Rapport d'audit

Auditeur : **BOTTET Damien**

Date de l'audit : **31/08/*2023***
Date de rédaction du rapport : **06/09/*2023***

Audit de sécurité du serveur *hébergeant l'application Wordpress*

Destinataires :

Camille BERT (Green Planet – DSI)

Commanditaire :
Camille BERT (Green Planet - DSI)

Contexte :
Je suis auditeur technique en freelance, et effectue régulièrement des missions d'audit de sécurité des SI.
La DSI de Green Planet se rapproche donc de moi pour me proposer une mission d'audit de sécurité à effectuer sur l'un de leurs serveurs, que j'accepte volontiers.
Lors de mon arrivée, la responsable du service Informatique, Camille Bert, m'accueille pour me décrire l'objectif de ma mission : auditer la sécurité de leur serveur web.

Camille BERT , me fourni alors les identifiants pour me connecter sur le compte **root** afin que je puisse mener à bien ma mission d'audit de sécurité.

Résultats :
Nombre total de recommandations : 47
Nombre de recommandations Critical : 34
Nombre de recommandations Warning : 13

Conclusion :

L'audit de sécurité réalisé sur le serveur Web de GreenPlanet a émis un nombre important de faille de sécurité, qu'il faudra les résoudre dans les plus bref délais.

Cela concerne principalement le système d'exploitation **Debian,** les processus de démarrage, le serveur web **Wordpress,** le serveur **Nginx,** la base de donnée **Mysql,** le réseau, le service **SSH.**

Cet audit a aussi permis de constater que, sur les éléments précédemment cités, c'est la configuration par défaut qui est généralement en vigueur sur votre serveur. Il est fortement recommandé de faire une configuration sécurisé afin d'éviter des cyberattaques.

TABLE DES MATIERES

1.Résumé des recommandations

Partie 1 : Résumé des recommandations Système :

N°	Recommandation	Type	Principe
SYS.1	Activer les flags PAE et NX dans le Bios	Critical	Défense en profondeur
SYS.2	Chiffrez les partitions sensible du système	Critical	Défense en profondeur
SYS.3	Protéger la partition /boot	Critical	Moindre privilège
SYS.4	Appliquez une politique de mise à jour régulière des mots de passe utilisateurs	Critical	Défense en profondeur
SYS.5	Autorisez uniquement les administrateurs à exécuter la commande sudo.	Critical	Moindre privilège
SYS.6	Mettez à niveau Debian et les paquets	Critical	Défense en profondeur
SYS.7	Éditez le fichiers /etc/sudoers afin que les administrateurs puissent maintenir le système	Critical	Moindre privilège
SYS.8	Créer un groupe d'administrateurs et y ajouter les utilisateurs qui auront ce rôle qui seront bien identifiés, afin de gérer la traçabilité des actions d'administration	Critical	Moindre privilège
SYS.9	Installez un antivirus sur le serveur	Critical	Défense en profondeur
SYS.10	Monitorez l'usage la mémoire vive	Warning	Moindre privilège
SYS.11	Fermez les ports inutiles	Critical	Minimisation
SYS.12	Utiliser des mots de passes spécifique pour les services extérieur	Warning	Défense en profondeur

Partie 2 : Résumé des recommandations Processus de démarrage :

N°	Recommandation	Type	Principe
BOO.1	Restreindre les droits sur « /etc/grub.d » à l'utilisateur « root » seulement. Mode 700	Critical	Moindre privilège
BOO.2	Empêcher la connexion directe de l'utilisateur « root » depuis une console virtuelle.	Critical	Défense en profondeur
BOO.3	Désactiver la combinaison « Ctrl+Alt+Suppr » sur le serveur afin deprévenir tout redémarrage depuis un accès physique à la machine.	Critical	Défense en profondeur
BOO.4	Désactiver les cibles inutiles démarrées automatiquement avec le serveur.	Critical	Minimisation
BOO.5	Désactiver les services non essentiels démarrées automatiquement avec le serveur.	Critical	Défense en profondeur
BOO.6	Désactiver les services non-essentiels démarrées automatiquementavec le serveur.	Critical	Défense en profondeur
BOO.7	Désactiver les Magic System Request Keys afin de prévenir toute utilisation de touches clavier pour réaliser des requêtes système	Warning	Défense en profondeur

BOO.8	Augmenter l'intervalle minimal de temps entre chaque tentative de connexion sur le module «pam_faildelay.so » afin de ralentir les attaques par dictionnaire.	**Warning**	Défense en profondeur
BOO.9	Passer l'option « iommu=force » au noyau lors du démarrage de Linux afin de protéger la mémoire contre des accès non contrôlés issus des périphériques du système.	**Warning**	Minimisation
BOO.10	Limiter le chargement de modules supplémentaires au démarrage du noyau.	**Warning**	Minimisation

Partie 3 : Résumé de recommandations Services :

N°	**Recommandation**	**Type**	**Principe**
SER.1	Mettez à jour régulièrement les paquets pour le bon fonctionnement	**Critical**	Défense en profondeur
SER.2	Désactiver le service dhclient	**Critical**	Minimisation
SER.3	Désactiver le service Bind9 (DNS) et bloquez le port 53 (DNS) en trafic entrant	**Critical**	Minimisation
SER.4	Utiliser des outils de supervision de fichiers de traces (Nagios et/ou Logwatch).	**Warning**	Défense en profondeur
SER.5	Désactiver le service NFS	**Warning**	Minimisation
SER.6	Isoler les services Nginx, MySQL et Bind9 avec «Docker ».	**Warning**	Défense en profondeur
SER.7	Externaliser les traces sur serveur de centralisation des logs.	**Warning**	Défense en profondeur

Partie 4 : Résumé des recommandations Réseau

N°	Recommandation	Type	Principe
NET.1	Désactiver les services ouvrant des ports inutiles (Asterisk et RPC).	**Critical**	Minimisation
NET.2	Configurer les interfaces réseau en IP statiques et désactiver l'interface eht2 si elle n'est pas utilisé	**Critical**	Minimisation
NET.3	Interdisez la connexion en SSH pour le root	**Critical**	Défense en profondeur
NET.4	Changer le port utilisé par le SSH.	**Critical**	Défense en profondeur
NET.5	Appliquer une politique au niveau du pare-feu de rejet par défaut des requêtes, et ensuite laisser passer les types de requêtes souhaitées.	**Critical**	Défense en profondeur
NET.6	Désactiver l'IPV6 si celui-ci n'est pas utilisé	**Warning**	Minimisation
NET.7	Recompiler le noyau avec une prise en charge de Netfilter sans avoir besoin de faire appel à des modules.	**Warning**	Minimisation

Partie 5 : Résumé des recommandations Nginx :

N°	Recommandation	Type	Principe
NGX.1	Mettez à jour régulièrement le serveur NGINX	**Critical**	Défense en profondeur
NGX.2	Configurez le site Web par pair de clé SSL pour une connexion sécurisé en HTTPS	**Critical**	Défense en profondeur
NGX.3	Masquez la version de NGINX afin de se protéger contre les cyberattaques	**Critical**	Défense en profondeur

Partie 6 : Résumé des recommandations MySQL:

N°	Recommandation	Type	Principe
SQL.01	Mettez à jour MySQL	**Critical**	Défense en profondeur
SQL.02	Choisissez un port d'écoute , différents de celui par défaut	**Critical**	Défense en profondeur
SQL.03	Ne saisissez pas de mot de passe en vous connectant sur MySQL. Cela évitera l'aperçu des commandes dans l'historique	**Critical**	Défense en profondeur
SQL.04	Changez les mots de passe régulièrement pour les utilisateurs ayant des privilèges élevés	**Critical**	Défense en profondeur

Partie 7 : Résumé des recommandations Wordpress :

N°	Recommandation	Type	Principe
WP.01	Mettez à jour Worpress	**Critical**	Défense en profondeur
WP.02	Créez un utilisateur dans la base de données wp_db avec les droits administrateurs	**Critical**	Défense en profondeur
WP.03	Modifiez les droits config.PHP	**Critical**	Défense en profondeur
WP.04	Installez un pare-feu pour le site Web (DNS)	**Warning**	Défense en profondeur

2. Méthodologie de l’audit

2.1. Principe de minimisation

Le principe de minimisation est la recommandation **R1** du guide de **l’ANSSI**
Lien de référence : **https://www.ssi.gouv.fr/uploads/2016/01/linux_configuration-fr-v1.2.pdf**

Ce principe indique que les systèmes conçus et installés doivent éviter autant que possible toute complexité inutile en vue de:
• Réduire la surface d’attaque au strict minimum
• Permettre une mise à jour et un suivi du système efficace
• Rendre l’activité de surveillance des systèmes plus accessible,dans la mesure où le nombre de composants à surveiller est réduit.

La mise en œuvre de ce principe est parfois délicate car il peut se retrouver rapidement en contradiction avec d’autres,tout aussi importants.Seule une étude de cas avec l’aide d’une expertise système et sécurité permettra de faire des choix raisonnables. Les chapitres suivants donneront des recommandations ciblées suivant les parties envisagées du système.

2.2. Principe de moindre privilège

Le principe de minimisation est la recommandation **R3** du guide de **l’ANSSI**
Lien de référence : **https://www.ssi.gouv.fr/uploads/2016/01/linux_configuration-fr-v1.2.pdf**

Ce principe définit que tout objet ou entité gérée par un système ne dispose que des droits strictement nécessaires à son exécution, et rien de plus. L’objectif est à la fois un gain en sécurité et sûreté:
• Les conséquences de dysfonctionnements ou vulnérabilités sont limitées aux privilèges octroyés
• L’altération ou la compromission du système nécessitent une escalade de privilèges, moins triviale et discrète à réaliser dans les cas où plusieurs couches de protection sont mises en place.

2.3. Principe défense en profondeur

Le principe de minimisation est la recommandation **R5** du guide de **l’ANSSI**
Lien de référence : **https://www.ssi.gouv.fr/uploads/2016/01/linux_configuration-fr-v1.2.pdf**

Le principe de défense en profondeur impose la conception de plusieurs couches de sécurité indépendantes et complémentaires en vue de retarder une attaque dont l’objectif est la compromission du système.
Sous Unix et dérivés, la défense en profondeur doit reposer sur une combinaison de barrières qu’il faut garder indépendantes les unes des autres. Par exemple:
• Authentification nécessaire avant d’effectuer des opérations, notamment quand elles sont privilégiées
• Journalisation centralisée d’évènements au niveau systèmes et services
• Utilisation préférentielle de services qui implémentent des mécanismes de cloisonnement ou de séparation de privilèges
• Utilisation de mécanismes de prévention d’exploitation.

3. Périmètre de l’Audit

3.1. Cible de l’audit :

Le périmètre de l’audit consiste à évaluer et prendre en compte les failles de sécurité du serveur Web **NGINX** qui tourne actuellement sur un serveur Linux **Debian.**
Le serveur linux **Debian** héberge un serveur de base de données **MySQL ,** mais aussi un logiciel de création de site Web **WordPress.**

3.2. Les éléments de la cible auditée :

La configuration du système est la suivante :

Composant	Version	Description
Debian (Jessie)	8.11	Système d’exploitation
NGINX	1.6.2	Serveur Web
WordPress	4.1.38	Logiciel de création de site Web
MySQL	5.5.62	Serveur de base de données

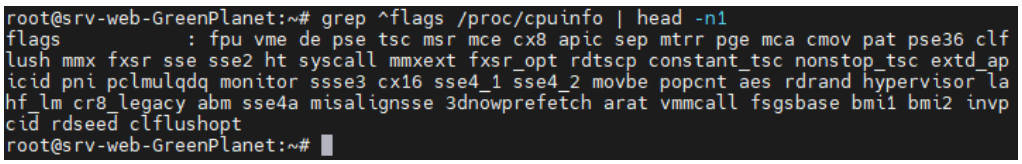
3.3. Serveur en production :

Il est important de noter que le serveur audité est en mode production. C’est la raison pour laquelle j’ai pris soin de ne pas en perturber le fonctionnement durant mon audit ni d’en changer la configuration ou le paramétrage.

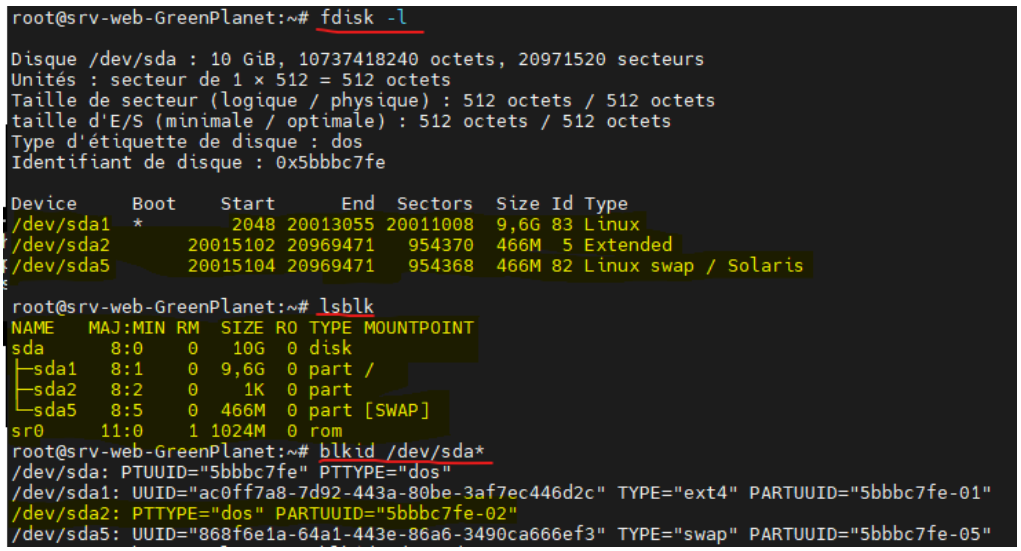
4. Détails des Recommandations

4.1.Détails des Recommandations Système :

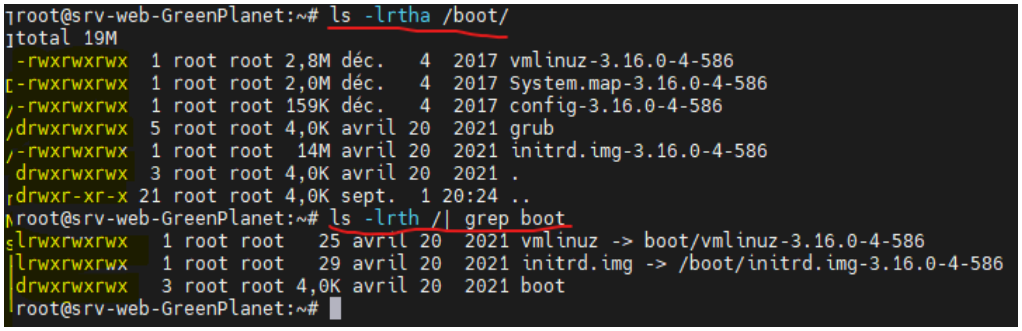
La recommandation **R24** du guide de **l’ANSSI**
Lien de référence : **https://www.ssi.gouv.fr/uploads/2016/01/linux_configuration-fr-v1.2.pdf**

SYS.1	Flags CPU (PAE et NX)
Objectif	Le CPU doit protéger l’exécution d’instructions stockées dans les régions mémoire qui sont non autorisée
Principe associé	Défense en profondeur
Type	**CRITICAL**
Commande	grep ^flags /proc/cpuinfo | head -n1 | egrep --color=auto ' (pae|nx) '
Capture	
Recommandations	Activer les flags PAE et NX dans le BIOS

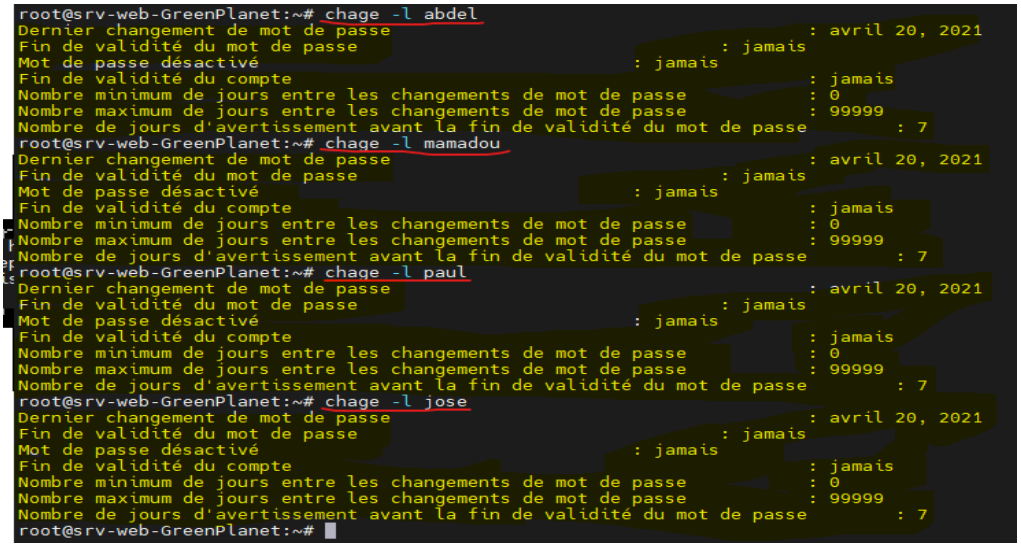
La recommandation **R8** du guide de **l'ANSSI**
Lien de référence : **https://www.ssi.gouv.fr/uploads/2016/01/linux_configuration-fr-v1.2.pdf**

SYS.2	Chiffrez les partitions sensible du système
Objectif	Isoler les partition /boot, /tmp, /home, /var et /var/log.
Principe associé	Défense en profondeur
Type	**CRITICAL**
Commande	Fdisk -l lsblk blikd /dev/sda*
Capture	
Recommandations	Chiffrer la partition / via les outils « ecryptfs-utils » et « cryptsetup ».

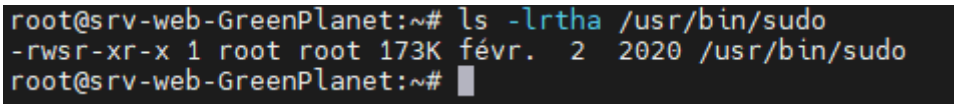
La recommandation **R29** du guide de **l'ANSSI**
Lien de référence : **https://www.ssi.gouv.fr/uploads/2016/01/linux_configuration-fr-v1.2.pdf**

SYS.3	Protéger la partition /boot
Objectif	Isoler les composants du système de fichiers
Principe associé	Moindre privilège
Type	**CRITICAL**
Commande	Ls -lrtha /boot/ ls -lrth /| grep boot
Capture	
Recommandations	Changer les permissions

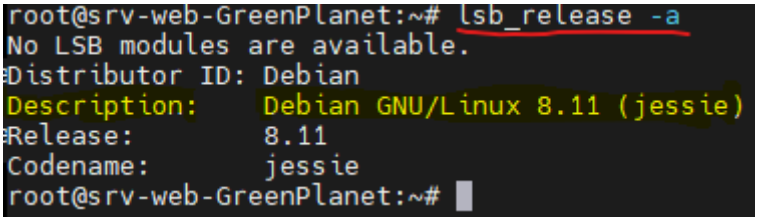
La recommandation **R5** du guide de **l'ANSSI**
Lien de référence : **https://www.ssi.gouv.fr/uploads/2016/01/linux_configuration-fr-v1.2.pdf**

SYS.4	Appliquez une politique de mise à jour régulière des mots de passe utilisateurs
Objectif	Changer les mots de passe utilisateurs
Principe associé	Défense en profondeur
Type	**CRITICAL**
Commande	chage -l *nom_utilisateur* *Ichage -m 7 -M 90 -W 10 nom_utilisateur*
Capture	
Recommandations	La commande suivante permet de forcer l'utilisateur à changer son mot de, min 7jours et max tous les 90 jours, avec une alerte 10 jours avant son expiration.

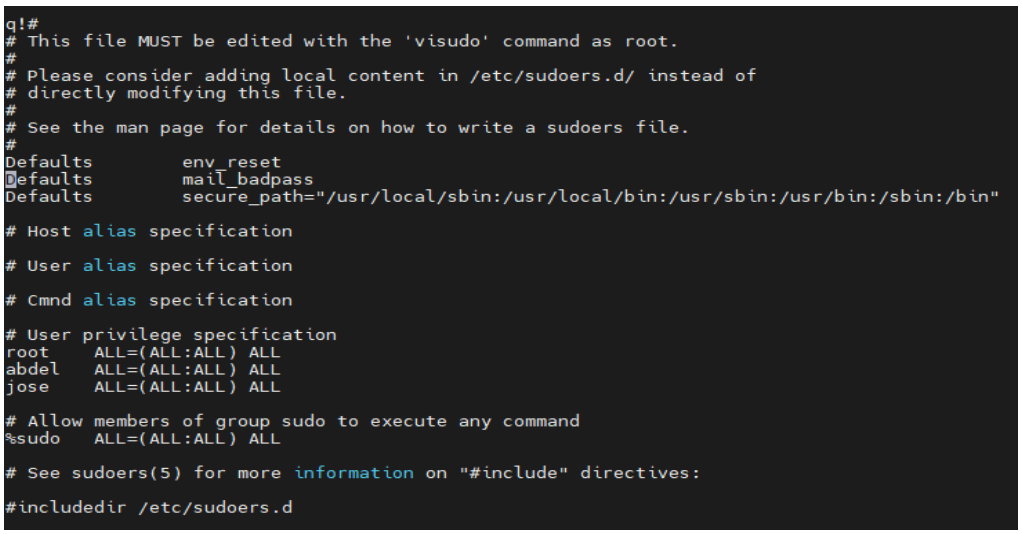
La recommandation **R38** du guide de **l'ANSSI**
Lien de référence : **https://www.ssi.gouv.fr/uploads/2016/01/linux_configuration-fr-v1.2.pdf**

SYS.5	Autorisez uniquement les administrateurs à exécuter la commande sudo.
Objectif	Donner les privilège pour le root et administrateur
Principe associé	Moindre privilège
Type	**CRITICAL**
Commande	ls -lrtha /usr/bin/sudo
Capture	
Recommandations	en tant qu'administrateur, rendre « sudo » exécutable uniquement par le groupe « admin » (+ utilisateur « root ») via les deux commandes suivantes : chmod 4750 /usr/bin/sudo chown root:admin /usr/bin/sudo

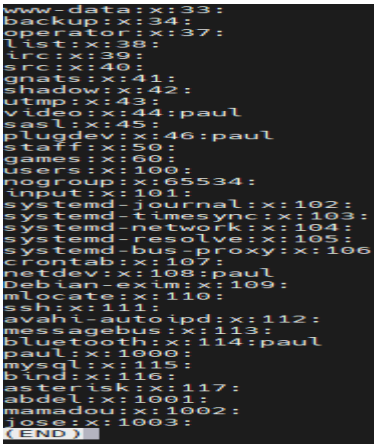
La recommandation **R61** du guide de **l'ANSSI**
Lien de référence : **https://www.ssi.gouv.fr/uploads/2016/01/linux_configuration-fr-v1.2.pdf**

SYS.6	Mettez à niveau Debian et les paquets
Objectif	Remise à niveau de Debian
Principe associé	Défense en profondeur
Type	**CRITICAL**
Commande	lsb_release -a
Capture	
Recommandations	Debian 8 est obsolète et ne bénéficie plus de mise à jour depuis le 17 juin 2018. Cela représente une faille de sécurité importante. En mode administrateur, il faudra changer le fichier /etc/apt/sources.list pour n'avoir que ces lignes : • deb http://deb.debian.org/debian stable main contrib non-free • deb http://security.debian.org/debian-security stable-security main contrib non-free Ensuite lancer la mise à niveau via la commande : apt full-upgrade

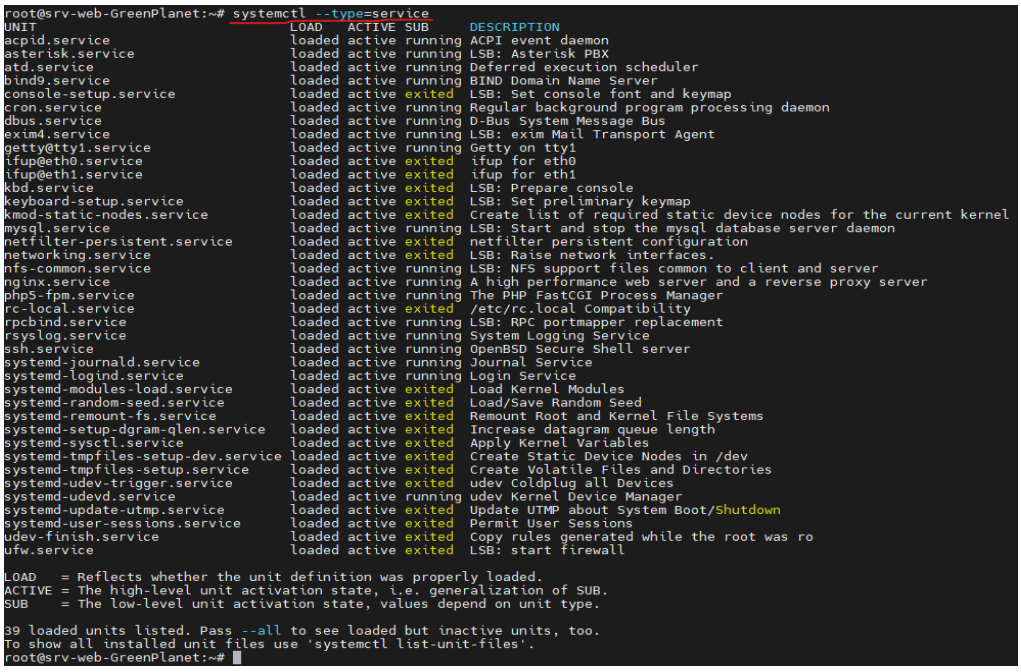
La recommandation **R38** du guide de **l'ANSSI**
Lien de référence : **https://www.ssi.gouv.fr/uploads/2016/01/linux_configuration-fr-v1.2.pdf**

SYS.7	Éditez le fichiers /etc/sudoers pour la maintenance du système
Objectif	Donner les droit aux administrateurs
Principe associé	Moindre privilège
Type	**CRITICAL**
Commande	Nano /etc/sudoers
Capture	
Recommandations	Ajoutez la ligne suivante dans le fichier /etc/sudoers : %admin ALL=(ALL) ALL

La recommandation **R37** du guide de **l'ANSSI**
Lien de référence : **https://www.ssi.gouv.fr/uploads/2016/01/linux_configuration-fr-v1.2.pdf**

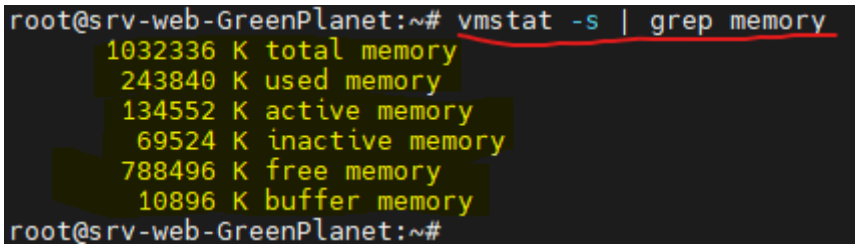
SYS.8	Groupe administrateur
Objectif	Disposer des droits administrateurs bien identifiés pour gérer la traçabilité des actions d'administration.
Principe associé	Moindre privilège
Type	**CRITICAL**
Commande	less /etc/group
Capture	 
Recommandations	En tant que root, créer un groupe « admin », et y intégrer les administrateurs

La recommandation **R56** du guide de **l'ANSSI**
Lien de référence : **https://www.ssi.gouv.fr/uploads/2016/01/linux_configuration-fr-v1.2.pdf**

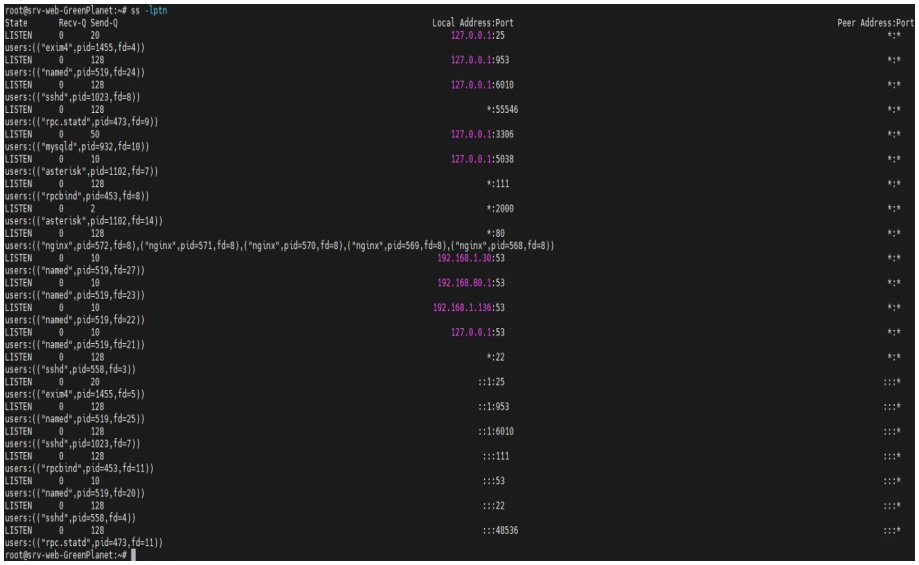
SYS.9	Installez un antivirus sur le serveur
Objectif	Installer un antivirus
Principe associé	Défense en profondeur
Type	**CRITICAL**
Commande	Systemctl --type=service
Capture	

Recommandations	Il est recommandé d’installer un antivirus

La recommandation **R8** du guide de **l’ANSSI**
Lien de référence : **https://www.ssi.gouv.fr/uploads/2016/01/linux_configuration-fr-v1.2.pdf**

SYS.10	Monitorez l’usage de la mémoire vive
Objectif	Suivre l’usage de la mémoire
Principe associé	Défense en profondeur
Type	**Warning**
Commande	vmstat -s | grep memory
Capture	
Recommandations	Pour monitorer l’usage de la RAM , il existe un logiciel appelé **Nagios**

La recommandation **2.1** du guide de **l’ANSSI** (principe minimisation)
Lien de référence : **https://www.ssi.gouv.fr/uploads/2016/01/linux_configuration-fr-v1.2.pdf**

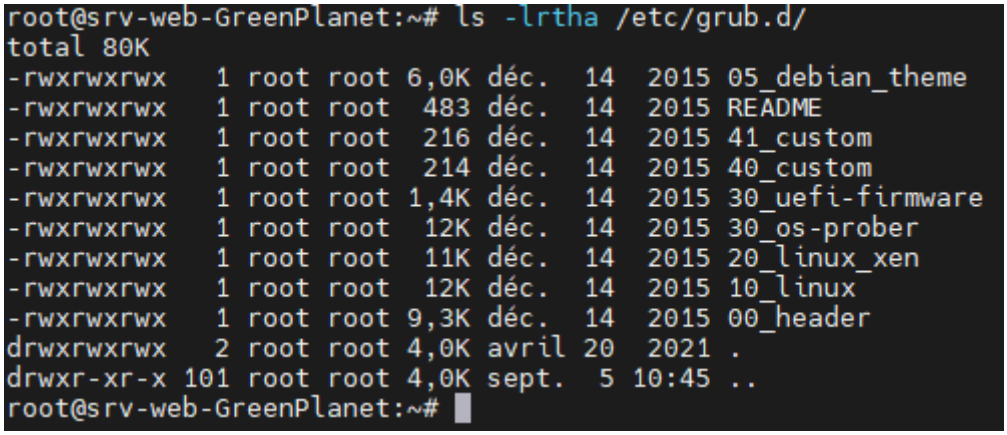
SYS.11	Fermez les ports inutiles
Objectif	Fermez tous les ports inutiles pour le serveur
Principe associé	Minimisation
Type	**CRITICAL**
Commande	Ss -lptn
Capture	
Recommandations	Fermez les ports inutiles pour le serveur et pour une meilleure sécurité

La recommandation **R31** du guide de **l'ANSSI**
Lien de référence : **https://www.ssi.gouv.fr/uploads/2016/01/linux_configuration-fr-v1.2.pdf**

SYS.12	Utiliser des mots de passes spécifique pour les services extérieur
Objectif	Sécuriser les connexion extérieur
Principe associé	Défense en profondeur
Type	**Warning**
Recommandations	Il est fortement recommandé de mettre des mots de passes différents des services extérieur

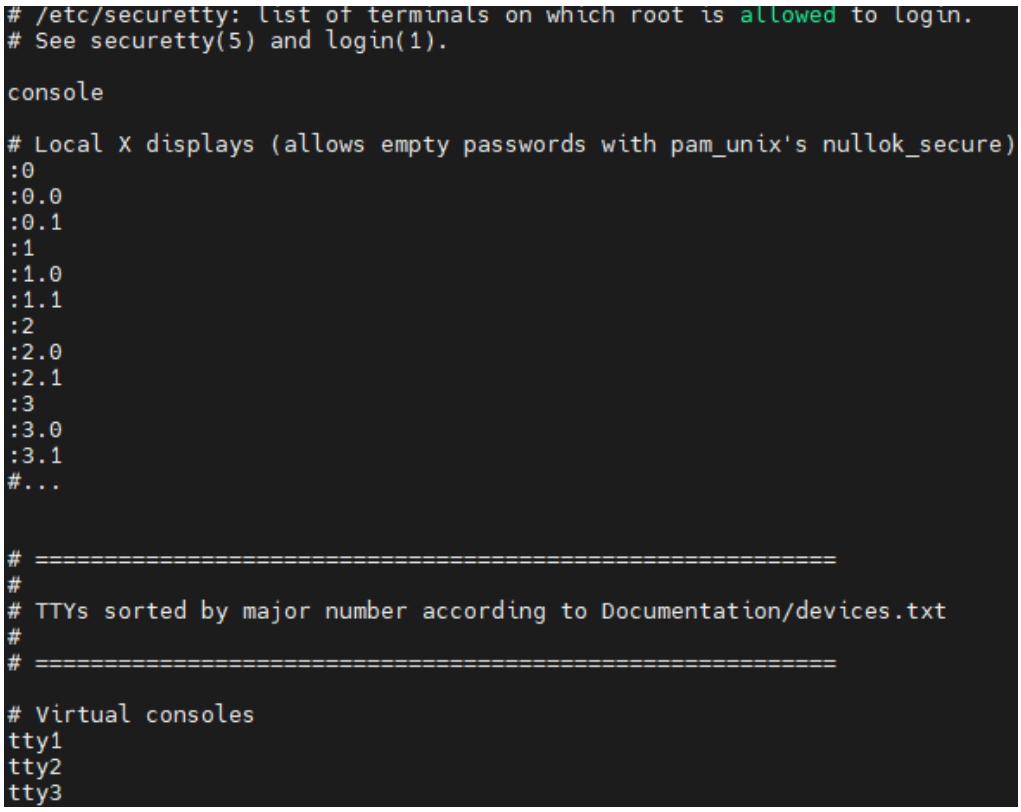
4.2.Détails des Recommandations Processus de démarrage

La recommandation **2.2** du guide de **l'ANSSI** (principe moindre privilège)
Lien de référence : **https://www.ssi.gouv.fr/uploads/2016/01/linux_configuration-fr-v1.2.pdf**

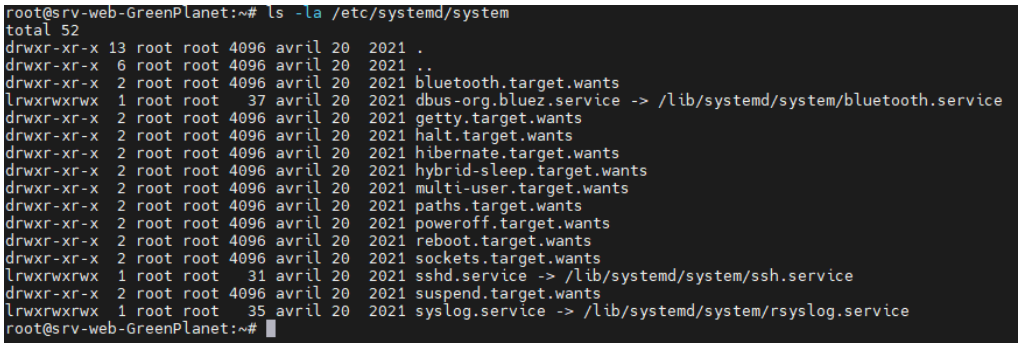
BOO.1	Restreindre les droits sur « /etc/grub.d » à l'utilisateur « root » seulement. Mode 700
Objectif	Mettez les droits uniquement à root
Principe associé	Moindre privilège
Type	**CRITICAL**
Commande	ls -lrtha /etc/grub.d/
Capture	
Recommandations	Passer les droits sur l'arborescence « /etc/grub.d/ » à 700 via la commande en mode root : Chmod -R 700 /etc/grub.d

La recommandation **2.1** du guide de **l'ANSSI** (défense en profondeur)
Lien de référence : **https://www.ssi.gouv.fr/uploads/2016/01/linux_configuration-fr-v1.2.pdf**

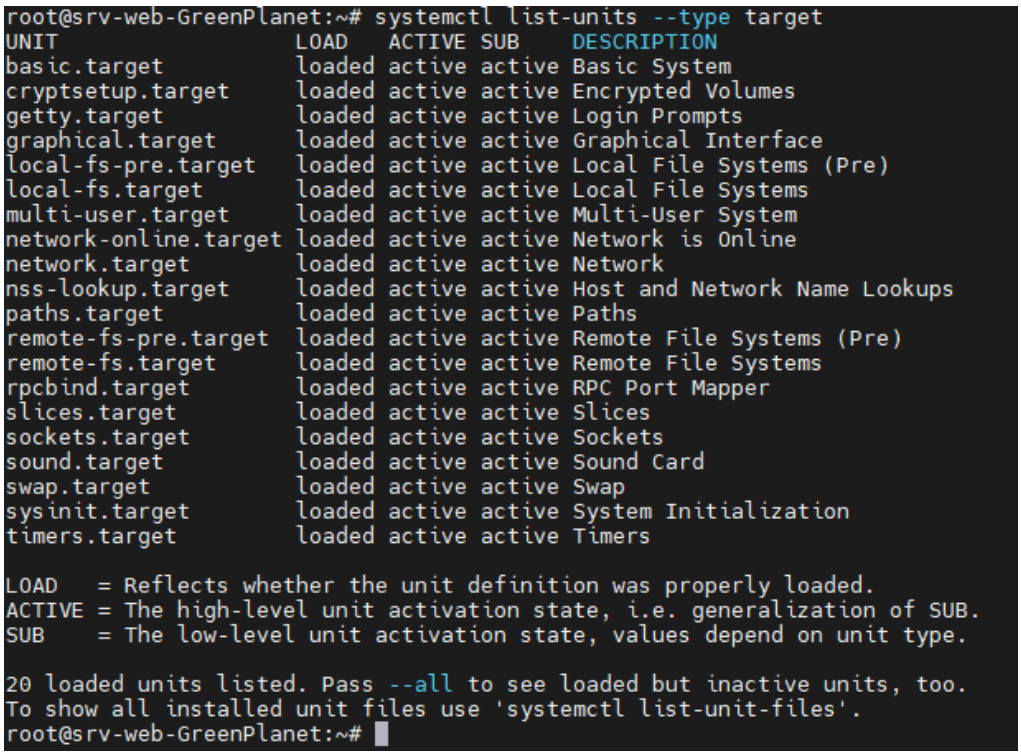
BOO.2	Empêcher la connexion directe de l'utilisateur « root » depuis une console virtuelle.
Objectif	Empêcher la connexion directe de l'utilisateur « root » depuis une console virtuelle.
Principe associé	Défense en profondeur
Type	**CRITICAL**
Commande	less /etc/securetty

Capture	
Recommandations	Vider le contenu du fichier « /etc/securetty » en tapant la commande suivante en tant qu'administrateur : echo > /etc/securetty

La recommandation **R9** du guide de **l'ANSSI**
Lien de référence : **https://www.ssi.gouv.fr/uploads/2016/01/linux_configuration-fr-v1.2.pdf**

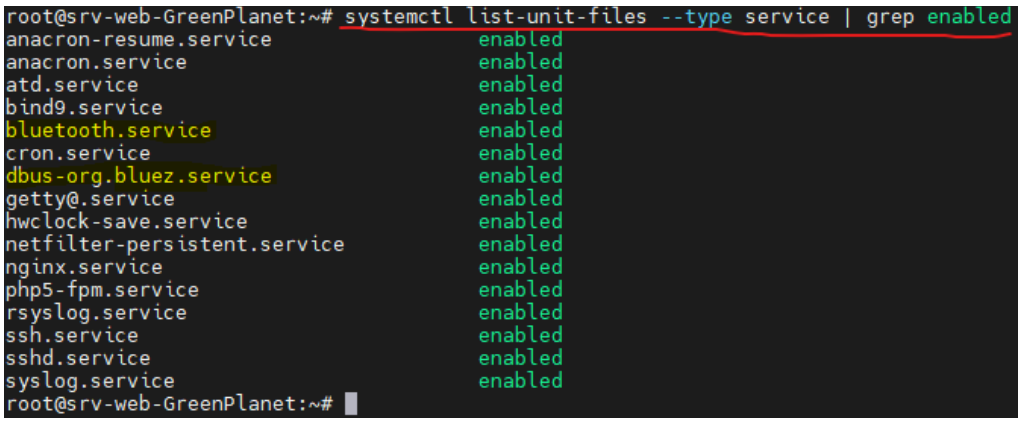
BOO.3	Désactiver la combinaison « Ctrl+Alt+Suppr » sur le serveur afin deprévenir tout redémarrage depuis un accès physique à la machine.
Objectif	Prévenir tout redémarrage depuis un accès physique à la machine.
Principe associé	Défense en profondeur
Type	**CRITICAL**
Commande	ls -la /etc/systemd/system
Capture	
Recommandations	Désactiver la combinaison « Ctrl+Alt+Suppr » sur le serveur en tapant la commande suivante en tant qu'administrateur : ln -sf /dev/null /etc/systemd/system/ctrl-alt-del.target

La recommandation **R62** du guide de **l'ANSSI**
Lien de référence : **https://www.ssi.gouv.fr/uploads/2016/01/linux_configuration-fr-v1.2.pdf**

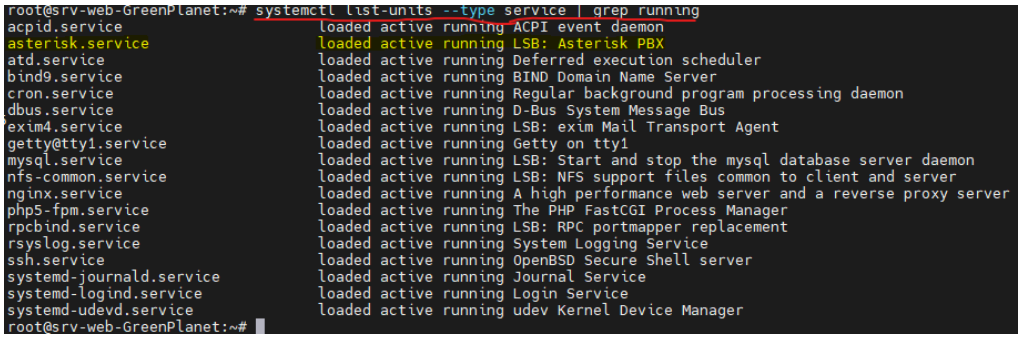
BOO.4	Désactiver les cibles inutiles démarrées automatiquement avec le serveur.
Objectif	Désactiver les cibles inutiles
Principe associé	minimisation
Type	**CRITICAL**
Commande	systemctl list-units –type target
Capture	
Recommandations	Désactiver les cibles inutiles démarrées automatiquement avec le serveur via les commandes exécutées en tant qu'administrateur : systemctl stop sound.target systemctl disable sound.target systemctl stop graphical.target systemctl disable graphical.target

La recommandation **R62** du guide de **l'ANSSI**
Lien de référence : **https://www.ssi.gouv.fr/uploads/2016/01/linux_configuration-fr-v1.2.pdf**

BOO.5	Désactiver les services non essentiels démarrées automatiquement avec le serveur.
Objectif	Désactiver les services inutiles
Principe associé	Défense en profondeur
Type	**CRITICAL**
Commande	systemctl list-unit-files --type service | grep enabled

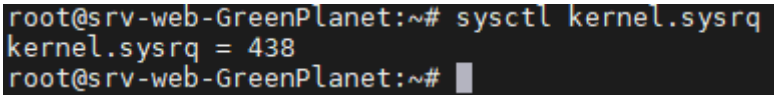
Capture	
Recommandations	désactiver le service Bluetooth en tant qu'administrateur via les commandes suivantes : systemctl stop bluetooth.service systemctl disable bluetooth.service systemctl stop dbus-org.bluez.service systemctl disable dbus-org.bluez.service

La recommandation **R9** du guide de **l'ANSSI**
Lien de référence : **https://www.ssi.gouv.fr/uploads/2016/01/linux_configuration-fr-v1.2.pdf**

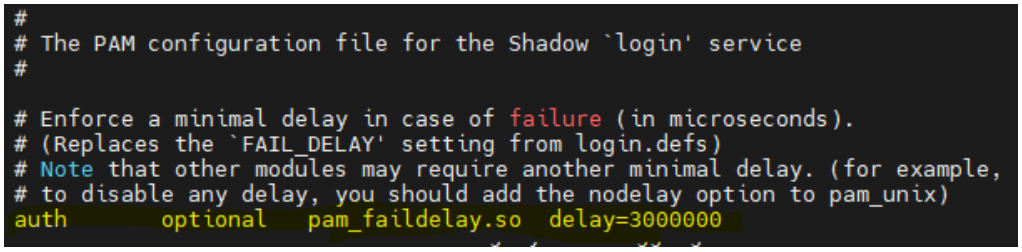
BOO.6	Désactiver les services non-essentiels démarrées automatiquement avec le serveur.
Objectif	Objectif Désactivation des services non essentiels
Principe associé	Défense en profondeur
Type	**CRITICAL**
Commande	systemctl list-units --type service | grep running
Capture	
Recommandations	

La recommandation **R9** du guide de **l'ANSSI**
Lien de référence : **https://www.ssi.gouv.fr/uploads/2016/01/linux_configuration-fr-v1.2.pdf**

BOO.7	Désactiver les Magic System Request Keys afin de prévenir toute utilisation de touches clavier pour réaliser des requêtes système
Objectif	
Principe associé	Défense en profondeur
Type	**Warning**

Commande	sysctl kernel.sysrq
Capture	
Recommandations	Désactiver les Magic System Request Keys en tapant la commande suivante en tant qu'administrateur : echo "kernel.sysrq=0" >> /etc/sysctl.conf

La recommandation **R9** du guide de **l'ANSSI**
Lien de référence : **https://www.ssi.gouv.fr/uploads/2016/01/linux_configuration-fr-v1.2.pdf**

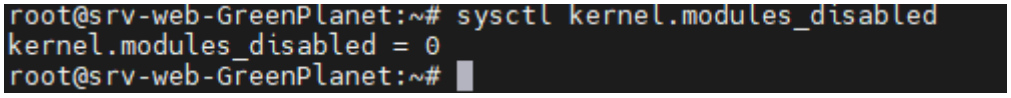
BOO.8	Augmenter l'intervalle minimal de temps entre chaque tentative de connexion sur le module «pam_faildelay.so » afin de ralentir les attaques par dictionnaire.
Objectif	Ralentir les attaques par dictionnaire
Principe associé	Défense en profondeur
Type	**Warning**
Commande	less /etc/pam.d/login
Capture	
Recommandations	Augmenter l'intervalle minimal de temps entre chaque tentative de connexion sur le module « pam_faildelay.so » du fichier « /etc/pam.d/login » à 5 ou 10 secondes en éditant le fichier en tant qu'administrateur, par exemple : « delay=5000000 ».

La recommandation **R9** du guide de **l'ANSSI**
Lien de référence : **https://www.ssi.gouv.fr/uploads/2016/01/linux_configuration-fr-v1.2.pdf**

BOO.9	Passer l'option « iommu=force » au noyau lors du démarrage de Linux afin de protéger la mémoire contre des accès non contrôlés issus des périphériques du système.
Objectif	Ce service permet de protéger la mémoire contre des accès non contrôlés issus des périphériques du système. Par défaut, Linux gère IOMMU et va, selon le contexte, l'activer ou non. Il est recommandé de forcer l'activation de ce service en passant une option supplémentaire lors du démarrage du noyau.
Principe associé	Minimisation
Type	**Warning**
Commande	grep linuz /boot/grub/grub.cfg | head -1
Capture	

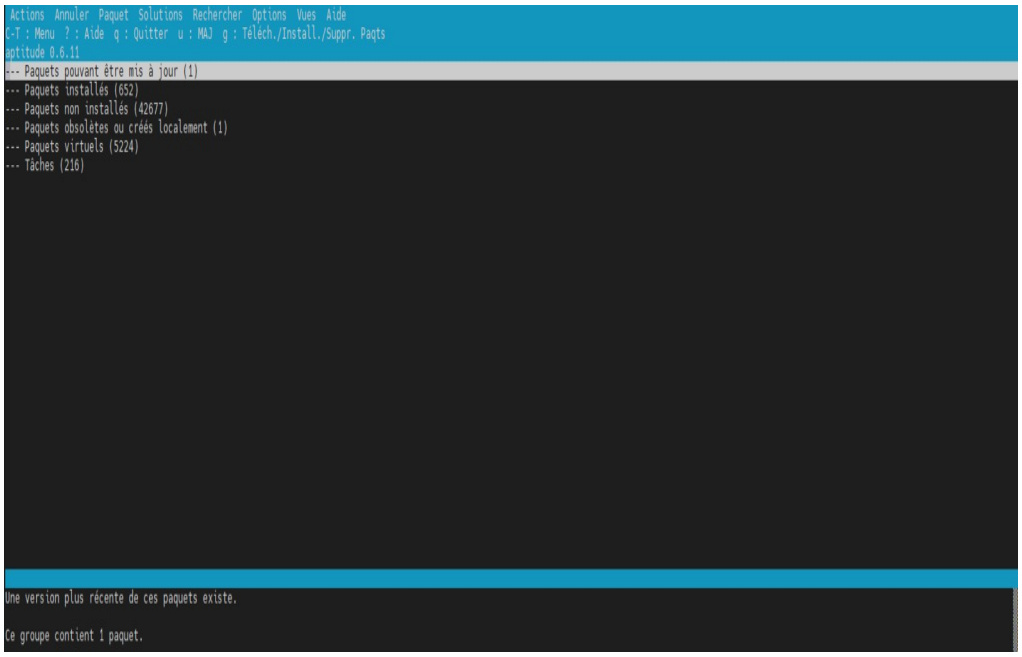
Recommandations	Configuration de la mémoire », passer l'option « iommu=force » au noyau lors du démarrage de Linux. En mode administrateur, modifier « /etc/default/grub » : GRUB_CMDLINE_LINUX="iommu=force"

La recommandation **R9** du guide de **l'ANSSI**
Lien de référence : **https://www.ssi.gouv.fr/uploads/2016/01/linux_configuration-fr-v1.2.pdf**

BOO.10	Limiter le chargement de modules supplémentaires au démarrage du noyau.
Objectif	Limitation du chargement de modules supplémentaires
Principe associé	Minimisation
Type	**Warning**
Commande	sysctl kernel.modules_disabled
Capture	
Recommandations	Taper la commande suivante en tant qu'administrateur : sysctl kernel.modules_disabled=1

4.3.Détails des Recommandations Services

La recommandation **R61** du guide de **l'ANSSI**
Lien de référence : **https://www.ssi.gouv.fr/uploads/2016/01/linux_configuration-fr-v1.2.pdf**

SER.1	Mettez à jour régulièrement les paquets pour le bon fonctionnement
Objectif	Mettre à jour les paquets
Principe associé	Défense en profondeur
Type	**CRITICAL**
Commande	aptitude
Capture	

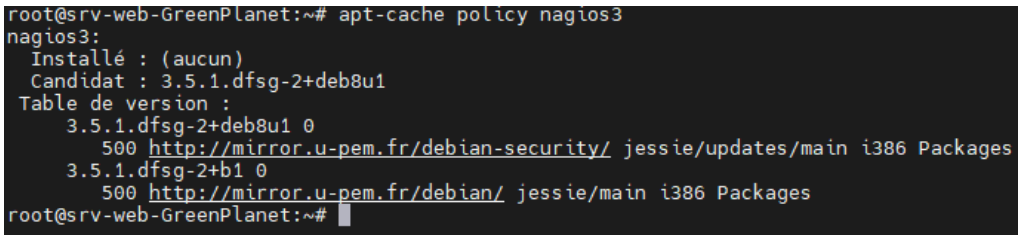
Recommandations	Mettez les paquets à jour pour ne pas avoir de problème avec certains services ou modules

La recommandation **3.1** du guide de **l'ANSSI** (minimisation)
Lien de référence : **https://www.ssi.gouv.fr/uploads/2016/01/linux_configuration-fr-v1.2.pdf**

SER.2	Désactiver le service dhclient
Objectif	Désactiver le dhcclient si aucune utilité
Principe associé	Minimisation
Type	**CRITICAL**
Commande	Systemctl disable dhclient
Recommandations	Configurer les interfaces réseaux

La recommandation **R62** du guide de **l'ANSSI**
Lien de référence : **https://www.ssi.gouv.fr/uploads/2016/01/linux_configuration-fr-v1.2.pdf**

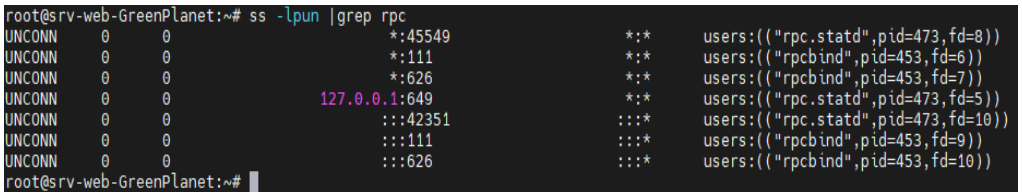
SER.3	Désactiver le service Bind9 (DNS) et bloquez le port 53 (DNS) en trafic entrant
Objectif	il n'y a aucun service DNS sur le serveur
Principe associé	Minimisation
Type	**CRITICAL**
Commande	Systemctl stop bind9 systemctl disable bind9
Recommandations	Il est préférable de désactiver Bind9 puisqu'il le DNS n'est pas utilisé

SER.4	Utiliser des outils de supervision de fichiers de traces (Nagios et/ou Logwatch).
Objectif	Recevoir des alertes en cas de problème majeur grâce l'analyse des fichiers de trace
Principe associé	Défense en profondeur
Type	Warning
Commande	apt-cache policy nagios apt-cache policy logwatch
Capture	

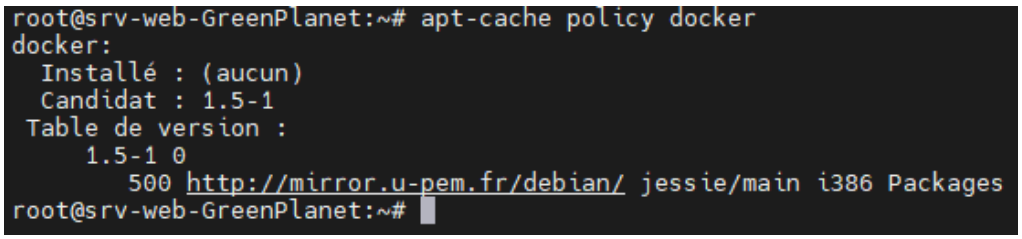
```
root@srv-web-GreenPlanet:~# apt-cache policy nagios3
nagios3:
  Installé : (aucun)
  Candidat : 3.5.1.dfsg-2+deb8u1
 Table de version :
     3.5.1.dfsg-2+deb8u1 0
        500 http://mirror.u-pem.fr/debian-security/ jessie/updates/main i386 Packages
     3.5.1.dfsg-2+b1 0
        500 http://mirror.u-pem.fr/debian/ jessie/main i386 Packages
root@srv-web-GreenPlanet:~#
```

Capture	
Recommandation	Installer un processus de supervision automatique du contenu des fichiers. Par exemple des sondes Nagios qui viendraient consulter, à intervalle de temps régulier, les lignes des fichiers, afin de lever des alertes lorsque nécessaire ; Installer un parseur de fichiers de trace. Celui-ci permet notamment de recevoir, par mail, un résumé des lignes jugées critiques dans tous les fichiers parsés. Logwatch est très efficace en la matière.

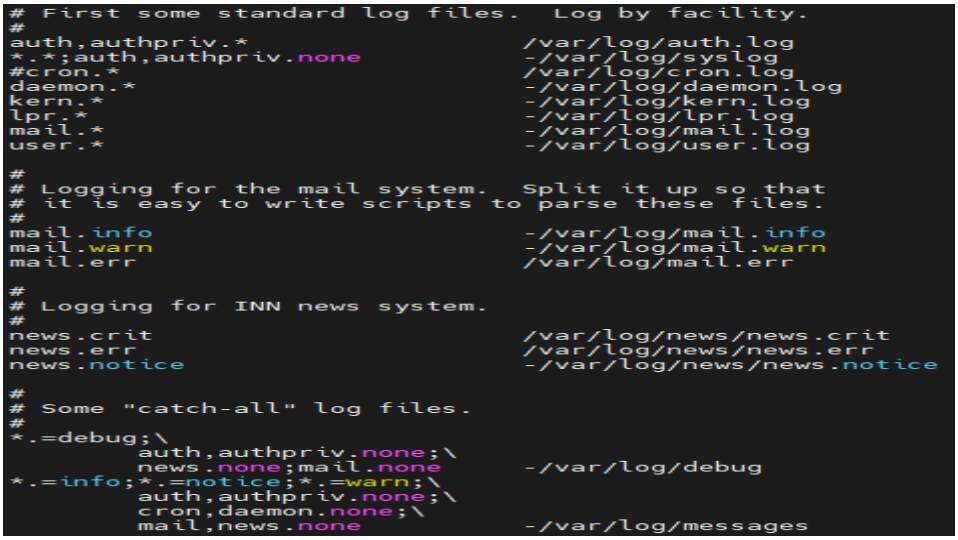
La recommandation **R62** du guide de **l'ANSSI**
Lien de référence : **https://www.ssi.gouv.fr/uploads/2016/01/linux_configuration-fr-v1.2.pdf**

SER.5	Désactiver le service NFS
Objectif	Désactiver NFS
Principe associé	Minimisation
Type	**Warning**
Commande	Ss -lpun | grep rpc
Capture	
Recommandations	Pour désactiver le protocole NFS, exécuter les commandes suivantes : 1- Désactivez les services NFS : update-rc,d nfs-common disable update-rc,d rpcbind disable 2- Stoppez les daemons correspondants : service nfs-common stop service rpcbind stop 3- Vérifiez qu'aucun service NFS n'est actif : netstat -intp | grep rpc

La recommandation **R5** du guide de **l'ANSSI**
Lien de référence : **https://www.ssi.gouv.fr/uploads/2016/01/linux_configuration-fr-v1.2.pdf**

SER.6	Isoler les services Nginx, MySQL et Bind9 avec «Docker ».
Objectif	Exécuter les processus critiques séparément les uns des autres afin d'optimiser l'utilisation de infrastructure tout en bénéficiant du même niveau de sécurité que celui des systèmes distincts
Principe associé	Défense en profondeur
Type	**Warning**
Commande	apt-cache policy docker
Capture	
Recommandations	apt install docker Puis installer le conteneurs Nginx, MySQL et BIND9 via la commande : docker pull *nom_service* Configurer les différents services

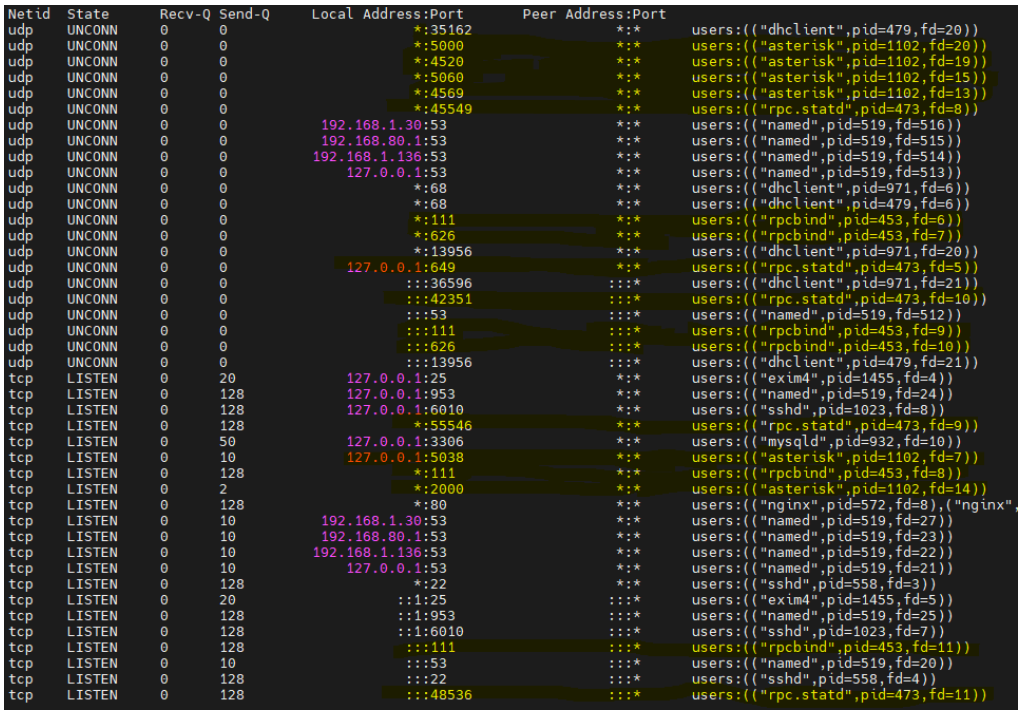
La recommandation **R7** du guide de **l'ANSSI**
Lien de référence : **https://www.ssi.gouv.fr/uploads/2016/01/linux_configuration-fr-v1.2.pd**

SER.7	Externaliser les traces sur serveur de centralisation des logs.
Objectif	Disposer de traces dans les fichiers de l'arborescence locale, mais aussi dans des fichiers distants, en passant par le service réseau d'un serveur de centralisation des logs.
Principe associé	Défense en profondeur
Type	**Warning**
Commande	vi /etc/rsyslog.conf
Capture	

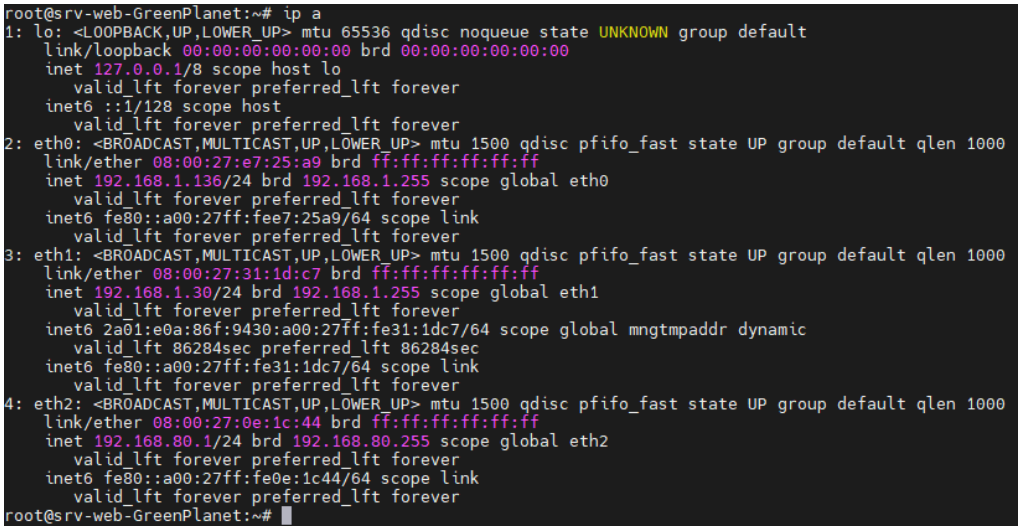
Recommandations	En tant qu'administrateur, éditer le fichier « /etc/rsyslog.conf » pour indiquer la destination réseau du fichier distant (via UDP ou TCP) pour chaque fichier log, par exemple : daemon,* @@*serveur_distant*:*port*

4.4.Détails des Recommandations Réseau

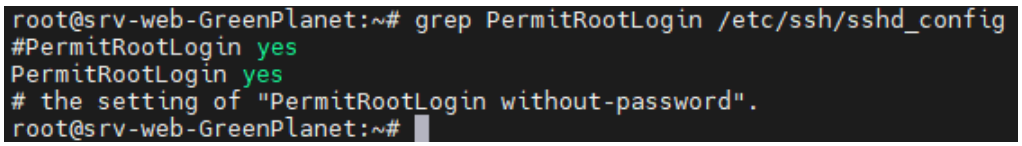
La recommandation **R42** du guide de **l'ANSSI**
Lien de référence : **https://www.ssi.gouv.fr/uploads/2016/01/linux_configuration-fr-v1.2.pdf**

NET.1	Désactiver les services ouvrant des ports inutiles (Asterisk et RPC).
Objectif	Désactivation des services qui ouvrent des ports inutiles
Principe associé	Minimisation
Type	**CRITICAL**
Commande	ss -lptun | less
Capture	
Recommandations	Les services RPC et Astrisk sont inutiles dans le cas de ce serveur web. En tant qu'administrateur, désactiver ces deux services via les commandes suivantes : systemctl stop rpcbind.service systemctl disable rpcbind.service systemctl stop asterisk.service systemctl disable asterisk.service

La recommandation **R12** du guide de **l'ANSSI**
Lien de référence : **https://www.ssi.gouv.fr/uploads/2016/01/linux_configuration-fr-v1.2.pdf**

NET.2	Configurer les interfaces réseau en IP statiques et désactiver l'interface eht2 si elle n'est pas utilisé
Objectif	Désactiver l'interface eth2 , elle n'est pas utilisé pour ce serveur
Principe associé	Minimisation
Type	**CRITICAL**
Commande	Ip a
Capture	
Recommandations	Editez le fichiers /etc/network/interfaces afin d'intégrer vos adresses IP

La recommandation **R25** du guide de **l'ANSSI**
Lien de référence : **https://www.ssi.gouv.fr/uploads/2016/01/linux_configuration-fr-v1.2.pdf**

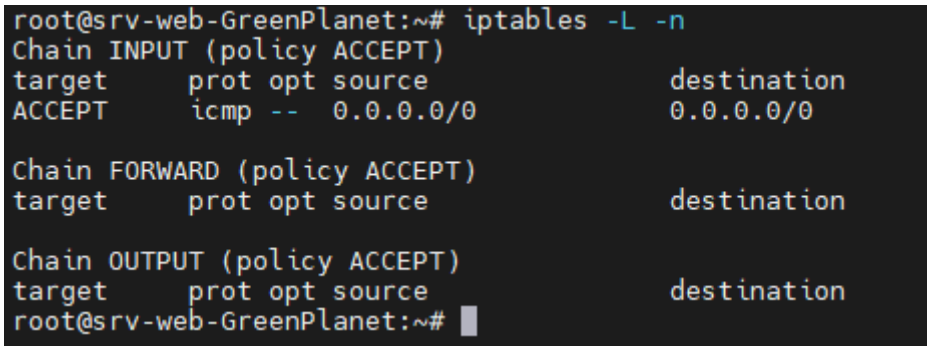
NET.3	Interdisez la connexion en SSH pour le root
Objectif	Réduire le risque de compromission du système par l'interdiction de connexion du compte « root » en SSH
Principe associé	Défense en profondeur
Type	**CRITICAL**
Commande	grep PermitRootLogin /etc/ssh/sshd_config
Capture	
Recommandations	En tant qu'administrateur, il faudra éditer le fichier « /etc/ssh/sshd_config » pour interdire l'accès au compte « root » en SSH : PermitRootLogin no

La recommandation **R25** du guide de **l'ANSSI**
Lien de référence : **https://www.ssi.gouv.fr/uploads/2016/01/linux_configuration-fr-v1.2.pdf**

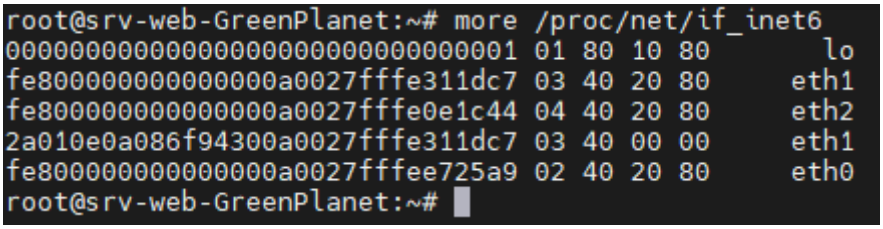
NET.4	Changer le port utilisé par le SSH.
Objectif	Réduire le risque de compromission du système par le changement du port par

	défaut pour le SSH
Principe associé	Défense en profondeur
Type	**CRITICAL**
Commande	grep Port /etc/ssh/sshd_config
Capture	
Recommandations	En tant qu'administrateur, il faudra éditer le fichier « /etc/ssh/sshd_config » pour changer le port utilisé par le SSH en mettant le port 7777, par exemple : Port 7777

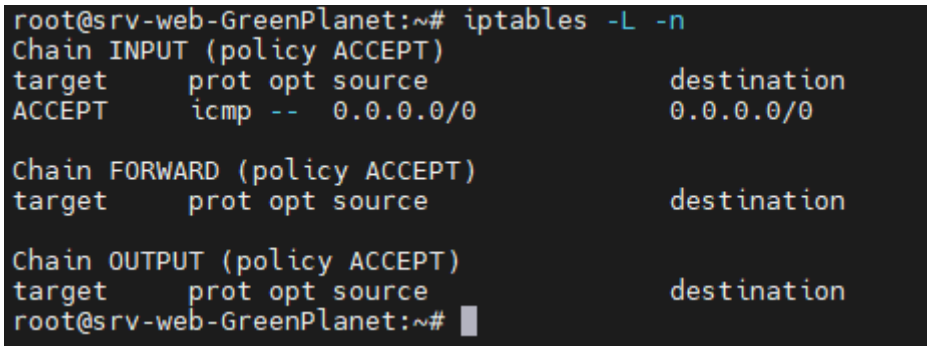
La recommandation **R64** du guide de **l'ANSSI**
Lien de référence : **https://www.ssi.gouv.fr/uploads/2016/01/linux_configuration-fr-v1.2.pdf**

NET.5	Appliquer une politique au niveau du pare-feu de rejet par défaut des requêtes, et ensuite laisser passer les types de requêtes souhaitées.
Objectif	Gestion des règles du pare-feu
Principe associé	Défense en profondeur
Type	**CRITICAL**
Commande	iptables -L -n
Capture	
Recommandations	La seule règle qui existe est d'accepter toutes les requêtes ICMP en entrées depuis et vers n'importe quelle adresse IPv4 et sur n'importe quel port. Il n'y a pas de règles pour gérer les autres types de requêtes, que ce soit en entrée, en sortie ou en acheminement. La politique par défaut est d'accepter les requêtes. Or, il faut plutôt rejeter par défaut, et ensuite laisser passer les requêtes souhaitées. En tant qu'administrateur, il faudra modifier le fichier « /etc/iptables.conf », par exemple : :INPUT DROP [0:0] :FORWARD DROP [0:0] :OUTPUT DROP [0:0] -A INPUT -i eth1 -p tcp –dport 80 -j ACCEPT -A INPUT -o eth1 -p tcp –dport 80 -j ACCEPT

La recommandation **R64** du guide de **l'ANSSI**
Lien de référence : **https://www.ssi.gouv.fr/uploads/2016/01/linux_configuration-fr-v1.2.pdf**

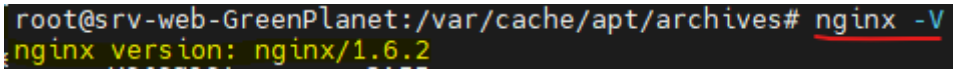
NET.6	Désactiver l'IPV6 si celui-ci n'est pas utilisé
Objectif	Désactiver l'IPV6
Principe associé	Minimisation
Type	**Warning**
Commande	More /proc/net/if_inet6
Capture	
Recommandations	Si l'IPV6 n'est pas utilisé sur le serveur, mieux vaut le désactiver

La recommandation **R64** du guide de **l'ANSSI**
Lien de référence : **https://www.ssi.gouv.fr/uploads/2016/01/linux_configuration-fr-v1.2.pdf**

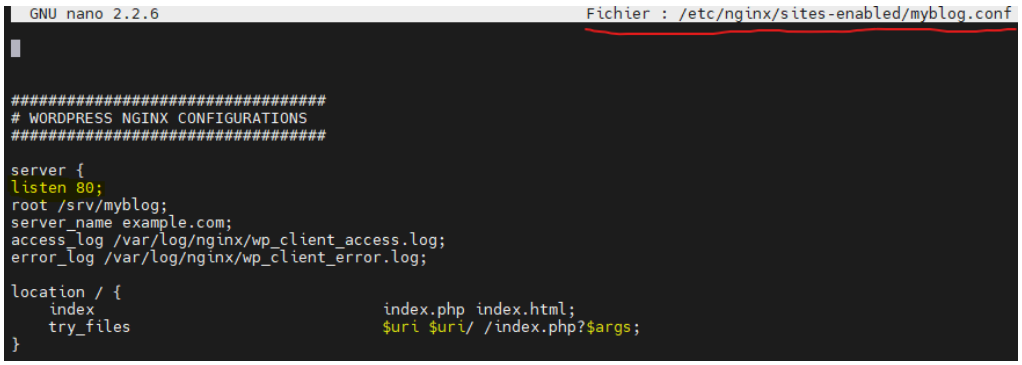
NET.7	Recompiler le noyau avec une prise en charge de Netfilter sans avoir besoin de faire appel à des modules.
Objectif	Accès au pare-feu Netfilter par le noyau sans la contrainte module
Principe associé	Minimisation
Type	**Warning**
Commande	grep IPTABLES /boot/config-`uname -r`
Capture	
Recommandations	Le résultat indique que le code Netfilter est compilé comme un module et qu'il est nécessaire de le charger pour accéder aux fonctionnalités du pare-feu. Cela ne convient pas au vu de la recommandation émise sur le noyau vis-à-vis du blocage du chargement de modules supplémentaires. Il faudra recompiler le noyau avec une prise en charge de Netfilter sans avoir besoin de faire appel à des modules.

4.5.Détails des Recommandations Nginx

La recommandation **R79** du guide de **l'ANSSI**
Lien de référence : **https://www.ssi.gouv.fr/uploads/2016/01/linux_configuration-fr-v1.2.pdf**

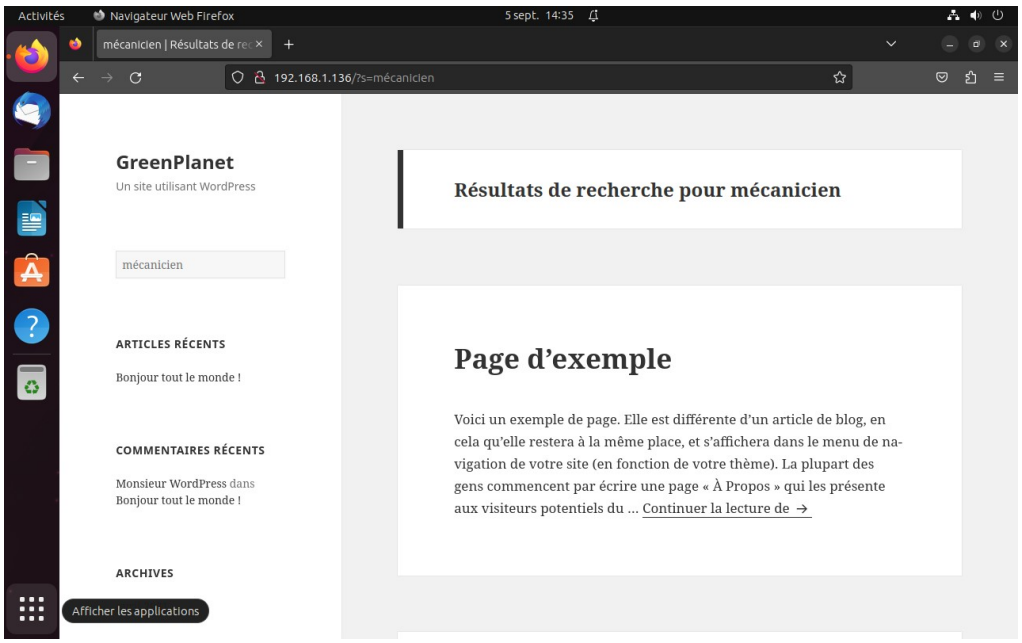
NGX1	Mettez à jour régulièrement le serveur NGINX
Objectif	Mettre à jour NGINX
Principe associé	Défense en profondeur
Type	**CRITICAL**
Commande	Nginx -V
Capture	
Recommandations	Il faut absolument mettre NGINX à jours vers la version 1.20.0 pour éviter des bugs correctif et des failles de sécurité

La recommandation **R79** du guide de **l'ANSSI**
Lien de référence : **https://www.ssi.gouv.fr/uploads/2016/01/linux_configuration-fr-v1.2.pdf**

NGX2	Configurez le site Web par pair de clé SSL pour une connexion sécurisé en HTTPS
Objectif	Générer deux pairs de clé SSL (privé et publique)
Principe associé	Défense en profondeur
Type	**CRITICAL**
Commande	Nano /etc/nginx/sites-enable/myblog.conf
Capture	
Recommandations	Pour la sécurité du site web en HTTPS via le port 443, il est fortement recommandé de générer des clés SSL

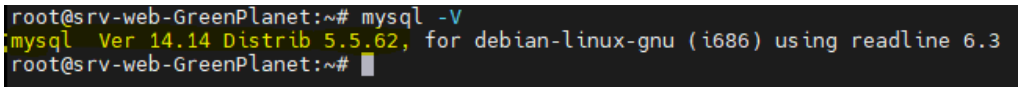
La recommandation **3.3** du guide de **l'ANSSI** (défense en profondeur)
Lien de référence : **https://www.ssi.gouv.fr/uploads/2016/01/linux_configuration-fr-v1.2.pdf**

NGX3	Masquez la version de NGINX afin de se protéger contre les cyberattaques
Objectif	Masquez le numéros de version , pour éviter des attaques pirates
Principe associé	Défense en profondeur
Type	**CRITICAL**
Commande	Nano /etc/nginx/nginx.conf

Capture	
Recommandations	Il est fortement conseillé d'éviter le HTTP (non sécurisé) pour une connexion en HTTPS (sécurisé avec jeu de clé SSL)

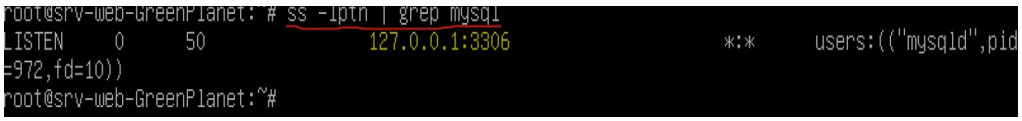
4.6.Détails des Recommandations MySQL

La recommandation **R61** du guide de **l'ANSSI**
Lien de référence : **https://www.ssi.gouv.fr/uploads/2016/01/linux_configuration-fr-v1.2.pdf**

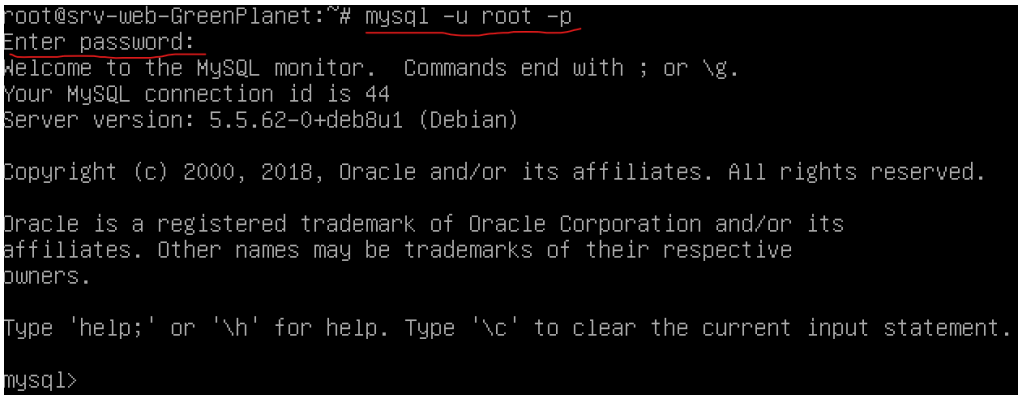
SQL.1	Mettez à jour MySQL
Objectif	Mettez à jour les paquets pour éviter des problème de sécurité
Principe associé	Défense en profondeur
Type	**CRITICAL**
Commande	Mysql -V
Capture	
Recommandations	La version présente dans le serveur est trop ancienne, Il est fortement recommandé dé mettre MySQL à jour régulièrement

La recommandation **R61** du guide de **l'ANSSI**
Lien de référence : **https://www.ssi.gouv.fr/uploads/2016/01/linux_configuration-fr-v1.2.pdf**

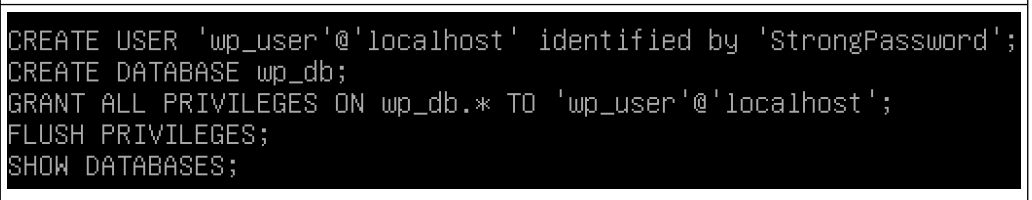
SQL.2	Choisissez un port d'écoute , différents de celui par défaut
Objectif	Choisissez un port d'écoute différent pour la sécurité
Principe associé	Défense en profondeur
Type	**CRITICAL**
Commande	Ss -lptn | grep mysql

Capture	
Recommandations	Il est fortement conseillé de changer le port d'écoute de mysql , il est actuellement par défaut

La recommandation **R61** du guide de **l'ANSSI**
Lien de référence : **https://www.ssi.gouv.fr/uploads/2016/01/linux_configuration-fr-v1.2.pdf**

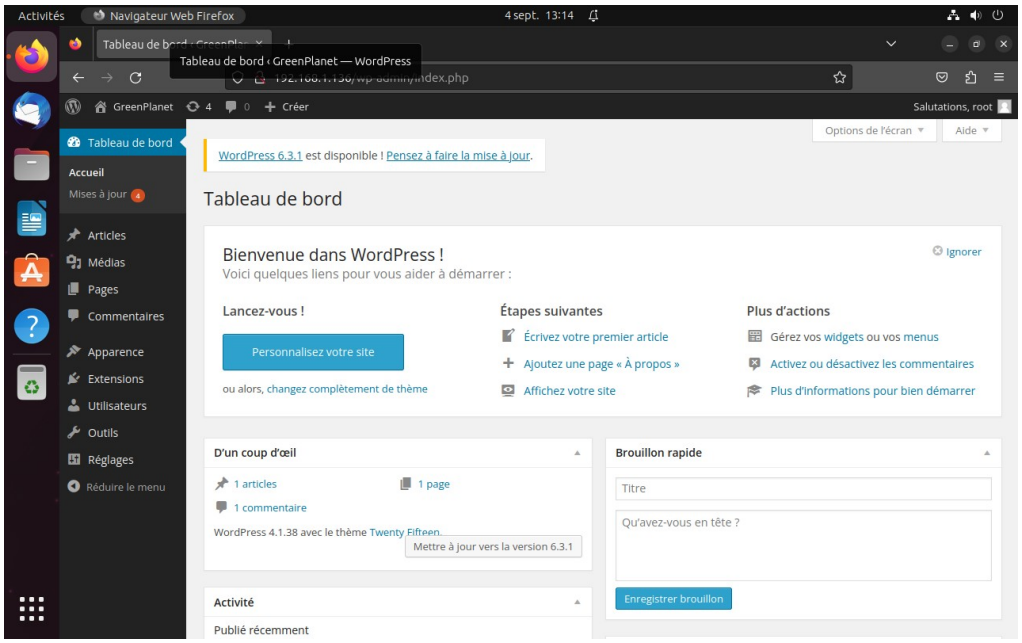
SQL.3	Ne saisissez pas de mot de passe en vous connectant sur MySQL. Cela évitera l'aperçu des commandes dans l'historique
Objectif	Evitez de saisir les mots de passes lors de la connexion à la base de données
Principe associé	Défense en profondeur
Type	**CRITICAL**
Commande	Mysql -u root -p
Capture	
Recommandations	Ne pas montrer le mot de passe en effectuant la commande. Cela se verras dans l'historique des commandes.

La recommandation **R61** du guide de **l'ANSSI**
Lien de référence : **https://www.ssi.gouv.fr/uploads/2016/01/linux_configuration-fr-v1.2.pdf**

SQL.4	Changez les mots de passe régulièrement pour les utilisateurs ayant des privilèges élevés
Objectif	Changez le mot de passe régulièrement pour la sécurité
Principe associé	Défense en profondeur
Type	**CRITICAL**
Commande	Nano .mysql_history
Capture	
Recommandations	Il est fortement recommandé de désactiver l'historique, pour ne pas voir tout les mots de passes des utilisateurs

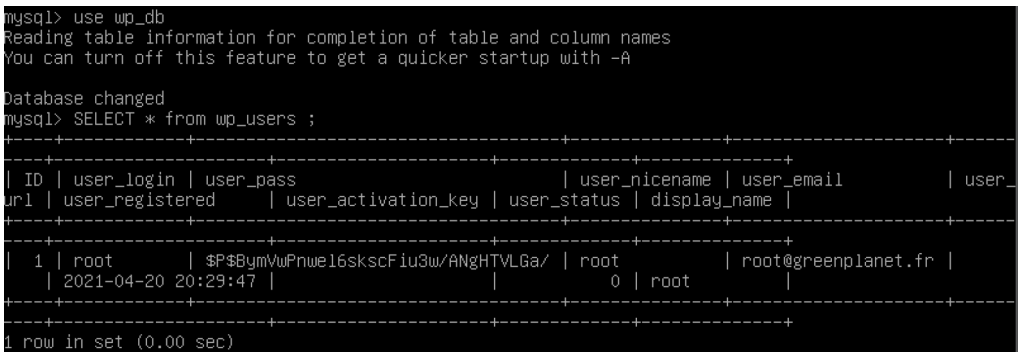
4.7.Détails des Recommandations Wordpress

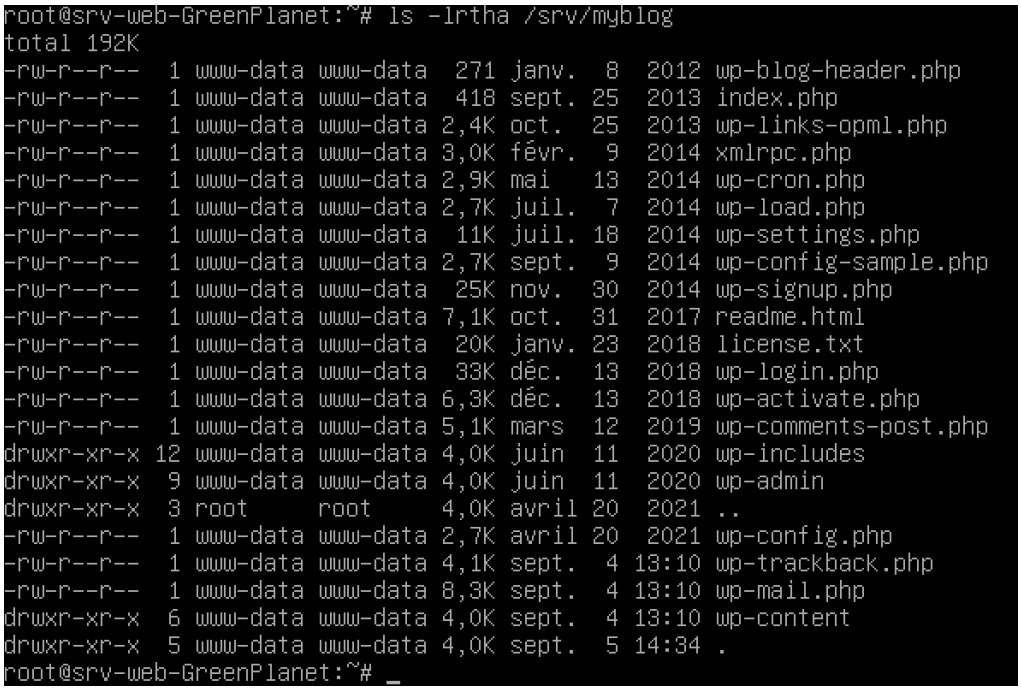
La recommandation **R61** du guide de **l'ANSSI**
Lien de référence : **https://www.ssi.gouv.fr/uploads/2016/01/linux_configuration-fr-v1.2.pdf**

WP.1	Mettez à jour Worpress
Objectif	Mettre à niveau régulièrement
Principe associé	Défense en profondeur
Type	**CRITICAL**
Commande	http://192.168.1.136/wp-admin
Capture	
Recommandations	

La recommandation **R61** du guide de **l'ANSSI**
Lien de référence : **https://www.ssi.gouv.fr/uploads/2016/01/linux_configuration-fr-v1.2.pdf**

WP.2	Créez un utilisateur dans la base de données wp_db avec les droits administrateurs
Objectif	Changez les droits des utilisateurs
Principe associé	Défense en profondeur
Type	**CRITICAL**
Commande	Use wp_db SELECT * from wp_users ;

Capture	
Recommandations	Use wp_db CREATE USER ‘wp_user’@’localhost’ identified by ‘Motdepasserobuste’ ; GRANT ALL PRIVILEGES ON wp_db * TO ‘wp_user’@localhost’ ; FLUSH PRIVILEGES ;

WP.3	Modifiez les droits config.PHP
Objectif	Mettez les droits nécessaire pour le serveur WordPress (config.PHP)
Principe associé	Défense en profondeur
Type	**CRITICAL**
Commande	Ls -lrtha /srv/myblog
Capture	
Recommandations	Il est recommandé de mettre les droits à 440 ou à 400 chmod 400 /srv/myblog/wp-config.php

La recommandation **R79** du guide de **l’ANSSI**
Lien de référence : **https://www.ssi.gouv.fr/uploads/2016/01/linux_configuration-fr-v1.2.pdf**

WP.4	Installez un pare-feu pour le site Web (DNS)
Objectif	Mettez un pare-feu pour gérer le trafic entrant/Sortant sur le serveur

Principe associé	Défense en profondeur
Type	**Warning**
Commande	Se référer https://www.it-connect.fr/configurer-un-pare-feu-local-sous-debian-11-avec-ufw/
Recommandations	le pare-feu de site Web de niveau DNS : ce type de pare-feu gère le trafic via des serveurs proxy garantissant l’envoi d’un trafic sur votre serveur Web.