AUDIT DE SÉCURITÉ SERVEUR WEB

Auteur : Ibine ABDALLAH
Entreprise : Atex
Date : 30/8/20

Table des matières

Grille de Gestion

Date	Auteur	Correcteur	Validateur	Commentaire
24/7/20	Ibine ABDALLAH	Ibine ABDALLAH	Ibine ABDALLAH	Création de la documentation

Contexte

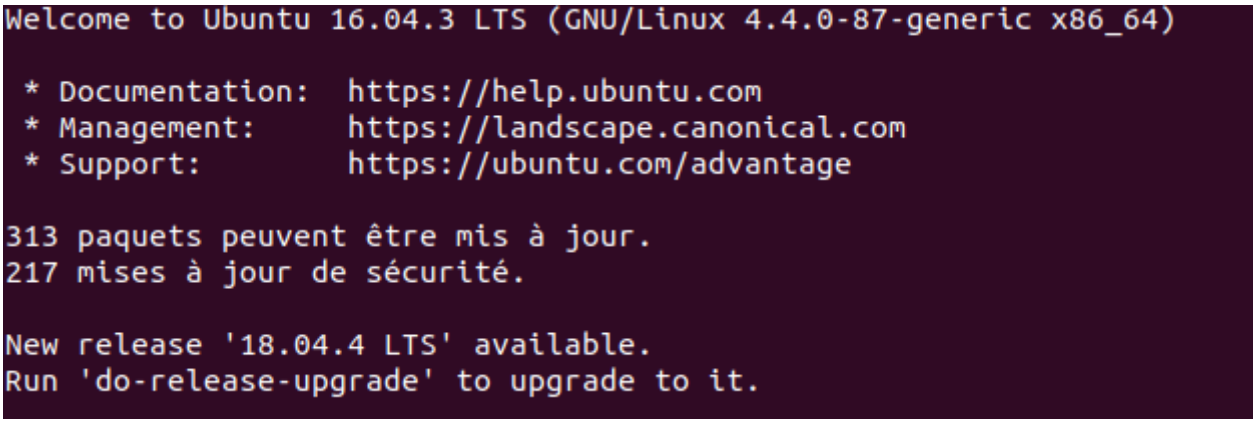
En tant que freelance. Le client m'a demandé de réaliser un audit de sécurité de son serveur. Le client a déjà une infrastructure complète, ce serveur servira uniquement de serveur Web

Le client m'a donné les droits d'accès sur son serveur. Je me lance donc dans l'audit du serveur qui se découpera en trois parties:

- une analyse manuelle
- Une analyse logicielle avec lynis
- Un rapport d'analyse qui résume l'ensemble de l'audit

I / Audit manuel

1) État du serveur



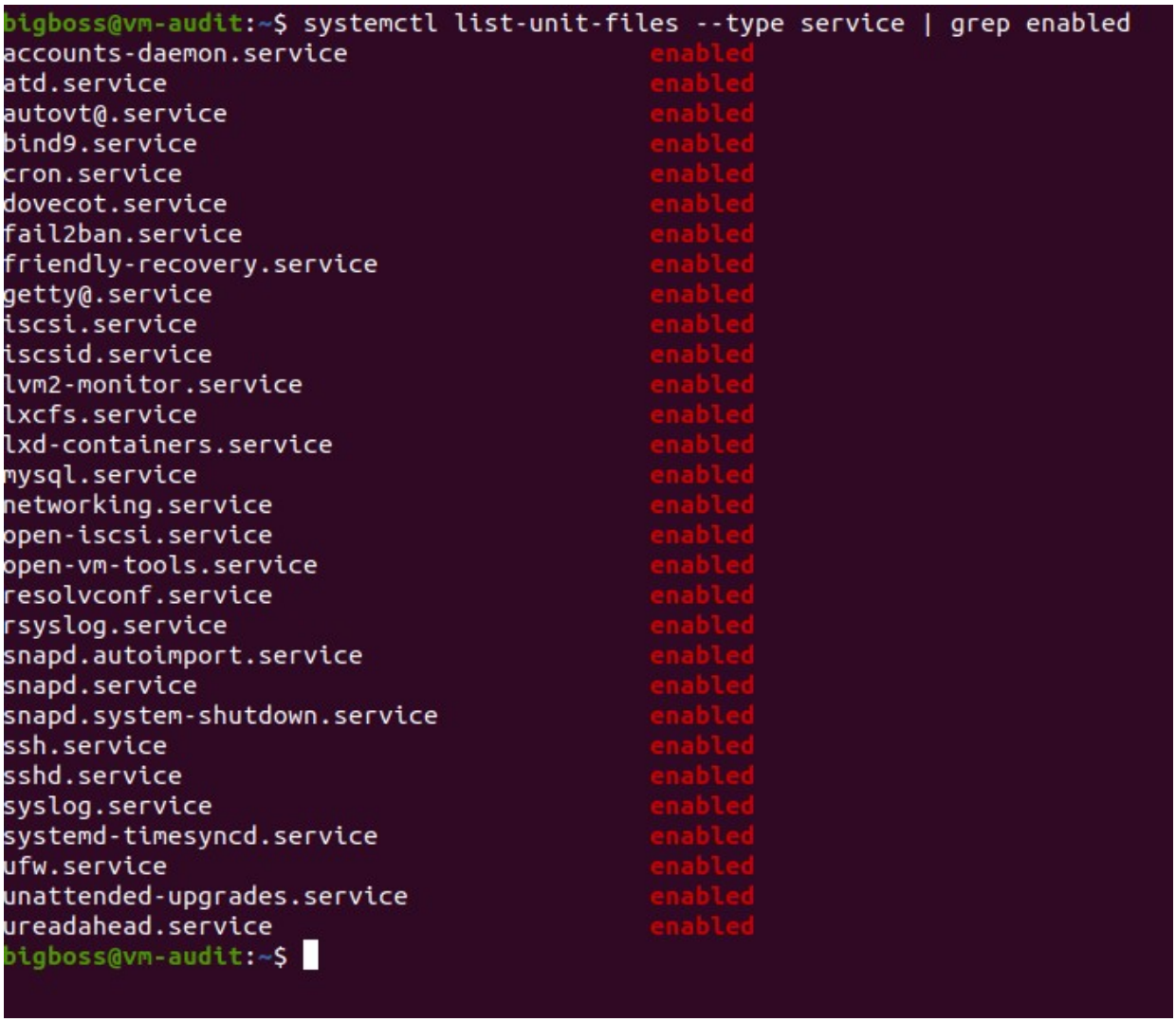
Vous devez faire la mise à jour du serveur (update & upgrade)
Vous devez faire la mise à jour de l'os 16.04 vers 18.04

Une version Ubuntu LTS a un suivi de 5 ans, ce qui signifie que la version 16.04 arrive bientôt au terme de sa maintenance

2) Service lancé

Services actifs au démarrage

Commande : systemctl list-unit-files --type=service | grep "enabled"



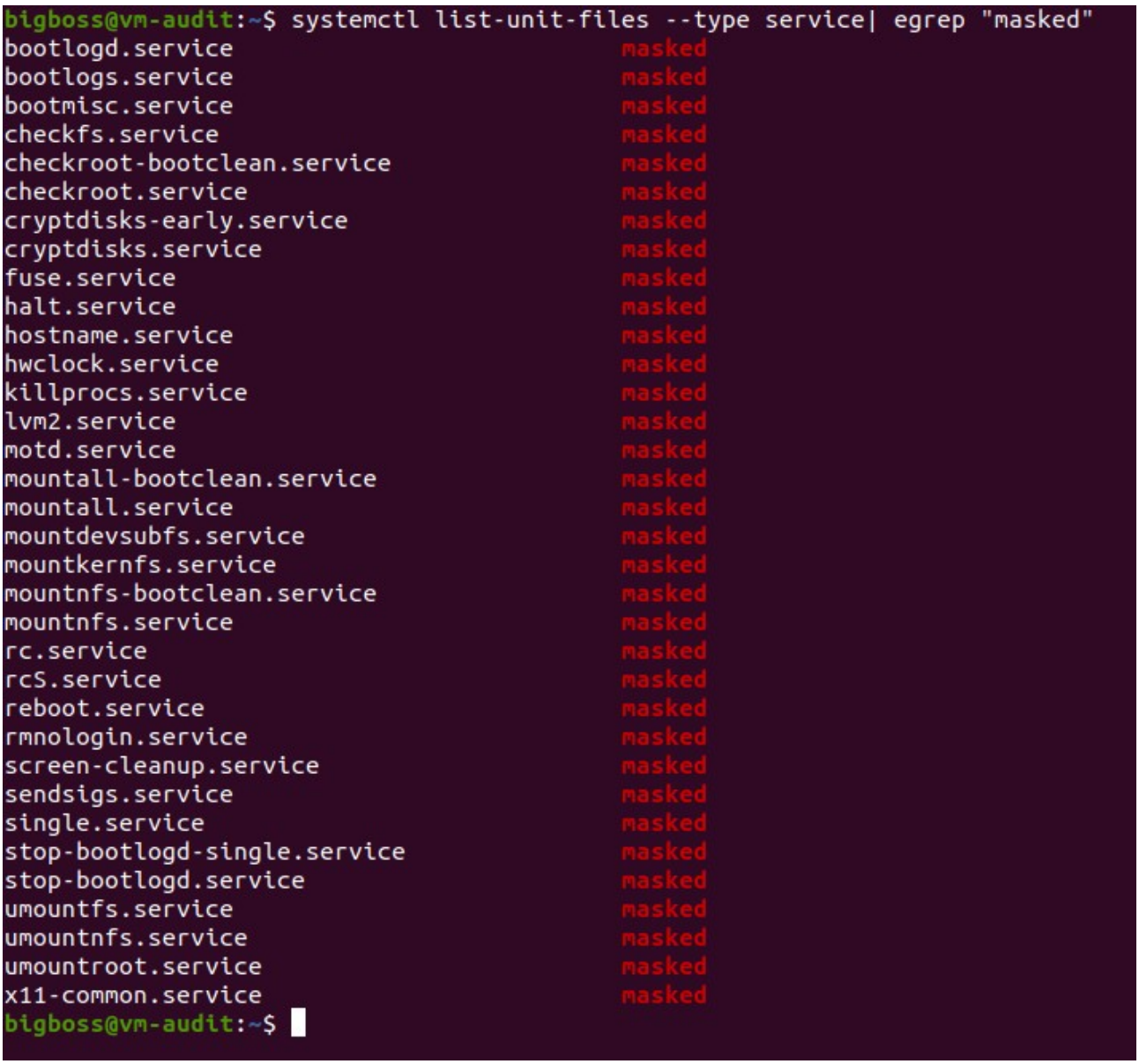
Les services lancés au démarrage du serveur :

accounts-daemon.service	enabled
autovt@.service	enabled
cron.service	enabled
fail2ban.service	enabled
mysql.service	enabled
networking.service	enabled
rsyslog.service	enabled
ssh.service	enabled
sshd.service	enabled
syslog.service	enabled
ufw.service	enabled
unattended-upgrades.service	enabled
resolvconf.service	enabled
systemd-timesyncd.service	enabled
open-iscsi.service	enabled
getty@.service	enabled
iscsi.service	enabled
iscsid.service	enabled
lvm2-monitor.service	enabled

friendly-recovery.service	enabled
bind9.service	enabled
ureadahead.service	enabled
snapd.autoimport.service	enabled
snapd.service	enabled
snapd.system-shutdown.service	enabled
open-vm-tools.service	enabled
lxcfs.service	enabled
lxd-containers.service	enabled
dovecot.service	enabled
atd.service	enabled

3) Services masqués

Commande : systemctl list-unit-files --type=service | grep "masked"



Les services masqués sont des services qu'on cache car on ne veut pas qu'ils soient activés via un autre service dont ils dépendent. Masqué un service c'est une alternative pour ne pas désinstaller le service et le désactiver.

4) Services désactivés

Commande : systemctl list-unit-files --type=service | grep "disabled"

```
bigboss@vm-audit:~$ systemctl list-unit-files --type service | grep disable
acpid.service                              disabled
bind9-pkcs11.service                       disabled
bind9-resolvconf.service                   disabled
console-getty.service                      disabled
console-shell.service                      disabled
dbus-org.freedesktop.network1.service      disabled
dbus-org.freedesktop.resolve1.service      disabled
debug-shell.service                        disabled
dm-event.service                           disabled
keyboard-setup.service                     disabled
lvm2-lvmetad.service                       disabled
lvm2-lvmpolld.service                      disabled
rsync.service                              disabled
serial-getty@.service                      disabled
systemd-bootchart.service                  disabled
systemd-networkd-wait-online.service       disabled
systemd-networkd.service                   disabled
systemd-resolved.service                   disabled
bigboss@vm-audit:~$
```

5) Services à conserver

5.1) Apache

Configuration apache2 (ici)

```
bigboss@vm-audit:~$ apt-show-versions apache2 -a
apache2:amd64 2.4.18-2ubuntu3.4 install ok installed
apache2:amd64 2.4.18-2ubuntu3    xenial          fr.archive.ubuntu.com
apache2:amd64 2.4.18-2ubuntu3.13 xenial-security security.ubuntu.com
apache2:amd64 2.4.18-2ubuntu3.15 xenial-updates  fr.archive.ubuntu.com
apache2:amd64/xenial-updates 2.4.18-2ubuntu3.4 upgradeable to 2.4.18-2ubun
tu3.15
apache2:i386 2.4.18-2ubuntu3    xenial          fr.archive.ubuntu.com
apache2:i386 2.4.18-2ubuntu3.13 xenial-security security.ubuntu.com
apache2:i386 2.4.18-2ubuntu3.15 xenial-updates  fr.archive.ubuntu.com
apache2:i386 not installed
```

Point à corriger :

Mettre à jours le paquet
Disable directory browser listing (indexe)
Run Apache from a non-privileged account (chmod –R 750)
HTTP Request Methods (LimitExcept GET POST HEAD)
Disable Trace HTTP Request (telnet)
Cookie with HttpOnly and secure flag
Clickjacking Attack
Server Side Include
X-XSS Protection
Disable HTTP 1.0 Protocol
Timeout value configuration (le mettre à 60)
SSL (ajouté un certificat au site)
Mod Security

5.2) Rsyslog

Configuration Rsyslog | (ici)

```
bigboss@vm-audit:~$ apt-show-versions rsyslog -a
rsyslog:amd64 8.16.0-1ubuntu3 install ok installed
rsyslog:amd64 8.16.0-1ubuntu3   xenial         fr.archive.ubuntu.com
rsyslog:amd64 8.16.0-1ubuntu3.1 xenial-updates fr.archive.ubuntu.com
rsyslog:amd64/xenial 8.16.0-1ubuntu3 upgradeable to 8.16.0-1ubuntu3.1
rsyslog:i386 8.16.0-1ubuntu3   xenial         fr.archive.ubuntu.com
rsyslog:i386 8.16.0-1ubuntu3.1 xenial-updates fr.archive.ubuntu.com
rsyslog:i386 not installed
```

Mettre à jours le paquet
Configurez rsyslog pour envoyer les logs sur le serveur dédié

5.3) Networking

Modifiez le port SSH pour un accès interne. Pour MySQL le retirer su front-end vers une autre machine en back-end.

5.4) Mysql

Configuration MySQL| (ici)

```
bigboss@vm-audit:~$ apt-show-versions mysql-server -a
mysql-server:all 5.7.19-0ubuntu0.16.04.1 install ok installed
mysql-server:all 5.7.11-0ubuntu6         xenial          fr.archive.ubuntu.com
mysql-server:all 5.7.31-0ubuntu0.16.04.1 xenial-security security.ubuntu.com
mysql-server:all 5.7.31-0ubuntu0.16.04.1 xenial-updates  fr.archive.ubuntu.com
mysql-server:all/xenial-security 5.7.19-0ubuntu0.16.04.1 upgradeable to 5.7.31-0ubuntu0.16.04.1
```

Mettre à jours le paquet
Créez un compte de service avec les droits adéquates
Exécutez la commande mysql_secure_installation
Désactiver la connexion distante
supprimé .mysql_history et créer un lien symbolique vers /dev/null
limité les connexions au serveurs

Chroot mysql

5.5) ssh

Configuration SSH (ici)

```
bigboss@vm-audit:~$ apt-show-versions openssh-server -a
openssh-server:amd64 1:7.2p2-4ubuntu2.2 install ok installed
openssh-server:amd64 1:7.2p2-4           xenial          fr.archive.ubuntu.com
openssh-server:amd64 1:7.2p2-4ubuntu2.8  xenial-security security.ubuntu.com
openssh-server:amd64 1:7.2p2-4ubuntu2.10 xenial-updates  fr.archive.ubuntu.com
openssh-server:amd64/xenial-updates 1:7.2p2-4ubuntu2.2 upgradeable to 1:7.2p2-4ubuntu2.10
openssh-server:i386 1:7.2p2-4           xenial          fr.archive.ubuntu.com
openssh-server:i386 1:7.2p2-4ubuntu2.8  xenial-security security.ubuntu.com
openssh-server:i386 1:7.2p2-4ubuntu2.10 xenial-updates  fr.archive.ubuntu.com
openssh-server:i386 not installed
```

Point à corriger :

Mettre à jours le paquet
Mot de passe fort
Utiliser un cryptage robuste
MFA
Disable Root
Disconnect Idle Sessions
Whitelist Users
Change Ports
SSH Keys
Disable Password Authentication
Disable X11Forwarding
Fail2Ban
Autoriser uniquement les connexions interne

5.6) Unattended-upgrades

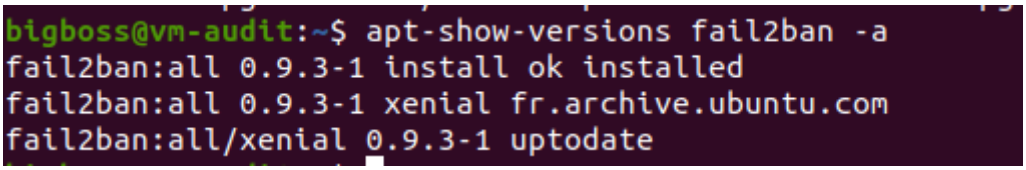
Configuration unattended-upgrades | (ici)

```
bigboss@vm-audit:~$ apt-show-versions unattended-upgrades -a
unattended-upgrades:all 0.90ubuntu0.7 install ok installed
unattended-upgrades:all 0.90                      xenial          fr.archive.ubuntu.com
unattended-upgrades:all 0.90ubuntu0.10            xenial-security security.ubuntu.com
unattended-upgrades:all 1.1ubuntu1.18.04.7~16.04.6 xenial-updates  fr.archive.ubuntu.com
unattended-upgrades:all/xenial-updates 0.90ubuntu0.7 upgradeable to 1.1ubuntu1.18.04.7~16.04.6
```

Mettre à jours le paquet

5.7) Fail2ban

Configuration fail2ban (ici)



Mettre à jour le paquet
Ajoutez les jails manquantes :

[apache]
[apache-noscript]
[apache-overflows]
[apache-badbots]
[apache-dos]
[apache-auth]
[apache-nohome]
[apache-botsearch]
[apache-fakegooglebot]
[apache-modsecurity]
[apache-shellshock]
[php-url-fopen]
[mysqld-auth]

Recommandation concernant l’infrastructure du client, nous vous recommandons de mettre en place une architecture n-tier afin de réduire les vecteurs d’attaque.

5.8) CVE

Vous trouverez une liste de différentes CVE ci-dessous

CVE	services	Contexte	Priorité
CVE-2019-0217	Apache2	Avec Apache HTTP Server 2.4 version 2.4.38 et antérieures, le module mod_auth_digest pouvait permettre à un utilisateur valide de s'authentifier à l'aide d'un autre nom d'utilisateur	Medium
CVE-2019-17041	rsyslog	C'est un débordement dans l'analyseur pour les messages de journal AIX. L'analyseur essaie de localiser un délimiteur de message de journal sans succès. Du coup les logs sont décalé	Low
CVE-2020-14145	ssh	Fuite d'informations dans la négociation de l'algorithme côté client avec Openssh. Cela permet aux attaquants de cibler les tentatives de connexion	Low
CVE-2020-2572	mysql	Faille permettant à un attaquant hautement privilégié, avec un accès réseau via plusieurs protocoles de	Medium

		compromettre MySQL Serveur	
CVE-2013-7177	fail2ban	Faille permettant aux attaquants de déclencher le blocage d'une adresse IP arbitraire via une adresse e-mail qui correspond à une expression régulière mal conçue.	Medium
CVE-2015-1330	unattended-upgrades	Faille permettant aux attaquants de charger des paquets non arbitraires via des dépôts non spécifiés	Medium
CVE-2018-10900	network-manager	Faille permettant à un attaquant d'exécuter des commandes arbitraires en tant que root.	Medium

Site de référence pour les CVE ici

6) Services à retirer

Vous trouverez ci-dessous la liste des services non requis sur le serveur web. Afin de vous prémunir de potentiel vecteur d'attaque, retiré tous les services non requis.

ureadahead.service	enabled
snapd.autoimport.service	enabled
snapd.service	enabled
snapd.system-shutdown.service	enabled
open-vm-tools.service	enabled
lxcfs.service	enabled
lxd-containers.service	enabled
dovecot.service	enabled
atd.service	enabled
accounts-daemon.service	enabled
open-iscsi.service	enabled
iscsi.service	enabled
iscsid.service	enabled
autovt@.service	enabled
friendly-recovery.service	enabled
ufw.service	enabled

7) Ports ouvert

```
bigboss@vm-audit:~$ sudo netstat -lptune | grep "LISTEN"
tcp        0      0 0.0.0.0:110             0.0.0.0:*               LISTEN      0          15587      1146/dovecot
tcp        0      0 0.0.0.0:143             0.0.0.0:*               LISTEN      0          15599      1146/dovecot
tcp        0      0 192.168.1.30:53         0.0.0.0:*               LISTEN      111        19536      1097/named
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN      111        16370      1097/named
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      0          20135      1102/sshd
tcp        0      0 0.0.0.0:25              0.0.0.0:*               LISTEN      0          17469      1422/master
tcp        0      0 127.0.0.1:953           0.0.0.0:*               LISTEN      111        16864      1097/named
tcp6       0      0 :::3306                 :::*                    LISTEN      107        17009      1171/mysqld
tcp6       0      0 :::110                  :::*                    LISTEN      0          15588      1146/dovecot
tcp6       0      0 :::143                  :::*                    LISTEN      0          15600      1146/dovecot
tcp6       0      0 :::80                   :::*                    LISTEN      0          16916      1242/apache2
tcp6       0      0 :::53                   :::*                    LISTEN      111        16363      1097/named
tcp6       0      0 :::22                   :::*                    LISTEN      0          20137      1102/sshd
tcp6       0      0 :::25                   :::*                    LISTEN      0          17470      1422/master
tcp6       0      0 ::1:953                 :::*                    LISTEN      111        16865      1097/named
bigboss@vm-audit:~$
```

Ci-dessus vous trouverez la liste des ports ouvert sur votre serveur web. Pensez à fermer tous les ports non utilisés et dans la mesure du possible modifier les ports par défaut.

22: SSH
3306: MYSQL
80: HTTP
53: DNS
25: SMTP
68: Bootstrap (BOOTP)
110: POP3
143: IMAP
953: BIND remote name daemon control (RNDC)
443 : HTTPS ouvrir le 443

Une redirection de port est configurée pour vous permettre d'accéder au port 80 de la machine virtuelle en tapant l'adresse http://localhost:8080 → Il y a une erreur sur le fichier port dans apache. On voit que le port d'écoute n'est pas le 8080 mais 80. Donc le site est indisponible

8) Comptes actifs

```
bigboss@vm-audit:~$ cat /etc/passwd | grep "/bin/bash"
root:x:0:0:root:/root:/bin/bash
bigboss:x:1000:1000:bigboss,,,:/home/bigboss:/bin/bash
pierre:x:1001:1001:Pierre,,,:/home/pierre:/bin/bash
marie:x:1002:1002:Marie,,,:/home/marie:/bin/bash
daniel:x:1001:1001,Daniel,,,:/home/daniel:/bin/bash
bigboss@vm-audit:~$
```

Ci-dessus vous trouverez la liste des utilisateurs présents sur le serveur

8.1) Droits sur les comptes

```
bigboss@vm-audit:/home$ ls -lrtha
total 24K
drwxr-xr-x 23 root    root    4,0K juil.  3  2018 ..
drwxr-xr-x  2 pierre  pierre  4,0K juil.  4  2018 pierre
drwxr-xr-x  2 marie   marie   4,0K juil.  4  2018 marie
drwxr-xr-x  6 root    root    4,0K juil.  4  2018 .
drwxr-xr-x  2 pierre  pierre  4,0K juil.  4  2018 daniel
drwxr-xr-x  3 bigboss bigboss 4,0K août   1 13:59 bigboss
bigboss@vm-audit:/home$ id bigboss
uid=1000(bigboss) gid=1000(bigboss) groupes=1000(bigboss),4(adm),24(cdrom),27(su
do),30(dip),46(plugdev),110(lxd),122(lpadmin),123(sambashare)
bigboss@vm-audit:/home$ id pierre
uid=1001(pierre) gid=1001(pierre) groupes=1001(pierre)
bigboss@vm-audit:/home$ id marie
uid=1002(marie) gid=1002(marie) groupes=1002(marie)
bigboss@vm-audit:/home$
```

Vous pouvez apercevoir les différents comptes ainsi que leurs droits et groupe d'appartenance.

8.2) Comptes de services

```
bigboss@vm-audit:~$ cat /etc/passwd | grep "/usr/sbin/nologin"
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/
nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
sshd:x:115:65534::/var/run/sshd:/usr/sbin/nologin
```

Dans cette liste d'utilisateurs de services vous devez supprimer les utilisateurs non requis

Compte de service à conserver :
daemon
bin
sys
man
www-data

9) Sécurité présents ou actifs sur la machine

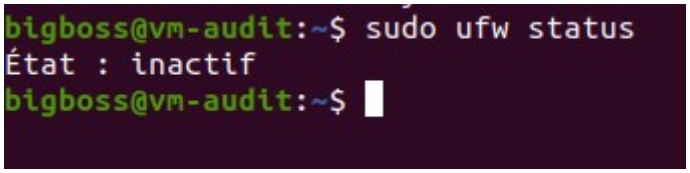
- pare-feu : (iptables et ufw : non configuré) ok

```
bigboss@vm-audit:~$ sudo iptables -L
[sudo] Mot de passe de bigboss :
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
f2b-sshd   tcp  --  anywhere             anywhere             multiport dp
orts ssh

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain f2b-sshd (1 references)
target     prot opt source               destination
RETURN     all  --  anywhere             anywhere
bigboss@vm-audit:~$
```



Vous pouvez voir que le firewall n’est pas configuré et que le service UFW est inactif.

10) Anti-virus

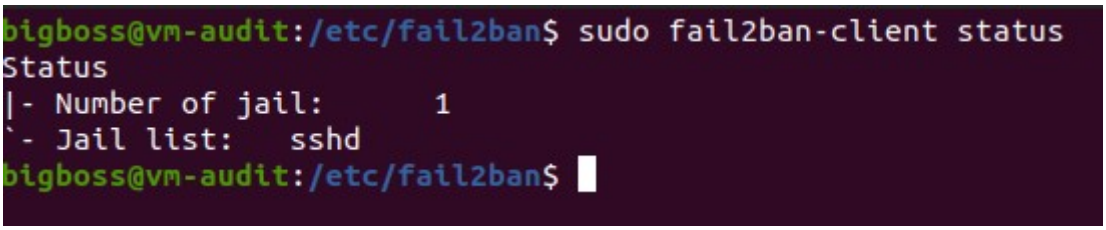
Comme vous avez pu le constater il n’y a aucun antivirus de présent sur le poste. Je vous recommande donc ClamAV et ClamTK. ClamTk est une interface graphique logicielle gratuite pour le logiciel antivirus en ligne de commande ClamAV

11) Anti-rootkit

Il n’y a pas d’anti-rootkit non plus je vous recommande donc rkhunter.

12) Systèmes de détection d’intrusion système ou réseau

(fail2ban non configuré) ok



Vous pouvez voir que fail2ban est bien installé par contre il n’y a qu’une seule jails de configurer. Il faut installer les autres jails

Example : [apache], [apache-noscript], [php-url-fopen], [squid], [mysqld-auth],

II/ Auditez logicielle via Lynis

Audit de la configuration du serveur WEB, Ubuntu 16.04.3 LTS, avec une PMAD et Lynis 3.0.0.

1) PROCESSUS DE DÉMARRAGE

N°	Recommandation	Type	Risque	Bénéfice	Priorité
BOO.1	Sécuriser le grup : Passer les droits sur l'arborescence /etc/grub.d à 700	CRITICAL	Intrusion et prise de contrôle à distance	Sécurisation du bootloader	1
BOO.2	User grub : Créer un utilisateur et son mot de passe chiffré dans le fichier 01_users afin de protéger l'accès au shell de Grub par une authentification	CRITICAL	Intrusion et prise de contrôle à distance	Sécurisation du bootloader	1
BOO.3	root_ssh: Vider le contenu du fichier /etc/securetty afin de bloquer toute connexion avec l'utilisateur root depuis une console virtuelle	CRITICAL	Intrusion et prise de contrôle à distance	Sécurisation du terminal	1

BOO.4	Ctrl+Alt+Supp : Désactiver la combinaison Ctrl+Alt+Supp sur le serveur pour prévenir tout redémarrage depuis un accès physique à la machine	CRITICAL	Intrusion et prise de contrôle local et distant	Sécurisation du terminal	1
BOO.5	app_no_used: Supprimer les applications inutiles démarrés automatiquement avec le serveur en passant par la cible par défaut	CRITICAL	Intrusion via un application inutilisé	Éviter d’ouvrir des portes aux intrusions. Risque inutiles	1
BOO.6	usb : Passer l'option iommu=force au noyau lors du démarrage de Linux (L'IOMMU sert à protéger les accès non authorisées à la mémoire vive)	Warning	Modification du grub	protéger les accès non authorisées à la mémoire vive	1
BOO.7	module: Bloquer le chargement de modules supplémentaires via la sysctl kernel.modules_disabled=1	warning	Modification du kernel	Protéger le kernel	1

BOO.8	Intervalle_connexion : Augmenter l'intervalle minimal de temps entre chaque tentative de connexion sur le module pam_faildelay.so du fichier /etc/pam.d/system-auth à 5 ou 10 secondes afin de ralentir les attaques par dictionnaire	Warning	Possibilité de d'intrusion	Ralentir les tentatives d'intrusion .	1
BOO.9	Magic_SysRq_key : Désactiver les Magic System Request Keys	Warning	Intrusion et prise de contrôle local et distant	Sécurisation du terminal	1
BOO.10	service_no_used : Supprimer les services inutiles démarrés automatiquement avec le serveur en passant par les dépendances de la cible par défaut	Warning	Intrusion via un service inutilisé	Éviter d'ouvrir des portes aux intrusions. Risque inutiles	1

2) Audit Système

N°	Recommandation	Type	Risque	Bénéfice	Priorité
SYS.1	PAE_NX :	CRITICAL	Exécution	Ces deux attributs	1

	Vérifier que le CPU dispose bien des flags PAE et NX		d'instructions stockées dans les régions mémoire non autorisées.	indiquent que le processeur protège l'exécution d'instructions stockées dans les régions mémoire non autorisées.	
SYS.2	Partition : Vérifier le chiffrement des partitions sensibles du système	CRITICAL	Possibilité d'accès non autorisés	Protéger le disque contre des accès non autorisés	1
SYS.3	mount_point : Vérifier les options des points de montage des systèmes de fichiers	CRITICAL	Accès au autre point de montage	Le cloisonnement limite les possibilité de modification	2
SYS.4	acces_host: Vérifier la protection de la partition / boot	CRITICAL	Modification des option de boot	Sécurisation des option de boot	1
SYS.5	mdp_pam_shadow: Vérifier que les mots de passe du module PAM sont en mode shadow	CRITICAL	Récupération du mot de passe	Sécuriser les mot de passe	1
SYS.6	mdp_pam_strong: Vérifier la robustesse des mots de passe avec le module pam_pwquality	CRITICAL	Accélération du piratage du mot de passe	Ralentir le piratage du mot de passe	1

SYS.7	mdp_pam_old: Vérifier que les comptes utilisateurs qui peuvent se connecter ont pour obligation de changer leur mot de passe régulièrement	CRITICAL	Accélération du piratage du mot de passe	Ralentir le piratage du mot de passe	1
SYS.8	stuid_setgid_stickybit: Examiner la liste des fichiers avec les droits spéciaux setuid , setgid et sticky bit	CRITICAL	Élévation des privilèges. Pour certaines commandes	Il faut les connaître pour les maîtrisée	1
SYS.9	admin_group: Vérifier la présence d'un groupe d'utilisateurs identifié comme administrateur de la machine	CRITICAL	Utilisation du compte root impossible de tracer les actions	Tracer toutes action administrateur et gérer les action qui nécessite une élévation	1
SYS.10	controle_package: Vérifier que les packages installés sur le système sont signés, sûrs et à jours	CRITICAL	Paquet corrompu	Être sur des paquets qu’on install	1
SYS.11	swap :	Warning	Dysfonction	Soulager la ram en	2

	Vérifier la présence d'un minimum de mémoire SWAP sur le système		nement de la machine	cas de surcharge	

3) Audit de services

N°	Recommandation	Type	Risque	Bénéfice	Priorité
SER.1	service_up: Vérifier le durcissement de la configuration des services lancés	CRITICAL	Facilite les attaques depuis l'extérieur	Ralenti les attaquesdepuis l'extérieur	1
SER.2	account_service: Vérifier les comptes système associés aux services	CRITICAL	Prise de contrôle du service et action non désiré sur le poste	Limitation des risque	1
SER.3	file_right: Vérifier les droits du système de fichiers associé aux comptes système exécutant des services	CRITICAL	Prise de contrôle du poste et action non désiré sur le poste	Limitation des risque	1
SER.4	log: Vérifier la présence des principaux fichiers de trace	CRITICAL	Récupération d'information importante via les log.	Analyse des log pour déboguer les pb,	1

	du système et leur droit d'accès. Ne pas oublier les faire une sauvegarde externe des log				
SER.5	cloisonnement: Vérifier qu'il est possible de virtualiser l'architecture applicative du serveur	Warning	Si le cloisonnement est mal fait un intrus peux prendre la main plus facilement	Ralentit le risque d’intrusion	3

4) Audit réseau et port

N°	Recommandation	Type	Risque	Bénéfice	Priorité
NET.1	open_port_V0: Examiner la liste des sockets et ports ouverts sur le réseau	CRITICAL	Potentiel risque inutiles	Ralentit le risque d’intrusion	1
NET.2	open_port_v1: Vérifier que les services qui ouvrant des ports sur une interface externe sont pertinents	CRITICAL	Potentiel risque inutiles	Ralentit le risque d’intrusion	1
NET.3	unused_port: Vérifier que les services qui ouvrent	CRITICAL	Potentiel risque inutiles	Ralentit le risque d’intrusion	1

	des ports inutiles sont désactivés				
NET.4	used_port: Vérifier que les ports par défaut des services ont été changés dans la mesure du possible	CRITICAL	Potentiel risque inutiles	Ralentit le risque d'intrusion	1
NET.5	firewall_V0: Vérifier que les règles Netfilter sont bien positionnées	CRITICAL	Potentiel risque inutiles	Ralentit le risque d'intrusion	1
NET.6	firewall_V1: Vérifier que les règles Netfilter par défaut sont définies dans le fichier de configuration	CRITICAL	Au redémarrage du serveur, les règles disparaîtrons	Permet de réinjecter les règles	1
NET.7	ssh_V0: Vérifier la présence et la version du protocole SSH supporté par le service exploité sur le serveur	CRITICAL	Impossible d'administrer le poste à distance ou incompatibilité de version.	Gestion à distance.	1
NET.8	ssh_V1: Examiner la directive PermitRootLogin du service	CRITICAL	Connexion en tant que root sur un terminal. On ne saura pas qui a fait quoi	Identifier chaque action nécessitant une élévation de droits	1
NET.9	ssh_V2:	CRITICAL	Prise de	Sécurisation du	1

	Vérifier le port d'écoute du service SSH		contrôle de la machine via le port par défaut	port	
NET.10	ssh_V3: Vérifier le durcissement avancé du service SSH (tentative de con Max 3, MAx session 2, changer le port,désactiver la redirection)	CRITICAL	Risque potentiel de prise de contrôle par un intrus	Ralentir les potentiel intrusions	1

Lynis security scan details:

```
Hardening index : 60 [############        ]
Tests performed : 263
Plugins enabled : 0
```

Les recommandations pour sécuriser un serveur Web de l'anssi

Ordre de priorité :

- 1 : A faire tout de suite
- 2 : A faire dès que possible
- 3 : A faire

Auditeur : Ibine ABDALLAH
Date de l'audit : 28/08/2020
Date de rédaction du rapport : 30/08/2020

RAPPORT D'AUDIT

Audit de sécurité du serveur WEB

Destinataires :

Sun Ken : Directeur des Systèmes d'Information
Jean Pierre : Directeur Marketing

Commanditaire :

Sun Ken : Directeur des Systèmes d'Information

Contexte :

Cet audit concerne le serveur hébergé à distance chez **Atex** fournissant le site web de l'entreprise.

Ibine ABDALLAH a effectué cet audit depuis les locaux de l'entreprise, avec une prise en main sur le serveur via SSH avec le compte bigboss. Il s'est connecter sur le serveur en question puis il a installé Lynis afin de pouvoir lancé l'audit de l'OS.

L'objectif de l'audit est double :

- Préconniser les actions de sécurisation en contexte opérationnel sans impact sur le service ;
- Préconniser les actions de sécurisation dans l'optique de rapatrier le serveur sur le réseau de l'entreprise.

Résultats :

Nombre de recommandations TOTAL : 36
Nombre de recommandations CRITICAL : 34
Nombre de recommandations WARNING : 2

Conclusion :

L'audit du serveur WEB a démontré que le système hébergé sur ce serveur est **non conforme à la politique de l'entreprise**. Ainsi, les conclusions de cet audit recommandent des **actions de sécurisation indispensables et immédiates sur le serveur**. La plupart peuvent être effectuées sans incidence sur le service rendu.

Dans une optique de rapatriement du serveur et du service sur le réseau de l'entreprise, il est **fortement recommandé d'effectuer une nouvelle installation**, avec les pré-requis et les reflexions de sécurité pensés au préalable à la configuration des services de l'application.