TP - Mise en place et audit des mesures de sécurité sur un serveur Linux

L'objectif de ce tp était de sécuriser un serveur Linux en s'appuyant directement sur les bonnes pratiques de la norme internationale ISO 27001.

```
[root@srv-secure ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:0c:29:12:79:76 brd ff:ff:ff:ff:ff:ff
    altname enp3s0
    inet 192.168.100.129/24 brd 192.168.100.255 scope global dynamic noprefixroute ens160
       valid_lft 1738sec preferred_lft 1738sec
    inet6 fe80::20c:29ff:fe12:7976/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

```
GNU nano 5.6.1                                  /etc/ssh/sshd_config
# If you just want the PAM account and session checks to run without
# PAM authentication, then enable this but set PasswordAuthentication
# and KbdInteractiveAuthentication to 'no'.
# WARNING: 'UsePAM no' is not supported in RHEL and may cause several
# problems.
#UsePAM no

#AllowAgentForwarding yes
#AllowTcpForwarding yes
#GatewayPorts no
#X11Forwarding no
#X11DisplayOffset 10
#X11UseLocalhost yes
#PermitTTY yes
#PrintMotd yes
#PrintLastLog yes
#TCPKeepAlive yes
#PermitUserEnvironment no
#Compression delayed
#ClientAliveInterval 0
#ClientAliveCountMax 3
#UseDNS no
#PidFile /var/run/sshd.pid
#MaxStartups 10:30:100
#PermitTunnel no
#ChrootDirectory none
#VersionAddendum none

# no default banner path
#Banner none

# override default of no subsystems
Subsystem       sftp    /usr/libexec/openssh/sftp-server

# Example of overriding settings on a per-user basis
#Match User anoncvs
#       X11Forwarding no
#       AllowTcpForwarding no
#       PermitTTY no
#       ForceCommand cvs server
Port 2222
PermitRootLogin no
PasswordAuthentication no
MaxAuthTries 3
AllowUsers admin
```

Sécurisation de l’accès distant (SSH) : J'ai procédé au durcissement du service SSH afin de protéger le serveur contre les intrusions. Les mesures suivantes ont été appliquées :

Changement du port d'écoute : Utilisation d'un port non-standard pour masquer le service face aux scans automatisés.

Interdiction du login Root : Désactivation de l'accès direct au compte super-utilisateur pour renforcer la traçabilité.

Protection contre la force brute : Limitation du nombre de tentatives d'authentification autorisées.

Contrôle d'accès : Restriction des connexions aux seuls utilisateurs autorisés.

Ces actions permettent de réduire significativement la surface d'attaque du serveur.

```
[root@srv-secure ~]# sudo semanage port -l | grep ssh
ssh_port_t                     tcp      22
[root@srv-secure ~]# sudo semanage port -a -t ssh_port_t -p tcp 2222
[ 1423.349630] SELinux:  Converting 346 SID table entries...
[ 1423.369861] SELinux:  policy capability network_peer_controls=1
[ 1423.370157] SELinux:  policy capability open_perms=1
[ 1423.370353] SELinux:  policy capability extended_socket_class=1
[ 1423.370547] SELinux:  policy capability always_check_network=0
[ 1423.370821] SELinux:  policy capability cgroup_seclabel=1
[ 1423.371000] SELinux:  policy capability nnp_nosuid_transition=1
[ 1423.371176] SELinux:  policy capability genfs_seclabel_symlinks=1
[root@srv-secure ~]# sudo semanage port -l | grep ssh
ssh_port_t                     tcp      2222, 22
```

Après vérification, le service SSH a été ajouté sur le port personnalisé 2222. Une règle a donc été ajoutée pour autoriser ce port.

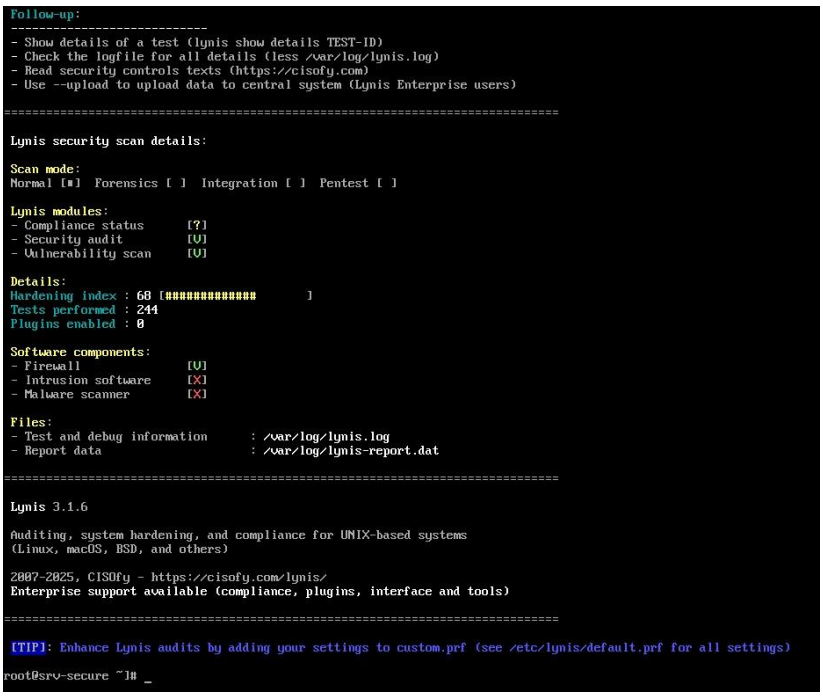
```
[root@srv-secure ~]# systemctl enable firewalld
[ 1659.712166] systemd-rc-local-generator[12718]: /etc/rc.d/rc.local is not marked executable, skipping.
[root@srv-secure ~]# systemctl start firewalld
[root@srv-secure ~]# systemctl status firewalld
● firewalld.service - firewalld - dynamic firewall daemon
     Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; preset: enabled)
     Active: active (running) since Wed 2026-04-01 13:16:48 CEST; 27min ago
       Docs: man:firewalld(1)
   Main PID: 840 (firewalld)
      Tasks: 2 (limit: 10415)
     Memory: 43.9M (peak: 64.3M)
        CPU: 765ms
     CGroup: /system.slice/firewalld.service
             └─840 /usr/bin/python3 -s /usr/sbin/firewalld --nofork --nopid

avril 01 13:16:47 srv-secure systemd[1]: Starting firewalld - dynamic firewall daemon...
avril 01 13:16:48 srv-secure systemd[1]: Started firewalld - dynamic firewall daemon.
[root@srv-secure ~]#
```

Activation du pare-feu firewalld afin de contrôler les connexions entrantes sur le serveur.

```
[root@srv-secure ~]# firewall-cmd --set-default-zone=public
Warning: ZONE_ALREADY_SET: public
success
[root@srv-secure ~]# sudo firewall-cmd --add-port=2222/tcp --permanent
success
[root@srv-secure ~]# sudo firewall-cmd --add-port=80/tcp --permanent
*success
[root@srv-secure ~]# sudo firewall-cdm --reload
sudo: firewall-cdm : commande introuvable
[root@srv-secure ~]# sudo firewall-cmd --reload
success
[root@srv-secure ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: ens160
  sources:
  services: cockpit dhcpv6-client ssh
  ports: 2222/tcp 80/tcp
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
[root@srv-secure ~]#
```

Le pare-feu a été configuré afin de n'autoriser que les ports nécessaires au fonctionnement du serveur. Les ports SSH personnalisé (2222) et HTTP (80) ont été ouverts, tandis que les autres ports restent bloqués.

Cette configuration permet de réduire la surface d'attaque du serveur en limitant les services accessibles depuis le réseau.



Un audit de sécurité a été réalisé à l'aide de l'outil Lynis afin d'évaluer le niveau de protection du serveur après les différentes configurations mises en place

Le score de sécurité obtenu est de 68, ce qui indique un niveau de sécurisation correct mais encore perfectible.

L'analyse met en évidence que certaines protections sont bien en place, comme le pare-feu, mais que d'autres mécanismes de sécurité peuvent encore être ajoutés, notamment la détection d'intrusion et l'analyse de malwares.

Suite à l'audit, une amélioration a été envisagée en ajoutant un outil de détection de malwares afin de renforcer la sécurité du système.

Cette démarche s'inscrit dans une logique d'amélioration continue de la sécurité, conformément aux principes de la norme ISO 27001.

Ce TP m’a permis de mettre en place plusieurs mesures de sécurité et de vérifier leur efficacité à l’aide d’un audit. Il met en évidence l’importance de tester et d’améliorer régulièrement la sécurité d’un système.