Comment sécuriser une Debian

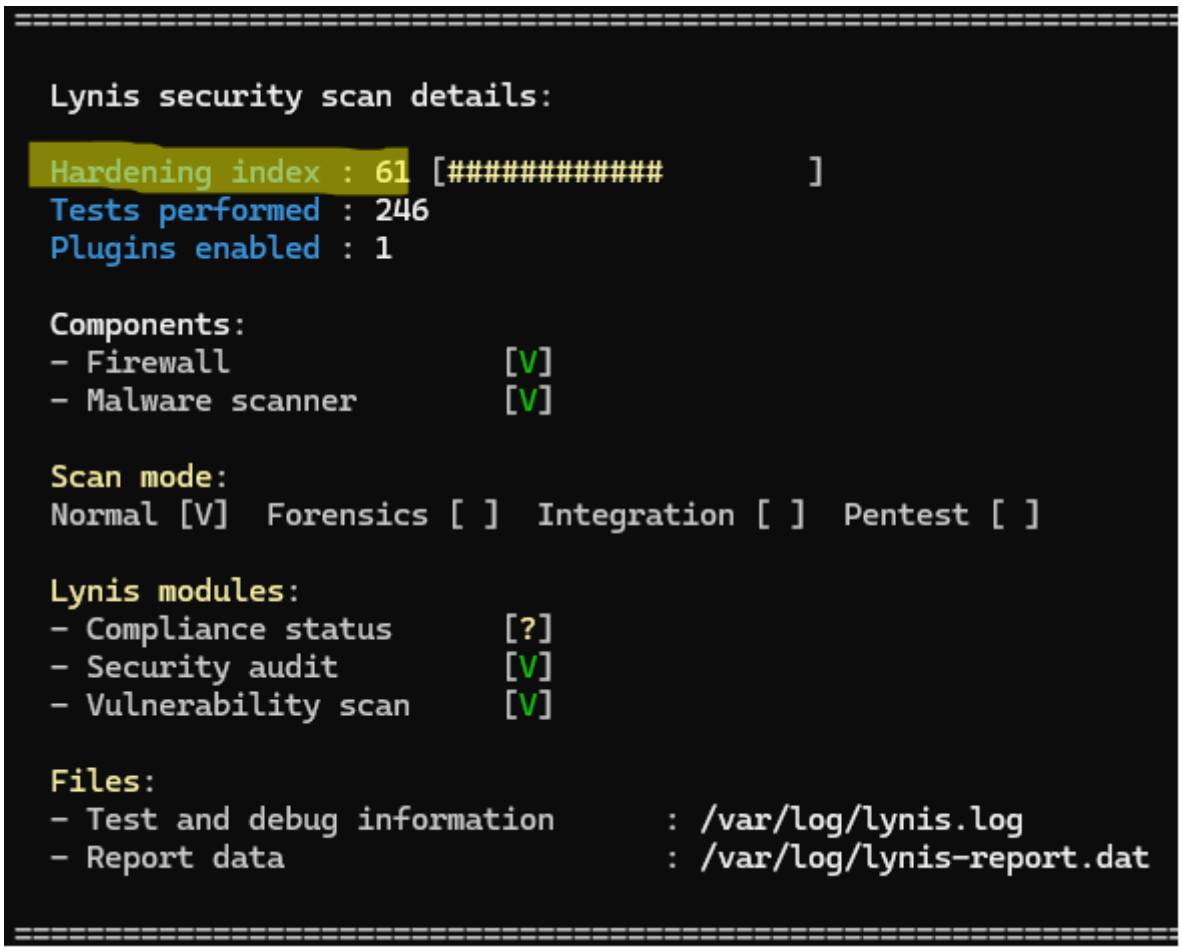
Mettre en place Lynis pour tester la fiabilité et la sécurisation d'une Debian.

1 - Pour installer Lynis :

#sudo apt install lynis

2 - Pour lancer un audit avec Lynis :

#lynis audit system



Installation d'un scanneur de virus (malware-scanner) sur les Debian.

1 - Pour installer le scanneur Clamav :

#sudo apt install clamav clamav-daemon

2 - Pour lancer un scanne :

#sudo clamscan –r /chemin/du/fichier/a/scanner

```
----------- SCAN SUMMARY -----------
Known viruses: 8700275
Engine version: 1.0.7
Scanned directories: 1636
Scanned files: 15099
Infected files: 0
Data scanned: 733.62 MB
Data read: 299.04 MB (ratio 2.45:1)
Time: 366.048 sec (6 m 6 s)
Start Date: 2024:11:26 08:35:10
End Date:   2024:11:26 08:41:16
```

Installation de Fail2Ban.

Fail2Ban est un outil de sécurité qui protège les serveurs contre les attaques par force brute en bannissant automatiquement les adresses IP suspectes après plusieurs tentatives de connexion échouées.

1 - Pour installer Fail2ban :

#sudo apt install fail2ban

2 - Copier le fichier modéle de fail2ban pour ensuite le modifier :

#sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local

```
btssio@Debian-Sauvegarde:~$ sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
btssio@Debian-Sauvegarde:~$ cd /etc/fail2ban/
btssio@Debian-Sauvegarde:/etc/fail2ban$ ls
action.d        fail2ban.d  jail.conf  jail.local       paths-common.conf  paths-opensuse.conf
fail2ban.conf   filter.d    jail.d     paths-arch.conf  paths-debian.conf
```

3 - Configurer le fichier de configuration “jail.local” :

```
  GNU nano 7.2                                    /etc/fail2ban/jail.local

[sshd]

# To use more aggressive sshd modes set filter parameter "mode" in jail.loc
# normal (default), ddos, extra or aggressive (combines all).
# See "tests/files/logs/sshd" or "filter.d/sshd.conf" for usage example and
#mode   = normal
enabled = true
port    = ssh
filter = sshd
logpath = %(sshd_log)s
backend = %(sshd_backend)s
maxretry = 2
findtime = 300
banaction = iptables-allports
bantime = 86400
ignoreip = 127.0.0.1
```

4 - Redémarrer Fail2ban et vérifier son statut :

#sudo systemctl restart fail2ban

#sudo systemctl status fail2ban

```
btssio@Debian-Sauvegarde:~$ sudo systemctl start fail2ban
btssio@Debian-Sauvegarde:~$ sudo systemctl status fail2ban
× fail2ban.service - Fail2Ban Service
     Loaded: loaded (/lib/systemd/system/fail2ban.service; enabled; preset: enabled)
     Active: failed (Result: exit-code) since Tue 2024-11-26 09:11:46 CET; 1s ago
   Duration: 133ms
       Docs: man:fail2ban(1)
    Process: 151599 ExecStart=/usr/bin/fail2ban-server -xf start (code=exited, status=255/EXCEPTION)
   Main PID: 151599 (code=exited, status=255/EXCEPTION)
        CPU: 123ms

nov. 26 09:11:46 Debian-Sauvegarde systemd[1]: Started fail2ban.service - Fail2Ban Service.
nov. 26 09:11:46 Debian-Sauvegarde fail2ban-server[151599]: 2024-11-26 09:11:46,335 fail2ban.configreader   [151599]: W>
nov. 26 09:11:46 Debian-Sauvegarde fail2ban-server[151599]: 2024-11-26 09:11:46,349 fail2ban               [151599]: E>
nov. 26 09:11:46 Debian-Sauvegarde fail2ban-server[151599]: 2024-11-26 09:11:46,356 fail2ban               [151599]: E>
nov. 26 09:11:46 Debian-Sauvegarde systemd[1]: fail2ban.service: Main process exited, code=exited, status=255/EXCEPTION
nov. 26 09:11:46 Debian-Sauvegarde systemd[1]: fail2ban.service: Failed with result 'exit-code'.
```

5 - Créer le fichier auth.log et mettre les droits :

#sudo touch /var/log/auth.log

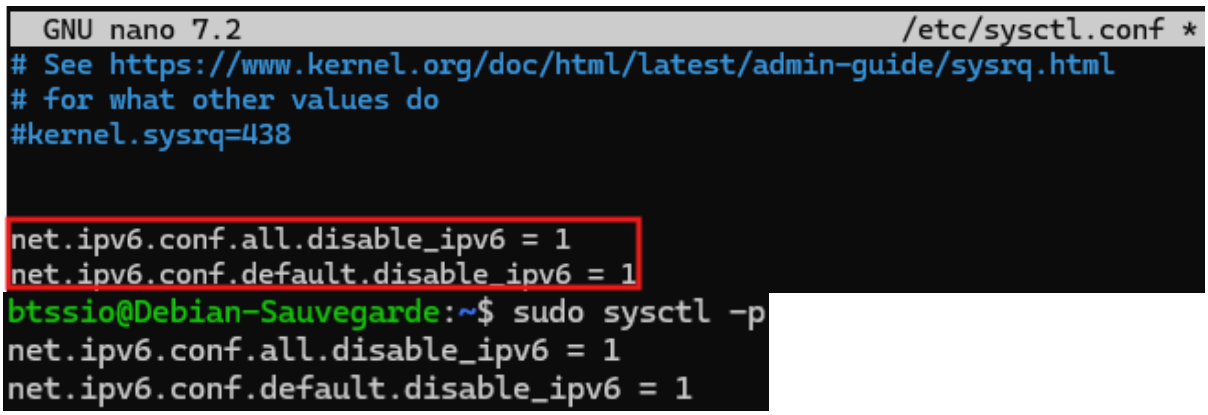
#sudo chmod 640 /var/log/auth.log

```
btssio@Debian-Sauvegarde:~$ sudo systemctl restart fail2ban
btssio@Debian-Sauvegarde:~$ sudo systemctl status fail2ban
● fail2ban.service - Fail2Ban Service
     Loaded: loaded (/lib/systemd/system/fail2ban.service; enabled; preset: enabled)
     Active: active (running) since Tue 2024-11-26 09:21:16 CET; 3s ago
       Docs: man:fail2ban(1)
   Main PID: 151634 (fail2ban-server)
      Tasks: 5 (limit: 2315)
     Memory: 16.9M
        CPU: 160ms
     CGroup: /system.slice/fail2ban.service
             └─151634 /usr/bin/python3 /usr/bin/fail2ban-server -xf start

nov. 26 09:21:16 Debian-Sauvegarde systemd[1]: Started fail2ban.service - Fail2Ban Service.
nov. 26 09:21:16 Debian-Sauvegarde fail2ban-server[151634]: 2024-11-26 09:21:16,187 fail2ban.configreader   [151634]: W>
nov. 26 09:21:16 Debian-Sauvegarde fail2ban-server[151634]: Server ready
```

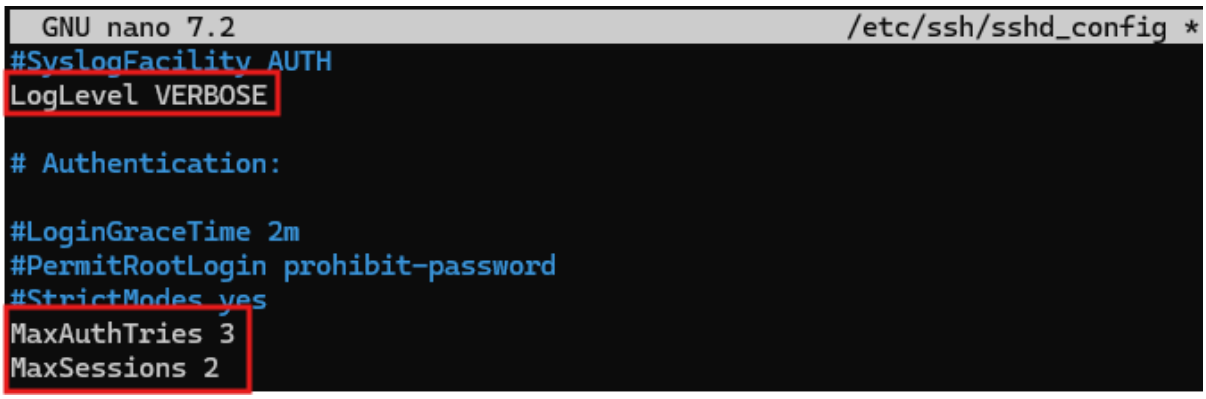
Protection du réseau.

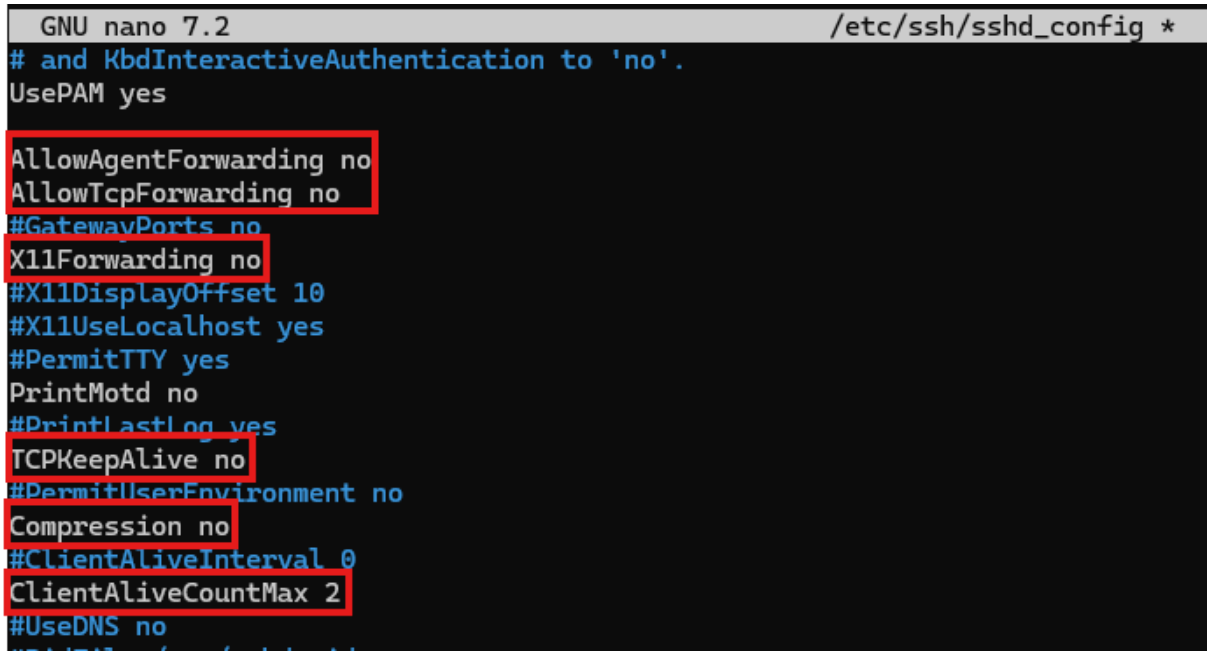
Désactiver IPv6 dans le fichier de conf “sysctl.conf” :



Autre Modification a effectué.

Décocher différents parametres dans le fichier de conf /etc/ssh/sshd_config :





Installation de module pour renforcer la sécurité.

```
  - PAM (Pluggable Authentication Modules):
    - libpam-tmpdir                                    [ Not Installed ]
- File System Checks:
  - DM-Crypt, Cryptsetup & Cryptmount:
- Software:
  - apt-listbugs                                       [ Not Installed ]
  - apt-listchanges                                    [ Installed and enabled for apt ]
  - needrestart                                        [ Not Installed ]
  - fail2ban                                           [ Installed with jail.local ]
```

1 - PAM :

#sudo apt install libpam-tmpdir

2 - Apt-listbugs :

#sudo apt install apt-listbugs

Montre les modifications importantes dans les paquets avant leur mise à jour :

sudo apt install apt-listchanges –y

3 – needrestart :

#sudo apt install needrestart

```
- Authentication:
  - PAM (Pluggable Authentication Modules):
    - libpam-tmpdir                                    [ Installed and Enabled ]
- File System Checks:
  - DM-Crypt, Cryptsetup & Cryptmount:
- Software:
  - apt-listbugs                                       [ Installed and enabled for apt ]
  - apt-listchanges                                    [ Installed and enabled for apt ]
  - needrestart                                        [ Installed ]
  - fail2ban                                           [ Installed with jail.local ]
```

```
================================================================================

  Lynis security scan details:

  Hardening index : 71 [##############      ]
  Tests performed : 255
  Plugins enabled : 1

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

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

  Lynis modules:
```