

SECURITE DES SI - Projet

1.Préparer une VM Linux et faites un travail de durcissement en inscrivant dans le rapport le détail de votre travail.

J'ai commencé par choisir Ubuntu Server en version légère comme système d'exploitation pour ma machine virtuelle, visant à sécuriser et à optimiser les performances. Pour faciliter la gestion des fichiers de configuration, j'ai installé Nano, un éditeur de texte en ligne de commande simple et efficace. Conscient de l'importance de la sécurité, j'ai décidé d'ajouter Lynis à mon arsenal, un outil d'audit de sécurité reconnu pour son efficacité dans l'identification des vulnérabilités et des conseils pour renforcer la sécurité de mon système. J'ai également installé Git, un outil essentiel pour le versionnage de code, qui me permet de télécharger et de gérer facilement des scripts de sécurité ou des applications depuis des dépôts en ligne. Pour m'assurer que ma VM reste sécurisée et à jour, j'ai exécuté les

commandes `sudo apt update` et `sudo apt upgrade`, actualisant ainsi les packages et appliquant les derniers correctifs de sécurité disponibles. Mon serveur Linux est maintenant en fonctionnement, équipé des outils nécessaires pour un durcissement efficace et prêt pour des configurations de sécurité plus spécifiques selon mes besoins.

J'ai donc effectuer le premiers scan Lynis en vue du durcissement:

```
root@your:/home/Linux/Lynis# ./Lynis audit system

[ Lynis 3.0.9 ]

#####
Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
welcome to redistribute it under the terms of the GNU General Public License.
See the LICENSE file for details about using this software.

2007-2021, CISofy - https://cisofy.com/lynis/
Enterprise support available (compliance, plugins, interface and tools)
#####

[+] Initializing program
-----
- Detecting OS... [ DONE ]
- Checking profiles... [ DONE ]

-----
Program version: 3.0.9
Operating system: Linux
Operating system name: Ubuntu
Operating system version: 23.10
Kernel version: 6.5.0
Hardware platform: x86_64
Hostname: your
-----
Profiles: /etc/lynis/default.prf
Log file: /var/log/lynis.log
Report file: /var/log/lynis-report.dat
Report version: 1.0
Plugin directory: /etc/lynis/plugins
-----
Auditor: [Not Specified]
Language: en
Test category: all
Test group: all
-----
- Program update status... [ NO UPDATE ]

[+] System tools
-----
- Scanning available tools...
- Checking system binaries...

[+] Plugins (phase 1)
-----
Note: plugins have more extensive tests and may take several minutes to complete

- Plugin: pam
  [...]
- Plugin: systemd
  [.....]
```

Premiere partie rien à signaler, je passe sur les boot and services :

```
[+] Boot and services
-----
- Service Manager [ systemd ]
- Checking UEFI boot [ DISABLED ]
- Checking presence GRUB2 [ FOUND ]
  - Checking for password protection [ NONE ]
- Check running services (systemctl) [ DONE ]
  Result: found 15 running services
- Check enabled services at boot (systemctl) [ DONE ]
  Result: found 32 enabled services
- Check startup files (permissions) [ OK ]
- Running 'systemd-analyze security'
  - auditd.service: [ EXPOSED ]
  - cron.service: [ UNSAFE ]
  - dbus.service: [ UNSAFE ]
  - dm-event.service: [ UNSAFE ]
  - emergency.service: [ UNSAFE ]
  - getty@tty1.service: [ UNSAFE ]
  - iscsid.service: [ UNSAFE ]
  - lvm2-lvmpolld.service: [ UNSAFE ]
  - multipathd.service: [ UNSAFE ]
  - networkd-dispatcher.service: [ UNSAFE ]
  - postfix@-.service: [ UNSAFE ]
  - rc-local.service: [ UNSAFE ]
  - rescue.service: [ UNSAFE ]
  - ssh.service: [ UNSAFE ]
  - systemd-ask-password-console.service: [ UNSAFE ]
  - systemd-ask-password-wall.service: [ UNSAFE ]
  - systemd-fsckd.service: [ UNSAFE ]
  - systemd-initctl.service: [ UNSAFE ]
  - systemd-journald.service: [ PROTECTED ]
  - systemd-logind.service: [ PROTECTED ]
  - systemd-networkd.service: [ PROTECTED ]
  - systemd-resolved.service: [ PROTECTED ]
  - systemd-rfkill.service: [ UNSAFE ]
  - systemd-timesyncd.service: [ PROTECTED ]
  - systemd-udev.service: [ MEDIUM ]
  - unattended-upgrades.service: [ UNSAFE ]
  - user@1000.service: [ UNSAFE ]
```

Les services suivant sont considérer comme sécurisé :

- polkit.service: - systemd-journald.service: - systemd-logind.service: systemd-networkd.service:
systemd-resolved.service: - systemd-udev.service:

Les services dans le tableau ci dessous devront etre sécurisé

SERVICE	Utilité	CORRECTIF
cloud-init-hotplugd.service	Un ensemble de scripts qui s'exécutent lors du démarrage d'une machine virtuelle dans un environnement cloud pour initialiser le système	

dbus.service	Intercommunication systèmes. Permet aux applications de communiquer entre elles.	limiter les accès autorisés et surveillez les activités suspectes.
dm-event.service:	Surveillance LVM. Écoute les événements des volumes logiques pour gérer les changements dynamiquement.	Sécurisez-le en restreignant l'accès physique au serveur et en chiffrant les données stockées.
emergency.service:	Mode urgence. Fournit un shell minimal pour la récupération système.	Pour le sécuriser, utilisez des mots de passe forts pour les comptes administratifs et désactivez le démarrage automatique.
getty@tty1.service:	Connexion console. Gère les sessions de connexion sur les terminaux.	Sécurisez-le en limitant les accès au terminal physique et en utilisant l'authentification à deux facteurs.
iscsid.service:	<p>Ce service est le démon du Initiator iSCSI, qui permet à votre serveur de se connecter à des cibles iSCSI pour l'utilisation de stockage réseau. iSCSI est largement utilisé dans les environnements d'entreprise pour connecter des serveurs à des baies de stockage réseau via le protocole IP standard.</p> <p>Sécurisation/Désactivation : Si vous n'utilisez pas de stockage iSCSI, désactiver ce service réduit la surface d'attaque potentieller</p>	
lvm2-lvmpolld.service:	Ce service est utilisé par LVM (Logical Volume Manager) pour surveiller et gérer les actions asynchrones sur les volumes logiques, comme les migrations de données ou les redimensionnements de volume.	

multipathd.service:	Gestion multipath. Gère les chemins multiples pour les périphériques de stockage pour améliorer la redondance et la performance.	Doit s'assurer que seuls les chemins valides et sécurisés sont utilisés, et surveillez régulièrement les configurations.
networkd-dispatcher.service:	networkd-dispatcher permet d'exécuter des scripts basés sur des événements réseau pour des configurations dynamiques, en travaillant avec systemd-networkd.	
- packagekit.service:	PackageKit est une couche d'abstraction qui permet aux utilisateurs d'interagir avec les logiciels et les systèmes de gestion de paquets de manière unifiée, sans se soucier des détails spécifiques à chaque système de paquets	<pre>linux@linux:~\$ sudo systemctl status packagekit (sudo) password for linux: packagekit.service - PackageKit Daemon Loaded: loaded (/lib/systemd/system/packagekit.service; static) Active: inactive (dead) linux@linux:~\$</pre> <p>Inactif de base</p> <p><u><code>sudo systemctl stop packagekit.service</code></u></p> <p><u><code>sudo systemctl disable packagekit.service</code></u></p> <p><u><code>sudo apt purge packagekit</code></u></p>
plymouth-start.service:	<p>Plymouth fournit une interface graphique pendant le processus de démarrage du système, affichant un écran de démarrage animé. Il gère également le dialogue de cryptage des disques (par exemple, la saisie de mots de passe pour les disques chiffrés).</p> <p>Importance sur Ubuntu Server : Sur la plupart des serveurs, surtout ceux sans interface graphique ou ceux qui ne nécessitent pas d'interaction utilisateur pendant le démarrage, Plymouth n'est pas nécessaire. Son utilité est principalement esthétique ou concerne l'interaction utilisateur lors du <code>sudo systemctl disable plymouth-start.service</code></p>	<p><code>sudo systemctl disable plymouth-start.service</code></p> <p><code>dpkg -l grep plymouth</code></p> <p><code>sudo apt-get purge \$(dpkg -l grep plymouth awk '{print \$2}')</code></p> <p><code>sudo apt-get autoremove</code> <code>apt-cache rdepends plymouth</code></p> <p><code>sudo update-grub</code> (pour vérifier si le démarrage est ok)</p>

rc-local.service:	Scripts personnalisés. Exécute des scripts personnalisés au démarrage du système.	
rescue.service:	Mode secours. Fournit un environnement minimal pour la réparation du système.	Protéger l'accès au mode de secours avec des mots de passe solides
snapd.aa-prompt-listener.service:	Très connu comme manager de Packets	Faire la commande " <u>snap list</u> " No snaps are installed yet. Pour vérifier les dépendances. Ici aucun, donc je fait la commande <u>sudo apt-get remove --purge snapd</u>
snapd.service:	DONE	Supression du manager de packet Snap car inutile
ssh.service:	Accès sécurisé en ssh	Utilisez des clés SSH plutôt que des mots de passe, désactivez l'accès root et limitez les adresses IP autorisées.
systemd-ask-password-console.service	Gestion des mots de passe	S'assurez-vous que seuls les utilisateurs autorisés peuvent répondre à ces invites et utiliser l'utilisation de l'authentification à deux facteurs.
systemd-ask-password-plymouth.service	Gestion des mots de passe	S'assurez-vous que seuls les utilisateurs autorisés peuvent répondre à ces invites et utiliser l'utilisation de l'authentification à deux facteurs.
systemd-ask-password-wall.service	Gestion des mots de passe	S'assurez-vous que seuls les utilisateurs autorisés peuvent répondre à ces invites et utiliser l'utilisation de l'authentification à deux facteurs.
systemd-fsckd.service	est utilisé pour fournir un démon de retour d'information pour fsck, l'utilitaire de vérification du système de fichiers. Lors du démarrage, si des vérifications du système de fichiers sont nécessaires,	

	<p>systemd-fsckd affiche des progrès et des messages pour informer l'utilisateur.</p> <p>Comme pour systemd-initctl.service, désactiver systemd-fsckd.service n'est généralement pas recommandé car il joue un rôle important dans le processus de démarrage, surtout si des vérifications du système de fichiers sont nécessaires après un arrêt incorrect ou si le système de fichiers est marqué comme "sale".</p>	
systemd-initctl.service	<p>Le service systemd-initctl.service est un service systemd qui fournit une compatibilité avec les systèmes SysVinit en redirigeant les appels à /dev/initctl vers systemd. Ce service permet à systemd de traiter les requêtes de contrôle du système qui étaient traditionnellement gérées par SysVinit.</p> <p>Sécuriser systemd-initctl.service ou tout autre service systemd consiste généralement à s'assurer que le service est correctement configuré, ne s'exécute pas avec des privilèges inutilement élevés, et est exposé le moins possible. Voici quelques recommandations générales pour sécuriser les services systemd :</p>	sudo systemctl disable systemd-initctl.service
systemd-rfkill.service	Permet aux utilisateurs de conserver leurs préférences en matière d'activation/désactivation du Wi-Fi et du Bluetooth entre les redémarrages.	
thermald.service	Regule la température. Dans le cas d'une VM, le principe de minimisation s'applique	<p><u>sudo systemctl stop thermald</u></p> <p><u>sudo systemctl disable thermald</u></p> <p><u>sudo apt-get remove --purge thermald</u></p>

unattended-upgrades.service	Mises à jour automatiques. Installe automatiquement les mises à jour de sécurité.	A configurer pour appliquer uniquement les mises à jour de sécurité fiables et surveiller les journaux pour toute installation échouée.
user@1000.service	Gestion de session utilisateur. Gère les processus et services lancés par l'utilisateur avec l'ID 1000.	
Apport	Un système qui collecte automatiquement des données sur les plantages des logiciels et les erreurs sur les systèmes basés sur Ubuntu et peut les envoyer à Ubuntu pour analyse. (Y compris les données sensibles)	Pas présent sur le système, sinon sudo systemctl disable apport.service

A la suite de ceci,

```
[+] Boot and services
-----
- Service Manager [ systemd ]
- Checking UEFI boot [ DISABLED ]
- Checking presence GRUB2 [ FOUND ]
- Checking for password protection [ NONE ]
- Check running services (systemctl) [ DONE ]
  Result: found 14 running services
- Check enabled services at boot (systemctl) [ DONE ]
  Result: found 30 enabled services
- Check startup files (permissions) [ OK ]
- Running 'systemd-analyze security'
  - apache2.service: [ UNSAFE ]
  - dbus.service: [ UNSAFE ]
  - dm-event.service: [ UNSAFE ]
  - emergency.service: [ UNSAFE ]
  - getty@tty1.service: [ UNSAFE ]
  - iscsid.service: [ UNSAFE ]
  - lvm2-lvmpolld.service: [ UNSAFE ]
  - multipathd.service: [ UNSAFE ]
  - networkd-dispatcher.service: [ UNSAFE ]
  - postfix@-.service: [ UNSAFE ]
  - rc-local.service: [ UNSAFE ]
  - rescue.service: [ UNSAFE ]
  - ssh.service: [ UNSAFE ]
  - systemd-ask-password-console.service: [ UNSAFE ]
  - systemd-ask-password-wall.service: [ UNSAFE ]
  - systemd-fsckd.service: [ UNSAFE ]
  - systemd-initctl.service: [ UNSAFE ]
  - systemd-journald.service: [ PROTECTED ]
  - systemd-logind.service: [ PROTECTED ]
  - systemd-networkd.service: [ PROTECTED ]
  - systemd-resolved.service: [ PROTECTED ]
  - systemd-rfkill.service: [ UNSAFE ]
  - systemd-timesyncd.service: [ PROTECTED ]
  - systemd-udev.service: [ MEDIUM ]
  - unattended-upgrades.service: [ UNSAFE ]
  - user@1000.service: [ UNSAFE ]
```

J'ai considérablement réduit la surface d'attaque

Pour améliorer la sécurité de ma configuration cloud sur le serveur, j'ai pris des mesures spécifiques pour restreindre l'accès au fichier cloud.cfg.

Tout d'abord, j'ai modifié les permissions du fichier en utilisant la commande `sudo chmod 640 /etc/cloud/cloud.cfg`. Cela signifie que désormais, seuls le propriétaire a le droit de lire et de modifier le fichier, tandis que les membres du groupe ne peuvent que le lire, et les autres utilisateurs ne disposent d'aucun droit d'accès.

Ensuite, pour m'assurer que seul l'utilisateur root et le groupe root ont le contrôle sur le fichier, j'ai exécuté la commande `sudo chown root:root /etc/cloud/cloud.cfg`. Cette étape est essentielle car elle garantit que les permissions accordées ne permettent pas aux utilisateurs non autorisés de lire ou de modifier ce fichier de configuration sensible.

```

GNU nano 6.2 /etc/cloud/cloud.cfg
# The top level settings are used as module
# and base configuration.

# A set of users which may be applied and/or used by various modules
# when a 'default' entry is found it will reference the 'default_user'
# from the distro configuration specified below
users:
- default

# If this is set, 'root' will not be able to ssh in and they
# will get a message to login instead as the default $user
disable_root: true

# This will cause the set+update hostname module to not operate (if true)
preserve_hostname: false

# If you use datasource_list array, keep array items in a single line.
# If you use multi line array, ds-identify script won't read array items.
# Example datasource config
# datasource:
#   EC2:
#     metadata_urls: [ 'blah.com' ]
#     timeout: 5 # (defaults to 50 seconds)
#     max_wait: 10 # (defaults to 120 seconds)

# The modules that run in the 'init' stage
cloud_init_modules:
- migrator
- seed_random
- bootcmd
- write_files
- growpart
- resizefs
- disk_setup
- mounts
- set_hostname
- update_hostname
- update_etc_hosts
- ca_certs
- rsyslog
- users_groups
- ssh

# The modules that run in the 'config' stage
cloud_config_modules:
- wireguard
- snap
- ubuntu_autoinstall
- ssh_import_id
- keyboard
- locale
- set_passwords
- grub_dpkg
- apt_pipelining
- apt_configure
- ubuntu_advantage
- ntp
- timezone
- disable_ec2_metadata
- runcmd
- byobu

# The modules that run in the 'final' stage
cloud_final_modules:
- package_update_upgrade_install
- fan
- landscape
- lxd
- ubuntu_drivers
- write_files_deferred
- puppet
- chef
- ansible
- mcollective
- salt_minion
- reset_rmc
- rightscale_userdata
- scripts_vendor

```

J'ai également procédé à l'initialisation de cloud-init en mode local avec la commande `sudo cloud-init -d init --local`, ce qui permet de valider les configurations sans dépendre de ressources externes.

En conclusion, après avoir examiné les configurations de cloud-init et du service `cloud-init-hotplugd.service`, je me suis assuré qu'ils sont correctement sécurisés et à jour. J'ai également pris en compte la possibilité de consulter la documentation de cloud-init ou de contacter le support technique de mon fournisseur de services cloud

pour obtenir des conseils supplémentaires sur la sécurisation de ces services. Si la fonctionnalité de branchement à chaud n'est pas nécessaire pour mes opérations, je pourrais envisager de désactiver ce service pour réduire encore plus les risques.

```
sudo chmod 640 /etc/cloud/cloud.cfg
sudo chown root:root /etc/cloud/cloud.cfg
```

Sécurisation du Service ssh

Pour sécuriser la configuration SSH, je désactive l'authentification basée sur l'hôte et les mots de passe vides, je limite l'utilisation des fichiers rhosts, je bloque l'authentification par mot de passe au profit des clés SSH, je désactive le transfert X11 et je m'assure que les configurations de PAM et de bannières sont correctes et sécurisées. Enfin, je redémarre le service SSH pour appliquer les modifications.

SSH :

- Commande :

```
- sudo sed -i 's/^#AllowTcpForwarding yes/AllowTcpForwarding no/'
/etc/ssh/sshd_config
- sudo sed -i 's/^#ClientAliveCountMax 3/ClientAliveCountMax 2/'
/etc/ssh/sshd_config
- sudo sed -i 's/^#LogLevel INFO/LogLevel VERBOSE/' /etc/ssh/sshd_config
- sudo sed -i 's/^#MaxAuthTries 6/MaxAuthTries 3/' /etc/ssh/sshd_config
- sudo sed -i 's/^#MaxSessions 10/MaxSessions 2/' /etc/ssh/sshd_config
- sudo sed -i 's/^#Port 22/Port 2222/' /etc/ssh/sshd_config
- sudo sed -i 's/^#TCPKeepAlive yes/TCPKeepAlive no/' /etc/ssh/sshd_config
- sudo sed -i 's/^#AllowAgentForwarding yes/AllowAgentForwarding no/'
/etc/ssh/sshd_config
```

- sudo systemctl restart sshd

- Service : SSH (Secure Shell).

- Vulnérabilité : Configurations SSH par défaut ou laxistes.

- Attaque protégée : Protège contre les accès non autorisés, les redirections de ports malveillantes et autres exploits liés à SSH.

```

# This is the sshd server system-wide configuration file. See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.

include /etc/ssh/sshd_config.d/*.conf

# Port and ListenAddress options are not used when sshd is socket-activated,
# which is now the default in Ubuntu. See sshd_config(5) and
# /usr/share/doc/openssh-server/README.Debian.gz for details.
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
#HostbasedAuthentication no
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication no
#PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
#KbdInteractiveAuthentication no

# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
#KerberosGetAFSToken no

# GSSAPI options
#GSSAPIAuthentication no
#GSSAPICleanupCredentials yes
#GSSAPIStrictAcceptorCheck yes

```

1.2. Kernel Hardening

J'ai identifié que la configuration par défaut de umask dans /etc/login.defs pourrait être rendue plus stricte, en utilisant par exemple une valeur de 027. Cette modification vise à renforcer la sécurité en restreignant les permissions par défaut pour les nouveaux fichiers et répertoires créés par les utilisateurs, limitant ainsi l'accès des autres utilisateurs aux fichiers personnels. Pour plus d'informations, je me suis référé à la documentation de Lynis disponible sur CISOfy.

Ensuite, pour minimiser les risques liés aux services inutiles, j'ai pris la décision de masquer systemd-rfkill.service et systemd-rfkill.socket en utilisant les commandes `sudo systemctl mask systemd-rfkill.service` et `sudo systemctl mask systemd-rfkill.socket`. Cette action empêche leur démarrage automatique, ce qui réduit la surface d'attaque potentielle du système.

Enfin, je suis conscient que pour appliquer toute modification au noyau Linux, il est nécessaire d'exécuter la commande `sudo sysctl -p`. Cette étape est cruciale pour activer immédiatement les changements de configuration sans avoir à redémarrer le système, assurant ainsi que les ajustements de sécurité prennent effet immédiatement. ces invites et utiliser l'utilisation de l'authentification à deux facteurs.

Rappel : pour appliquer tout modification au kernal, executer la commande `sudo sysctl -p`

```
[+] Kernel Hardening
-----
- Comparing sysctl key pairs with scan profile
- dev.tty.ldisc_autoload (exp: 0) [ DIFFERENT ]
- fs.protected_fifos (exp: 2) [ DIFFERENT ]
- fs.protected_hardlinks (exp: 1) [ OK ]
- fs.protected_regular (exp: 2) [ OK ]
- fs.protected_symlinks (exp: 1) [ OK ]
- fs.suid_dumpable (exp: 0) [ DIFFERENT ]
- kernel.core_uses_pid (exp: 1) [ DIFFERENT ]
- kernel.ctrl-alt-del (exp: 0) [ OK ]
- kernel.dmesg_restrict (exp: 1) [ OK ]
- kernel.kptr_restrict (exp: 2) [ DIFFERENT ]
- kernel.modules_disabled (exp: 1) [ DIFFERENT ]
- kernel.perf_event_paranoid (exp: 3) [ DIFFERENT ]
- kernel.randomize_va_space (exp: 2) [ OK ]
- kernel.sysrq (exp: 0) [ DIFFERENT ]
- kernel.unprivileged_bpf_disabled (exp: 1) [ DIFFERENT ]
- kernel.yama.ptrace_scope (exp: 1 2 3) [ OK ]
- net.core.bpf_jit_harden (exp: 2) [ DIFFERENT ]
- net.ipv4.conf.all.accept_redirects (exp: 0) [ DIFFERENT ]
- net.ipv4.conf.all.accept_source_route (exp: 0) [ OK ]
- net.ipv4.conf.all.bootp_relay (exp: 0) [ OK ]
- net.ipv4.conf.all.forwarding (exp: 0) [ OK ]
- net.ipv4.conf.all.log_martians (exp: 1) [ DIFFERENT ]
- net.ipv4.conf.all.mc_forwarding (exp: 0) [ OK ]
- net.ipv4.conf.all.proxy_arp (exp: 0) [ OK ]
- net.ipv4.conf.all.rp_filter (exp: 1) [ DIFFERENT ]
- net.ipv4.conf.all.send_redirects (exp: 0) [ DIFFERENT ]
- net.ipv4.conf.default.accept_redirects (exp: 0) [ DIFFERENT ]
- net.ipv4.conf.default.accept_source_route (exp: 0) [ DIFFERENT ]
- net.ipv4.conf.default.log_martians (exp: 1) [ DIFFERENT ]
- net.ipv4.icmp_echo_ignore_broadcasts (exp: 1) [ OK ]
- net.ipv4.icmp_ignore_bogus_error_responses (exp: 1) [ OK ]
- net.ipv4.tcp_syncookies (exp: 1) [ OK ]
- net.ipv4.tcp_timestamps (exp: 0 1) [ OK ]
- net.ipv6.conf.all.accept_redirects (exp: 0) [ DIFFERENT ]
- net.ipv6.conf.all.accept_source_route (exp: 0) [ OK ]
- net.ipv6.conf.default.accept_redirects (exp: 0) [ DIFFERENT ]
- net.ipv6.conf.default.accept_source_route (exp: 0) [ OK ]

[+] Hardening
-----
- Installed compiler(s) [ NOT FOUND ]
- Installed malware scanner [ NOT FOUND ]
- Non-native binary formats [ FOUND ]
```

Pour garantir la conformité de ma configuration système aux recommandations de sécurité, j'ai entrepris deux étapes importantes :

Première étape : J'ai supprimé le fichier `/etc/sysctl.conf`. Cette action a pour but de repartir sur une base vierge pour la configuration du noyau, me permettant ainsi d'éliminer toute directive obsolète ou non sécurisée qui pourrait y figurer.

Seconde étape : J'ai appliqué les directives spécifiques de l'ANSSI (Agence nationale de la sécurité des systèmes d'information) concernant la configuration du

noyau. L'ANSSI fournit des recommandations détaillées pour renforcer la sécurité des systèmes d'information. En suivant ces directives, je m'assure que la configuration de mon système est conforme aux standards de sécurité nationaux et internationaux, optimisant ainsi la protection contre les vulnérabilités et les attaques potentielles.

Ces étapes sont essentielles pour assurer que mon système est configuré de manière à respecter les meilleures pratiques de sécurité, conformément aux exigences de l'ANSSI et aux principes généraux de durcissement des systèmes d'information.

Les sysctl détaillées dans cet exemple sont recommandées pour un hôte de type « serveur » n'effectuant pas de routage et ayant une configuration IPv6 minimaliste. Elles sont présentées telles que rencontrées dans le fichier `/etc/sysctl.conf` :

Listing 6.1 – Paramétrage des sysctl réseau d'un « serveur »

```
# Pas de routage entre les interfaces
net.ipv4.ip_forward = 0
# Filtrage par chemin inverse
net.ipv4.conf.all.rp_filter = 1
net.ipv4.conf.default.rp_filter = 1
# Ne pas envoyer de redirections ICMP
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.default.send_redirects = 0
# Refuser les paquets de source routing
net.ipv4.conf.all.accept_source_route = 0
net.ipv4.conf.default.accept_source_route = 0
# Ne pas accepter les ICMP de type redirect
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.secure_redirects = 0
net.ipv4.conf.default.accept_redirects = 0
net.ipv4.conf.default.secure_redirects = 0
# Loguer les paquets ayant des IPs anormales
net.ipv4.conf.all.log_martians = 1
# RFC 1337
net.ipv4.tcp_rfc1337 = 1
# Ignorer les réponses non conformes à la RFC 1122
net.ipv4.icmp_ignore_bogus_error_responses = 1
# Augmenter la plage pour les ports éphémères
net.ipv4.ip_local_port_range = 32768 65535
# Utiliser les SYN cookies
net.ipv4.tcp_syncookies = 1
# Désactiver le support des "router solicitations"
net.ipv6.conf.all.router_solicitations = 0
net.ipv6.conf.default.router_solicitations = 0
# Ne pas accepter les "router preferences" par "router advertisements"
net.ipv6.conf.all.accept_ra_rtr_pref = 0
net.ipv6.conf.default.accept_ra_rtr_pref = 0
# Pas de configuration auto des prefix par "router advertisements"
net.ipv6.conf.all.accept_ra_pinfo = 0
net.ipv6.conf.default.accept_ra_pinfo = 0
# Pas d'apprentissage du routeur par défaut par "router advertisements"
net.ipv6.conf.all.accept_ra_defrtr = 0
net.ipv6.conf.default.accept_ra_defrtr = 0
# Pas de configuration auto des adresses à partir des "router advertisements"
net.ipv6.conf.all.autoconf = 0
net.ipv6.conf.default.autoconf = 0
# Ne pas accepter les ICMP de type redirect
net.ipv6.conf.all.accept_redirects = 0
net.ipv6.conf.default.accept_redirects = 0
# Refuser les paquets de source routing
net.ipv6.conf.all.accept_source_route = 0
net.ipv6.conf.default.accept_source_route = 0
# Nombre maximal d'adresses autoconfigurées par interface
net.ipv6.conf.all.max_addresses = 1
net.ipv6.conf.default.max_addresses = 1
```


Les sysctl détaillées dans cet exemple sont les sysctl système recommandées par défaut. Elles sont présentées telles que rencontrées dans le fichier `/etc/sysctl.conf` :

Listing 6.2 – Liste de sysctl recommandées

```
# Désactivation des SysReq
kernel.sysrq = 0
# Pas de core dump des exécutable setuid
fs.suid_dumpable = 0
# Interdiction de déréférencer des liens vers des fichiers dont
# l'utilisateur courant n'est pas le propriétaire
# Peut empêcher certains programmes de fonctionner correctement
fs.protected_symlinks = 1
fs.protected_hardlinks = 1
# Activation de l'ASLR
kernel.randomize_va_space = 2
# Interdiction de mapper de la mémoire dans les adresses basses (0)
vm.mmap_min_addr = 65536
# Espace de choix plus grand pour les valeurs de PID
kernel.pid_max = 65536
# Obfuscation des adresses mémoire kernel
kernel.kptr_restrict = 1
# Restriction d'accès au buffer dmesg
kernel.dmesg_restrict = 1
# Restreint l'utilisation du sous système perf
kernel.perf_event_paranoid = 2
kernel.perf_event_max_sample_rate = 1
kernel.perf_cpu_time_max_percent = 1
```

Les commandes suivantes empêchent le chargement des modules noyau après démarrage du système.

Listing 6.3 – Bloquage du chargement des modules en ligne de commande

```
# commande non sauvegardée après redémarrage
sysctl -w kernel.modules_disabled=1
```

ou par la modification du fichier `/etc/sysctl.conf` :

Listing 6.4 – Bloquage du chargement des modules via le fichier `sysctl.conf`

```
# Interdiction de chargement des modules (sauf ceux déjà chargés à
# ce point) par modification du fichier /etc/sysctl.conf
kernel.modules_disabled = 1
```

3e étape : ajuster les recommandation e Lynis

J'ai défini `kernel.core_uses_pid=1` pour associer les dumps de core à l'ID du processus, améliorant ainsi la traçabilité et la sécurité.

Pour `kernel.perf_event_paranoid`, j'ai opté pour une valeur de 3, ce qui restreint l'accès aux événements de performance aux utilisateurs ayant les privilèges nécessaires. Cela diverge légèrement de la recommandation de l'ANSSI qui suggère

une valeur de 2, mais j'ai choisi un niveau de restriction plus élevé pour maximiser la sécurité.

J'ai activé `net.ipv4.conf.default.log_martians=1` pour enregistrer les paquets suspects, ce qui aide à détecter les tentatives d'accès non autorisées ou les configurations incorrectes du réseau.

Avec `dev.tty.ldisc_autoload=0`, j'ai désactivé le chargement automatique des disciplines de ligne TTY, réduisant le risque d'exploitations basées sur des modules automatiquement chargés.

J'ai configuré `fs.protected_fifos=2` et `kernel.kptr_restrict=2` pour renforcer la protection contre les écritures non autorisées dans les FIFOs et limiter l'exposition des adresses du noyau, respectivement.

En définissant `kernel.unprivileged_bpf_disabled=1` et `net.core.bpf_jit_harden=2`, j'ai désactivé l'utilisation des filtres BPF (Berkeley Packet Filter) par les utilisateurs non privilégiés et renforcé la sécurité du compilateur JIT BPF, réduisant ainsi le risque d'exploitations malveillantes.

Suite à ces modifications, j'ai vérifié la configuration à l'aide de Lynis et d'autres outils d'audit, confirmant que mon système est désormais conforme aux recommandations de sécurité. Toutes les modifications apportées ont pour but de durcir la sécurité du système, tout en veillant à maintenir un équilibre entre sécurité et fonctionnalité. Le résultat est satisfaisant : mon système est sécurisé et prêt à faire face aux défis de sécurité actuels.

Le résultat Lynis pour le kernel en vue du hardening (Tout les services présent)

[+] Kernel Hardening

```
- Comparing sysctl key pairs with scan profile
- dev.tty.ldisc_autoload (exp: 0) [ OK ]
- fs.protected_fifos (exp: 2) [ OK ]
- fs.protected_hardlinks (exp: 1) [ OK ]
- fs.protected_regular (exp: 2) [ OK ]
- fs.protected_symlinks (exp: 1) [ OK ]
- fs.suid_dumpable (exp: 0) [ OK ]
- kernel.core_uses_pid (exp: 1) [ OK ]
- kernel.ctrl-alt-del (exp: 0) [ OK ]
- kernel.dmesg_restrict (exp: 1) [ OK ]
- kernel.kptr_restrict (exp: 2) [ OK ]
- kernel.modules_disabled (exp: 1) [ OK ]
- kernel.perf_event_paranoid (exp: 3) [ OK ]
- kernel.randomize_va_space (exp: 2) [ OK ]
- kernel.sysrq (exp: 0) [ OK ]
- kernel.unprivileged_bpf_disabled (exp: 1) [ OK ]
- kernel.yama.ptrace_scope (exp: 1 2 3) [ OK ]
- net.core.bpf_jit_harden (exp: 2) [ OK ]
- net.ipv4.conf.all.accept_redirects (exp: 0) [ OK ]
- net.ipv4.conf.all.accept_source_route (exp: 0) [ OK ]
- net.ipv4.conf.all.bootp_relay (exp: 0) [ OK ]
- net.ipv4.conf.all.forwarding (exp: 0) [ OK ]
- net.ipv4.conf.all.log_martians (exp: 1) [ OK ]
- net.ipv4.conf.all.mc_forwarding (exp: 0) [ OK ]
- net.ipv4.conf.all.proxy_arp (exp: 0) [ OK ]
- net.ipv4.conf.all.rp_filter (exp: 1) [ OK ]
- net.ipv4.conf.all.send_redirects (exp: 0) [ OK ]
- net.ipv4.conf.default.accept_redirects (exp: 0) [ OK ]
- net.ipv4.conf.default.accept_source_route (exp: 0) [ OK ]
- net.ipv4.conf.default.log_martians (exp: 1) [ OK ]
- net.ipv4.icmp_echo_ignore_broadcasts (exp: 1) [ OK ]
- net.ipv4.icmp_ignore_bogus_error_responses (exp: 1) [ OK ]
- net.ipv4.tcp_syncookies (exp: 1) [ OK ]
- net.ipv4.tcp_timestamps (exp: 0 1) [ OK ]
- net.ipv6.conf.all.accept_redirects (exp: 0) [ OK ]
- net.ipv6.conf.all.accept_source_route (exp: 0) [ OK ]
- net.ipv6.conf.default.accept_redirects (exp: 0) [ OK ]
- net.ipv6.conf.default.accept_source_route (exp: 0) [ OK ]
```

1.3 Hardening Guide Anssi

```
GNU nano 7.2 /etc/security/limits.conf *
# /etc/security/limits.conf
#
#This file sets the resource limits for the users logged in via PAM.
#It does not affect resource limits of the system services.
#
#Also note that configuration files in /etc/security/limits.d directory,
#which are read in alphabetical order, override the settings in this
#file in case the domain is the same or more specific.
#That means, for example, that setting a limit for wildcard domain here
#can be overridden with a wildcard setting in a config file in the
#subdirectory, but a user specific setting here can be overridden only
#with a user specific setting in the subdirectory.
#
#Each line describes a limit for a user in the form:
#
#<domain>          <type> <item> <value>
#
#Where:
#<domain> can be:
#
#   - a user name
#   - a group name, with @group syntax
#   - the wildcard *, for default entry
#   - the wildcard %, can be also used with %group syntax,
#       for maxlogin limit
#   - NOTE: group and wildcard limits are not applied to root.
#       To apply a limit to the root user, <domain> must be
#       the literal username root.
#
#<type> can have the two values:
#
#   - "soft" for enforcing the soft limits
#   - "hard" for enforcing hard limits
#
#<item> can be one of the following:
#
#   - core - limits the core file size (KB)
#   - data - max data size (KB)
#   - fsize - maximum filesize (KB)
#   - memlock - max locked-in-memory address space (KB)
#   - nofile - max number of open file descriptors
#   - rss - max resident set size (KB)
#   - stack - max stack size (KB)
#   - cpu - max CPU time (MIN)
#   - nproc - max number of processes
#   - as - address space limit (KB)
#   - maxlogins - max number of logins for this user
#   - maxsyslogins - max number of logins on the system
#   - priority - the priority to run user process with
#   - locks - max number of file locks the user can hold
#   - sigpending - max number of pending signals
#   - msgqueue - max memory used by POSIX message queues (bytes)
#   - nice - max nice priority allowed to raise to values: [-20, 19]
#   - rtprio - max realtime priority
#   - chroot - change root to directory (Debian-specific)
#
#<domain>          <type> <item>          <value>
#
*                   soft   core           0
#root              hard   core           100000
#*                 hard   rss            10000
#@student          hard   nproc          20
#@faculty          soft   nproc          20
#@faculty          hard   nproc          50
#ftp               hard   nproc          0
#ftp               -      chroot         /ftp
#@student          -      maxlogins      4

* soft core 0
* hard core 0

# End of file
```

Pour renforcer la surveillance de la sécurité de mon système et détecter la présence éventuelle de rootkits, j'ai décidé d'installer deux "chiens de garde" logiciels spécialisés dans la détection de ces menaces. Voici les commandes que j'ai utilisées

Installation de RKHunter (Rootkit Hunter) :

```
sudo apt-get install rkhunter
```

RKHunter est un outil qui scanne le système à la recherche de rootkits, backdoors et diverses vulnérabilités. Il utilise des tests de signatures ainsi que des vérifications de hash pour détecter les modifications suspectes.

Installation de Chkrootkit :

```
sudo apt-get install chkrootkit
```

Chkrootkit est un autre outil qui permet de chercher localement les signes de compromission du système par des rootkits. Il effectue plusieurs tests pour vérifier la présence de modifications suspectes ou de logiciels malveillants connus.

Installation de Audit D :

```
sudo apt-get install auditd
```

La commande `sudo apt-get install auditd` sert à installer le service d'audit `auditd` sur les systèmes Linux basés sur Debian ou Ubuntu. Elle permet de surveiller les activités de sécurité sur le système, essentielles pour détecter les activités suspectes et assurer la conformité réglementaire.

En installant ces trois outils, je m'assure une couche supplémentaire de surveillance pour détecter activement les menaces potentielles et les activités malveillantes sur mon système. L'utilisation régulière de ces outils, combinée à des mises à jour de sécurité et à d'autres pratiques de durcissement, contribue grandement à maintenir l'intégrité et la sécurité de mon système Linux.

J'ai passer la commande suivante :

Les commandes suivantes empêchent le chargement des modules noyau après démarrage du système.

Listing 6.3 – Bloquage du chargement des modules en ligne de commande

```
# commande non sauvegardée après redémarrage
sysctl -w kernel.modules_disabled=1
```

ou par la modification du fichier `/etc/sysctl.conf` :

Listing 6.4 – Bloquage du chargement des modules via le fichier `sysctl.conf`

```
# Interdiction de chargement des modules (sauf ceux déjà chargés à
# ce point) par modification du fichier /etc/sysctl.conf
kernel.modules_disabled = 1
```

6.3.1 Désactivation des comptes utilisateurs inutilisés



Désactivation des comptes utilisateurs inutilisés

Les comptes utilisateurs inutilisés doivent être désactivés au niveau du système.

Cette désactivation passe par l'invalidation du compte au niveau de son mot de passe (suppression du champ `pw_passwd` dans le `shadow` et shell de login à `/bin/false`).

Listing 6.5 – Désactivation de compte utilisateur

```
# Verrouillage d'un compte
usermod -L <compte>
# Désactivation de son shell de login
usermod -s /bin/false <compte>
```

`wc -l /etc/passwd | awk '{print $1}'`

consiste à compter les lignes dans le fichier `/etc/passwd`, qui contient une entrée pour chaque utilisateur du système.

```
root@linux:/home/linux# wc -l /etc/passwd | awk '{print $1}'
28
root@linux:/home/linux# getent passwd | wc -l
28
root@linux:/home/linux# getent passwd {1000..60000} | wc -l
1
root@linux:/home/linux# ^C
```

`getent passwd | wc -l`

`getent passwd {1000..60000} | wc -l`

Cette commande filtre les utilisateurs ayant des UID entre 1000 et 60000, ce qui devrait inclure la plupart des comptes "humains", et exclure les comptes système qui ont généralement des UID en dessous de 1000

Sécuriser le Répertoire /etc/sudoers.d

Les permissions recommandées pour le répertoire /etc/sudoers.d sont 755 (rwxr-xr-x) ou encore plus restrictives, comme 750 (rwxr-x---), et appartenant à l'utilisateur root et au groupe root. Ces permissions permettent au propriétaire (root) de lire, écrire et exécuter, tandis que les membres du groupe et les autres utilisateurs peuvent seulement lire et exécuter, sans pouvoir écrire. Si 750, seul root et les utilisateurs du groupe spécifié peuvent lire et exécuter, rendant le répertoire inaccessible aux autres utilisateurs.

Pour corriger les permissions et la propriété, procédez comme suit :

```
ls -ld /etc/sudoers.d
```

```
sudo chmod 750 /etc/sudoers.d
```

Le umask système doit être positionné à 0027 (par défaut, tout fichier créé n'est lisible que par l'utilisateur et son groupe, et modifiable uniquement par son propriétaire). Le umask pour les utilisateurs doit être positionné à 0077 (tout fichier créé par un utilisateur n'est lisible et modifiable que par lui).

ERASECHAR	0177
KILLCHAR	025
UMASK	027

```
#
# Password aging controls:
#
#     PASS_MAX_DAYS   Maximum number of days a password may be used.
#     PASS_MIN_DAYS   Minimum number of days allowed between password changes.
#     PASS_WARN_AGE   Number of days warning given before a password expires.
#
PASS_MAX_DAYS   90
PASS_MIN_DAYS   10
PASS_WARN_AGE   7
```

1.4 Suggestion Lynis

Sécurisation du démarrage avec GRUB :

- Commande : `echo 'set superusers="nom_utilisateur"' | sudo tee -a /etc/grub.d/40_custom && echo 'password_pbkdf2 nom_utilisateur grub.pbkdf2.sha512.hash' | sudo tee -a /etc/grub.d/40_custom`
- Service : Chargeur de démarrage GRUB.
- Vulnérabilité : Modification non autorisée des paramètres de démarrage.
- Attaque protégée : Empêche un attaquant d'altérer le démarrage pour contourner les mécanismes de sécurité.

```
GNU nano 7.2 /etc/grub.d/40_custom
#!/bin/sh
exec tail -n +3 $0
# This file provides an easy way to add custom menu entries.  Simply type the
# menu entries you want to add after this comment.  Be careful not to change
# the 'exec tail' line above.
```

Gestion des utilisateurs et authentification :

- Commande :
 - `sudo sed -i 's/^# SHA_CRYPT_MAX_ROUNDS.*/SHA_CRYPT_MAX_ROUNDS 5000/' /etc/login.defs`
 - `sudo apt-get install libpam-cracklib`
 - `sudo chage -M 90 linux`
- Service : Authentification utilisateur.
- Vulnérabilité : Mots de passe faibles ou jamais expirés.

- Attaque protégée : Renforce la sécurité des mots de passe, empêchant les attaques par force brute ou l'utilisation indéfinie de mots de passe compromis.

Bannières et avertissements :

- Commande :

- echo 'Avertissement légal' | sudo tee /etc/issue

- echo 'Avertissement légal' | sudo tee /etc/issue.net

- Service : Connexions au système.

- Vulnérabilité : Utilisateurs non informés des politiques ou des conséquences légales.

- Attaque protégée : Décourage l'accès non autorisé en informant les utilisateurs des implications légales.

```
GNU nano 7.2 /etc/issue *
Ubuntu 23.10 \n \l

Authorized access only. All activity may be monitored and reported.
echo 'Avertissement légal' | sudo tee /etc/issue
echo 'Avertissement légal' | sudo tee /etc/issue.net
```

Comptabilité :

- Commande :

- sudo apt-get install sysstat

- sudo nano /etc/audit/audit.rules

- Service : Surveillance et audit du système.

- Vulnérabilité : Manque de visibilité sur les actions système.

- Attaque protégée : Permet une analyse détaillée des événements, aidant à détecter et à enquêter sur les activités suspectes.

```

Reenter password:
grub-mkpasswd-pbkdf2: error: passwords don't match.
root@your:/home/linux/lynis# sudo nano /etc/grub.d/40_custom
root@your:/home/linux/lynis# sudo grub-mkpasswd-pbkdf2
Enter password:
Reenter password:
PBKDF2 hash of your password is grub.pbkdf2.sha512.10000.135F96E75D65040964065E2AAB3275708AE2017519F73424C714CDE3AD7570B3FBE9
8320FE9FBE0EE30705151EEB80FC3B83187B2C11C566168376FEAB4A8F1.60F46C48C943CBBECA6242A6234140A66117998F02785B2D1E58A563F365F3C293
F2D102BFF674561EF9302EAB1B299205466FCBB60AE9DC62681554FD82F7CE
root@your:/home/linux/lynis# █

```

J'ai donc obtenue une note de 82 sur Lynis

```

Follow-up:
-----
- Show details of a test (lynis show details TEST-ID)
- Check the logfile for all details (less /var/log/lynis.log)
- Read security controls texts (https://cisofy.com)
- Use --upload to upload data to central system (Lynis Enterprise users)

=====

Lynis security scan details:

Hardening index : 82 [#####]
Tests performed : 271
Plugins enabled : 2

Components:
- Firewall [V]
- Malware scanner [V]

Scan mode:
Normal [V] Forensics [ ] Integration [ ] Pentest [ ]

Lynis modules:
- Compliance status [?]
- Security audit [V]
- Vulnerability scan [V]

Files:
- Test and debug information : /var/log/lynis.log
- Report data : /var/log/lynis-report.dat

=====

Lynis 3.0.9

Auditing, system hardening, and compliance for UNIX-based systems
(Linux, macOS, BSD, and others)

2007-2021, CISofy - https://cisofy.com/lynis/
Enterprise support available (compliance, plugins, interface and tools)

=====

[TIP]: Enhance Lynis audits by adding your settings to custom.prfl (see /etc/lynis/default.prfl for all settings)

```

2. Partie TLS/SSL.

En effectuant la configuration SSL pour mon serveur Apache, j'ai rencontré quelques problèmes que j'ai réussi à résoudre. Initialement, en essayant d'activer le site par

défaut pour SSL avec la commande `a2ensite default-ssl`, j'ai reçu un message indiquant que le dossier `'sites-enabled/'` n'existait pas. J'ai donc vérifié la présence du répertoire avec `ls sites-enabled/` et j'ai confirmé son existence, ce qui signifie que la commande `a2ensite` s'est mal exécutée à cause d'une faute de frappe ou d'un problème similaire.

Installation du service apache2

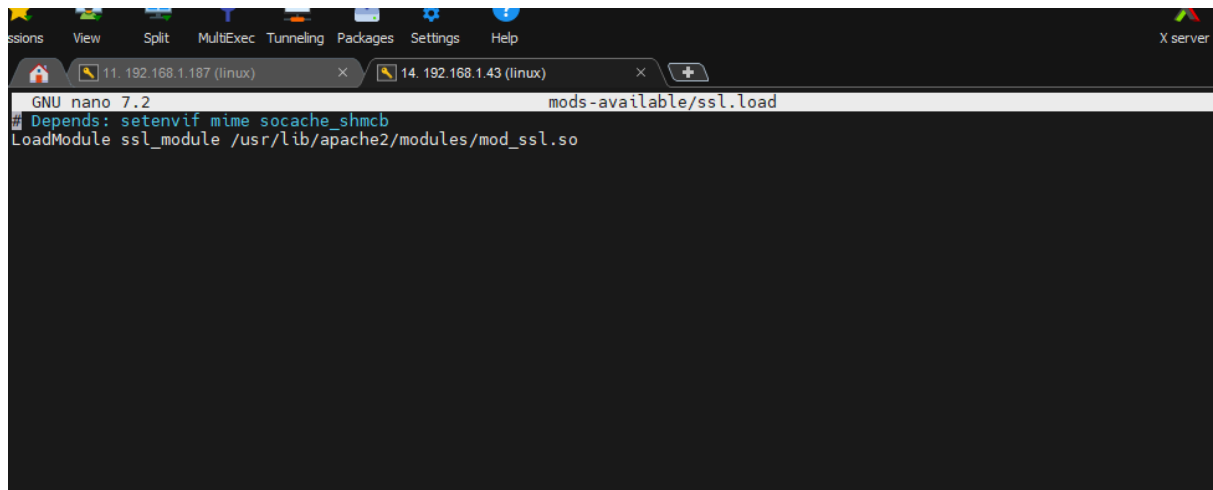
```
root@your:/home/linux# systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; preset: enabled)
   Active: active (running) since Sun 2024-02-25 18:48:10 UTC; 1min 36s ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 43904 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
  Main PID: 43909 (apache2)
    Tasks: 55 (limit: 6591)
   Memory: 7.0M
      CPU: 487ms
   CGroup: /system.slice/apache2.service
           └─43909 /usr/sbin/apache2 -k start
             └─43910 /usr/sbin/apache2 -k start
               └─43911 /usr/sbin/apache2 -k start

Feb 25 18:48:10 your systemd[1]: Starting apache2.service - The Apache HTTP Server...
Feb 25 18:48:10 your apachectl[43907]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name,
Feb 25 18:48:10 your systemd[1]: Started apache2.service - The Apache HTTP Server.
lines 1-17/17 (END)
```

Après un examen approfondi de la configuration SSL/TLS de notre serveur, nous avons mis en œuvre des mesures de renforcement conformément aux recommandations de Mozilla pour la configuration SSL. Nous avons choisi le modèle "intermédiaire" adapté à la majorité des serveurs, qui permet une excellente compatibilité tout en assurant un haut niveau de sécurité.

Nous avons désactivé les protocoles obsolètes et moins sécurisés tels que SSLv2, SSLv3, TLS 1.0 et TLS 1.1, garantissant ainsi que notre serveur n'offre que des protocoles modernes et sûrs tels que TLS 1.2 et TLS 1.3. De plus, nous avons appliqué une politique stricte de transport sécurisé HTTP (HSTS) pour forcer les connexions HTTPS, ce qui réduit le risque de downgrade attacks et d'autres vecteurs d'attaque associés aux connexions non sécurisées.

Après avoir corrigé l'erreur et activé le site SSL, j'ai rechargé la configuration d'Apache avec `systemctl reload apache2`. Pour m'assurer que le SSL fonctionnait correctement, j'ai testé l'accès à mon serveur via HTTPS en utilisant la commande `curl -I https://192...`



```
s: cannot access 'sites-enabled/': No such file or directory
oot@linux:/etc/apache2#
oot@linux:/etc/apache2# ls sites-enabled/
00-default.conf
oot@linux:/etc/apache2# a2ensite default-ssl
Enabling site default-ssl.
To activate the new configuration, you need to run:
  systemctl reload apache2
oot@linux:/etc/apache2#
```

a2ensite default-ssl pour activer la configuration par défaut SSL d'Apache.
Assurez-vous d'avoir le fichier default-ssl.conf dans le répertoire sites-available/.

```
Enabling site default-ssl.
To activate the new configuration, you need to run:
  systemctl reload apache2
root@linux:/etc/apache2# systemctl restart apache2
root@linux:/etc/apache2# curl -I https://127.0.0.1
curl: (60) SSL: no alternative certificate subject name matches target host name '127.0.0.1'
More details here: https://curl.se/docs/sslcerts.html

curl failed to verify the legitimacy of the server and therefore could not
establish a secure connection to it. To learn more about this situation and
how to fix it, please visit the web page mentioned above.
root@linux:/etc/apache2#
```

Screen du scan testssh

```

root@your:~# ./testssl.sh localhost
bash: ./testssl.sh: Is a directory
root@your:~# cd testssl.sh/
root@your:~/testssl.sh# ls
CHANGELOG.md  CREDITS.md  Dockerfile  Dockerfile.md  Readme.md  doc  openssl-iana.mapping.html  testssl.sh
CONTRIBUTING.md  Coding_Convention.md  Dockerfile.git  LICENSE  bin  etc  t  utils
root@your:~/testssl.sh# ./testssl.sh 127.0.0.1

#####
testssl.sh      3.2rc3 from https://testssl.sh/dev/
(62b5859 2024-02-09 09:56:58)

This program is free software. Distribution and
modification under GPLv2 permitted.
USAGE w/o ANY WARRANTY. USE IT AT YOUR OWN RISK!

Please file bugs @ https://testssl.sh/bugs/

#####

Using "OpenSSL 1.0.2-bad (1.0.2k-dev)" [~179 ciphers]
on your: ./bin/openssl.Linux.x86_64
(built: "Sep  1 14:03:44 2022", platform: "linux-x86_64")

Start 2024-02-19 15:46:23      -->> 127.0.0.1:443 (127.0.0.1) <<--

rDNS (127.0.0.1):      localhost.
Service detected:      HTTP

Testing protocols via sockets except NPN+ALPN_

SSLv2      not offered (OK)
SSLv3      not offered (OK)
TLS 1      not offered
TLS 1.1    not offered
TLS 1.2    offered (OK)
TLS 1.3    offered (OK): final
NPN/SPDY   not offered
ALPN/HTTP2 http/1.1 (offered)

Testing cipher categories_

NULL ciphers (no encryption)      not offered (OK)
Anonymous NULL Ciphers (no authentication)  not offered (OK)
Export ciphers (w/o ADH+NULL)      not offered (OK)
LOW: 64 Bit + DES, RC[2,4], MD5 (w/o export)  not offered (OK)
Triple DES Ciphers / IDEA          not offered
Obsoleted CBC ciphers (AES, ARIA etc.)  offered
Strong encryption (AEAD ciphers) with no FS  offered (OK)
Forward Secrecy strong encryption (AEAD ciphers)  offered (OK)

Testing server's cipher preferences_

Hexcode  Cipher Suite Name (OpenSSL)      KeyExch.  Encryption Bits      Cipher Suite Name (IANA/RFC)
-----
SSLv2
-
SSLv3
-
TLSv1
-
TLSv1.1

```

Tout est ok ici en appliquant

moz://a SSL Configuration Generator

Server Software

- ☒ Apache
- ☐ AWS ALB
- ☐ AWS ELB
- ☐ Caddy
- ☐ Coturn
- ☐ Dovecot
- ☐ Exim
- ☐ Go
- ☐ HAProxy
- ☐ Jetty
- ☐ lighttpd
- ☐ MySQL
- ☐ nginx
- ☐ Oracle HTTP
- ☐ Postfix
- ☐ PostgreSQL
- ☐ ProFTPd
- ☐ Redis
- ☐ Squid
- ☐ stunnel
- ☐ Tomcat
- ☐ Traefik

Mozilla Configuration

- ☐ Modern
Services with clients that support TLS 1.3 and don't need backward compatibility
- ☒ Intermediate
General-purpose servers with a variety of clients, recommended for almost all systems
- ☐ Old
Compatible with a number of very old clients, and should be used only as a last resort

Environment

Server Version	2.4.41
OpenSSL Version	1.1.1k

Miscellaneous

<input checked="" type="checkbox"/>	HTTP Strict Transport Security
This also redirects to HTTPS, if possible	
<input checked="" type="checkbox"/>	OCSP Stapling

apache 2.4.41, intermediate config, OpenSSL 1.1.1k

Supports Firefox 27, Android 4.4.2, Chrome 31, Edge, IE 11 on Windows 7, Java 8u31, OpenSSL 1.0.1, Opera 20, and Safari 9

```
# generated 2024-02-25, Mozilla Guideline v5.7, Apache 2.4.41, OpenSSL 1.1.1k, intermediate configuration
# https://ssl-config.mozilla.org/#server=apache&version=2.4.41&config=intermediate&openssl=1.1.1k&guideline=5.7

# this configuration requires mod_ssl, mod_socache_shmcb, mod_rewrite, and mod_headers
<VirtualHost *:80>
    RewriteEngine On
    RewriteCond %{REQUEST_URI} !^/\.well-known/acme\-\challenge/
    RewriteRule ^(.*)$ https://%{HTTP_HOST}$1 [R=301,L]
</VirtualHost>

<VirtualHost *:443>
    SSLEngine on

    # curl https://ssl-config.mozilla.org/ffdhe2048.txt >> /path/to/signed_cert_and_intermediate_certs_and_dhparams
    SSLCertificateFile /path/to/signed_cert_and_intermediate_certs_and_dhparams
    SSLCertificateKeyFile /path/to/private_key

    # enable HTTP/2, if available
    Protocols h2 http/1.1

    # HTTP Strict Transport Security (mod_headers is required) (63072000 seconds)
    Header always set Strict-Transport-Security "max-age=63072000"
</VirtualHost>

# intermediate configuration
SSLProtocol all -SSLv3 -TLSv1 -TLSv1.1
SSLCipherSuite ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:DHE-RSA-CHACHA20-POLY1305
SSLHonorCipherOrder off
SSLSessionTickets off

SSLUseStapling On
SSLStaplingCache "shmcb:logs/ssl_stapling(32768)"
```

Copy

```

TLsv1.2 (no server order, thus listed by strength)
xc030 ECDHE-RSA-AES256-GCM-SHA384 ECDH 521 AESGCM 256 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
xc028 ECDHE-RSA-AES256-SHA384 ECDH 521 AES 256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
xc014 ECDHE-RSA-AES256-SHA ECDH 521 AES 256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
x9f DHE-RSA-AES256-GCM-SHA384 DH 2048 AESGCM 256 TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
xcca8 ECDHE-RSA-CHACHA20-POLY1305 ECDH 521 ChaCha20 256 TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
xccaa DHE-RSA-CHACHA20-POLY1305 DH 2048 ChaCha20 256 TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256
xc0a3 DHE-RSA-AES256-CCM8 DH 2048 AESCCM8 256 TLS_DHE_RSA_WITH_AES_256_CCM_8
xc09f DHE-RSA-AES256-CCM DH 2048 AESCCM 256 TLS_DHE_RSA_WITH_AES_256_CCM
x6b DHE-RSA-AES256-SHA256 DH 2048 AES 256 TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
x39 DHE-RSA-AES256-SHA DH 2048 AES 256 TLS_DHE_RSA_WITH_AES_256_CBC_SHA
xc077 ECDHE-RSA-CAMELLIA256-SHA384 ECDH 521 Camellia 256 TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384
xc4 DHE-RSA-CAMELLIA256-SHA256 DH 2048 Camellia 256 TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256
x88 DHE-RSA-CAMELLIA256-SHA DH 2048 Camellia 256 TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
x9d AES256-GCM-SHA384 RSA AESGCM 256 TLS_RSA_WITH_AES_256_GCM_SHA384
xc0a1 AES256-CCM8 RSA AESCCM8 256 TLS_RSA_WITH_AES_256_CCM_8
xc09d AES256-CCM RSA AESCCM 256 TLS_RSA_WITH_AES_256_CCM
x3d AES256-SHA256 RSA AES 256 TLS_RSA_WITH_AES_256_CBC_SHA256
x35 AES256-SHA RSA AES 256 TLS_RSA_WITH_AES_256_CBC_SHA
xc0 CAMELLIA256-SHA256 RSA Camellia 256 TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256
x84 CAMELLIA256-SHA RSA Camellia 256 TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
xc051 ARIA256-GCM-SHA384 RSA ARIAGCM 256 TLS_RSA_WITH_ARIA_256_GCM_SHA384
xc053 DHE-RSA-ARIA256-GCM-SHA384 DH 2048 ARIAGCM 256 TLS_DHE_RSA_WITH_ARIA_256_GCM_SHA384
xc061 ECDHE-ARIA256-GCM-SHA384 ECDH 521 ARIAGCM 256 TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384
xc02f ECDHE-RSA-AES128-GCM-SHA256 ECDH 521 AESGCM 128 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
xc027 ECDHE-RSA-AES128-SHA256 ECDH 521 AES 128 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
xc013 ECDHE-RSA-AES128-SHA ECDH 521 AES 128 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
x9e DHE-RSA-AES128-GCM-SHA256 DH 2048 AESGCM 128 TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
xc0a2 DHE-RSA-AES128-CCM8 DH 2048 AESCCM8 128 TLS_DHE_RSA_WITH_AES_128_CCM_8
xc09e DHE-RSA-AES128-CCM DH 2048 AESCCM 128 TLS_DHE_RSA_WITH_AES_128_CCM
xc0a0 AES128-CCM8 RSA AESCCM8 128 TLS_RSA_WITH_AES_128_CCM_8
xc09c AES128-CCM RSA AESCCM 128 TLS_RSA_WITH_AES_128_CCM
x67 DHE-RSA-AES128-SHA256 DH 2048 AES 128 TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
x33 DHE-RSA-AES128-SHA DH 2048 AES 128 TLS_DHE_RSA_WITH_AES_128_CBC_SHA
xc076 ECDHE-RSA-CAMELLIA128-SHA256 ECDH 521 Camellia 128 TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256
x8e DHE-RSA-CAMELLIA128-SHA256 DH 2048 Camellia 128 TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256
x45 DHE-RSA-CAMELLIA128-SHA DH 2048 Camellia 128 TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
x9c AES128-GCM-SHA256 RSA AESGCM 128 TLS_RSA_WITH_AES_128_GCM_SHA256
x3c AES128-SHA256 RSA AES 128 TLS_RSA_WITH_AES_128_CBC_SHA256
x2f AES128-SHA RSA AES 128 TLS_RSA_WITH_AES_128_CBC_SHA
x8a CAMELLIA128-SHA256 RSA Camellia 128 TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256
x41 CAMELLIA128-SHA RSA Camellia 128 TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
xc050 ARIA128-GCM-SHA256 RSA ARIAGCM 128 TLS_RSA_WITH_ARIA_128_GCM_SHA256
xc052 DHE-RSA-ARIA128-GCM-SHA256 DH 2048 ARIAGCM 128 TLS_DHE_RSA_WITH_ARIA_128_GCM_SHA256
xc060 ECDHE-ARIA128-GCM-SHA256 ECDH 521 ARIAGCM 128 TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256

TLsv1.3 (no server order, thus listed by strength)
x1302 TLS_AES_256_GCM_SHA384 ECDH 253 AESGCM 256 TLS_AES_256_GCM_SHA384
x1303 TLS_CHACHA20_POLY1305_SHA256 ECDH 253 ChaCha20 256 TLS_CHACHA20_POLY1305_SHA256
x1301 TLS_AES_128_GCM_SHA256 ECDH 253 AESGCM 128 TLS_AES_128_GCM_SHA256

```

Has server cipher order? no (NOT ok)
(limited sense as client will pick)

Testing robust forward secrecy (FS) -- omitting Null Authentication/Encryption, 3DES, RC4

```

FS is offered (OK) TLS_AES_256_GCM_SHA384 TLS_CHACHA20_POLY1305_SHA256 ECDHE-RSA-AES256-GCM-SHA384
ECDHE-RSA-AES256-SHA384 ECDHE-RSA-AES256-SHA DHE-RSA-AES256-GCM-SHA384
ECDHE-RSA-CHACHA20-POLY1305 DHE-RSA-CHACHA20-POLY1305 DHE-RSA-AES256-CCM8 DHE-RSA-AES256-CCM
DHE-RSA-AES256-SHA256 DHE-RSA-AES256-SHA ECDHE-RSA-CAMELLIA256-SHA384
DHE-RSA-CAMELLIA256-SHA256 DHE-RSA-CAMELLIA256-SHA DHE-RSA-ARIA256-GCM-SHA384
ECDHE-ARIA256-GCM-SHA384 TLS_AES_128_GCM_SHA256 ECDHE-RSA-AES128-GCM-SHA256
ECDHE-RSA-AES128-SHA256 ECDHE-RSA-AES128-SHA DHE-RSA-AES128-GCM-SHA256 DHE-RSA-AES128-CCM8
DHE-RSA-AES128-CCM DHE-RSA-AES128-SHA256 DHE-RSA-AES128-SHA ECDHE-RSA-CAMELLIA128-SHA256
DHE-RSA-CAMELLIA128-SHA256 DHE-RSA-CAMELLIA128-SHA DHE-RSA-ARIA128-GCM-SHA256
ECDHE-ARIA128-GCM-SHA256
Elliptic curves offered: prime256v1 secp384r1 secp521r1 X25519 X448
Finite field group: ffdhe2048 ffdhe3072 ffdhe4096 ffdhe6144 ffdhe8192
TLS 1.2 sig_algs offered: RSA+SHA224 RSA+SHA256 RSA+SHA384 RSA+SHA512 RSA-PSS-RSAE+SHA256 RSA-PSS-RSAE+SHA384
RSA-PSS-RSAE+SHA512
TLS 1.3 sig_algs offered: RSA-PSS-RSAE+SHA256 RSA-PSS-RSAE+SHA384 RSA-PSS-RSAE+SHA512

```

Testing server defaults (Server Hello)

```

TLS extensions (standard) "renegotiation info/#65281" "EC point formats/#11" "supported versions/#43" "key share/#51"
"supported_groups/#10" "max fragment length/#1" "application layer protocol negotiation/#16"
"encrypt-then-mac/#22" "extended master secret/#23"
Session Ticket RFC 5077 hint no -- no lifetime advertised
SSL Session ID support yes
Session Resumption Tickets no, ID: yes
TLS clock skew Random values, no fingerprinting possible
Certificate Compression none

```


Testing server defaults (Server Hello)

```
TLS extensions (standard)    "renegotiation info/#65281" "EC point formats/#11" "supported versions/#43" "key share/#51"
                             "supported_groups/#10" "max fragment length/#1" "application layer protocol negotiation/#16"
                             "encrypt-then-mac/#22" "extended master secret/#23"
Session Ticket RFC 5077 hint no -- no lifetime advertised
SSL Session ID support       yes
Session Resumption           Tickets no, ID: yes
TLS clock skew               Random values, no fingerprinting possible
Certificate Compression      none
Client Authentication        none
Signature Algorithm           SHA256 with RSA
Server key size               RSA 2048 bits (exponent is 65537)
Server key usage              --
Server extended key usage     --
Serial                        5818F53CE39861DDB304253B50FB64F4AE6A27BE (OK: length 20)
Fingerprints                  SHA1 D481E6FE31BCDBA4927CFDE802445A532F9D09F0
                             SHA256 6C3F9F4FFDB9EF427354FF5CA183558E7EA462CA03FD3790775C53F94CF169DE

Common Name (CN)             linux
subjectAltName (SAN)         linux
Trust (hostname)              certificate does not match supplied URI
Chain of trust                NOT ok (self signed)
EV cert (experimental)       no
Certificate Validity (UTC)    3634 >= 60 days (2024-02-03 18:30 --> 2034-01-31 18:30)
                             >= 10 years is way too long
ETS/"eTLS", visibility info  not present
Certificate Revocation List   --
OCSP URI                     NOT ok -- neither CRL nor OCSP URI provided
OCSP stapling                 not offered
OCSP must staple extension    --
DNS CAA RR (experimental)    not offered
Certificate Transparency      --
Certificates provided         1
Issuer                        linux
Intermediate Bad OCSP (exp.) ok
```

Testing HTTP header response @ "/"

```
HTTP Status Code             200 OK
HTTP clock skew               0 sec from localtime
Strict Transport Security      not offered
Public Key Pinning            --
Server banner                 Apache/2.4.57 (Ubuntu)
Application banner            --
Cookie(s)                     (none issued at "/")
Security headers               --
Reverse Proxy banner          --
```

Testing vulnerabilities

```
Heartbleed (CVE-2014-0160)    not vulnerable (OK), no heartbeat extension
CCS (CVE-2014-0224)           not vulnerable (OK)
Ticketbleed (CVE-2016-9244), experimental. not vulnerable (OK), no session ticket extension
ROBOT                         not vulnerable (OK)
Secure Renegotiation (RFC 5746) supported (OK)
Secure Client-Initiated Renegotiation not vulnerable (OK)
CRIME, TLS (CVE-2012-4929)    not vulnerable (OK)
BREACH (CVE-2013-3587)        potentially NOT ok, "gzip" HTTP compression detected. - only supplied "/" tested
                             Can be ignored for static pages or if no secrets in the page
POODLE, SSL (CVE-2014-3566)   not vulnerable (OK), no SSLv3 support
TLS_FALLBACK_SCSV (RFC 7507) No fallback possible (OK), no protocol below TLS 1.2 offered
SWEET32 (CVE-2016-2183, CVE-2016-6329) not vulnerable (OK)
FREAK (CVE-2015-0204)         not vulnerable (OK)
DROWN (CVE-2016-0800, CVE-2016-0703) not vulnerable on this host and port (OK)
                             make sure you don't use this certificate elsewhere with SSLv2 enabled services, see
                             https://search.censys.io/search?resource=hosts&virtual_hosts=INCLUDE&q=6C3F9F4FFDB9
                             EF427354FF5CA183558E7EA462CA03FD3790775C53F94CF169DE
LOGJAM (CVE-2015-4000), experimental common prime with 2048 bits detected: RFC3526/Oakley Group 14 (2048 bits),
                             but no DH EXPORT ciphers
BEAST (CVE-2011-3389)         not vulnerable (OK), no SSL3 or TLS1
LUCKY13 (CVE-2013-0169), experimental potentially VULNERABLE, uses cipher block chaining (CBC) ciphers with TLS. Check patches
Winshock (CVE-2014-6321), experimental not vulnerable (OK)
```


ROBOT	not vulnerable (OK)
Secure Renegotiation (RFC 5746)	supported (OK)
Secure Client-Initiated Renegotiation	not vulnerable (OK)
CRIME, TLS (CVE-2012-4929)	not vulnerable (OK)
BREACH (CVE-2013-3587)	potentially NOT ok, "gzip" HTTP compression detected. - only supplied "/" tested
POODLE, SSL (CVE-2014-3566)	Can be ignored for static pages or if no secrets in the page
TLS_FALLBACK_SCSV (RFC 7507)	not vulnerable (OK), no SSLv3 support
SWEET32 (CVE-2016-2183, CVE-2016-6329)	No fallback possible (OK), no protocol below TLS 1.2 offered
FREAK (CVE-2015-0204)	not vulnerable (OK)
DROWN (CVE-2016-0800, CVE-2016-0703)	not vulnerable on this host and port (OK)
EF427354FF5CA183558E7EA462CA03FD3790775C53F94CF169DE	make sure you don't use this certificate elsewhere with SSLv2 enabled services, see https://search.censys.io/search?resource=hosts&virtual_hosts=INCLUDE&q=6C3F9F4FFDB9
LOGJAM (CVE-2015-4000), experimental	common prime with 2048 bits detected: RFC3526/0akley Group 14 (2048 bits), but no DH EXPORT ciphers
BEAST (CVE-2011-3389)	not vulnerable (OK), no SSL3 or TLS1
LUCKY13 (CVE-2013-0169), experimental	potentially VULNERABLE, uses cipher block chaining (CBC) ciphers with TLS. Check patches
Winshock (CVE-2014-6321), experimental	not vulnerable (OK)
RC4 (CVE-2013-2566, CVE-2015-2808)	no RC4 ciphers detected (OK)

Running client simulations (HTTP) via sockets			
Browser	Protocol	Cipher Suite Name (OpenSSL)	Forward Secrecy
Android 6.0	TLSv1.2	ECDHE-RSA-AES128-GCM-SHA256	256 bit ECDH (P-256)
Android 7.0 (native)	TLSv1.2	ECDHE-RSA-AES128-GCM-SHA256	256 bit ECDH (P-256)
Android 8.1 (native)	TLSv1.2	ECDHE-RSA-AES128-GCM-SHA256	253 bit ECDH (X25519)
Android 9.0 (native)	TLSv1.3	TLS_AES_128_GCM_SHA256	253 bit ECDH (X25519)
Android 10.0 (native)	TLSv1.3	TLS_AES_128_GCM_SHA256	253 bit ECDH (X25519)
Android 11 (native)	TLSv1.3	TLS_AES_128_GCM_SHA256	253 bit ECDH (X25519)
Android 12 (native)	TLSv1.3	TLS_AES_128_GCM_SHA256	253 bit ECDH (X25519)
Chrome 79 (Win 10)	TLSv1.3	TLS_AES_128_GCM_SHA256	253 bit ECDH (X25519)
Chrome 101 (Win 10)	TLSv1.3	TLS_AES_128_GCM_SHA256	253 bit ECDH (X25519)
Firefox 66 (Win 8.1/10)	TLSv1.3	TLS_AES_128_GCM_SHA256	253 bit ECDH (X25519)
Firefox 100 (Win 10)	TLSv1.3	TLS_AES_128_GCM_SHA256	253 bit ECDH (X25519)
IE 6 XP	No connection		
IE 8 Win 7	No connection		
IE 8 XP	No connection		
IE 11 Win 7	TLSv1.2	ECDHE-RSA-AES256-SHA384	256 bit ECDH (P-256)
IE 11 Win 8.1	TLSv1.2	ECDHE-RSA-AES256-SHA384	256 bit ECDH (P-256)
IE 11 Win Phone 8.1	TLSv1.2	AES128-SHA256	No FS
IE 11 Win 10	TLSv1.2	ECDHE-RSA-AES256-GCM-SHA384	256 bit ECDH (P-256)
Edge 15 Win 10	TLSv1.2	ECDHE-RSA-AES256-GCM-SHA384	253 bit ECDH (X25519)
Edge 101 Win 10 21H2	TLSv1.3	TLS_AES_128_GCM_SHA256	253 bit ECDH (X25519)
Safari 12.1 (iOS 12.2)	TLSv1.3	TLS_CHACHA20_POLY1305_SHA256	253 bit ECDH (X25519)
Safari 13.0 (macOS 10.14.6)	TLSv1.3	TLS_CHACHA20_POLY1305_SHA256	253 bit ECDH (X25519)
Safari 15.4 (macOS 12.3.1)	TLSv1.3	TLS_AES_128_GCM_SHA256	253 bit ECDH (X25519)
Java 7u25	No connection		
Java 8u161	TLSv1.2	ECDHE-RSA-AES256-SHA384	256 bit ECDH (P-256)
Java 11.0.2 (OpenJDK)	TLSv1.3	TLS_AES_128_GCM_SHA256	256 bit ECDH (P-256)
Java 17.0.3 (OpenJDK)	TLSv1.3	TLS_AES_256_GCM_SHA384	253 bit ECDH (X25519)
go 1.17.8	TLSv1.3	TLS_AES_128_GCM_SHA256	253 bit ECDH (X25519)
LibreSSL 2.8.3 (Apple)	TLSv1.2	ECDHE-RSA-CHACHA20-POLY1305	253 bit ECDH (X25519)
OpenSSL 1.0.2e	TLSv1.2	ECDHE-RSA-AES256-GCM-SHA384	256 bit ECDH (P-256)
OpenSSL 1.1.0l (Debian)	TLSv1.2	ECDHE-RSA-AES256-GCM-SHA384	253 bit ECDH (X25519)
OpenSSL 1.1.1d (Debian)	TLSv1.3	TLS_AES_256_GCM_SHA384	253 bit ECDH (X25519)
OpenSSL 3.0.3 (git)	TLSv1.3	TLS_AES_256_GCM_SHA384	253 bit ECDH (X25519)
Apple Mail (16.0)	TLSv1.2	ECDHE-RSA-AES256-GCM-SHA384	256 bit ECDH (P-256)
Thunderbird (91.9)	TLSv1.3	TLS_AES_128_GCM_SHA256	253 bit ECDH (X25519)

Rating (experimental)	
Rating specs (not complete)	SSL Labs's 'SSL Server Rating Guide' (version 2009q from 2020-01-30)
Specification documentation	https://github.com/ssllabs/research/wiki/SSL-Server-Rating-Guide
Protocol Support (weighted)	0 (0)
Key Exchange (weighted)	0 (0)
Cipher Strength (weighted)	0 (0)
Final Score	0
Overall Grade	T
Grade cap reasons	Grade capped to T. Issues with the chain of trust (self signed)
	Grade capped to M. Domain name mismatch
	Grade capped to A. HSTS is not offered

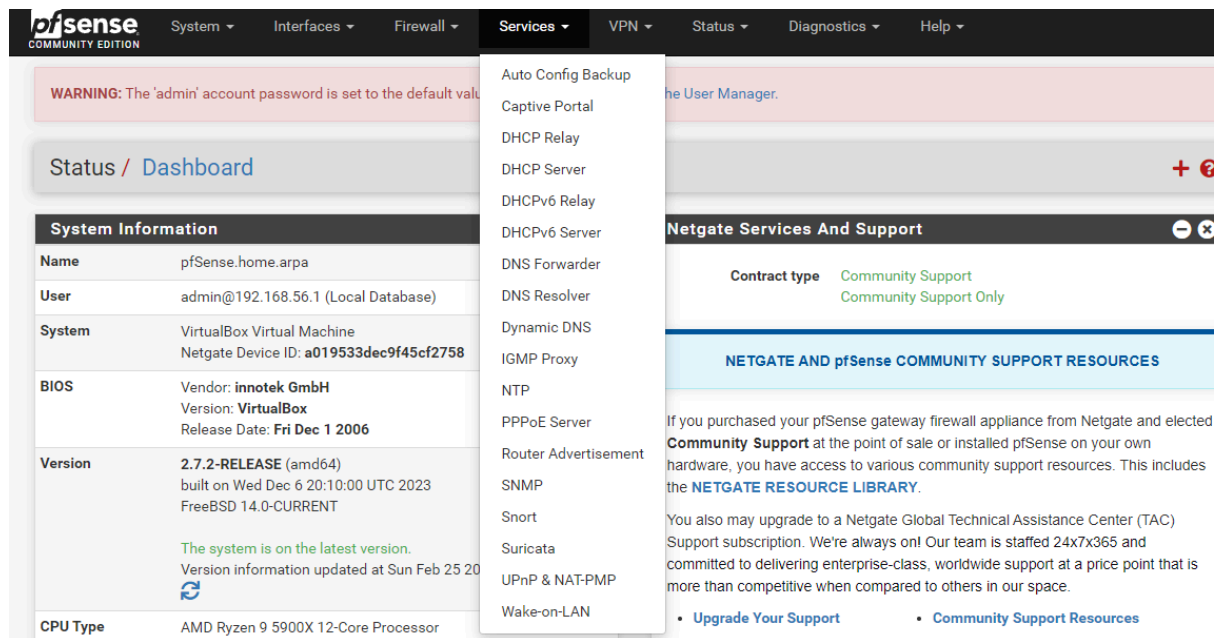
Après avoir effectué un scan SSL de mon serveur, je constate qu'il ne présente aucune vulnérabilité connue. Le scan a minutieusement vérifié les protocoles, les suites de chiffrement et d'éventuelles vulnérabilités spécifiques telles que Heartbleed, POODLE et BEAST. Heureusement, mon serveur est bien configuré pour éviter ces failles de sécurité.

3. La partie réseau a été traitée dans le TP3. Rajouter sur le parefeu pfSense les points suivants :

a. Règles de filtrage qui permettent de détecter et bloquer les balayages réseau. Vous pouvez utiliser un IDS pour la détection des intrusions.

Activation et configuration de l'IDS

Suite à notre recherche, j'ai trouvé deux IDS, Snort et Suricata. Je l'est ait correctement installé et activé sur votre système pfSense. (depuis l'interface web de pfSense) :



Pour la suite des question, je pense utilisé Suricata, qui est un très bon IDS.

2. Configuration des règles de détection de balayages réseau

Ensuite, j'ai configuré des règles spécifiques dans Suricata pour détecter les balayages réseau. Ces règles sont essentielles car elles me permettent d'identifier des tentatives d'accès non autorisées ou des scans de ports. J'ai filtré et activé des règles liées aux scans de réseau dans l'onglet Rules.

3. Règles de filtrage sur pfSense

Je me suis rendu dans Firewall > Rules pour configurer ces règles supplémentaires.

En plus de l'IDS, configurez des règles de filtrage sur pfSense pour bloquer les adresses IP connues pour leurs activités de balayage réseau.

Accédez à Firewall > Rules.

J'ai configuré Suricata pour qu'il génère des alertes ou bloque automatiquement le trafic suspect, en m'assurant que ces actions sont bien reflétées dans les journaux de pfSense.

B. Ajouter les règles qui permettent de protéger les parefeux et les services internes des attaques DoS. Expliquer votre méthode.

Je commence par identifier et sélectionner des règles spécifiques au sein de Suricata qui sont conçues pour détecter les comportements associés aux attaques DoS. Sur l'interface de pfSense, je navigue dans Services > Suricata puis SID Management. Ici, je peux filtrer et activer des règles qui sont spécifiquement conçues pour détecter les attaques DoS. Des exemples de ces règles incluent celles qui surveillent les tentatives de connexion répétitives et rapides ou les volumes anormaux de trafic en peu de temps.

Services / Suricata / SID Management

Interfaces

Global Settings

Updates

Alerts

Blocks

Files

Pass Lists

Suppress

Logs View

Logs Mgmt

SID Mgmt

Sync

IP Lists

General Settings

Enable Automatic SID State Management

☒

Enable automatic management of rule state and content using SID Management Configuration Lists. Default is Not Checked.
When checked, Suricata will automatically enable/disable/modify text rules upon each update using criteria specified in SID Management Configuration Lists. The supported configuration list format is the same as that used by PulledPork and Oinkmaster. See the included sample conf lists for usage examples. Either upload existing configurations to the firewall or create new ones by clicking ADD below.

SID Management Configuration Lists

SID Mods List Name	Last Modified Time	List Actions
disablesid-sample.conf	Dec-20 2023 6:27 pm	  
dropsid-sample.conf	Dec-20 2023 6:27 pm	  
enablesid-sample.conf	Dec-20 2023 6:27 pm	  
modifysid-sample.conf	Dec-20 2023 6:27 pm	  

+ Add

 Import

 Download

Interface SID Management List Assignments

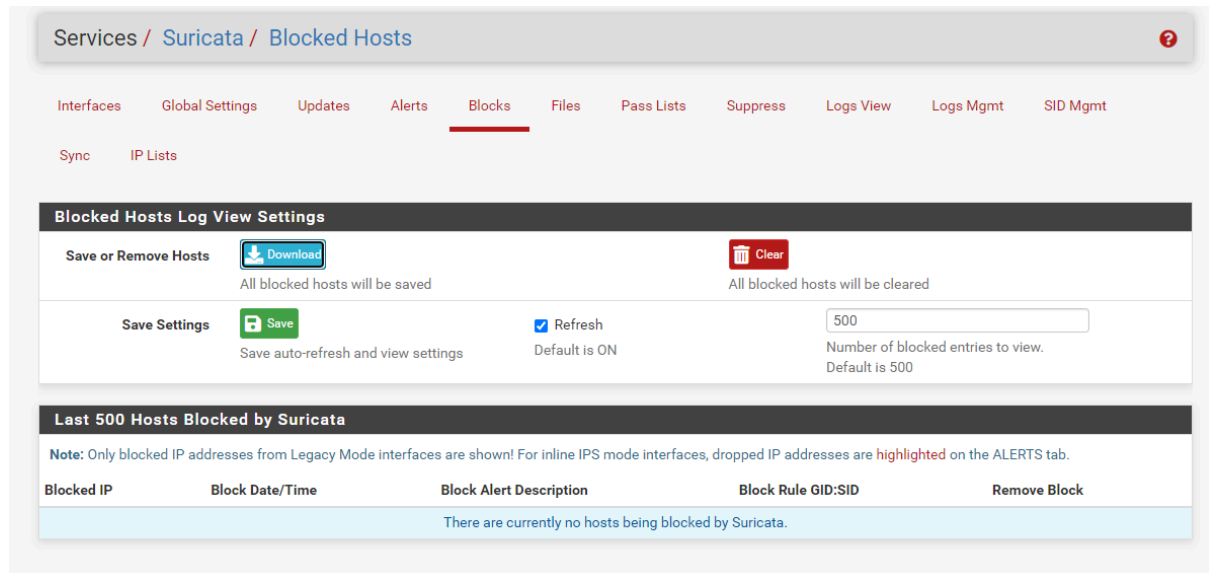
Rebuild	Interface	SID State Order	Enable SID List	Disable SID List	Modify SID List	Drop SID List	Reject SID List
---------	-----------	-----------------	-----------------	------------------	-----------------	---------------	-----------------

Save

Remember to save changes before exiting this page

i

Dans Services > Suricata > Blocked Hosts, j'active l'option de blocage automatique des adresses IP qui déclenchent les règles de détection de DoS. Cela permet de bloquer immédiatement les sources d'attaque potentielles sans intervention manuelle.



Après avoir configuré les règles et les seuils, je teste la configuration pour m'assurer qu'elle fonctionne correctement. Je peux simuler des attaques DoS en utilisant des outils comme hping3

```
sudo hping3 -S --scan 1-1000 scanme.nmap.org
```

C. Ecrire des règles de protection contre les attaques par usurpation d'adresse IP

Pour écrire des règles de protection contre ce type d'attaque dans Suricata, voici ce que je ferais :

Identifier le trafic légitime : Je commencerais par déterminer quelles sont les plages d'adresses IP légitimes pour mon réseau. Toute adresse source ne faisant pas partie de ces plages et tentant de communiquer avec mon réseau interne serait suspecte.

Ecrire des règles de détection : J'ai écrit des règles dans Suricata pour détecter les paquets avec des adresses IP sources qui ne devraient pas être routées sur Internet ou qui ne font pas partie des plages d'adresses légitimes pour mon réseau. Par exemple, si mon réseau interne utilise la plage 192.168.1.0/24, une règle génère une alerte pour tout trafic entrant prétendant provenir de cette plage, car ce trafic devrait normalement être interne et non routé sur Internet.

Implémenter l'ingénierie de trafic : Pour les réseaux où je connais les chemins habituels du trafic, je pourrais écrire des règles qui alertent ou bloquent le trafic provenant de chemins inattendus, ce qui pourrait indiquer une usurpation.

Voici la règle Suricata pour détecter une tentative d'usurpation d'adresse IP :

alert ip ![192.168.1.0/24] any -> 192.168.56.70 any (msg:"Tentative d'usurpation d'adresse IP détectée"; sid:1000001; rev:1;)

D. Le parefeu est accessible par SSH. Faites le nécessaire afin de bloquer une adresse IP pour une heure après 5 tentatives de connexions SSH échouées.

Pour bloquer une adresse IP pendant une heure après 5 tentatives de connexion SSH échouées, je pourrais utiliser un outil comme fail2ban (Que j'ai précédemment installé) sur le pare-feu. fail2ban est un logiciel qui analyse les fichiers de journalisation (logs) pour détecter des motifs d'échecs de connexion et applique des règles de pare-feu pour bloquer l'adresse IP source correspondante. Voici les étapes générales que je suivrais :

Installer fail2ban : Si fail2ban n'est pas déjà installé sur le pare-feu, je me connecterais via SSH et utiliserais le gestionnaire de paquets du système pour l'installer. Par exemple, sur un système basé sur Debian, je pourrais utiliser `apt-get install fail2ban`.

Configurer fail2ban : Je créerais ou éditerais un fichier de configuration pour fail2ban dans `/etc/fail2ban/jail.local`. Voici un exemple de configuration :

```

GNU nano 7.2 /etc/fail2ban/jail.local *
#
# apprise
#
# ban IP on CloudFlare & send an e-mail with whois report and relevant log lines
# to the destemail.
action_cf_mwl = cloudflare[cfuser="%(cfemail)s", cftoken="%(cfapikey)s"]
               %(mta)s-whois-lines[sender="%(sender)s", dest="%(destemail)s", logpath="%(logpath)s", chain="%(chain)s"]

# Report block via blocklist.de fail2ban reporting service API
#
# See the IMPORTANT note in action.d/blocklist_de.conf for when to use this action.
# Specify expected parameters in file action.d/blocklist_de.local or if the interpolation
# 'action_blocklist_de' used for the action, set value of 'blocklist_de_apikey'
# in your 'jail.local' globally (section [DEFAULT]) or per specific jail section (resp. in
# corresponding jail.d/my-jail.local file).
#
action_blocklist_de = blocklist_de[email="%(sender)s", service="%(__name__)s", apikey="%(blocklist_de_apikey)s", agent="%(fa

# Report ban via abuseipdb.com.
#
# See action.d/abuseipdb.conf for usage example and details.
#
action_abuseipdb = abuseipdb

# Choose default action. To change, just override value of 'action' with the
# interpolation to the chosen action shortcut (e.g. action_mwl, action_mw, etc) in jail.local
# globally (section [DEFAULT]) or per specific section
action = %(action_)s

#
# JAILS
#
#
# SSH servers
#

[sshd]

# To use more aggressive sshd modes set filter parameter "mode" in jail.local:
# normal (default), ddos, extra or aggressive (combines all).
# See "tests/files/logs/sshd" or "filter.d/sshd.conf" for usage example and details.
#mode = normal
port = ssh
logpath = %(sshd_log)s
backend = %(sshd_backend)s
maxretry = 5
bantime = 3600

[dropbear]

port = ssh
logpath = %(dropbear_log)s
backend = %(dropbear_backend)s

```

logpath = par default

maxretry = 5

bantime = 3600 (bantime) à 3600 secondes (1 heure).

J'ai pu tester la configuration pour m'assurer que fail2ban bloque effectivement une adresse IP après 5 tentatives de connexion SSH échouées. (En ayant taper de mauvais identifiant...)