

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

- 1.1. Partie 1 : Résumé des recommandations Système
- 1.2. Partie 2 : Résumé des recommandations Processus de démarrage
- 1.3. Partie 3 : Résumé de recommandations Services
- 1.4. Partie 4 : Résumé des recommandations Réseau
- 1.5. Partie 5 : Résumé des recommandations Nginx
- 1.6. Partie 6 : Résumé des recommandations MySQL
- 1.7. Partie 7 : Résumé des recommandations Wordpress

2. Méthodologie de l'audit

- 2.1. Principe de minimisation
- 2.2. Principe de moindre privilège
- 2.3. Principe défense en profondeur

3. Périmètre de l'Audit

- 3.1. Cible de l'audit
- 3.2. Les éléments de la cible auditée
- 3.3. Serveur en production

4. Détails des Recommandations

- 4.1. Détails des Recommandations Système
- 4.2. Détails des Recommandations Processus de démarrage
- 4.3. Détails des Recommandations Services
- 4.4. Détails des Recommandations Réseau
- 4.5. Détails des Recommandations Nginx
- 4.6. Détails des Recommandations MySQL
- 4.7. Détails des Recommandations Wordpress

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	Monitorer 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 de prévenir 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 automatiquement avec 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 Wordpress	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'événements 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 :

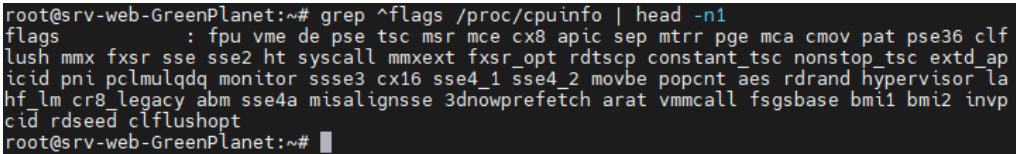
Il est important de noter que le serveur audité est en mode production. C'est la raison pour laquelle j'ai pris soin de ne pas perturber le fonctionnement durant mon audit ni d'en changer la configuration ou le paramétrage.

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	<code>grep ^flags /proc/cpuinfo head -n1 egrep --color=auto ' (pae nx) '</code>
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 blkid /dev/sda*
Capture	<pre> root@srv-web-GreenPlanet:~# fdisk -l Disque /dev/sda : 10 GiB, 10737418240 octets, 20971520 secteurs Unités : secteur de 1 x 512 = 512 octets Taille de secteur (logique / physique) : 512 octets / 512 octets taille d'E/S (minimale / optimale) : 512 octets / 512 octets Type d'étiquette de disque : dos Identifiant de disque : 0x5bbbc7fe Device Boot Start End Sectors Size Id Type /dev/sda1 * 2048 20013055 20011008 9,6G 83 Linux /dev/sda2 20015102 20969471 954370 466M 5 Extended /dev/sda5 20015104 20969471 954368 466M 82 Linux swap / Solaris root@srv-web-GreenPlanet:~# lsblk NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT sda 8:0 0 10G 0 disk ├─sda1 8:1 0 9,6G 0 part / ├─sda2 8:2 0 1K 0 part └─sda5 8:5 0 466M 0 part [SWAP] sr0 11:0 1 1024M 0 rom root@srv-web-GreenPlanet:~# blkid /dev/sda* /dev/sda: PTUUID="5bbbc7fe" PTTYPE="dos" /dev/sda1: UUID="ac0ff7a8-7d92-443a-80be-3af7ec446d2c" TYPE="ext4" PARTUUID="5bbbc7fe-01" /dev/sda2: PTTYPE="dos" PARTUUID="5bbbc7fe-02" /dev/sda5: UUID="868f6e1a-64a1-443e-86a6-3490ca666ef3" TYPE="swap" PARTUUID="5bbbc7fe-05" </pre>
Recommandations	Chiffrer la partition / via les outils « ecryptfs-utils » et « cryptsetup ».

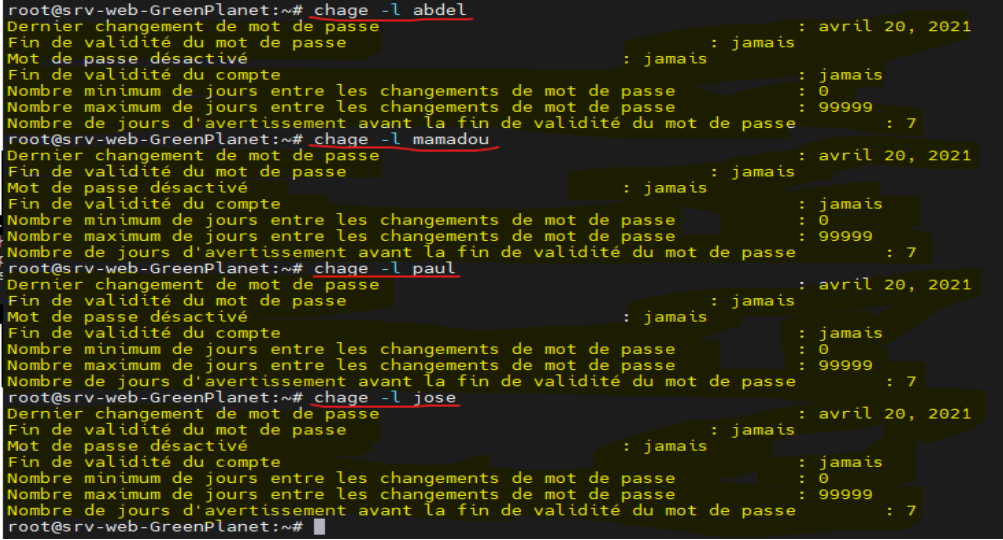
La recommandation **R29** du guide de l'ANSSI

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	<pre> root@srv-web-GreenPlanet:~# ls -lrtha /boot/ total 19M -rwxrwxrwx 1 root root 2,8M déc. 4 2017 vmlinuz-3.16.0-4-586 -rwxrwxrwx 1 root root 2,0M déc. 4 2017 System.map-3.16.0-4-586 -rwxrwxrwx 1 root root 159K déc. 4 2017 config-3.16.0-4-586 drwxrwxrwx 5 root root 4,0K avril 20 2021 grub -rwxrwxrwx 1 root root 14M avril 20 2021 initrd.img-3.16.0-4-586 drwxrwxrwx 3 root root 4,0K avril 20 2021 . drwxr-xr-x 21 root root 4,0K sept. 1 20:24 .. root@srv-web-GreenPlanet:~# ls -lrth / grep boot -rwxrwxrwx 1 root root 25 avril 20 2021 vmlinuz -> boot/vmlinuz-3.16.0-4-586 -rwxrwxrwx 1 root root 29 avril 20 2021 initrd.img -> /boot/initrd.img-3.16.0-4-586 drwxrwxrwx 3 root root 4,0K avril 20 2021 boot root@srv-web-GreenPlanet:~# </pre>
Recommandations	Changer les permissions

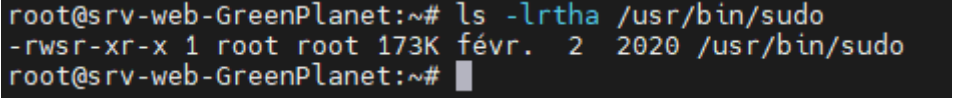
La recommandation **R5** du guide de l'ANSSI

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	<code>chage -l nom_utilisateur</code> <code>Ichage -m 7 -M 90 -W 10 nom_utilisateur</code>
Capture	 <pre> root@srv-web-GreenPlanet:~# chage -l abdel Dernier changement de mot de passe : avril 20, 2021 Fin de validité du mot de passe : jamais Mot de passe désactivé : jamais Fin de validité du compte : jamais Nombre minimum de jours entre les changements de mot de passe : 0 Nombre maximum de jours entre les changements de mot de passe : 99999 Nombre de jours d'avertissement avant la fin de validité du mot de passe : 7 root@srv-web-GreenPlanet:~# chage -l mamadou Dernier changement de mot de passe : avril 20, 2021 Fin de validité du mot de passe : jamais Mot de passe désactivé : jamais Fin de validité du compte : jamais Nombre minimum de jours entre les changements de mot de passe : 0 Nombre maximum de jours entre les changements de mot de passe : 99999 Nombre de jours d'avertissement avant la fin de validité du mot de passe : 7 root@srv-web-GreenPlanet:~# chage -l paul Dernier changement de mot de passe : avril 20, 2021 Fin de validité du mot de passe : jamais Mot de passe désactivé : jamais Fin de validité du compte : jamais Nombre minimum de jours entre les changements de mot de passe : 0 Nombre maximum de jours entre les changements de mot de passe : 99999 Nombre de jours d'avertissement avant la fin de validité du mot de passe : 7 root@srv-web-GreenPlanet:~# chage -l jose Dernier changement de mot de passe : avril 20, 2021 Fin de validité du mot de passe : jamais Mot de passe désactivé : jamais Fin de validité du compte : jamais Nombre minimum de jours entre les changements de mot de passe : 0 Nombre maximum de jours entre les changements de mot de passe : 99999 Nombre de jours d'avertissement avant la fin de validité du mot de passe : 7 root@srv-web-GreenPlanet:~# </pre>
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.

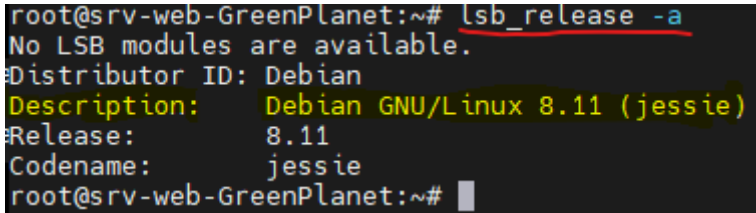
La recommandation **R38** du guide de l'ANSSI

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	<code>ls -lrtha /usr/bin/sudo</code>
Capture	 <pre> root@srv-web-GreenPlanet:~# ls -lrtha /usr/bin/sudo -rwsr-xr-x 1 root root 173K févr. 2 2020 /usr/bin/sudo root@srv-web-GreenPlanet:~# </pre>
Recommandations	en tant qu'administrateur, rendre « sudo » exécutable uniquement par le groupe « admin » (+ utilisateur « root ») via les deux commandes suivantes : <code>chmod 4750 /usr/bin/sudo</code> <code>chown root:admin /usr/bin/sudo</code>

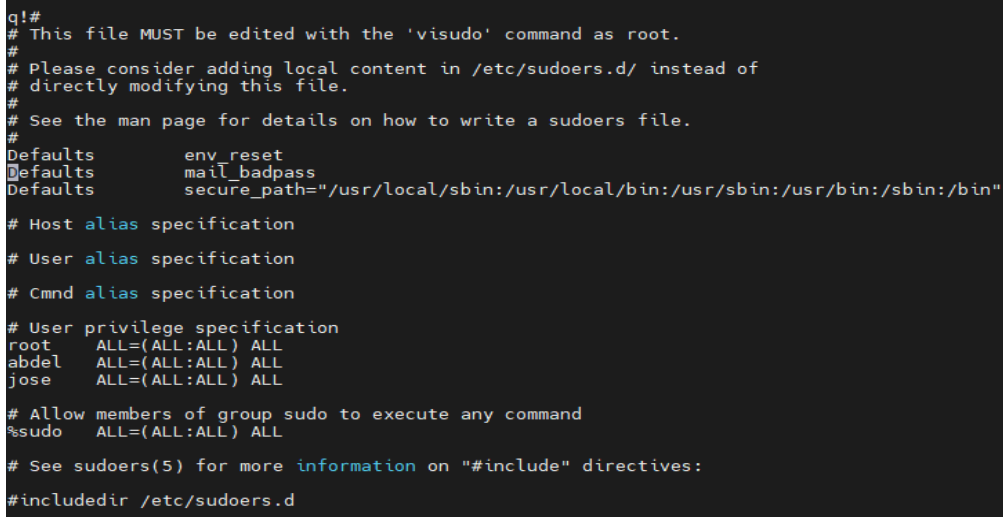
La recommandation **R61** du guide de l'ANSSI

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	<p>Debian 8 est obsolète et ne bénéficie plus de mise à jour depuis le 17 juin 2018. Cela représente une faille de sécurité importante.</p> <p>En mode administrateur, il faudra changer le fichier /etc/apt/sources.list pour n'avoir que ces lignes :</p> <ul style="list-style-type: none">• deb http://deb.debian.org/debian stable main contrib non-free• deb http://security.debian.org/debian-security stable-security main contrib non-free <p>Ensuite lancer la mise à niveau via la commande : apt full-upgrade</p>


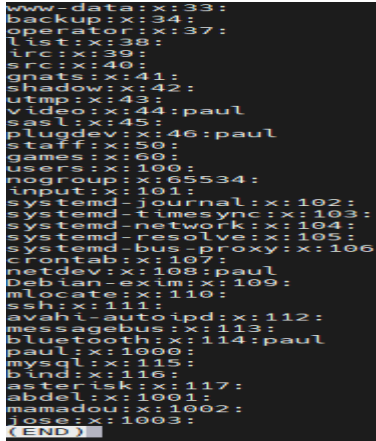
La recommandation **R38** du guide de l'ANSSI

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

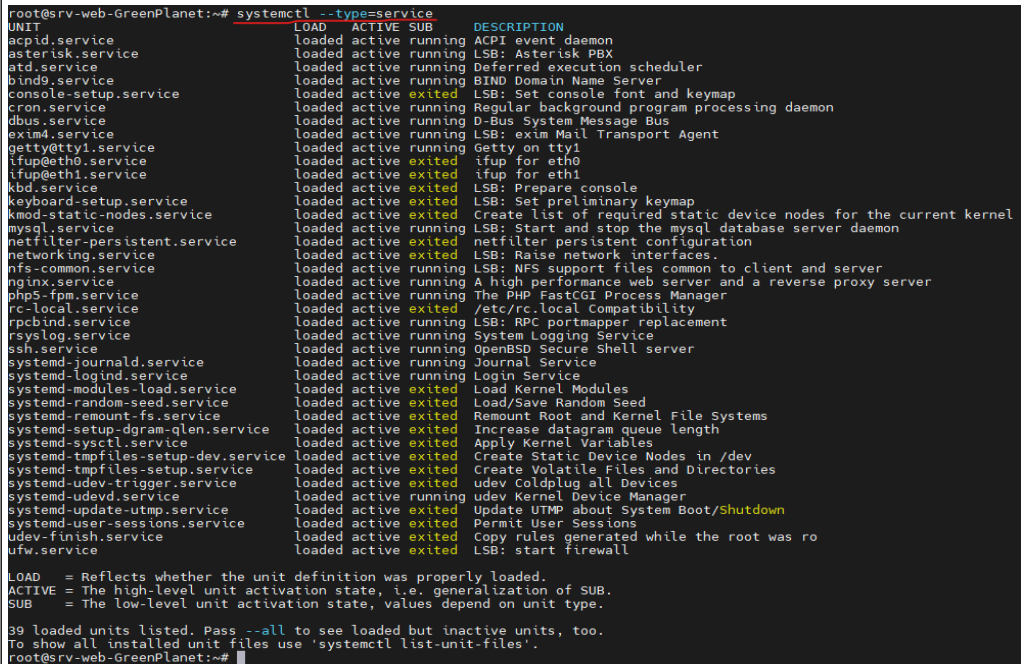
La recommandation **R37** du guide de l'ANSSI

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

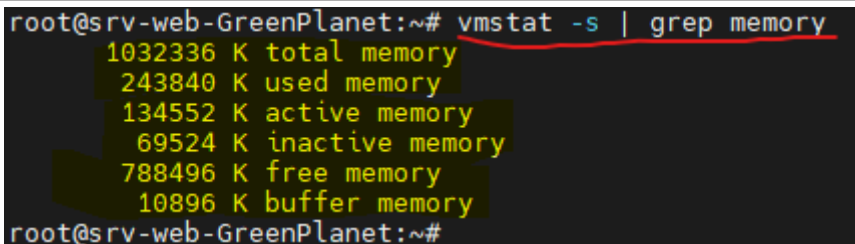
Lien de référence : https://www.ssi.gouv.fr/uploads/2016/01/linux_configuration-fr-v1.2.pdf

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
-----------------	--

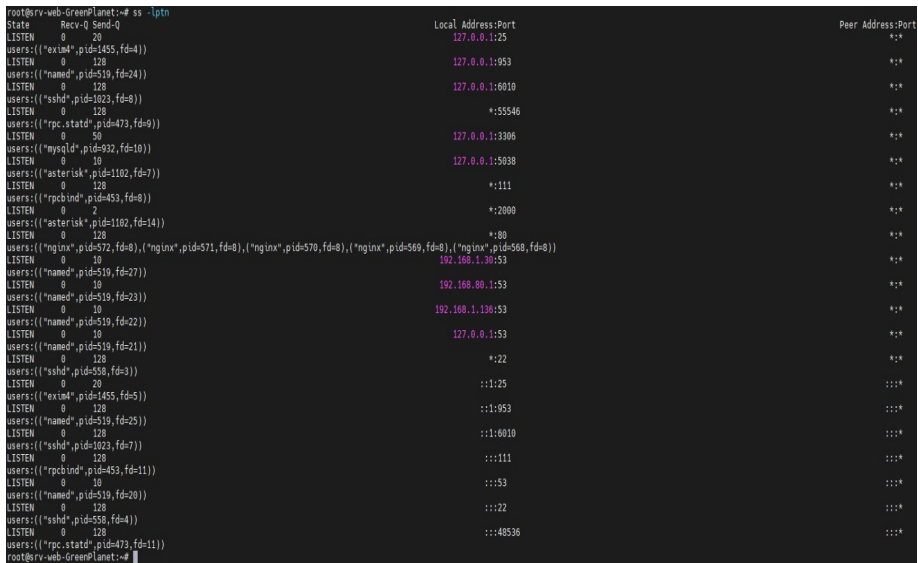
La recommandation **R8** du guide de l'ANSSI

Lien de référence : https://www.ssi.gouv.fr/uploads/2016/01/linux_configuration-fr-v1.2.pdf

SYS.10	Monitez 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	 <pre> root@srv-web-GreenPlanet:~# vmstat -s grep memory 1032336 K total memory 243840 K used memory 134552 K active memory 69524 K inactive memory 788496 K free memory 10896 K buffer memory root@srv-web-GreenPlanet:~# </pre>
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	 <pre> root@srv-web-GreenPlanet:~# ss -lptn State Recv-Q Send-Q Local Address:Port Peer Address:Port LISTEN 0 20 *:* *:* users:((("exim4",pid=1455,fd=4)) LISTEN 0 128 127.0.0.1:953 *:* users:((("named",pid=519,fd=24)) LISTEN 0 128 127.0.0.1:6010 *:* users:((("sshd",pid=1023,fd=8)) LISTEN 0 128 *:* *:* users:((("rpc.statd",pid=473,fd=9)) LISTEN 0 50 127.0.0.1:3306 *:* users:((("mysqld",pid=932,fd=10)) LISTEN 0 10 127.0.0.1:5038 *:* users:((("asterisk",pid=1102,fd=7)) LISTEN 0 128 *:* *:* users:((("rpcbind",pid=453,fd=8)) LISTEN 0 2 *:* *:* users:((("asterisk",pid=1102,fd=14)) LISTEN 0 128 *:* *:* users:((("nginx",pid=572,fd=8),("nginx",pid=571,fd=8),("nginx",pid=570,fd=8),("nginx",pid=569,fd=8),("nginx",pid=568,fd=8)) LISTEN 0 10 192.168.1.30:53 *:* users:((("named",pid=519,fd=27)) LISTEN 0 10 192.168.80.1:53 *:* users:((("named",pid=519,fd=23)) LISTEN 0 10 192.168.1.196:53 *:* users:((("named",pid=519,fd=22)) LISTEN 0 10 127.0.0.1:53 *:* users:((("named",pid=519,fd=21)) LISTEN 0 128 *:* *:* users:((("sshd",pid=558,fd=3)) LISTEN 0 20 *:* *:* users:((("exim4",pid=1455,fd=5)) LISTEN 0 128 *:* *:* users:((("named",pid=519,fd=25)) LISTEN 0 128 *:* *:* users:((("sshd",pid=1022,fd=7)) LISTEN 0 128 *:* *:* users:((("rpcbind",pid=453,fd=11)) LISTEN 0 10 127.0.0.1:53 *:* users:((("named",pid=519,fd=20)) LISTEN 0 128 *:* *:* users:((("sshd",pid=558,fd=4)) LISTEN 0 128 *:* *:* users:((("rpc.statd",pid=473,fd=11)) root@srv-web-GreenPlanet:~# </pre>
Recommandations	Fermez les ports inutiles pour le serveur et pour une meilleure sécurité

La recommandation **R31** du guide de l'ANSSI

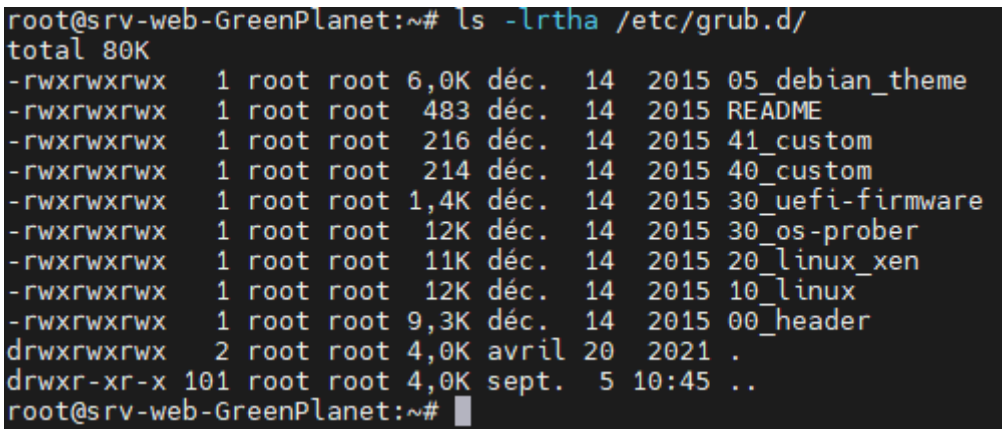
Lien de référence : https://www.ssi.gouv.fr/uploads/2016/01/linux_configuration-fr-v1.2.pdf

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	<pre># /etc/securetty: list of terminals on which root is allowed to login. # See securetty(5) and login(1). console # Local X displays (allows empty passwords with pam_unix's nullok_secure) :0 :0.0 :0.1 :1 :1.0 :1.1 :2 :2.0 :2.1 :3 :3.0 :3.1 #... # ===== # # TTYs sorted by major number according to Documentation/devices.txt # # ===== # Virtual consoles tty1 tty2 tty3</pre>
Recommandations	Vider le contenu du fichier « /etc/securetty » en tapant la commande suivante en tant qu'administrateur : <code>echo > /etc/securetty</code>

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 de prévenir 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	<code>ls -la /etc/systemd/system</code>
Capture	<pre>root@srv-web-GreenPlanet:~# ls -la /etc/systemd/system total 52 drwxr-xr-x 13 root root 4096 avril 20 2021 . drwxr-xr-x 6 root root 4096 avril 20 2021 .. drwxr-xr-x 2 root root 4096 avril 20 2021 bluetooth.target.wants lrwxrwxrwx 1 root root 37 avril 20 2021 dbus-org.bluez.service -> /lib/systemd/system/bluetooth.service drwxr-xr-x 2 root root 4096 avril 20 2021 getty.target.wants drwxr-xr-x 2 root root 4096 avril 20 2021 halt.target.wants drwxr-xr-x 2 root root 4096 avril 20 2021 hibernate.target.wants drwxr-xr-x 2 root root 4096 avril 20 2021 hybrid-sleep.target.wants drwxr-xr-x 2 root root 4096 avril 20 2021 multi-user.target.wants drwxr-xr-x 2 root root 4096 avril 20 2021 paths.target.wants drwxr-xr-x 2 root root 4096 avril 20 2021 poweroff.target.wants drwxr-xr-x 2 root root 4096 avril 20 2021 reboot.target.wants drwxr-xr-x 2 root root 4096 avril 20 2021 sockets.target.wants lrwxrwxrwx 1 root root 31 avril 20 2021 sshd.service -> /lib/systemd/system/ssh.service drwxr-xr-x 2 root root 4096 avril 20 2021 suspend.target.wants lrwxrwxrwx 1 root root 35 avril 20 2021 syslog.service -> /lib/systemd/system/rsyslog.service root@srv-web-GreenPlanet:~#</pre>
Recommandations	Désactiver la combinaison « Ctrl+Alt+Suppr » sur le serveur en tapant la commande suivante en tant qu'administrateur : <code>ln -sf /dev/null /etc/systemd/system/ctrl-alt-del.target</code>

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	<pre> root@srv-web-GreenPlanet:~# systemctl list-units --type target UNIT LOAD ACTIVE SUB DESCRIPTION basic.target loaded active active Basic System cryptsetup.target loaded active active Encrypted Volumes getty.target loaded active active Login Prompts graphical.target loaded active active Graphical Interface local-fs-pre.target loaded active active Local File Systems (Pre) local-fs.target loaded active active Local File Systems multi-user.target loaded active active Multi-User System network-online.target loaded active active Network is Online network.target loaded active active Network nss-lookup.target loaded active active Host and Network Name Lookups paths.target loaded active active Paths remote-fs-pre.target loaded active active Remote File Systems (Pre) remote-fs.target loaded active active Remote File Systems rpcbind.target loaded active active RPC Port Mapper slices.target loaded active active Slices sockets.target loaded active active Sockets sound.target loaded active active Sound Card swap.target loaded active active Swap sysinit.target loaded active active System Initialization timers.target loaded active active Timers LOAD = Reflects whether the unit definition was properly loaded. ACTIVE = The high-level unit activation state, i.e. generalization of SUB. SUB = The low-level unit activation state, values depend on unit type. 20 loaded units listed. Pass --all to see loaded but inactive units, too. To show all installed unit files use 'systemctl list-unit-files'. root@srv-web-GreenPlanet:~# </pre>
Recommandations	<p>Désactiver les cibles inutiles démarrées automatiquement avec le serveur via les commandes exécutées en tant qu'administrateur :</p> <pre> systemctl stop sound.target systemctl disable sound.target systemctl stop graphical.target systemctl disable graphical.target </pre>

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	<pre> root@srv-web-GreenPlanet:~# <u>systemctl list-unit-files --type service grep enabled</u> anacron-resume.service enabled anacron.service enabled atd.service enabled bind9.service enabled bluetooth.service enabled cron.service enabled dbus-org.bluez.service enabled getty@.service enabled hwclock-save.service enabled netfilter-persistent.service enabled nginx.service enabled php5-fpm.service enabled rsyslog.service enabled ssh.service enabled sshd.service enabled syslog.service enabled root@srv-web-GreenPlanet:~# </pre>
Recommandations	<p>désactiver le service Bluetooth en tant qu'administrateur via les commandes suivantes :</p> <pre> systemctl stop bluetooth.service systemctl disable bluetooth.service systemctl stop dbus-org.bluez.service systemctl disable dbus-org.bluez.service </pre>

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	<code>systemctl list-units --type service grep running</code>
Capture	<pre> root@srv-web-GreenPlanet:~# <u>systemctl list-units --type service grep running</u> acpid.service loaded active running ACPI event daemon asterisk.service loaded active running LSB: Asterisk PBX atd.service loaded active running Deferred execution scheduler bind9.service loaded active running BIND Domain Name Server cron.service loaded active running Regular background program processing daemon dbus.service loaded active running D-Bus System Message Bus exim4.service loaded active running LSB: exim Mail Transport Agent getty@tty1.service loaded active running Getty on tty1 mysql.service loaded active running LSB: Start and stop the mysql database server daemon nfs-common.service loaded active running LSB: NFS support files common to client and server nginx.service loaded active running A high performance web server and a reverse proxy server php5-fpm.service loaded active running The PHP FastCGI Process Manager rpcbind.service loaded active running LSB: RPC portmapper replacement rsyslog.service loaded active running System Logging Service ssh.service loaded active running OpenBSD Secure Shell server systemd-journald.service loaded active running Journal Service systemd-logind.service loaded active running Login Service systemd-udevd.service loaded active running udev Kernel Device Manager root@srv-web-GreenPlanet:~# </pre>
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	<pre>root@srv-web-GreenPlanet:~# sysctl kernel.sysrq kernel.sysrq = 438 root@srv-web-GreenPlanet:~#</pre>
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	<pre># # The PAM configuration file for the Shadow 'login' service # # Enforce a minimal delay in case of failure (in microseconds). # (Replaces the 'FAIL_DELAY' setting from login.defs) # Note that other modules may require another minimal delay. (for example, # to disable any delay, you should add the nodelay option to pam_unix) auth optional pam_faildelay.so delay=3000000</pre>
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

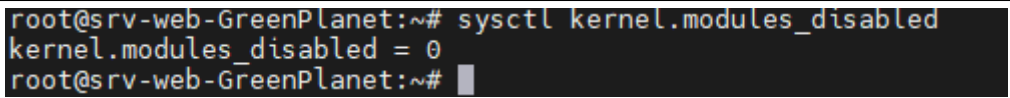
Lien de référence : https://www.ssi.gouv.fr/uploads/2016/01/linux_configuration-fr-v1.2.pdf

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 linux /boot/grub/grub.cfg head -1
Capture	<pre>root@srv-web-GreenPlanet:~# grep linux /boot/grub/grub.cfg head -1 linux /boot/vmlinuz-3.16.0-4-586 root=UUID=ac0ff7a8-7d92-443a-80be-3af7ec446d2c ro quiet root@srv-web-GreenPlanet:~#</pre>

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	<pre> 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:~# </pre>

Capture	<pre> root@srv-web-GreenPlanet:~# apt-cache policy logwatch logwatch: Installé : (aucun) Candidat : 7.4.1-2 Table de version : 7.4.1-2 0 500 http://mirror.u-pem.fr/debian/ jessie/main i386 Packages root@srv-web-GreenPlanet:~# </pre>
Recommandation	<p>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.</p>

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	<pre> root@srv-web-GreenPlanet:~# ss -lpun grep rpc UNCONN 0 0 *:45549 *: users:(("rpc.statd",pid=473,fd=8)) UNCONN 0 0 *:111 *: users:(("rpcbind",pid=453,fd=6)) UNCONN 0 0 *:626 *: users:(("rpcbind",pid=453,fd=7)) UNCONN 0 0 127.0.0.1:649 *: users:(("rpc.statd",pid=473,fd=5)) UNCONN 0 0 :::42351 :::* users:(("rpc.statd",pid=473,fd=10)) UNCONN 0 0 :::111 :::* users:(("rpcbind",pid=453,fd=9)) UNCONN 0 0 :::626 :::* users:(("rpcbind",pid=453,fd=10)) root@srv-web-GreenPlanet:~# </pre>
Recommandations	<p>Pour désactiver le protocole NFS, exécuter les commandes suivantes :</p> <ol style="list-style-type: none"> 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	<pre>root@srv-web-GreenPlanet:~# apt-cache policy docker docker: Installé : (aucun) Candidat : 1.5-1 Table de version : 1.5-1 0 500 http://mirror.u-pem.fr/debian/ jessie/main i386 Packages root@srv-web-GreenPlanet:~#</pre>
Recommandations	apt install docker Puis installer le conteneurs Nginx, MySQL et BIND9 via la commande : docker pull <i>nom_service</i> 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.pdf

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	<pre># First some standard log files. Log by facility. # auth,authpriv.* /var/log/auth.log *.:*;auth,authpriv.none /var/log/syslog #cron.* /var/log/cron.log daemon.* /var/log/daemon.log kern.* /var/log/kern.log lpr.* /var/log/lpr.log mail.* /var/log/mail.log user.* /var/log/user.log # # Logging for the mail system. Split it up so that # it is easy to write scripts to parse these files. # mail.info /var/log/mail.info mail.warn /var/log/mail.warn mail.err /var/log/mail.err # # Logging for INN news system. # news.crit /var/log/news/news.crit news.err /var/log/news/news.err news.notice /var/log/news/news.notice # # Some "catch-all" log files. # *.*=debug;\ auth,authpriv.none;\ news.none;mail.none /var/log/debug *.*=info;*.=notice;*.=warn;\ auth,authpriv.none;\ cron,daemon.none;\ mail,news.none /var/log/messages</pre>

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	<pre> Netid State Recv-Q Send-Q Local Address:Port Peer Address:Port users(("dhclient",pid=479,fd=20)) udp UNCONN 0 0 *:35162 *: users(("asterisk",pid=1102,fd=20)) udp UNCONN 0 0 *:5000 *: users(("asterisk",pid=1102,fd=19)) udp UNCONN 0 0 *:4520 *: users(("asterisk",pid=1102,fd=15)) udp UNCONN 0 0 *:5060 *: users(("asterisk",pid=1102,fd=13)) udp UNCONN 0 0 *:4569 *: users(("rpc.statd",pid=473,fd=8)) udp UNCONN 0 0 *:45549 *: users(("named",pid=519,fd=516)) udp UNCONN 0 0 192.168.1.30:53 *: users(("named",pid=519,fd=515)) udp UNCONN 0 0 192.168.80.1:53 *: users(("named",pid=519,fd=514)) udp UNCONN 0 0 192.168.1.136:53 *: users(("named",pid=519,fd=513)) udp UNCONN 0 0 127.0.0.1:53 *: users(("dhclient",pid=971,fd=6)) udp UNCONN 0 0 *:68 *: users(("dhclient",pid=479,fd=6)) udp UNCONN 0 0 *:111 *: users(("rpcbind",pid=453,fd=6)) udp UNCONN 0 0 *:626 *: users(("rpcbind",pid=453,fd=7)) udp UNCONN 0 0 *:13956 *: users(("dhclient",pid=971,fd=20)) udp UNCONN 0 0 127.0.0.1:649 *: users(("rpc.statd",pid=473,fd=5)) udp UNCONN 0 0 :::36596 ::: users(("dhclient",pid=971,fd=21)) udp UNCONN 0 0 :::42351 ::: users(("rpc.statd",pid=473,fd=10)) udp UNCONN 0 0 :::53 ::: users(("named",pid=519,fd=512)) udp UNCONN 0 0 :::111 ::: users(("rpcbind",pid=453,fd=9)) udp UNCONN 0 0 :::626 ::: users(("rpcbind",pid=453,fd=10)) udp UNCONN 0 0 :::13956 ::: users(("dhclient",pid=479,fd=21)) tcp LISTEN 0 20 127.0.0.1:25 *: users(("exim4",pid=1455,fd=4)) tcp LISTEN 0 128 127.0.0.1:953 *: users(("named",pid=519,fd=24)) tcp LISTEN 0 128 127.0.0.1:6010 *: users(("sshd",pid=1023,fd=8)) tcp LISTEN 0 128 *:55546 *: users(("rpc.statd",pid=473,fd=9)) tcp LISTEN 0 50 127.0.0.1:3306 *: users(("mysqld",pid=932,fd=10)) tcp LISTEN 0 10 127.0.0.1:5038 *: users(("asterisk",pid=1102,fd=7)) tcp LISTEN 0 128 *:111 *: users(("rpcbind",pid=453,fd=8)) tcp LISTEN 0 2 *:2000 *: users(("asterisk",pid=1102,fd=14)) tcp LISTEN 0 128 *:80 *: users(("nginx",pid=572,fd=8),("nginx", tcp LISTEN 0 10 192.168.1.30:53 *: users(("named",pid=519,fd=27)) tcp LISTEN 0 10 192.168.80.1:53 *: users(("named",pid=519,fd=23)) tcp LISTEN 0 10 192.168.1.136:53 *: users(("named",pid=519,fd=22)) tcp LISTEN 0 10 127.0.0.1:53 *: users(("named",pid=519,fd=21)) tcp LISTEN 0 128 *:22 *: users(("sshd",pid=558,fd=3)) tcp LISTEN 0 20 :::1:25 ::: users(("exim4",pid=1455,fd=5)) tcp LISTEN 0 128 :::1:953 ::: users(("named",pid=519,fd=25)) tcp LISTEN 0 128 :::1:6010 ::: users(("sshd",pid=1023,fd=7)) tcp LISTEN 0 128 :::111 ::: users(("rpcbind",pid=453,fd=11)) tcp LISTEN 0 10 :::53 ::: users(("named",pid=519,fd=20)) tcp LISTEN 0 128 :::22 ::: users(("sshd",pid=558,fd=4)) tcp LISTEN 0 128 :::48536 ::: users(("rpc.statd",pid=473,fd=11)) </pre>
Recommandations	<p>Les services RPC et Astrisk sont inutiles dans le cas de ce serveur web.</p> <p>En tant qu'administrateur, désactiver ces deux services via les commandes suivantes :</p> <pre> systemctl stop rpcbind.service systemctl disable rpcbind.service systemctl stop asterisk.service systemctl disable asterisk.service </pre>

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 eth2 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	<pre> root@srv-web-GreenPlanet:~# ip a 1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00 inet 127.0.0.1/8 scope host lo valid_lft forever preferred_lft forever inet6 ::1/128 scope host valid_lft forever preferred_lft forever 2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000 link/ether 08:00:27:e7:25:a9 brd ff:ff:ff:ff:ff:ff inet 192.168.1.136/24 brd 192.168.1.255 scope global eth0 valid_lft forever preferred_lft forever inet6 fe80::a00:27ff:fee7:25a9/64 scope link valid_lft forever preferred_lft forever 3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000 link/ether 08:00:27:31:1d:c7 brd ff:ff:ff:ff:ff:ff inet 192.168.1.30/24 brd 192.168.1.255 scope global eth1 valid_lft forever preferred_lft forever inet6 2a01:e0a:86f:9430:a00:27ff:fe31:1dc7/64 scope global mngtmpaddr dynamic valid_lft 86284sec preferred_lft 86284sec inet6 fe80::a00:27ff:fe31:1dc7/64 scope link valid_lft forever preferred_lft forever 4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000 link/ether 08:00:27:0e:1c:44 brd ff:ff:ff:ff:ff:ff inet 192.168.80.1/24 brd 192.168.80.255 scope global eth2 valid_lft forever preferred_lft forever inet6 fe80::a00:27ff:fe0e:1c44/64 scope link valid_lft forever preferred_lft forever root@srv-web-GreenPlanet:~# </pre>
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	<pre> root@srv-web-GreenPlanet:~# grep PermitRootLogin /etc/ssh/sshd_config #PermitRootLogin yes PermitRootLogin yes # the setting of "PermitRootLogin without-password". root@srv-web-GreenPlanet:~# </pre>
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	<pre>root@srv-web-GreenPlanet:~# grep Port /etc/ssh/sshd_config Port 22 root@srv-web-GreenPlanet:~# █</pre>
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	<pre>root@srv-web-GreenPlanet:~# iptables -L -n Chain INPUT (policy ACCEPT) target prot opt source destination ACCEPT icmp -- 0.0.0.0/0 0.0.0.0/0 Chain FORWARD (policy ACCEPT) target prot opt source destination Chain OUTPUT (policy ACCEPT) target prot opt source destination root@srv-web-GreenPlanet:~# █</pre>
Recommandations	<p>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.</p> <p>La politique par défaut est d'accepter les requêtes. Or, il faut plutôt rejeter par défaut, et ensuite laisser passer les requêtes souhaitées.</p> <p>En tant qu'administrateur, il faudra modifier le fichier « /etc/iptables.conf », par exemple :</p> <pre>: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</pre>

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	<pre>root@srv-web-GreenPlanet:~# more /proc/net/if_inet6 00000000000000000000000000000001 01 80 10 80 lo fe8000000000000000a0027fffe311dc7 03 40 20 80 eth1 fe8000000000000000a0027fffe0e1c44 04 40 20 80 eth2 2a010e0a086f94300a0027fffe311dc7 03 40 00 00 eth1 fe8000000000000000a0027fffe725a9 02 40 20 80 eth0 root@srv-web-GreenPlanet:~#</pre>
Recommandations	Si l'IPv6 n'est pas utilisé sur le serveur, mieux vaut le désactiver

La recommandation **R64** du guide de l'ANSSI

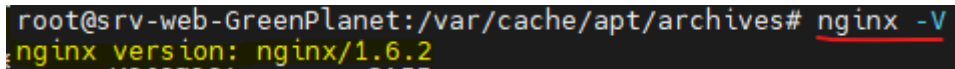
Lien de référence : https://www.ssi.gouv.fr/uploads/2016/01/linux_configuration-fr-v1.2.pdf

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	<pre>root@srv-web-GreenPlanet:~# iptables -L -n Chain INPUT (policy ACCEPT) target prot opt source destination ACCEPT icmp -- 0.0.0.0/0 0.0.0.0/0 Chain FORWARD (policy ACCEPT) target prot opt source destination Chain OUTPUT (policy ACCEPT) target prot opt source destination root@srv-web-GreenPlanet:~#</pre>
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

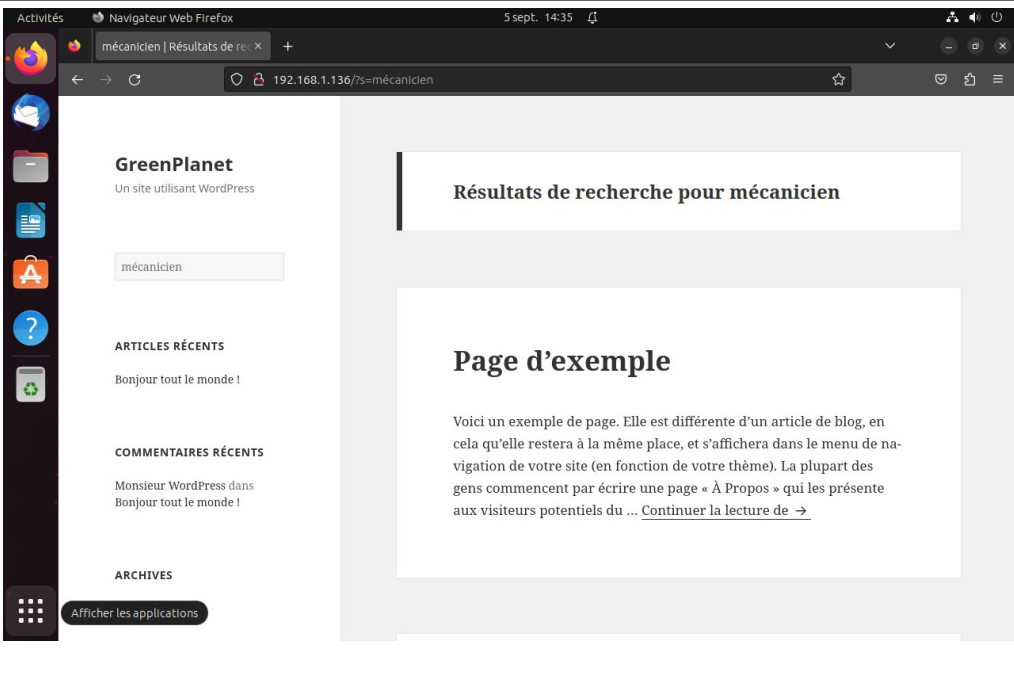
Lien de référence : https://www.ssi.gouv.fr/uploads/2016/01/linux_configuration-fr-v1.2.pdf

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-enabled/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

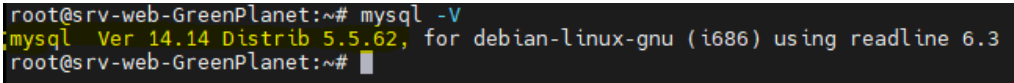
NGX3	Masquez la version de NGINX afin de se protéger contre les cyberattaques
Objectif	Masquez le numéros de version , pour éviter des attaques pirates
Principe associé	Défense en profondeur
Type	CRITICAL
Commande	Nano /etc/nginx/nginx.conf

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 de 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	<pre>root@srv-web-GreenPlanet:~# ss -lptn grep mysql LISTEN 0 50 127.0.0.1:3306 *:* users:((("mysqld",pid=972,fd=10)) root@srv-web-GreenPlanet:~#</pre>
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	<pre>root@srv-web-GreenPlanet:~# mysql -u root -p Enter password: Welcome to the MySQL monitor. Commands end with ; or \g. Your MySQL connection id is 44 Server version: 5.5.62-0+deb8u1 (Debian) Copyright (c) 2000, 2018, Oracle and/or its affiliates. All rights reserved. Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners. Type 'help;' or '\h' for help. Type '\c' to clear the current input statement. mysql></pre>
Recommandations	Ne pas montrer le mot de passe en effectuant la commande. Cela se verra dans l'historique des commandes.

La recommandation **R61** du guide de l'ANSSI

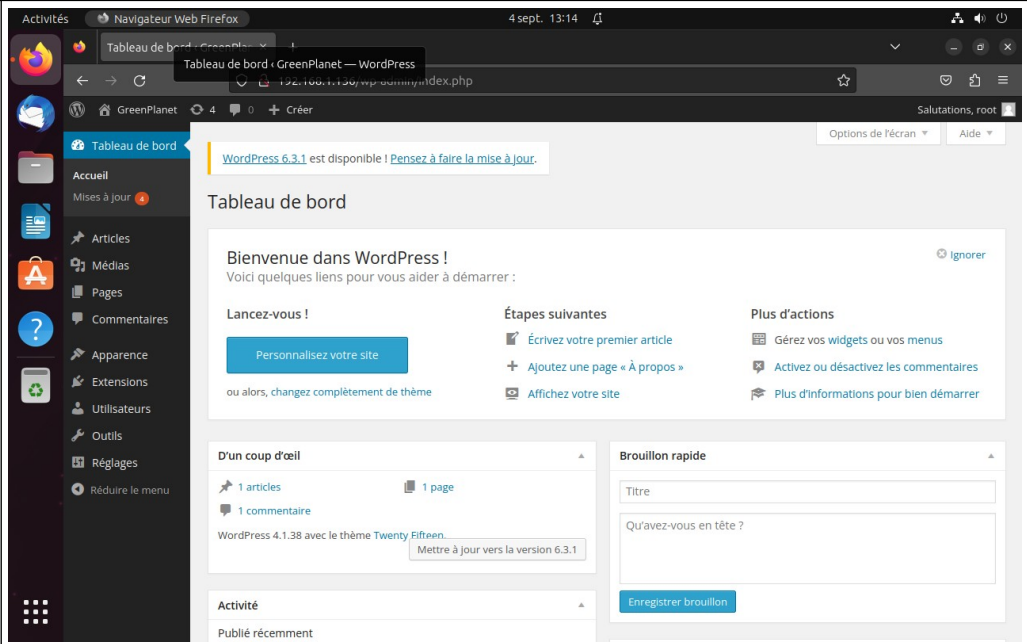
Lien de référence : https://www.ssi.gouv.fr/uploads/2016/01/linux_configuration-fr-v1.2.pdf

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	<pre>CREATE USER 'wp_user'@'localhost' identified by 'StrongPassword'; CREATE DATABASE wp_db; GRANT ALL PRIVILEGES ON wp_db.* TO 'wp_user'@'localhost'; FLUSH PRIVILEGES; SHOW DATABASES;</pre>
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 Wordpress
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	<pre>mysql> use wp_db Reading table information for completion of table and column names You can turn off this feature to get a quicker startup with -A Database changed mysql> SELECT * from wp_users ; +-----+-----+-----+-----+-----+-----+ ID user_login user_pass user_nicename user_email user_ url user_registered user_activation_key user_status display_name +-----+-----+-----+-----+-----+-----+ 1 root \$P\$BumVwPnwel6skscFiu3w/ANGHTVLGa/ root root@greenplanet.fr 2021-04-20 20:29:47 0 root +-----+-----+-----+-----+-----+-----+ 1 row in set (0.00 sec)</pre>
Recommandations	<p>Use wp_db CREATE USER 'wp_user'@'localhost' identified by 'Motdepasserobuste' ; GRANT ALL PRIVILEGES ON wp_db * TO 'wp_user'@localhost' ; FLUSH PRIVILEGES ;</p>

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	<pre>root@srv-web-GreenPlanet:~# ls -lrtha /srv/myblog total 192K -rw-r--r-- 1 www-data www-data 271 janv. 8 2012 wp-blog-header.php -rw-r--r-- 1 www-data www-data 418 sept. 25 2013 index.php -rw-r--r-- 1 www-data www-data 2,4K oct. 25 2013 wp-links-opml.php -rw-r--r-- 1 www-data www-data 3,0K févr. 9 2014 xmlrpc.php -rw-r--r-- 1 www-data www-data 2,9K mai 13 2014 wp-cron.php -rw-r--r-- 1 www-data www-data 2,7K juil. 7 2014 wp-load.php -rw-r--r-- 1 www-data www-data 11K juil. 18 2014 wp-settings.php -rw-r--r-- 1 www-data www-data 2,7K sept. 9 2014 wp-config-sample.php -rw-r--r-- 1 www-data www-data 25K nov. 30 2014 wp-signup.php -rw-r--r-- 1 www-data www-data 7,1K oct. 31 2017 readme.html -rw-r--r-- 1 www-data www-data 20K janv. 23 2018 license.txt -rw-r--r-- 1 www-data www-data 33K déc. 13 2018 wp-login.php -rw-r--r-- 1 www-data www-data 6,3K déc. 13 2018 wp-activate.php -rw-r--r-- 1 www-data www-data 5,1K mars 12 2019 wp-comments-post.php drwxr-xr-x 12 www-data www-data 4,0K juin 11 2020 wp-includes drwxr-xr-x 9 www-data www-data 4,0K juin 11 2020 wp-admin drwxr-xr-x 3 root root 4,0K avril 20 2021 .. -rw-r--r-- 1 www-data www-data 2,7K avril 20 2021 wp-config.php -rw-r--r-- 1 www-data www-data 4,1K sept. 4 13:10 wp-trackback.php -rw-r--r-- 1 www-data www-data 8,3K sept. 4 13:10 wp-mail.php drwxr-xr-x 6 www-data www-data 4,0K sept. 4 13:10 wp-content drwxr-xr-x 5 www-data www-data 4,0K sept. 5 14:34 . root@srv-web-GreenPlanet:~#</pre>
Recommandations	<p>Il est recommandé de mettre les droits à 440 ou à 400 chmod 400 /srv/myblog/wp-config.php</p>

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.