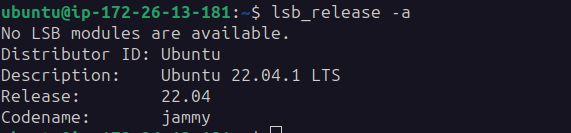
Rapport de test Pratique

1. Préparation et Endurcissement du Serveur
2. Installation d’un nouveau serveur linux. Dans mon cas j’ai opté pour Ubuntu Server 22.04.1 LTS.

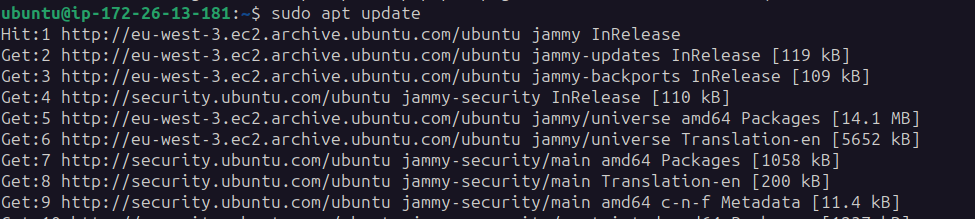


1. Check-list de sécurisation d’un serveur linux

* Faire des mises à jour régulières du système.
* Changement du port SSH.
* Installer et configurer un pare-feu histoire de limiter les accès sur le serveur.
* Désactiver la connexion SSH pour les utilisateurs root.

1. Endurcir la sécurité du serveur en se basant sur la check-list

* Faire des mises à jour régulières du système : Pour ce faire il suffit d’exécuter un apt-update.



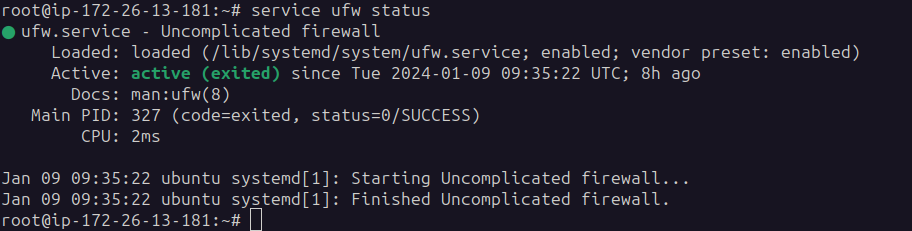
* Changement du port SSH

Pour cela on se rend dans le fichier de configuration de SSH et on remplace le port par défaut (22) par 2022 :

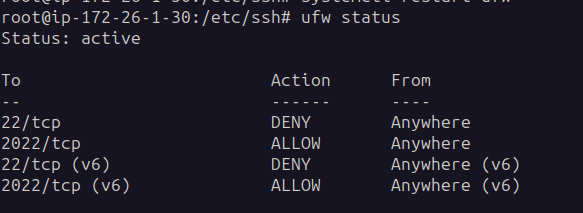


* Installer et configurer un pare-feu histoire de limiter les accès sur le serveur

Dans mon cas ici j’ai choisi comme gestionnaire de pare-feu “UFW”. Il est préinstallé sur ubuntu server. Par défaut il est down. Nous pouvons vérifier son status avec cette commande : “ufw status ou service ufw status”.



Pour activer le pare-feu il suffit de faire un “sudo ufw enable ou sudo service ufw enable”. J’ajoute maintenant mon port ssh (2022) sur mon pare-feu :



* Désactiver la connexion SSH pour les utilisateurs root.

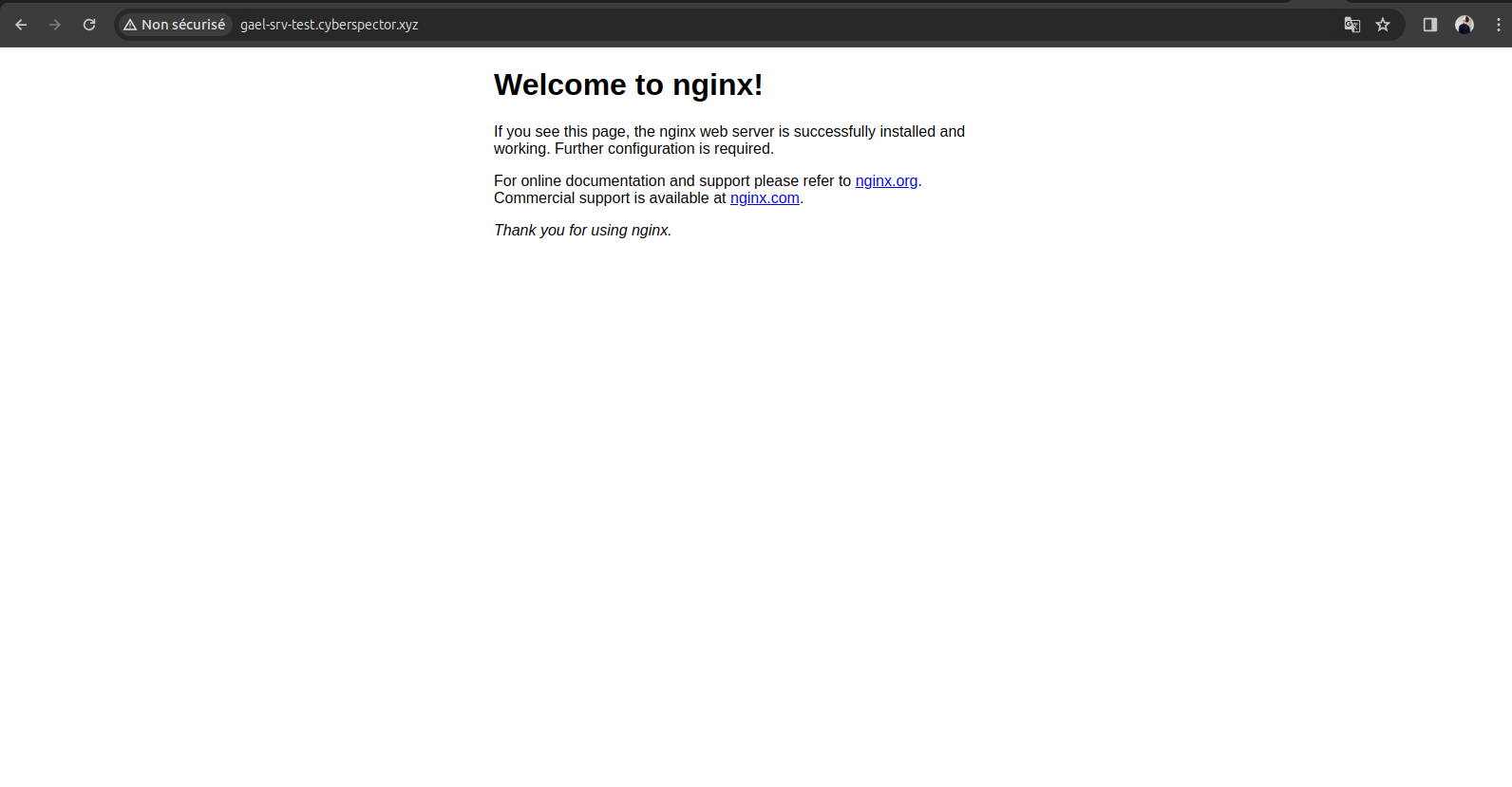
Dans le fichier de configuration SSH sshd\_config nous allons modifier la ligne PermitRootLogin yes en remplaçant yes par no pour désactiver les connexions SSH pour l’utilisateur root :



1. Mise en Place du Serveur Web Sécurisé
2. Installez et configurez un serveur web

Dans mon cas j’ai opté pour le serveur nginx. Ce dernier est installable en exécutant la commande “sudo apt-get install nginx”.

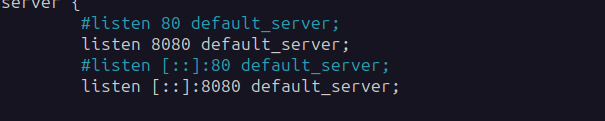
Je peux maintenant accéder à mon serveur web en faisant par une requête http “http://gael-srv-test.cyberspector.xyz/”.



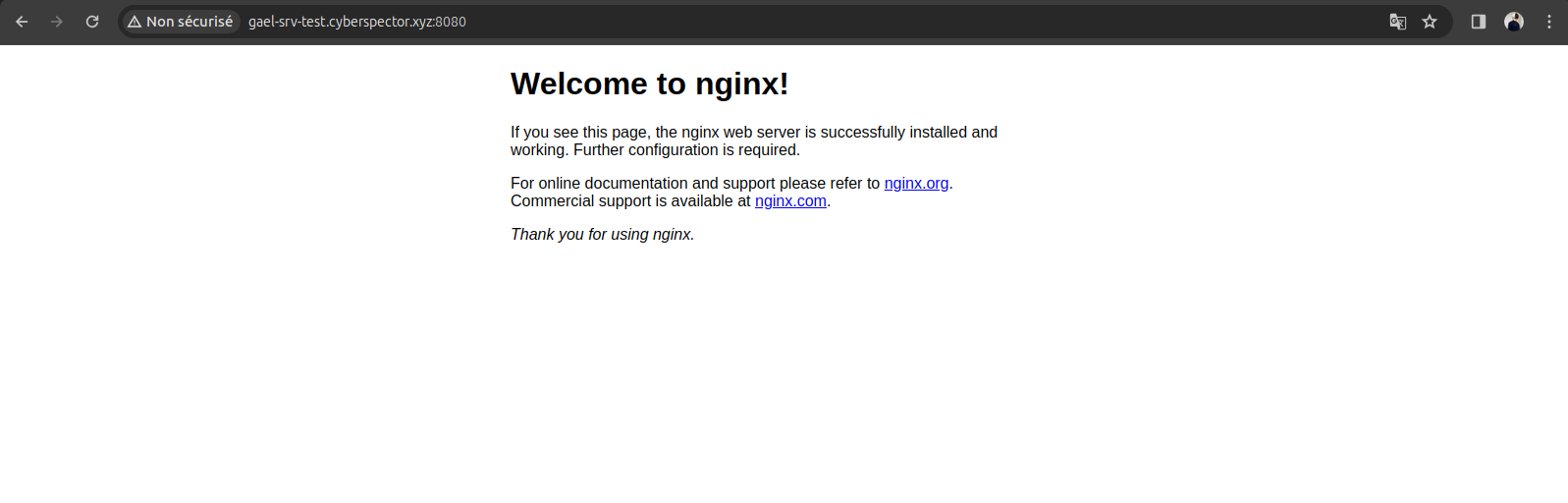
Petit rappel j’ai dû ajouter le port http par défaut (80) a mon pare-feu pour que les requêtes aillent sur mon serveur.

1. Sécurisez le serveur web.

Dans un premier temps je vais changer le port par défaut (80 -> 8080) pour les requêtes http vers le serveur nginx en modifiant la ligne “listen port” du fichier de configuration de nginx.

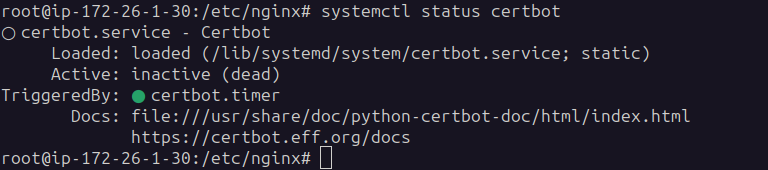


Il faudra aussi ajouter le nouveau port (8080) au pare-feu.



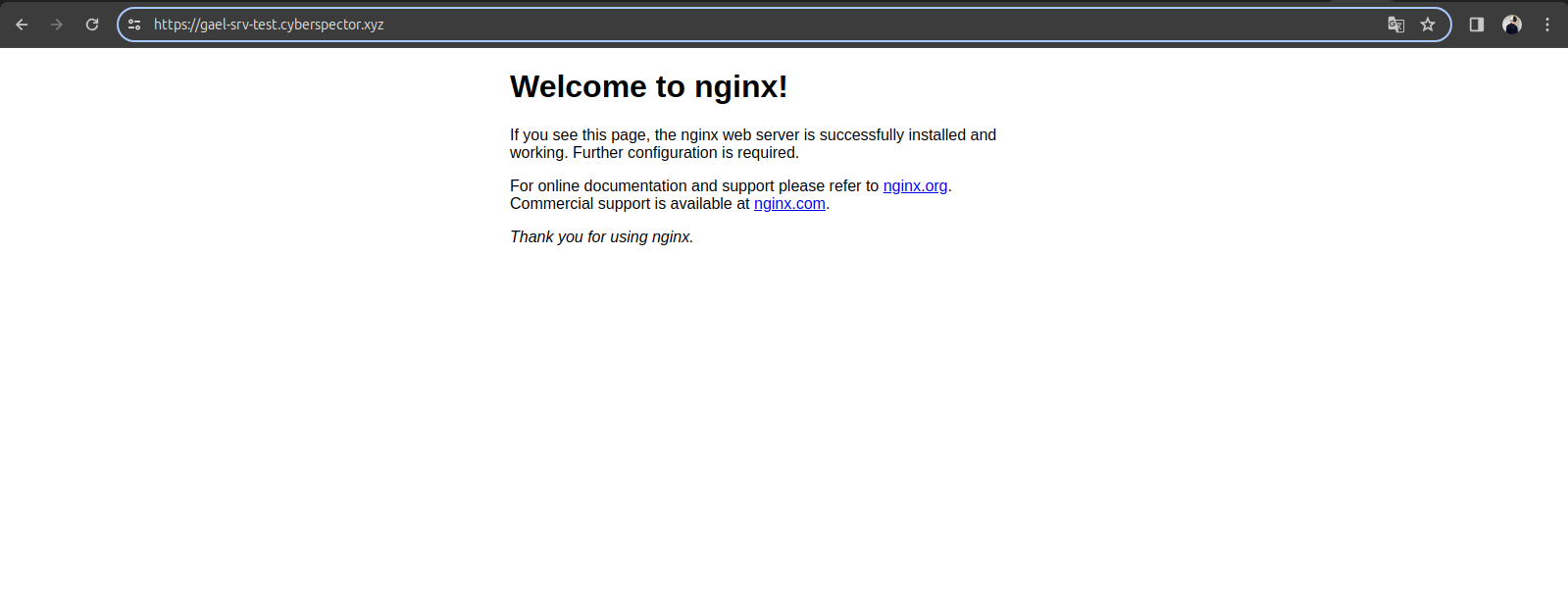
Dans un second temps je vais sécuriser le site web avec HTTPS, en faisant la demande d’un certificat SSL/TLS gratuit avec Let's Encrypt à partir de Certbot :

D’abord je vais commencer par installer Certbot avec la commande : sudo apt install certbot.



Ensuite il me faut exécuter cette commande “sudo certbot –nginx -d gael-srv-test.cyberspector.xyz” et suivre ensuite les instructions de Certbot pour obtenir un certificat sécuriser pour mon site web.





Nous pouvons voir que le site est bel et bien sécurisé à présent.