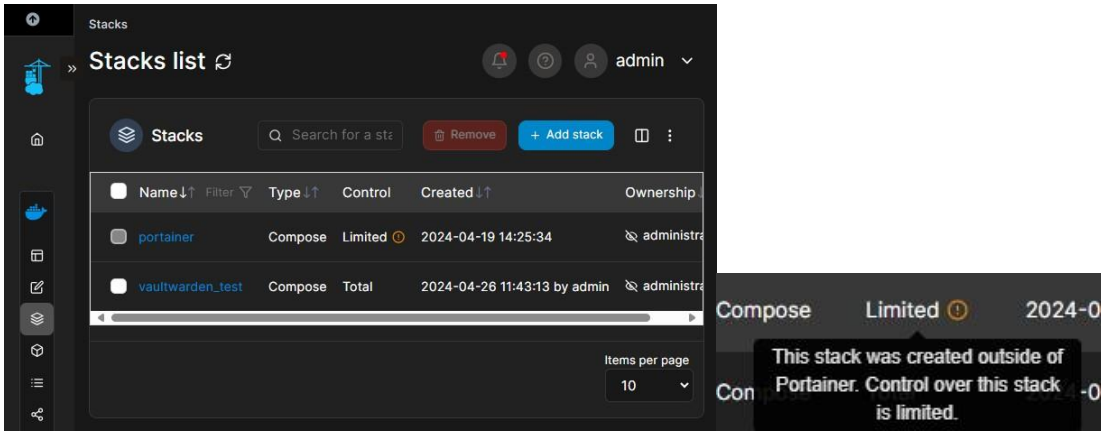


Figure 8&9 : Interface du client léger de Docker. Le stack Portainer est marqué comme Limited

Le site est très utile pour avoir accès à différentes informations importantes d'un simple coup d'œil et pour le paramétrer efficacement (figure 10).

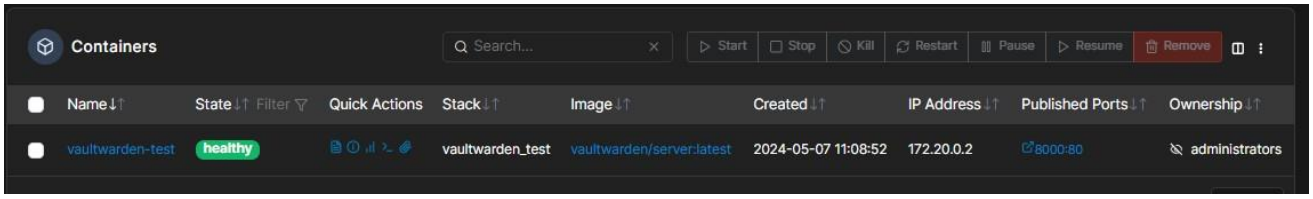


Figure 10 : Interface de Docker, diagnostique d'un des containers

Dans l'onglet « Editor », je peux modifier le fichier docker compose. Je lui attribue des ports ainsi que le chemin ou seront stockées les données de manière persistante (c'est-à-dire conservées même si le conteneur est supprimé) (figure 11). Plus tard j'ai ajouté la valeur de ADMIN_TOKEN. C'est une passphrase, un long mot de passe. Nous verrons son utilité ultérieurement dans le rapport.

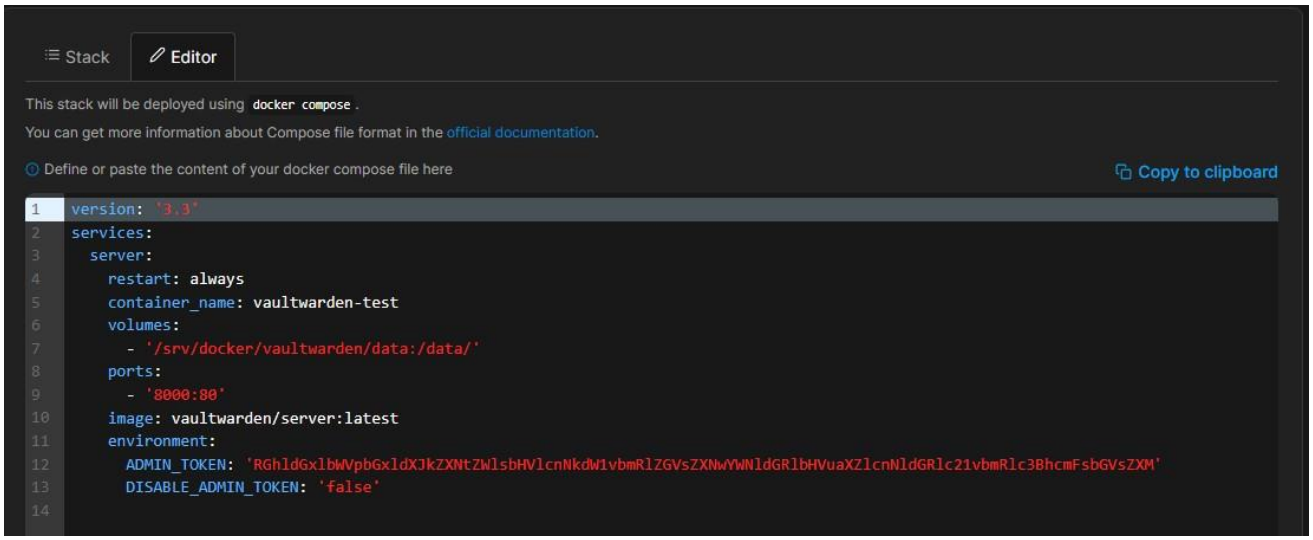


Figure 11 : Interface de Docker pour modifier le fichier docker -compose. Les deux dernières lignes on été ajoutés plus tard et seront expliquées

La mise en place du site Docker s'est déroulée sans difficulté. Le prochain client léger à installer est Vaultwarden. Toutefois, un élément spécifique rend cette tâche plus complexe.

2.3 Vaultwarden

2.3.1 Connexion sécurisée

Dans cette section, je vais vous expliquer comment j'ai mis en place le client léger de Vaultwarden. Tandis que le site Docker permet une gestion plus efficace et ergonomique, il est obligatoire de déployer Vaultwarden pour gérer le service de gestionnaire de mots de passe.

Comme mentionné précédemment, le premier problème rencontré est lié à la connexion sécurisée. Jusqu'à présent, les connexions se faisaient en HTTP ; cependant, Vaultwarden exige une connexion en **HTTPS** (figure 12).

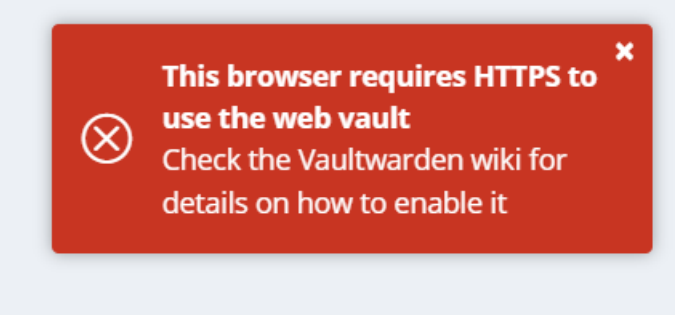


Figure 12 : Message d'erreur

Pour activer le HTTPS sur un serveur Apache2, il est nécessaire de suivre plusieurs étapes :

1. **Créer des certificats SSL** : J'utilise la suivante pour générer un certificat et une clé privée :

```
openssl req -new -x509 -days 365 -nodes -out /etc/ssl/certs/mailserver.crt -
keyout /etc/ssl/private/mailserver.key
```

Figure 13 & 14 : Capture d'écran des extraits du certificat et de la clé nouvellement crées

2. **Activer le module SSL dans Apache** : J'effectue la commande suivante pour activer le module SSL Apache SSL signifie « Secure Sockets Layer », c'est un protocole de sécurité qui crée un lien chiffré entre un serveur Web et un navigateur Web.

   ```
   a2enmod ssl
   ```

3. **Configurer Apache pour utiliser le SSL** : J'ajoute une configuration pour le site HTTPS dans le fichier de configuration Apache en ajoutant le chemin des deux fichiers précédemment crées (figure 15) :

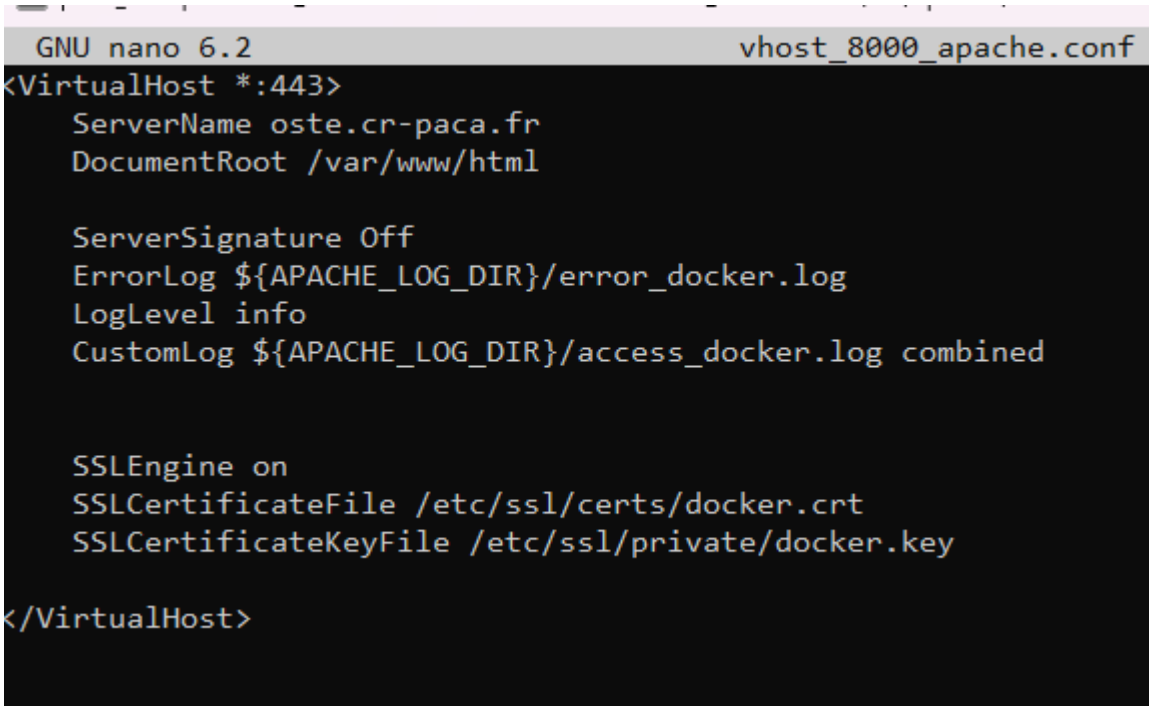


Figure 15 : Capture d'écran du fichier vhost_8000_apache.conf . Il permet la configuration en HTTPS

Sécurisation de la Communication Totale

4. **Vérification :**

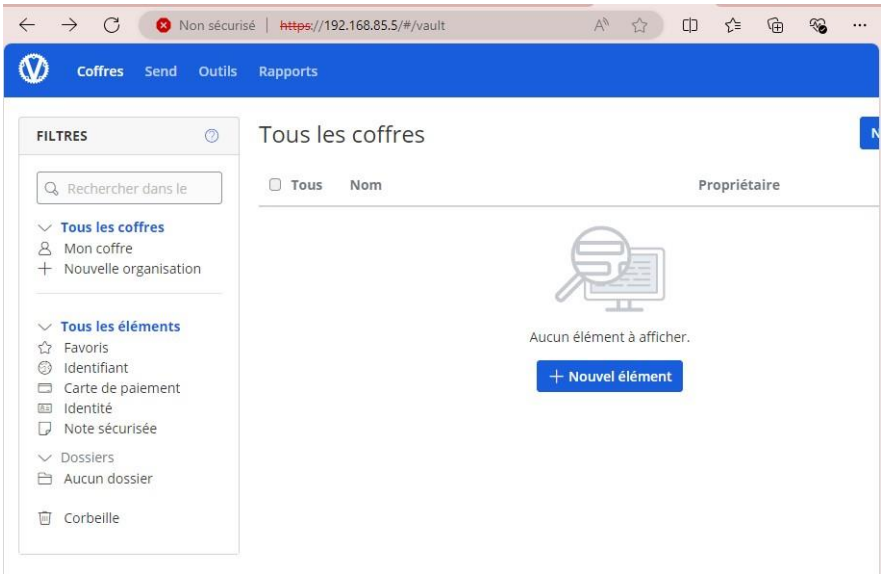


Figure 16 : Capture d'écran de Vaultwarden. Ça marche !

La connexion fonctionne. J'ai pu créer un compte et m'y connecter (figure 16).

2.3.2 Bilan mi-projet

Vaultwarden est fonctionnel à l'aide de Docker et je peux m'y connecter à l'aide de mon navigateur depuis le réseau de la Région. C'est une étape importante qui a été franchie. Bien qu'il me reste encore beaucoup de modifications et d'ajouts nécessaires, je me retrouve à un mi-chemin symbolique ; j'ai un gestionnaire de mots de passe fonctionnel, mais je ne l'ai pas encore modifié.
Je produis un rapport pour que mes collègues voient mon avancement, me corrige en cas d'erreur et pour qu'ils me conseillent pour la suite. Ce rapport m'aide également, comme j'ai pu l'apprendre en cours de PPP, il est important de faire des comptes-rendus pour mettre au clair ma progression et savoir vers où me diriger pour la suite du projet. Pour se faire, je reprends les exigences une à une afin de voir si elles sont déjà respectées, et étudier les priorités restantes (les points validés sont en italiques) :

Application open-source : Vaultwarden est bien open source, on peut valider ce point.

NAS local : Le gestionnaire tourne depuis une VM que la région SUD possède. Les mots de passe sont stockés en local, ce qui répond à l'attendu.

Déployable à l'échelle d'une entreprise : Pour le moment, cette solution est adaptée pour une famille ou un TPE (très petite entreprise), c'est-à-dire une vingtaine de membres maximum. La mise en place de ce service peut se faire facilement pour l'ensemble des équipes réseaux et cybersécurité. Pour déployer ce gestionnaire pour les milliers agents de la région il faudrait trouver des pistes d'amélioration. Par exemple, il serait intéressant d'automatiser les invitations dans les différents coffres ou automatiser la création de compte pour tous les agents. Ces améliorations ne sont pas prioritaires comparées à d'autres et peut dépendre des travaux que je mène. Je garde cette étape pour la fin.

Déployer l'application en ligne: Pour l'instant, Vaultwarden n'est pas accessible depuis un appareil en dehors du réseau de la région. Cette étape est cruciale, car elle implique l'utilisation d'outils essentiels tels que les pares-feux et les DNS. Je la considère comme une priorité, car il est indispensable pour moi de maîtriser au mieux ces domaines afin de disposer des ressources nécessaires pour la suitedu stage. Ce sera mon prochain objectif.

Compte utilisateur unique **:** Il peut y avoir un compte unique par utilisateur à l'aide cette solution.

Authentification à double facteur : L'authentification à double facteur est possible mais pas encore mise en place.

Contrôle d'accès : N'importe quelle adresse électronique peut se faire inviter. Cette exigence n'est pas respectée pour le moment.

Support de la langue française : L'application est en française, cependant les emails sont envoyés en anglais (emails d'erreurs, de logs, de confirmation…). C'est quelque chose qu'il faut changer.

Maintenant que j'ai mis au clair les points qu'il faut que j'améliore, je peux commencer à reprendre le projet. A commencer par publier l'application :

2.4 Déployer l'application en ligne

Actuellement, l'application tourne sur le réseau privé de la région. Il m'est demandé qu'elle soit accessible depuis Internet. Cette opération nécessite de prendre en main 3 outils différents ; les 2 pare-feu, un reverse Proxy ainsi que le DNS.

Fonctionnement des requêtes

Pour qu'un internaute veut se connecter à une application, il doit passer par divers équipements informatiques, que j'ai pu étudier, pour établir une connexion sécurisée. Une explication plus détaillée se trouve en annexe.

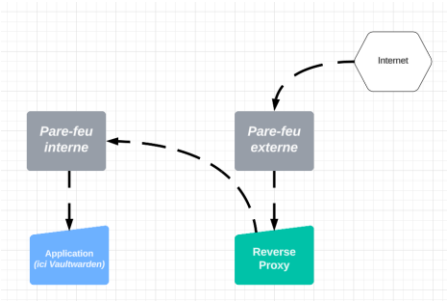


Figure 17 : Schéma gestion des requêtes

Manipulations

Pour commencer, j'ai entré dans le DNS l'adresse que je souhaite que les utilisateurs saisissent, en l'associant à une adresse IP spécifique. Le nom de domaine est « maregionsud », j'utilise un sous domaine personnalisé (« bm. »). Finalement l'adresse choisie est mb.maregionsud.fr

Chaque nouvelle application implique la création d'un nouveau tunnel. Ces tunnels doivent être paramétrés sur le reverse Proxy. Comme la région possède deux reverse Proxy (un actif et un passif), on utilise un proxy management pour ces manipulations. Cela permet de paramétrer les deux outils au même moment.

Figure 18 : Capture d'écran du FWi (Fortinet). Cette ligne autorise le trafic pour l'application

Le tunnel traduit l'adresse de la VM à l'aide du reverse Proxy vers l'adresse privé sur le serveur. Il permet également de faire le « chemin » inverse, c'est-à-dire traduire l'adresse privé de Vaultwarden vers son adresse publique.

Résultat

A l'aide de ces manipulation, il est maintenant possible de se connecter à mon gestionnaire de mots de passe de manière sécurisée sans être dans le réseau local. Sur l'exemple ci-dessous, je m'y suis connecté en 4G, et ma connexion est sécurisée (figure 19) ainsi que journalisée (figure 20). Par exemple, je n'aurai pas pu me connecter à l'aide d'une adresse suspecte, déjà connue et bannie de la Region SUD. Ces mesures de sécurité est un sujet que j'ai également étudié durant mon stage, j'aurai l'occasion d'en parler dans la suite de ce rapport. L'exigence d'externaliser l'application est complétée, et d'une !

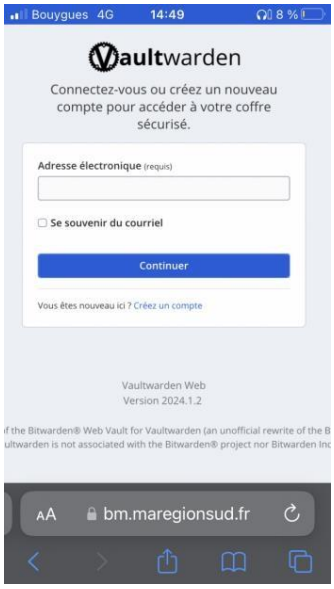


Figure 19 : Capture d'écran de mon téléphone, connecté à Vaultwarden

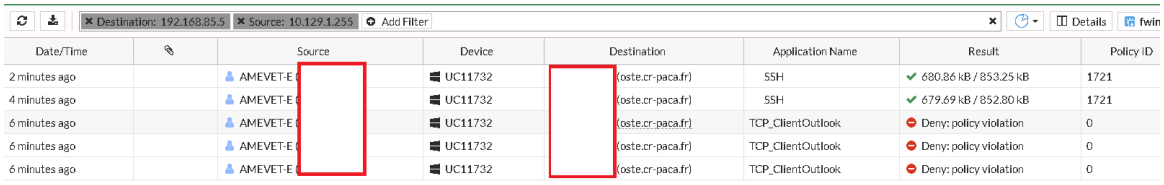


Figure 20 : Extraits des logs où on peut voir des tests unitaires sur la faisabilité de la connexion.

2.5 Contrôle d'accès

Il est fortement recommandé de limiter l'accès à l'organisation aux comptes crée à partir d'une adresse électronique de la région, avec le nom de domaine « …@maregionsud.fr ». Cette manipulation se fait dans l'interface admin de l'application, à l'adresse « 192.168.85.5/admin/ ».
Une fois sur la page, un admin token est demandé (figure 21). Il ne faut pas le confondre avec le mot de passe de l'administrateur, l'admin token s'agit d'une passphrase entrée dans le docker-compose. Comme mentionné dans la partie 2.2.2 de ce rapport, j'inclus alors une ligne de code qui permet de définir ce token (figure 11).

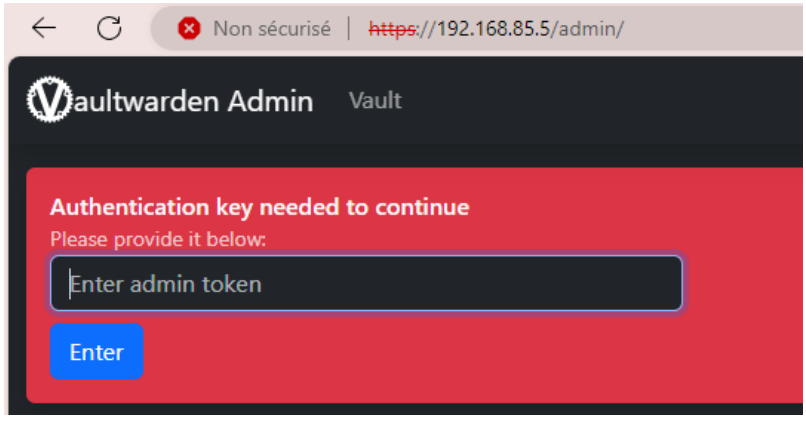


Figure 21 : Capture d'écran de la page d'accueil de l'accès admin à mon organisation Vaultwarden

Cette nouvelle page de configuration offre des options avancées de modification et de paramétrage (figure 22).

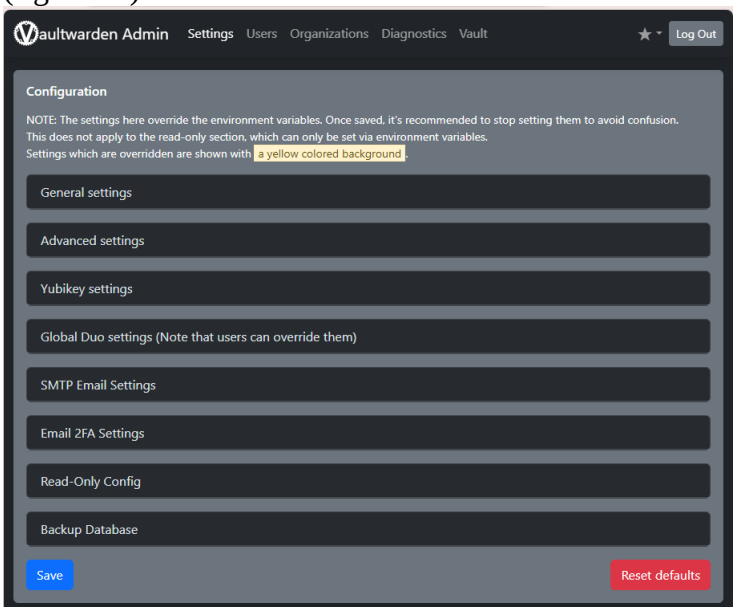


Figure 22 : Organisation de la page admin

Dans l'onglet « General settings », j'ajoute le domaine à la whiteliste afin de restreindre les comptes à l'adresse de la région. Une whiteliste définit l'ensemble des entités qui sont autorisées a rejoindre un système, ici l'organisation (figure 23).

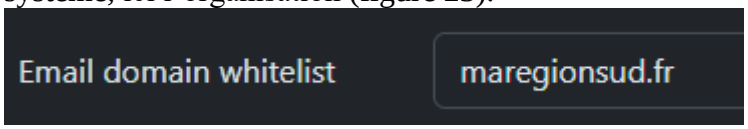


Figure 23 : Extrait du paramètre qui permet d'entrer une whitelist

Je profite de cette avancée pour prendre des initiatives et implémenter des nouvelles règles, avant de les faire confirmer par mon responsable, telles qu'interdire les utilisateurs à changer leur adresse électronique de connexion, définir une adresse de récupération en cas de perte du mot de passe ou encore mettre une limite de emails envoyés automatiquement lors des tentatives de connexion.
A l'aide de cette manipulation, les comptes qui peuvent rejoindre l'organisation doivent être crée depuis le domaine de la région SUD. A noter que la mesure n'est pas retro-active, les comptes qui ont déjà été créé depuis un autre domaine sont toujours fonctionnels. Malgré ça, cette exigence est validée.

2.6 Support de la langue française

L'application doit envoyer des emails en français. Je trouve sur GitHub* ces modèles traduit en français, que je télécharge.
Je remplace le repertoire « email » présente à l'arborescence suivante :
/srv/docker/vaultwarden/data/templates/email
par le répertoire nouvellement téléchargé (figure 24).

```
reseau@vaultwarden:/srv/docker/vaultwarden/data/templates/email$ ls
admin_reset_password.hbs                        invite_confirmed.hbs
admin_reset_password.html.hbs                   invite_confirmed.html.hbs
change_email.hbs                                new_device_logged_in.hbs
change_email.html.hbs                           new_device_logged_in.html.hbs
delete_account.hbs                              pw_hint_none.hbs
delete_account.html.hbs                         pw_hint_none.html.hbs
email_footer.hbs                                pw_hint_some.hbs
email_footer_text.hbs                           pw_hint_some.html.hbs
email_header.hbs                                send_2fa_removed_from_org.hbs
emergency_access_invite_accepted.hbs            send_2fa_removed_from_org.html.hbs
emergency_access_invite_accepted.html.hbs       send_emergency_access_invite.hbs
emergency_access_invite_confirmed.hbs           send_emergency_access_invite.html.hbs
emergency_access_invite_confirmed.html.hbs      send_org_invite.hbs
emergency_access_recovery_approved.hbs          send_org_invite.html.hbs
emergency_access_recovery_approved.html.hbs     send_single_org_removed_from_org.hbs
emergency_access_recovery_initiated.hbs         send_single_org_removed_from_org.html.hbs
emergency_access_recovery_initiated.html.hbs    smtp_test.hbs
emergency_access_recovery_rejected.hbs          smtp_test.html.hbs
emergency_access_recovery_rejected.html.hbs     twofactor_email.hbs
emergency_access_recovery_reminder.hbs          twofactor_email.html.hbs
emergency_access_recovery_reminder.html.hbs     verify_email.hbs
emergency_access_recovery_timed_out.hbs         verify_email.html.hbs
emergency_access_recovery_timed_out.html.hbs    welcome.hbs
incomplete_2fa_login.hbs                        welcome.html.hbs
incomplete_2fa_login.html.hbs                   welcome_must_verify.hbs
invite_accepted.hbs                             welcome_must_verify.html.hbs
invite_accepted.html.hbs
```

Figure 24 : Liste de tous les mails disponibles

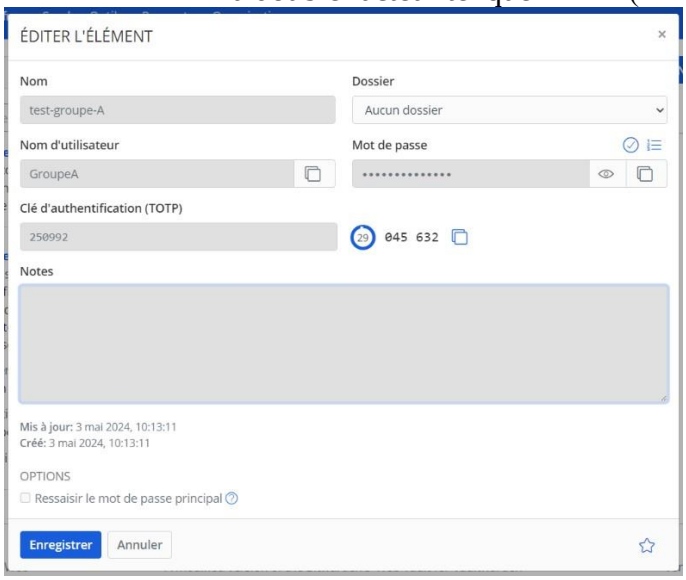
Le service va chercher dans ce répertoire les modèles de mail a envoyer. Maintenant qu'ils sont en français, l'exigence est respectée.

```
reseau@vaultwarden:/srv/docker/vaultwarden/data/templates/email$ cat admin_reset_password.hbs
Le mot de passe principal a été modifié
<!---------------->
Le mot de passe principal de {{user_name}} a été modifié par un administrateur de votre organis
 {{org_name}}. Si vous n'êtes pas à l'origine de cette demande, veuillez contacter immédiatemer
re administrateur.
```

Figure 24 : Exemple de mail qui peut être envoyé. Les « {{}} » permettent d'entrer des variables.

2.7 Authentificateur à double facteur

Alors que je travaillais sur une solution d'authentification à double facteur, avec l'application « TOTP Authentificator » (car elle est recommandée par Bitwarden), on me prévient que ça ne sera pas la peine car le service avait déjà une solution.
Heureusement, la communication s'est faite rapidement, je n'avais pas passé encore beaucoup de temps sur cette exigence. J'ai quand même pu explorer les technologies et techniques possibles pour l'authentification à double facteur tel que l'OTP (One-Time Password).



2.8 Adaptée à l'échelle d'une entreprise

Comme dit précédemment, je comptais sur les extensions de Bitwarden, compatibles avec Vaultwarden, pour améliorer les capacités d'adaptabilité de ce gestionnaire. La solution la plus recommandée est « Bitwarden Directory Connector » (BDC).
Ce logiciel doit se connecter à mon organisation. Pour se connecter, il faut rentrer l'URL de l'organisation (figure 25) ainsi que des identifiants propres à cette dernière (figure 27). Cependant, la connexion était refusée. Le message d'erreur est très court (« Error : Failed to stetch ») et je n'ai pas de log particulier. J'ai abandonné ce logiciel après avoir passer beaucoup de temps à chercher une solution. L'alternative était une version CLI de cette extension. La connexion fonctionne (figure 26), cependant, mon stage se finissait bientôt et il me restait encore beaucoup d'autres missions à découvrir. Le CLI n'était pas très ergonomique et le prendre en main m'aurais demandé un investissement et un temps que je n'avais plus. Cela dit, ça reste une bonne piste pour améliorer le projet. Je commence à rédiger le rapport de ce travail afin que mes collègues puissent le prendre en main.

Figure 25 : Logo de BDC

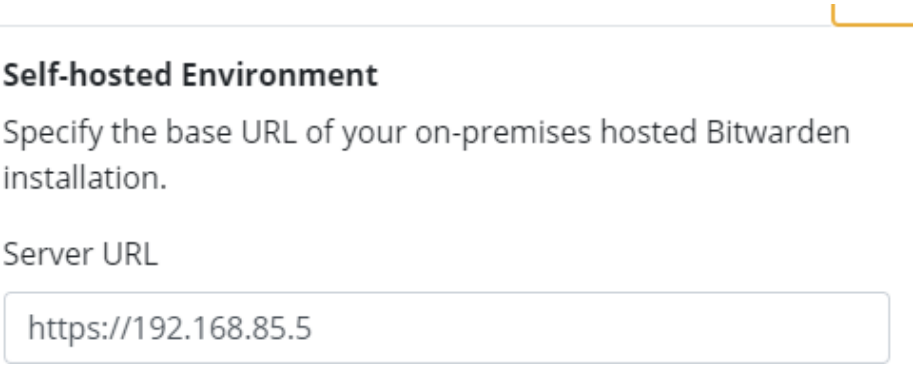


Figure 25 : Champ à remplir sur Bitwarden Directoty Connector

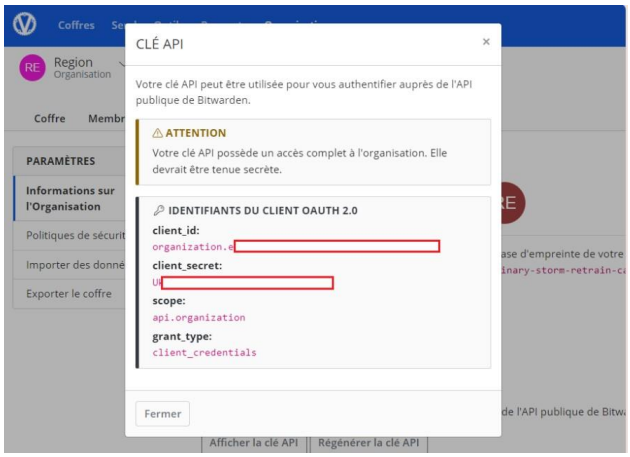


Figure 27 : Identifiants de l'organisation

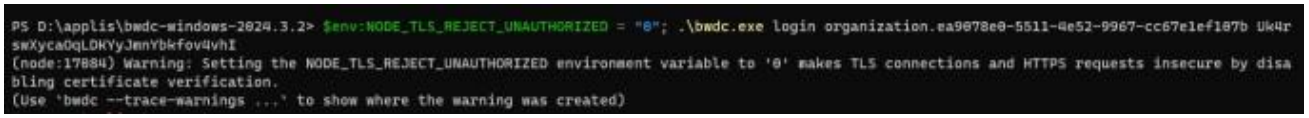


Figure 26 : Capture d'écran du CLI

2.9 Projet rendu

Finalement, j'ai pu rendre un gestionnaire de mots de passe fonctionnel qui répondait à tous les points qu'on m'avait demandé. Il y avait encore des pistes d'amélioration possibles, notamment s'il sera déployé pour tous les agents de la Région.
C'est un projet dont je suis fier et j'espère qu'il sera utile. Mes cours d'administration système du BUT m'ont aidé pour déployer les sites, et mes cours de réseau m'ont permis de répondre à une grande partie des exigences. J'ai trouvé ça très intéressant de mettre en pratique des connaissances techniques tout en alliant différents domaines.

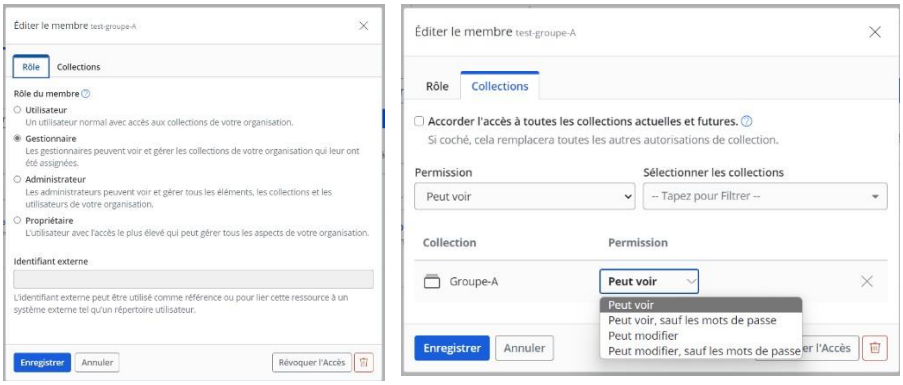


Figure 26 & 27 : Exemples d'utilisations

3 Missions complémentaires

3.1 Mission réseau

Plus d'une centaine d'équipements réseaux sont déployés dans les bâtiments de la région. Une tâche fréquente est de changer les équipements en cas de panne, d'obsolescence ou de changement d'infrastructure. A l'aide mes études, j'ai pu aider à remplacer différents équipements réseau. Dans cette partie, je vais vous présenter une mission clé lorsque l'on travaille dans ce domaine. Une autre mission que j'ai eue à mener se trouve en annexe.

Contextualisation

Comme dis précédemment, il y a plusieurs raisons pour lesquelles il faut remplacer un équipement. Le cas que je vais présenter ici est celui du switch de l'hémicycle (figure 28). Il avait un débit de connexion insuffisant et manquait de VLAN. L'hémicycle est la salle où les élus viennent débattre et voter des lois. Chaque bureau doit être connecté de manière filaire au local technique, il y en a 200.

Figure 28 : Photo libre de droit de l'hémicycle

Préparations

Pour répondre aux besoins actuels, la connexion doit se faire à l'aide d'une fibre de 10 Giga. Le switch installé ne supportait que la connexion 1 Giga. Je commence par intégrer sur le nouveau switch des modules plus modernes avec un débit de 10 giga (figure 29).

Figure 29 : Figure 1Cisco Module transceiver SFP+ 10GE 10GBase-LR

Ce dernier est d'un modèle plus récent. Il s'agit du Catalyst 9200 48 PoE+ (figure 30). Comme son nom l'indique, il a plus de ports (48) et peut accueillir plus de VLAN. Je copie l'ancienne configuration (qui était accessible depuis une base de données) sur laquelle j'ajoute les VLAN nouvelles.

Figure 30 Catalyst 9200 48 PoE+ (Cisco)

Mise en place

Une fois le nouveau switch prêt, je rejoins le local technique de l'hémicycle pour l'installer. J'ai pris en photo les différentes étapes de l'installation. Je commence par repérer le switch à débrancher (figure 31), puis j'étiquette tous les câbles avant de les débrancher (figure 32). Enfin, je branche les câbles à l'aide des étiquettes, je branche les câbles supplémentaires pour les nouvelles VLAN (figure 33).

Une fois cette partie terminée, le reste de l'équipe vérifie si tout fonctionne correctement et me tient au courant.

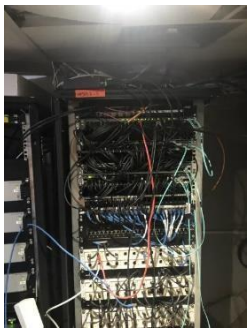


Figure 31


Figure 32

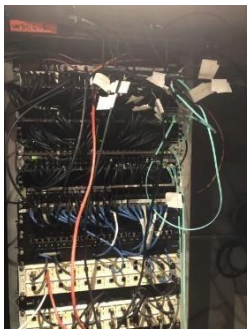


Figure 33

3.2 Observation Cybersécurité

J'ai pu rencontrer 5 agents responsables de la cybersécurité de la Région. Tout au long du stage, ils m'ont initié à leur métier en me présentant leur travail, leurs missions ainsi que leurs outils. J'ai eu l'occasion de les observer et de les aider. Leur partage fait écho à ma formation, tout en me faisant découvrir de nombreuses nouvelles facettes de ce milieu. Il m'a également permis de mieux comprendre l'application pratique de ce que j'avais étudié en cours. À la vue de tout ce que ça m'a apporté, il me semble nécessaire de mentionner les principaux aspects que j'ai approfondis.

3.2.1 Gestion des tickets

Présentation des acteurs

La région SUD travaille avec la plateforme SOC Sekoia pour répondre en temps réel aux alertes de cybersécurité. Un SOC (Security Operations Centers) est une équipe spécialisée dans la supervision et l'administration de la sécurité du système d'information. L'équipe travaille à l'aide de divers outils, tels que des outils de collecte, de corrélation d'événements et d'intervention à distance. L'entreprise Sekoia assiste l'équipe de cybersécurité de la Région SUD.

Avantages de Sekoia

Un de mes collègues m'a expliqué pourquoi ils avaient choisi Sekoia, et pourquoi ils allaient changer. Le contrat avec ce SOC présentes des avantages et des inconvénients. Les avantages de ce marché sont une expertise spécialisée sur certains domaines de cybersécurité, ce qui permet de résoudre certaine attaque efficacement, des dépenses initiales réduites ainsi qu'une surveillance 24h/24 à l'aide d'un SIEM.

Différentes alertes

Les outils de surveillance du SOC examine le réseau en temps réel à la recherche des comportements suspects. Delors qu'il en remarque un, leur logiciel rédige un rapport qui est transmis au service de la Région SUD. Le rôle de la région SUD est d'évaluer si l'alerte relevée est un faux positif* ou une réelle menace. Les raisons qui poussent au SOC à nous alerter sont très nombreuses et

évoluent à l'aide d'une IA. Par exemple, ça peut être l'heure de connexion à un poste anormale, une connexion depuis un pays suspect, des potentiels DDoS, des modifications inhabituelles de fichiers sensibles, des communications avec des utilisateurs inconnus…
Les alertes sont classées dans 3 niveaux ;

- Les alerte de niveau 1 sont réglées automatiquement par les logiciels de sécurité, comme les pares-feux ou les antivirus. Il peut s'agir d'un agent qui essaie d'accéder à un site interdit par exemple.
- Les alertes de niveau 2 nécessite la vérification d'un agent ainsi qu'une intervention si nécessaire. J'en présente deux dans la suite de cette partie.
- Les alertes de niveau 3 sont souvent la conséquence d'une cyberattaque réussie. Il faut des spécialistes pour régler le problème au plus vite car il y a une réelle menace. Ce sont les ingénieurs du SOC qui s'en occupe dans la plupart des cas.

Durant mon stage, j'ai eu la mission de traiter certaines alertes. Voici les deux types d'alertes les plus fréquentes :

Cas n°1 : Erreur d'un utilisateur

Des fausses manipulations ou des erreurs provoquées par des utilisateurs sont responsables d'une partie importante des alertes relevées. L'exemple si dessous est celui d'un utilisateur qui a rentré un mot de passe erronée plusieurs fois d'affilé, ce qui semblable à un bruteforce (figure 34).

Figure 34 : Exemple de faux positif

Cette alerte relève une potentielle tentative de bruteforce. La méthode pour vérifier si c'est un faux positif et de vérifier ce que relève le SOC. Ici, il est mention de 8 échecs de connexion à 7 heure du matin. Je vérifie si c'est une horaire habituelle pour le poste concerné et je vérifie également s'il n'y a eu aucun autre comportement suspect après cet incident. L'horaire est habituel et il n'y a pas d'autre alerte, j'évalue cette alerte comme faux positif.

Cas n°2 : Tentative d'intrusion

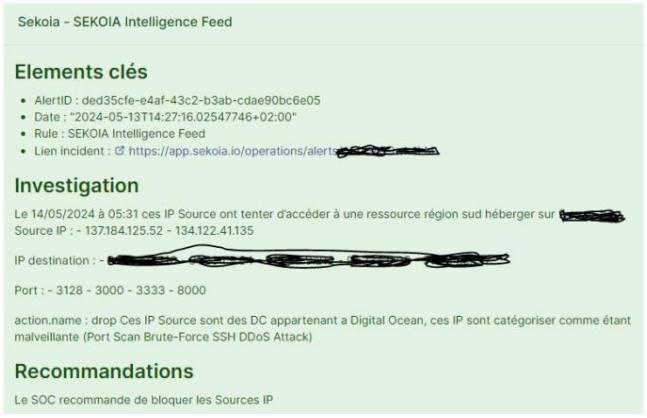


Figure 35 : Exemple de ticket de niveau 2

Sur cette alerte, on peut voir deux adresses qui ne sont pas répertoriées comme des IP d'agents, se connecter à des horaires suspectes.

A l'aide d'un site que le service utilise (figure 36), je viens vérifier si les IP sont connus des bases de données comme potentiellement dangereuses. Ici, 4 bases sur 94 reconnaissent l'origine de l'incident comme dangereuse.
L'ensemble des éléments qu'on a sur cette enquête me permettent d'évaluer cette situation comme anormale et dangereuse. Il faut suivre les recommandations du SOC, c'est-à-dire bloquer les IP. Je rédige un rapport similaire que je joins à mon collègue responsable. Ces IPs se feront bannir de tous les trafics de la région. C'est cette opération dont je faisais référence sur la partie « 2.4 Déployer l'application en ligne », mon gestionnaire de mots de passe et également concernés par ces mesures de sécurité.

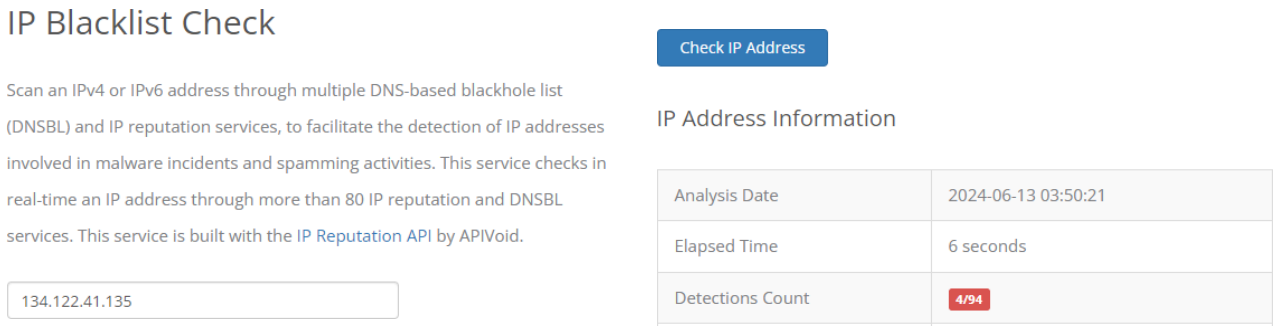


Figure 36 : Site pour vérifier les IP

Le SOC n'a relevé aucune autre alerte liée à celle-ci. Il est fort probable alors que la tentative a échoué. Aucune autre intervention est nécessaire. Cependant, certaine de ces tentatives peuvent réussir. C'est un cas critique et dans cette situation la procédure est différente.

Cas n°3 : Intrusion réussie

Comme dit précédemment, il est possible que des acteurs malveillants arrivent à s'introduire au sein du réseau. Je n'ai pas eu l'occasion d'en voir lors de mon stage, cependant j'ai pu étudier des anciennes alertes (que je ne peux partager pour des raisons de confidentialité). Lorsque ça arrive, le SOC ne peut pas évaluer la situation, il envoie généralement plusieurs alertes, car ce problème en entraine d'autre. Il demande l'autorisation pour avoir des accès particuliers afin de se renseigner plus en profondeur et/ou prendre le contrôle sur certaine machine. Cette procédure représente en une alerte de niveau 3. Le SOC a toujours apporté une solution dans les heures qui suivaient. Il est possible que les agents de la région interviennent également pour aider Sekoia dans leurs investigations. La région SUD a la réputation d'être un acteur fort dans la cybersécurité nationale. Aucune cyberattaque n'a abouti malgré de nombreuses tentatives. On m'a expliqué que les principaux risques étaient soit des ransomware* par des groupes de pirates ou soit des tentatives d'ingérences de pays/organisations malveillantes.

Pour conclure, j'ai trouvé cette mission très agréable, elle a fait écho à ma formation. Mes cours de cybersécurité m'ont familiarisé avec les contextes et le vocabulaire présentés. J'ai pu voir comment fonctionnait l'organisation d'un service de cybersécurité. C'était un domaine sur lequel j'avais des idées reçus, et ce genre d'immersion me permettent de mieux évaluer mes possibilités de mon projet professionnel.

3.2.2 Test d'intrusion Orange

La région SUD a sollicité les services de l'entreprise Orange pour un test d'intrusion (pentesting) de cinq jours couvrant l'ensemble du réseau. J'ai eu l'opportunité d'assister à leur travail,

et ils m’ont volontiers expliqué leurs méthodes et procédures. Je pouvais suivre leur travail grâce à l'expérience acquise lors de tests d'intrusion effectués durant mes études et sur des plateformes comme Hack The Box. Cependant, l'approche professionnelle adoptée par Orange était beaucoup plus avancée, utilisant des outils et des techniques que je ne connaissais pas. J’ai pu (re)découvrir des techniques ou des outils comme le Password spaying, Netexec ou Responder. Je présente plus de détail de cette partie dans l’annexe.

4 Conclusion

Ce stage a été une expérience formidable. J'ai eu l'occasion de voir concrètement comment les connaissances acquises durant mes études peuvent être appliquées à des situations réelles. Cela a été très gratifiant et m'a permis de comprendre l'importance pratique de ce que j'ai appris en cours.

Bien que le stage n’ait pas toujours été facile, il a souvent fallu s'investir pleinement et travailler de manière autonome, j'ai toujours bénéficié d'un bon accompagnement de la part de l'équipe. J’ai été mis plus d’une fois aux défis, ce qui a rendu l'expérience enrichissante.

Le contenu du stage était parfaitement cohérent avec mes études. J'ai non seulement pu approfondir des sujets déjà abordés, mais aussi en découvrir de nouveaux. Cette complémentarité entre la théorie et la pratique m'a beaucoup apporté.

Je suis maintenant sûr que les domaines de la cybersécurité et des réseaux me passionnent. J'attends avec impatience de pouvoir commencer une alternance pour découvrir plus en profondeur ce qui me plaît le plus dans ces domaines. J’ai acquis des compétences de savoir-être et plus d’autonomie que je n’avais pas forcément au début de ce stage, mais qui me seront utile pour mon alternance.

En conclusion, je suis vraiment enthousiaste à l'idée de débuter mon alternance. Cette prochaine étape sera l'occasion de continuer à apprendre et à m'épanouir dans un domaine qui me passionne.

5 Remerciements

Je tiens à remercier toutes les personnes qui ont contribué au bout déroulement de ce stage.

J'aimerais tout d'abord adresser mes remerciements à ma tutrice de stage Emmanuelle ROME, pour m'avoir toujours bien renseigné sur le fonctionnement de la Région et pour avoir consacré du temps au début de mon stage pour m'aider à m'introduire dans le service.
Je remercie tout autant Harun SENER, également au service architecture technique pour m'avoir donné des missions intéressantes et pour m'avoir expliqué le fonctionnement de leur réseau ainsi que leur datacenter. J'ai pu approfondir des notions que je connaissais déjà et en découvrir de nouvelles. Mes remerciements s'adressent également à JACQUIER Dominique et MURTAS Jérôme, respectivement chef de service et chef de service adjoint, pour m'avoir confié la responsabilité de faire le projet de gestionnaire de mots de passe. Ils m'ont apporté les moyens et les recommandations dont j'avais besoin pour le travailler en autonomie.

Enfin, j'aimerais remercier le corps professoral de mon BUT pour m'avoir motivé et donné les conseils qu'il fallait afin de trouver un stage qui me correspondait. Je suis reconnaissent notamment envers HOUSSAIN Corinne pour m'avoir donné des conseils afin de trouver une alternance ainsi que HOME Edouard pour m'avoir préparé au monde de l'entreprise.

6 Glossaire

BUT, Bachelor Universitaire de Technologie

Packet Tracer : Outil de simulation réseau développé par Cisco pour la formation et la pratique de la configuration réseau.

Machine virtuel (VM) : Machine virtualisée qui tourne sur une machine physique (ici sur des serveurs) et qui est accessible depuis plusieurs postes.

ANSII : L'Agence nationale de la sécurité des systèmes d'information, elle donne notamment des recommandations aux entreprises.

Actif/Passif : Méthode pour assurer la sécurité par redondance. L'actif est fonctionnel et le passif est prêt à prendre le relais si l'actif deviens hors-service

Logiciel d'accès : Logiciel permettant de se connecter à un système ou réseau, souvent utilisé pour le contrôle à distance. Utilisé ici pour se connecter à une VM qui n'est pas sur mon poste.

Conteneurisation : Technologie permettant d'exécuter des applications de manière isolée dans des conteneurs légers En utilisant Docker, j'ai pu simplifier le déploiement et améliorer la gestion de l'application sur ma VM.

Port : point virtuel de communication sur un ordinateur pour échanger des données via un réseau. Il faut associer chaque port à un service spécifique.

Client léger : Un client léger est entièrement géré par un serveur, de la gestion au stockage des données. On y accède à l'aide d'un navigateur, il n'y a pas de logiciel a installer.

HTTPS : HyperText Transfer Protocol Secure, protocole de communication sécurisé sur Internet.

http est également un protocole de communication mais celui-ci n’est pas chiffré

Module SSL : Composant logiciel assurant la sécurisation des communications via le protocole SSL/TLS.

Reverse Proxy : Serveur intermédiaire recevant les requêtes des clients avant de les transmettre aux serveurs appropriés.

Certificat et clef privée :

DNS : Domain Name System, système convertissant les noms de domaine en adresses IP. Exemple ; le DNS traduit www.amazon.com en 192.0.2.44.

PoE : Power over Ethernet, technologie permettant de fournir de l’électricité en même temps que des données via les câbles Ethernet.

Journaliser / LOG : Enregistrement des événements et activités sur un système informatique pour suivi et analyse.

Passphrase : Mot ou phrase complexe utilisé pour sécuriser l'accès à une ressource informatique, plus sûr qu'un simple mot de passe.

GitHub : Plateforme de développement collaboratif pour l'hébergement et la gestion de projets utilisant Git.

CLI : Command Line Interface, interface utilisateur permettant d'interagir avec un système informatique via des commandes texte.

SIEM : Security Information and Event Management, systèmes combinant la gestion des informations et des événements de sécurité.

Faux positif : Détection incorrecte d'une menace ou d'un événement de sécurité inexistant par un système de sécurité.

DDoS : Distributed Denial of Service, attaque visant à rendre un service indisponible en le submergeant de trafic.

Bruteforce : Méthode d'attaque consistant à essayer toutes les combinaisons possibles pour découvrir un mot de passe.

Ransomware : Logiciel malveillant qui chiffre les données d'une victime et demande une rançon pour les déchiffrer.

7 Bibliographie

-Recommandations relatives à l'interconnexion d'un système d'information à Internet. (19 juillet 2020). *Guide ANSII*

-Provence-Alpes-Côte d'Azur. (17 juin 2024). *Wikipédia, l'encyclopédie libre :* Provence-Alpes-Côte d'Azur — Wikipédia (wikipedia.org)

-Wiki de Vaultwarden (2024). *Wiki-Tech :* Bitwarden (Vaultwarden) | Wiki-Tech

- Héberger son gestionnaire de mot de passe : Vaultwarden (23 Avril 2022). *Zatoufly – Youtube* \ Créer son serveur Vaultwarden avec docker (zatoufly.fr)

-Forum officieux de Vaultwarden (2019-2024). *Github: https://github.com/dani-garcia/vaultwarden*

-Responder | Kali Linux Tools (11 mars 2024). *Kali.org : https://www.kali.org/tools/responder/*