



Mini-Projet DevSecOps – Audit et Sécurisation d'un Serveur Linux



Partie 1 – Exercices préparatoires

Exercice 1 : Reconnaissance de l'environnement

Notre environnement de test est en local hébergé sur Hyper-V avec un serveur CentOS Stream 10.

1. Version du noyau Linux : 6.12.0-66.el10.x86_64

```
centos@appserv01:~  
[sudo] Mot de passe de centos :  
6.12.0-66.el10.x86_64  
[centos@appserv01 ~]$ sudo uname -a  
Linux appserv01 6.12.0-66.el10.x86_64 #1 SMP PREEMPT_DYNAMIC Thu Mar 20 13:49:55  
UTC 2025 x86_64 GNU/Linux  
[centos@appserv01 ~]$ sudo hostnamectl  
Static hostname: appserv01  
Icon name: computer-vm  
Chassis: vm =  
Machine ID: 62eb5b346fac402395a6e54987cb60e1  
Boot ID: 5364bfba0c8945cb982ccf7f8349fb29  
Product UUID: c122aebd-c25d-6247-a2d3-e4f55b1c3f7c  
Virtualization: microsoft  
Operating System: CentOS Stream 10 (Coughlan)  
CPE OS Name: cpe:/o:centos:centos:10  
Kernel: Linux 6.12.0-66.el10.x86_64  
Architecture: x86-64  
Hardware Vendor: Microsoft Corporation  
Hardware Model: Virtual Machine  
Hardware Serial: 3000-8348-4950-9092-7574-6353-36  
Firmware Version: 090008  
Firmware Date: Fri 2018-12-07  
Firmware Age: 6y 6month 1w 2d  
[centos@appserv01 ~]$
```



Interprétation complète :

Ce noyau est :

- Basé sur Linux 6.12.0
- Build number : 66
- Construit avec des modifications provenant de CentOS Stream 10
- Compilé pour l'architecture x86_64 (64 bits)

Un noyau obsolète peut avoir plusieurs impacts négatifs dans un environnement de production ou de développement en exposant des failles de sécurité non corrigées par des vulnérabilités connues, il peut également apporter des incompatibilités avec des logiciels ou certains modules du noyau, ralentir les performances et dégrader les systèmes et services et enfin la maintenance difficile car moins de documentation et indisponibilité du support.

2. Les services de sécurité actifs de notre environnement de travail

```
centos@appserv01:/home/centos
[root@appserv01 centos]# systemctl list-units --type=service | grep -E 'firewalld|iptables|auditd|selinux'
auditd.service          loaded active running Security Audit Logging Service
firewalld.service       loaded active running firewalld - dynamic firewall daemon
[root@appserv01 centos]# sestatus
SELinux status:                enabled
SELinuxfs mount:              /sys/fs/selinux
SELinux root directory:       /etc/selinux
Loaded policy name:            targeted
Current mode:                  enforcing
Mode from config file:        enforcing
Policy MLS status:             enabled
Policy deny unknown status:    allowed
Memory protection checking:    actual (secure)
Max kernel policy version:     33
[root@appserv01 centos]#
```

03 services de sécurité actif : **auditd, firewalld et SELinux**

Auditd et firewalld sont activés, Selinux est activé et en mode enforcement (Pour appliquer les règles définies).

3. Les ports actuellement ouverts : 22, 323, 631, 9090, 5353 (en local)

Commande permettant de détecter les ports ouverts : **netstat -tuln** ou **ss -tuln** ou **firewall-cmd --list-all**

```
centos@appserv01:/home/centos
[root@appserv01 centos]# netstat -tuln
Connexions Internet actives (seulement serveurs)
Proto Recv-Q Send-Q Adresse locale Adresse distante Etat
tcp 0 0 127.0.0.1:631 0.0.0.0:* LISTEN
tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN
tcp6 0 0 :::22 :::* LISTEN
tcp6 0 0 :::631 :::* LISTEN
tcp6 0 0 :::9090 :::* LISTEN
udp 0 0 0.0.0.0:5353 0.0.0.0:*
udp 0 0 127.0.0.1:323 0.0.0.0:*
udp6 0 0 :::5353 :::*
udp6 0 0 :::323 :::*
[root@appserv01 centos]# ss -tuln
Netid State Recv-Q Send-Q Local Address:Port Peer Address:Port
udp UNCONN 0 0 0.0.0.0:5353 0.0.0.0:*
udp UNCONN 0 0 127.0.0.1:323 0.0.0.0:*
udp UNCONN 0 0 [::]:5353 [::]:*
udp UNCONN 0 0 [::1]:323 [::]:*
tcp LISTEN 0 4096 127.0.0.1:631 0.0.0.0:*
tcp LISTEN 0 128 0.0.0.0:22 0.0.0.0:*
tcp LISTEN 0 128 [::]:22 [::]:*
tcp LISTEN 0 4096 [::1]:631 [::]:*
tcp LISTEN 0 4096 *:9090 *:*
```


Vérification des ports ouverts non justifiés :

Protocole	Adresse locale	Port	État	Commentaire
tcp	127.0.0.1	631	LISTEN	Service d'impression (CUPS) en local
tcp	0.0.0.0	22	LISTEN	SSH accessible sur toutes interfaces IPv4
tcp6	:::	22	LISTEN	SSH accessible sur toutes interfaces IPv6
tcp6	::1	631	LISTEN	Service CUPS en local sur IPv6
tcp6	:::	9090	LISTEN	Service écoute sur port 9090 en IPv6
udp	0.0.0.0	5353		Multicast DNS (mDNS) sur IPv4
udp	127.0.0.1	323		Service de temps local (NTP)
udp6	:::	5353		Multicast DNS (mDNS) sur IPv6
udp6	::1	323		Service de temps local (NTP)

- Le serveur SSH écoute sur le port 22 et accepte des connexions sur toutes les interfaces (IPv4 et IPv6).
- Le service d'impression CUPS écoute localement sur 127.0.0.1:631 (et son équivalent IPv6).
- Un service écoute sur le port TCP 9090 sur IPv6.
- Les ports UDP 5353 sont utilisés par le mDNS (service réseau local pour résolution de noms).
- Le port UDP 323 est lié à un service de synchronisation d'heure (comme chrony ou ntpd).

Points attention:

- **Le port 9090** écoute sur toutes les interfaces IPv6 (:::9090) qui n'est pas censé être accessible publiquement, c'est potentiellement un risque.
- **mDNS (5353 UDP)** est souvent activé par défaut sur certains services pour la découverte réseau locale. En environnement serveur, il est souvent recommandé de désactiver ce service pour limiter la surface d'attaque, sauf si besoin d'une résolution de noms locale spécifique.
- **CUPS (631 TCP)** est local uniquement, donc le risque est limité, n'est pas nécessaire si pas d'impression, il pourrait aussi être désactivé.
- **NTP (323 UDP)** est un service de temps local avec risque limité

 centos@appserv01:/home/centos

```
[root@appserv01 centos]# sudo lsof -i :9090
COMMAND PID USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
systemd   1 root    80u  IPv6  8259      0t0  TCP *:websock (LISTEN)
[root@appserv01 centos]#
```

Conclusion : Le port 9090 (cockpit.socket pour la gestion des serveurs linux par une interface web) est celui qui mérite le plus d'attention dans cette liste, car c'est un port ouvert sur toutes les interfaces et qui peut représenter une porte d'entrée si le service associé est vulnérable ou mal configuré et si la gestion des ressources du serveur linux à distance n'est pas nécessaire.

🧠 Exercice 2: Recherche de fichiers et analyse de logs

1. Recherche de tous les fichiers contenant des secrets potentiels Mots-clés à rechercher sans tenir compte de la casse :

password, api_key, token, secret_key, .env.

Pour effectuer cette recherche, nous allons utiliser la commandes **find** avec des options de recherches sur des fichiers nommés, des formats d'extension précis ou la commande **grep** pour détecter des chaines sensibles dans tous les fichiers (les faire ressortir en couleur) ou une combinaison des commandes **find** et **grep**; et rediriger le résultat dans un fichier résultat.

```
[root@appserv01 centos]# find / -type f \( -iname "*secret*" -o -iname "*password*" -o -iname "token" -o -iname "*.env" -o -iname "*.pem" -o -iname "*key" \) 2>/dev/null > secret_result.txt
```

```
centos@appserv01/home/centos
[root@appserv01 centos]# find / -type f \( -iname "*secret*" -o -iname "*password*" -o -iname "token" -o -iname "*.env" -o -iname "*.pem" -o -iname "*key" \) 2>/dev/null > secret_result.txt
[root@appserv01 centos]# more secret_result.txt
/boot/grub2/1386-pc/legacy_password_test.mod
/boot/grub2/1386-pc/password_pbkdf2.mod
/home/centos/secret_result.txt
/proc/sys/net/ipv4/ipfrag_secret_interval
/proc/sys/net/ipv6/conf/all/stable_secret
/proc/sys/net/ipv6/conf/default/stable_secret
/proc/sys/net/ipv6/conf/eth0/stable_secret
/proc/sys/net/ipv6/conf/eth1/stable_secret
/proc/sys/net/ipv6/conf/lo/stable_secret
/proc/sys/net/ipv6/ipfrag_secret_interval
/run/user/452/systemd/generator.late/app-gnome-w3dkeyring-w3dsecrets@autostart.service
/run/user/1000/gnome/gnome-control-center-gnome-w3dkeyring-w3dsecrets@autostart.service
```

```
[root@appserv01 centos]# grep -RiE --color 'password|passwd|secret|api[_]?key|token|PRIVATE_KEY' / 2>/dev/null
```

```
centos@appserv01/home/centos
[root@appserv01 centos]# grep -RiE --color 'password|passwd|secret|api[_]?key|token|PRIVATE_KEY' / 2>/dev/null
/boot/grub2/1386-pc/legacy_password_test: cryptogrqry_ahab12 normal pbkdf2
/boot/grub2/1386-pc/moddep.lst:legacy_password_test: functional_test: legacycfg
/boot/grub2/1386-pc/moddep.lst:password: cryptog normal
/boot/grub2/1386-pc/moddep.lst:legacycfg: cryptogrqry_md5 normal password
/boot/grub2/1386-pc/command.lst:legacy_secret_password: legacycfg
/boot/grub2/1386-pc/command.lst:legacy_password: legacycfg
/boot/grub2/1386-pc/command.lst:password: password
/boot/grub2/1386-pc/command.lst:password_pbkdf2: password_pbkdf2
/boot/grub2/gnub.cfg: if [ -n "${GRUB2_PASSWORD}" ]; then
/boot/grub2/gnub.cfg: password_pbkdf2 root "${GRUB2_PASSWORD}"
```

```
[root@appserv01 centos]# find / -type f \( -name "*.env" -o -name "*.conf" -o -name "*.json" -o -name "*.php" \) -exec grep -iE 'password|passwd|secret|api[_]?key|token|PRIVATE_KEY' {} \; 2>/dev/null > secret_result3.txt
```

```
centos@appserv01/home/centos
[root@appserv01 centos]# find / -type f \( -name "*.env" -o -name "*.conf" -o -name "*.json" -o -name "*.php" \) -exec grep -iE 'password|passwd|secret|api[_]?key|token|PRIVATE_KEY' {} \; 2>/dev/null > secret_result3.txt
[root@appserv01 centos]# more secret_result3.txt
# To set a CHAP username and password for initiator
#node.session.auth.password = password
# To set a CHAP username and password for target(s)
#node.session.auth.password.in = password.in
# To set a discovery session CHAP username and password for the initiator
#discovery.session.auth.password = password
```

2. Analyser les logs d'authentification

Pour le faire nous analysons le fichier **/var/log/secure**

```
root@appserv01/home/centos
login as: centos
centos@10.0.0.10's password:
Web console: https://localhost:9090/

Last failed login: Mon Jun 16 15:35:35 EDT 2025 from 10.0.0.100 on ssh:notty
There were 6 failed login attempts since the last successful login.
Last login: Mon Jun 16 10:43:16 2025 from 10.0.0.100
[centos@appserv01 ~]$ sudo su
[sudo] Mot de passe de centos :
[root@appserv01 centos]# cat /var/log/secure
Apr 11 11:02:42 localhost sshd[995]: Server listening on 0.0.0.0 port 22.
```

Trouvez les tentatives de connexion échouées.

```
sudo grep "Failed" /var/log/secure
```

```
centos@appserv01 ~]$ sudo grep "Failed" /var/log/secure
Jun 16 15:35:27 localhost sshd-session[10070]: Failed password for centos from 10.0.0.100 port 57710 ssh2
Jun 16 15:35:32 localhost sshd-session[10070]: Failed password for centos from 10.0.0.100 port 57710 ssh2
Jun 16 15:35:34 localhost sshd-session[10070]: Failed password for centos from 10.0.0.100 port 57710 ssh2
Jun 16 15:35:34 localhost sshd-session[10070]: Failed password for centos from 10.0.0.100 port 57710 ssh2
Jun 16 15:35:34 localhost sshd-session[10070]: Failed password for centos from 10.0.0.100 port 57710 ssh2
Jun 16 15:35:35 localhost sshd-session[10070]: Failed password for centos from 10.0.0.100 port 57710 ssh2
Jun 16 15:57:58 localhost sudo[10208]: centos : TTY=pts/0 ; FWD=/home/centos ; USER=root ; COMMAND=/bin/grep Failed /var/log/secure
Jun 16 15:58:12 localhost sudo[10214]: centos : TTY=pts/0 ; FWD=/home/centos ; USER=root ; COMMAND=/bin/grep Failed /var/log/secure
[centos@appserv01 ~]$
```

3. Lister les fichiers récemment modifiés dans /etc

Pour le faire, exécuter la commande suivante :

sudo find /etc -type f -mtime -1

```
[centos@appserv01 ~]$ sudo find /etc -type f -mtime -1
/etc/modprobe.d/tuned.conf
/etc/cups/subscriptions.conf.0
/etc/cups/subscriptions.conf
/etc/NetworkManager/system-connections/Connexion filaire 1.nmconnection
/etc/tuned/active_profile
/etc/tuned/post_loaded_profile
/etc/tuned/rp_d_base_profile
/etc/tuned/profile_mode
/etc/hostname
/etc/resolv.conf
[centos@appserv01 ~]$
```

Le répertoire **/etc/** est critique par ce que c'est le répertoire qui contient l'ensemble des fichiers de configuration essentiels du système et des services.

Toutes modifications apportées à ce répertoire devront attirer notre vigilance et il faudra toujours penser au préalable à sa sauvegarde.

Exercice 3: Analyse des permissions sensibles

1. Identification des groupes à privilèges sur notre système

Pour le faire, nous allons rechercher les groupes dont l'ID est inférieur à **1000**. Ce sont les groupes "système", souvent utilisés pour les services ou l'administration.

Sudo getent group : permet d'obtenir tous les groupes

Sudo getent group | awk -F: '\$3 < 1000 { print \$1 ":" \$3 }'

Group	Group	Group
root:0	ftp:50	colord:997
bin:1	lock:54	geoclue:996
daemon:2	audio:63	sssd:995
sys:3	users:100	libstoragegmt:994
adm:4	tss:59	systemd-coredump:993
tty:5	dbus:81	wsdd:992
disk:6	utmp:22	clevis:991
lp:7	utempter:35	setroubleshoot:990
mem:8	avahi:70	pipewire:989
kmem:9	systemd-oom:999	flatpak:988
wheel:10	input:104	brlapi:987
cdrom:11	kvm:36	gdm:42
mail:12	render:105	gnome-initial-setup:986
man:15	sgx:106	dnsmasq:985
dialout:18	systemd-journal:190	sshd:74
floppy:19	polkitd:114	chrony:984
games:20	printadmin:998	tcpdump:72
tape:33	rtkit:172	plocate:983
video:39		gnome-remote-desktop:982

```

centos@appserv01:~$ sudo getent group | awk -F: '{ $3 < 1000 { print $1 ":" $3 } }' > privilegegroup
[centos@appserv01 ~]$ cat privilegegroup
root:0
bin:1
daemon:2
sys:3
adm:4
tty:5
disk:6
lp:7
mem:8
kmem:9
wheel:10
cdrom:11
mail:12
man:15
dialout:18
floppy:19
games:20
tape:33
video:39
ftp:50
lock:54
audio:63
users:100
tss:59
dbus:81
utmp:22
utempter:35

```

Sur les distributions linux, il y'a des groupes critiques qui confèrent les privilèges élevés :

Groupe	Rôle
root	Accès total
wheel	Peut utiliser sudo (équivalent root)
sudo	(si présent) peut utiliser sudo
adm	Accès aux logs système
systemd-journal	Lecture des journaux systemd
users	Groupe par défaut des utilisateurs normaux

Sur CentOS Stream 10, c'est souvent le groupe **wheel** qui permet de faire du **sudo**.

Vérification des utilisateurs qui en font partie : **getent group wheel**

```
centos@appserv01:~  
[centos@appserv01 ~]$ getent group wheel  
wheel:x:10:centos  
[centos@appserv01 ~]$
```

Pour identifier les utilisateurs ayant le privilège root implicite, il faudra tout simplement vérifier si cet utilisateur appartient au groupe **wheel**.

Pour identifier les utilisateurs ayant le privilège **root** explicite, il faut vérifier si sont **UID=0** ou rechercher les utilisateurs ou groupes avec des droits **sudo** accordés dans :

- **/etc/sudoers**
- **/etc/sudoers.d/**

```
awk -F: '($3 == 0) {printf "Utilisateur: %-20s UID: %s\n", $1, $3}' /etc/passwd
```

```
grep -E '^[^#].*ALL' /etc/sudoers 2>/dev/null
```

```
grep -E '^[^#].*ALL' /etc/sudoers.d/* 2>/dev/null
```

```
root@appserv01:/home/centos  
[root@appserv01 centos]# awk -F: '($3 == 0) {printf "Utilisateur: %-20s UID: %s\n", $1, $3}' /etc/passwd  
Utilisateur: root  
UID: 0  
[root@appserv01 centos]# grep -E '^[^#].*ALL' /etc/sudoers 2>/dev/null  
Defaults    env_keep += "LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET XAUTHORITY"  
root    ALL=(ALL)    ALL  
%wheel  ALL=(ALL)    ALL  
[root@appserv01 centos]# grep -E '^[^#].*ALL' /etc/sudoers.d/* 2>/dev/null  
[root@appserv01 centos]#
```

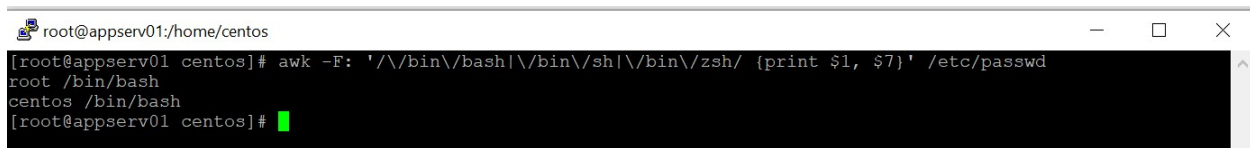

2. Les utilisateurs qui ont accès à un shell de connexion

Les utilisateurs qui ont accès à un *shell de connexion* (**login shell**) sont ceux qui ont un **shell** valide (comme **/bin/bash**, **/bin/sh**, **/bin/zsh**) défini dans le fichier **/etc/passwd** au niveau du champ **shell** (dernier champ sur la ligne).

Cependant, un **shell** comme **/sbin/nologin** ou **/bin/false** signifie que l'utilisateur ne peut pas se connecter (compte restreint ou de service).

Utilisons la commande suivante pour afficher les utilisateurs ayant un **shell de connexion** :

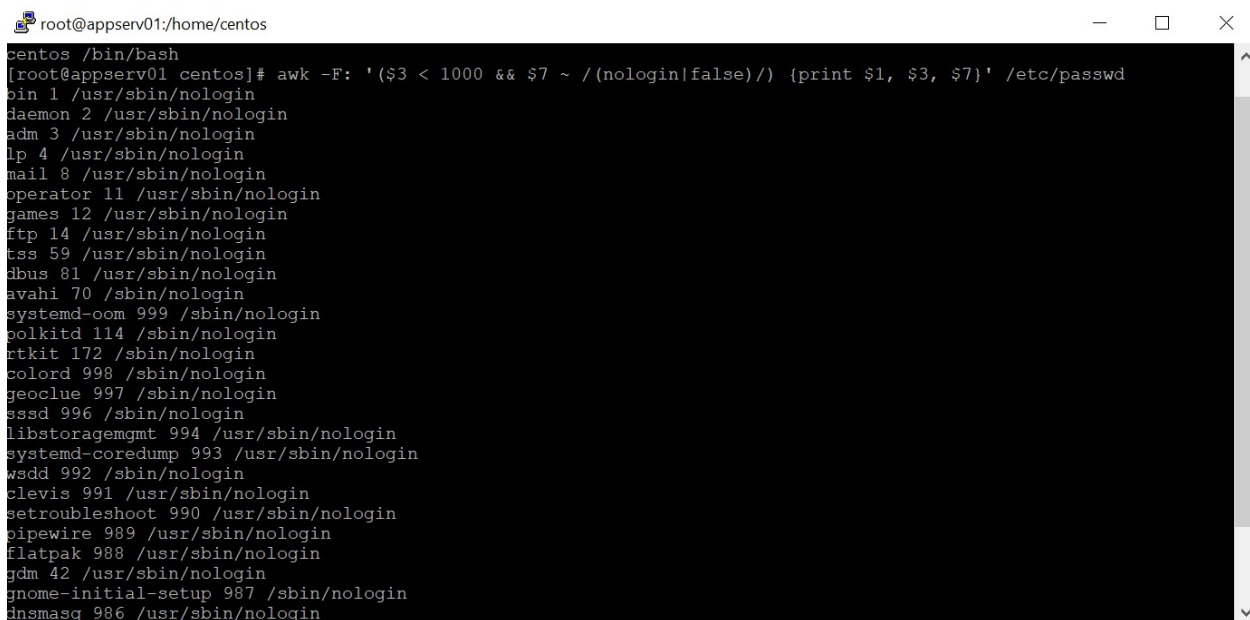
```
awk -F: '($7 !~ /(nologin|false)/) {print $1, $3, $7}' /etc/passwd
```



```
root@appserv01:/home/centos
[root@appserv01 centos]# awk -F: '/\bin\/bash|\bin\/sh|\bin\/zsh/ {print $1, $7}' /etc/passwd
root /bin/bash
centos /bin/bash
[root@appserv01 centos]#
```

Utilisons la commande suivante pour afficher les comptes de services restreints :

```
awk -F: '($3 < 1000 && $7 ~ /(nologin|false)/) {print $1, $3, $7}' /etc/passwd
```



```
root@appserv01:/home/centos
centos /bin/bash
[root@appserv01 centos]# awk -F: '($3 < 1000 && $7 ~ /(nologin|false)/) {print $1, $3, $7}' /etc/passwd
bin 1 /usr/sbin/nologin
daemon 2 /usr/sbin/nologin
adm 3 /usr/sbin/nologin
lp 4 /usr/sbin/nologin
mail 8 /usr/sbin/nologin
operator 11 /usr/sbin/nologin
games 12 /usr/sbin/nologin
ftp 14 /usr/sbin/nologin
tss 59 /usr/sbin/nologin
dbus 81 /usr/sbin/nologin
avahi 70 /sbin/nologin
systemd-oom 999 /sbin/nologin
polkitd 114 /sbin/nologin
rtkit 172 /sbin/nologin
colord 998 /sbin/nologin
geoclue 997 /sbin/nologin
sssd 996 /sbin/nologin
libstoragemgmt 994 /usr/sbin/nologin
systemd-coredump 993 /usr/sbin/nologin
wssd 992 /sbin/nologin
clevis 991 /usr/sbin/nologin
setroubleshoot 990 /usr/sbin/nologin
pipewire 989 /usr/sbin/nologin
flatpak 988 /usr/sbin/nologin
gdm 42 /usr/sbin/nologin
gnome-initial-setup 987 /sbin/nologin
dnsmasq 986 /usr/sbin/nologin
```


Partie 2 – Mini-Projet

Scénario : Vous êtes nouvellement recruté comme Expert DevSecOps pour auditer et sécuriser un serveur Linux qui hébergera une application web sensible. Vous avez 2 heures pour effectuer un audit initial, corriger les problèmes, automatiser les vérifications, et valider le déploiement de l'application web.

1. Audit initial

- Collecte des informations système

Static hostname: appserv01
Icon name: computer-vm
Chassis: vm
Machine ID: 62eb5b346fac402395a6e54987cb60e1
Boot ID: 5364bfba0c8945cb982ccf7f8349fb29
Product UUID: c122aebd-c25d-6247-a2d3-e4f55b1c3f7c
Virtualization: microsoft
Operating System: CentOS Stream 10 (Coughlan)
CPE OS Name: cpe:/o:centos:centos:10
Kernel: Linux 6.12.0-66.el10.x86_64
Architecture: x86-64
Hardware Vendor: Microsoft Corporation
Hardware Model: Virtual Machine
Hardware Serial: 3000-8348-4950-9092-7574-6353-36
Firmware Version: 090008
Firmware Date: Fri 2018-12-07
Firmware Age: 6y 6month 1w 4d

Liste totale de service

UNIT	LOAD	ACTIVE	STATUS	DESCRIPTION
accounts-daemon.service	loaded	active	running	Accounts Service
alsa-restore.service	loaded	inactive	dead	Save/Restore Sound Card State
alsa-state.service	loaded	inactive	dead	Manage Sound Card State (restore and store)
atd.service	loaded	active	running	Deferred execution scheduler
audit-rules.service	loaded	inactive	dead	Load Audit Rules
auditd.service	loaded	active	running	Security Audit Logging Service
auto-cpufreq.service	not-found	inactive	dead	auto-cpufreq.service
autofs.service	not-found	inactive	dead	autofs.service
avahi-daemon.service	loaded	active	running	Avahi mDNS/DNS-SD Stack
blk-availability.service	loaded	inactive	dead	Availability of block devices
chronyd.service	loaded	active	running	NTP client/server
cloud-init-local.service	not-found	inactive	dead	cloud-init-local.service
cockpit-issue.service	loaded	inactive	dead	Cockpit issue updater service
cockpit-session-socket-user.service	loaded	inactive	dead	Dynamic user for /run/cockpit/session socket
cockpit-wsinstance-http.service	loaded	inactive	dead	Cockpit Web Service http instance
cockpit-wsinstance-socket-user.service	loaded	inactive	dead	Dynamic user for /run/cockpit/wsinstance/ sockets
cockpit.service	loaded	inactive	dead	Cockpit Web Service
colord.service	loaded	active	running	Manage, Install and Generate Color Profiles

cpupower.service	not-found	inactive	dead	cpupower.service
crond.service	loaded	active	running	Command Scheduler
cups.service	loaded	active	running	CUPS Scheduler
dbus-broker.service	loaded	active	running	D-Bus System Message Bus
dm-event.service	loaded	inactive	dead	Device-mapper event daemon
dnf-makecache.service	loaded	inactive	dead	dnf makecache
dracut-cmdline.service	loaded	inactive	dead	dracut cmdline hook
dracut-initqueue.service	loaded	inactive	dead	dracut initqueue hook
dracut-mount.service	loaded	inactive	dead	dracut mount hook
dracut-pre-mount.service	loaded	inactive	dead	dracut pre-mount hook
dracut-pre-pivot.service	loaded	inactive	dead	dracut pre-pivot and cleanup hook
dracut-pre-trigger.service	loaded	inactive	dead	dracut pre-trigger hook
dracut-pre-udev.service	loaded	inactive	dead	dracut pre-udev hook
dracut-shutdown-onfailure.service	loaded	inactive	dead	Service executing upon dracut-shutdown failure to perform cleanup
dracut-shutdown.service	loaded	active	exited	Restore /run/initramfs on shutdown
ebtables.service	not-found	inactive	dead	ebtables.service
emergency.service	loaded	inactive	dead	Emergency Shell
fcoe.service	not-found	inactive	dead	fcoe.service
fips-crypto-policy-overlay.service	loaded	inactive	dead	Bind-mount FIPS crypto-policy in FIPS mode
firewalld.service	loaded	active	running	firewalld - dynamic firewall daemon
fstrim.service	loaded	inactive	dead	Discard unused blocks on filesystems from /etc/fstab
fwupd-refresh.service	loaded	inactive	dead	Refresh fwupd metadata and update motd
fwupd.service	loaded	active	running	Firmware update daemon
gdm.service	loaded	active	running	GNOME Display Manager
getty@tty1.service	loaded	inactive	dead	Getty on tty1
hypervkvpd.service	loaded	active	running	Hyper-V KVP daemon
hypervvssd.service	loaded	active	running	Hyper-V VSS daemon
initrd-cleanup.service	loaded	inactive	dead	Cleaning Up and Shutting Down Daemons
initrd-parse-etc.service	loaded	inactive	dead	Mountpoints Configured in the Real Root
initrd-switch-root.service	loaded	inactive	dead	Switch Root
initrd-udevadm-cleanup-db.service	loaded	inactive	dead	Cleanup udev Database
ip6tables.service	not-found	inactive	dead	ip6tables.service
ipset.service	not-found	inactive	dead	ipset.service
iptables.service	not-found	inactive	dead	iptables.service
irqbalance.service	loaded	active	running	irqbalance daemon
iscsi-init.service	loaded	inactive	dead	One time configuration for iscsi.service
iscsi-onboot.service	loaded	inactive	dead	Special handling of early boot iSCSI sessions
iscsi-shutdown.service	loaded	inactive	dead	Logout off all iSCSI sessions on shutdown
iscsi-starter.service	loaded	inactive	dead	iscsi-starter.service
iscsi.service	loaded	inactive	dead	Login and scanning of iSCSI devices
iscsid.service	loaded	inactive	dead	Open-iSCSI
iscsiuio.service	loaded	inactive	dead	iSCSI UserSpace I/O driver

kdump.service	loaded	active	exited	Crash recovery kernel arming
kmmod-static-nodes.service	loaded	active	exited	Create List of Static Device Nodes
ldconfig.service	loaded	inactive	dead	Rebuild Dynamic Linker Cache
libstoragemgmt.service	loaded	active	running	libstoragemgmt plug-in server daemon
logrotate.service	loaded	inactive	dead	Rotate log files
lvm2-activation-early.service	not-found	inactive	dead	lvm2-activation-early.service
lvm2-lvmpolld.service	loaded	inactive	dead	LVM2 poll daemon
lvm2-monitor.service	loaded	active	exited	Monitoring of LVM2 mirrors, snapshots etc. using dmeventd or progress polling
mcelog.service	loaded	active	running	Machine Check Exception Logging Daemon
mdmonitor.service	loaded	inactive	dead	Software RAID monitoring and management
ModemManager.service	loaded	active	running	Modem Manager
modprobe@configfs.service	loaded	inactive	dead	Load Kernel Module configfs
modprobe@dm_mod.service	loaded	inactive	dead	Load Kernel Module dm_mod
modprobe@dm_multipath.service	loaded	inactive	dead	Load Kernel Module dm_multipath
modprobe@drm.service	loaded	inactive	dead	Load Kernel Module drm
modprobe@efi_pstore.service	loaded	inactive	dead	Load Kernel Module efi_pstore
modprobe@fuse.service	loaded	inactive	dead	Load Kernel Module fuse
modprobe@loop.service	loaded	inactive	dead	Load Kernel Module loop
multipathd.service	loaded	inactive	dead	Device-Mapper Multipath Device Controller
NetworkManager-wait-online.service	loaded	active	exited	Network Manager Wait Online
NetworkManager.service	loaded	active	running	Network Manager
nsd.service	not-found	inactive	dead	nsd.service
ntpd.service	not-found	inactive	dead	ntpd.service
ntpdate.service	not-found	inactive	dead	ntpdate.service
nvme-fc-boot-connections.service	loaded	inactive	dead	Auto-connect to subsystems on FC-NVME devices found during boot
pcsd.service	loaded	inactive	dead	PC/SC Smart Card Daemon
plocate-updatedb.service	loaded	inactive	dead	Update the plocate database
plymouth-quit-wait.service	loaded	active	exited	Hold until boot process finishes up
plymouth-quit.service	loaded	inactive	dead	Terminate Plymouth Boot Screen
plymouth-read-write.service	loaded	active	exited	Tell Plymouth To Write Out Runtime Data
plymouth-start.service	loaded	active	exited	Show Plymouth Boot Screen
plymouth-switch-root.service	loaded	inactive	dead	Plymouth switch root service
polkit.service	loaded	active	running	Authorization Manager
power-profiles-daemon.service	not-found	inactive	dead	power-profiles-daemon.service
raid-check.service	loaded	inactive	dead	RAID setup health check
rbdmap.service	not-found	inactive	dead	rbdmap.service
rc-local.service	loaded	inactive	dead	/etc/rc.d/rc.local Compatibility
rescue.service	loaded	inactive	dead	Rescue Shell
rpmdb-migrate.service	loaded	inactive	dead	RPM database migration to /usr
rpmdb-rebuild.service	loaded	inactive	dead	RPM database rebuild
rsyslog.service	loaded	active	running	System Logging Service
rtkit-daemon.service	loaded	active	running	RealtimeKit Scheduling Policy Service

selinux-autorelabel-mark.service	loaded	inactive	dead	Mark the need to relabel after reboot
smartd.service	loaded	inactive	dead	Self Monitoring and Reporting Technology (SMART) Daemon
sntp.service	not-found	inactive	dead	sntp.service
ssh-host-keys-migration.service	loaded	inactive	dead	Update OpenSSH host key permissions
sshd-keygen@ecdsa.service	loaded	inactive	dead	OpenSSH ecdsa Server Key Generation
sshd-keygen@ed25519.service	loaded	inactive	dead	OpenSSH ed25519 Server Key Generation
sshd-keygen@rsa.service	loaded	inactive	dead	OpenSSH rsa Server Key Generation
sshd.service	loaded	active	running	OpenSSH server daemon
sssd-kcm.service	loaded	inactive	dead	SSSD Kerberos Cache Manager
sssd.service	loaded	inactive	dead	System Security Services Daemon
switcheroo-control.service	loaded	active	running	Switcheroo Control Proxy service
syslog.service	not-found	inactive	dead	syslog.service
systemd-ask-password-console.service	loaded	inactive	dead	Dispatch Password Requests to Console
systemd-ask-password-plymouth.service	loaded	inactive	dead	Forward Password Requests to Plymouth
systemd-ask-password-wall.service	loaded	inactive	dead	Forward Password Requests to Wall
systemd-battery-check.service	loaded	inactive	dead	Check battery level during early boot
systemd-binfmt.service	loaded	inactive	dead	Set Up Additional Binary Formats
systemd-boot-random-seed.service	loaded	inactive	dead	Update Boot Loader Random Seed
systemd-conftxt.service	loaded	inactive	dead	Merge System Configuration Images into /etc/
systemd-coredump@0-10319-0.service	loaded	failed	failed	Process Core Dump (PID 10319/UID 0)
systemd-coredump@1-10317-0.service	loaded	failed	failed	Process Core Dump (PID 10317/UID 0)
systemd-coredump@13-11716-0.service	loaded	failed	failed	Process Core Dump (PID 11716/UID 0)
systemd-coredump@14-11713-0.service	loaded	failed	failed	Process Core Dump (PID 11713/UID 0)
systemd-coredump@15-11712-0.service	loaded	failed	failed	Process Core Dump (PID 11712/UID 0)
systemd-coredump@16-11715-0.service	loaded	failed	failed	Process Core Dump (PID 11715/UID 0)
systemd-coredump@17-11717-0.service	loaded	failed	failed	Process Core Dump (PID 11717/UID 0)
systemd-coredump@18-11758-0.service	loaded	failed	failed	Process Core Dump (PID 11758/UID 0)
systemd-coredump@19-11759-0.service	loaded	failed	failed	Process Core Dump (PID 11759/UID 0)
systemd-coredump@20-11761-0.service	loaded	failed	failed	Process Core Dump (PID 11761/UID 0)
systemd-coredump@21-11760-0.service	loaded	failed	failed	Process Core Dump (PID 11760/UID 0)
systemd-coredump@22-11765-0.service	loaded	failed	failed	Process Core Dump (PID 11765/UID 0)
systemd-coredump@23-11766-0.service	loaded	failed	failed	Process Core Dump (PID 11766/UID 0)
systemd-coredump@24-11846-0.service	loaded	failed	failed	Process Core Dump (PID 11846/UID 0)
systemd-coredump@25-11847-0.service	loaded	failed	failed	Process Core Dump (PID 11847/UID 0)
systemd-coredump@26-11845-0.service	loaded	failed	failed	Process Core Dump (PID 11845/UID 0)
systemd-coredump@27-11848-0.service	loaded	failed	failed	Process Core Dump (PID 11848/UID 0)
systemd-coredump@28-11850-0.service	loaded	failed	failed	Process Core Dump (PID 11850/UID 0)
systemd-coredump@29-11849-0.service	loaded	failed	failed	Process Core Dump (PID 11849/UID 0)
systemd-coredump@3-10321-0.service	loaded	failed	failed	Process Core Dump (PID 10321/UID 0)
systemd-coredump@30-11969-0.service	loaded	failed	failed	Process Core Dump (PID 11969/UID 0)
systemd-coredump@31-11966-0.service	loaded	failed	failed	Process Core Dump (PID 11966/UID 0)
systemd-coredump@32-11971-0.service	loaded	failed	failed	Process Core Dump (PID 11971/UID 0)

systemd-coredump@36-12638-0.service	loaded	failed	failed	Process Core Dump (PID 12638/UID 0)
systemd-coredump@37-12639-0.service	loaded	failed	failed	Process Core Dump (PID 12639/UID 0)
systemd-coredump@38-12662-0.service	loaded	failed	failed	Process Core Dump (PID 12662/UID 0)
systemd-coredump@39-12665-0.service	loaded	failed	failed	Process Core Dump (PID 12665/UID 0)
systemd-coredump@4-10324-0.service	loaded	failed	failed	Process Core Dump (PID 10324/UID 0)
systemd-coredump@40-12664-0.service	loaded	failed	failed	Process Core Dump (PID 12664/UID 0)
systemd-coredump@5-10325-0.service	loaded	failed	failed	Process Core Dump (PID 10325/UID 0)
systemd-coredump@78-68803-0.service	loaded	failed	failed	Process Core Dump (PID 68803/UID 0)
systemd-coredump@82-118196-0.service	loaded	failed	failed	Process Core Dump (PID 118196/UID 0)
systemd-coredump@83-118198-0.service	loaded	failed	failed	Process Core Dump (PID 118198/UID 0)
systemd-coredump@84-118195-0.service	loaded	failed	failed	Process Core Dump (PID 118195/UID 0)
systemd-coredump@85-118197-0.service	loaded	failed	failed	Process Core Dump (PID 118197/UID 0)
systemd-coredump@86-118199-0.service	loaded	failed	failed	Process Core Dump (PID 118199/UID 0)
systemd-coredump@87-118229-0.service	loaded	failed	failed	Process Core Dump (PID 118229/UID 0)
systemd-coredump@88-118654-0.service	loaded	failed	failed	Process Core Dump (PID 118654/UID 0)
systemd-coredump@89-118720-0.service	loaded	failed	failed	Process Core Dump (PID 118720/UID 0)
systemd-firstboot.service	loaded	inactive	dead	First Boot Wizard
systemd-fsck-root.service	loaded	inactive	dead	File System Check on Root Device
systemd-hibernate-clear.service	loaded	inactive	dead	Clear Stale Hibernation Storage Info
systemd-hibernate-resume.service	loaded	inactive	dead	Resume from hibernation
systemd-hostnamed.service	loaded	inactive	dead	Hostname Service
systemd-hwdb-update.service	loaded	inactive	dead	Rebuild Hardware Database
systemd-initctl.service	loaded	inactive	dead	initctl Compatibility Daemon
systemd-journal-catalog-update.service	loaded	inactive	dead	Rebuild Journal Catalog
systemd-journal-flush.service	loaded	active	exited	Flush Journal to Persistent Storage
systemd-journald.service	loaded	active	running	Journal Service
systemd-logind.service	loaded	active	running	User Login Management
systemd-machine-id-commit.service	loaded	inactive	dead	Save Transient machine-id to Disk
systemd-modules-load.service	loaded	active	exited	Load Kernel Modules
systemd-network-generator.service	loaded	active	exited	Generate network units from Kernel command line
systemd-oomd.service	not-found	inactive	dead	systemd-oomd.service
systemd-pcrmachine.service	loaded	inactive	dead	TPM PCR Machine ID Measurement
systemd-pcrphase-initrd.service	loaded	inactive	dead	TPM PCR Barrier (initrd)
systemd-pcrphase-sysinit.service	loaded	inactive	dead	TPM PCR Barrier (Initialization)
systemd-pcrphase.service	loaded	inactive	dead	TPM PCR Barrier (User)
systemd-pstore.service	loaded	inactive	dead	Platform Persistent Storage Archival
systemd-quotacheck-root.service	loaded	inactive	dead	Root File System Quota Check
systemd-random-seed.service	loaded	active	exited	Load/Save OS Random Seed
systemd-remount-fs.service	loaded	active	exited	Remount Root and Kernel File Systems
systemd-repart.service	loaded	inactive	dead	Repartition Root Disk
systemd-rfkill.service	loaded	inactive	dead	Load/Save RF Kill Switch Status

systemd-soft-reboot.service	loaded	inactive	dead	Reboot System Userspace
systemd-sysctl.service	loaded	active	exited	Apply Kernel Variables
systemd-sysext.service	loaded	inactive	dead	Merge System Extension Images into /usr/ and /opt/
systemd-sysusers.service	loaded	inactive	dead	Create System Users
systemd-timesyncd.service	not-found	inactive	dead	systemd-timesyncd.service
systemd-tmpfiles-clean.service	loaded	inactive	dead	Cleanup of Temporary Directories
systemd-tmpfiles-setup-dev-early.service	loaded	active	exited	Create Static Device Nodes in /dev gracefully
systemd-tmpfiles-setup-dev.service	loaded	active	exited	Create Static Device Nodes in /dev
systemd-tmpfiles-setup.service	loaded	active	exited	Create System Files and Directories
systemd-tpm2-setup-early.service	loaded	inactive	dead	Early TPM SRK Setup
systemd-tpm2-setup.service	loaded	inactive	dead	TPM SRK Setup
systemd-udev-load-credentials.service	loaded	active	exited	Load udev Rules from Credentials
systemd-udev-settle.service	loaded	inactive	dead	Wait for udev To Complete Device Initialization
systemd-udev-trigger.service	loaded	active	exited	Coldplug All udev Devices
systemd-udevd.service	loaded	active	running	Rule-based Manager for Device Events and Files
systemd-update-done.service	loaded	inactive	dead	Update is Completed
systemd-update-utmp-runlevel.service	loaded	inactive	dead	Record Runlevel Change in UTMP
systemd-update-utmp.service	loaded	active	exited	Record System Boot/Shutdown in UTMP
systemd-user-sessions.service	loaded	active	exited	Permit User Sessions
systemd-userdbd.service	loaded	active	running	User Database Manager
systemd-vconsole-setup.service	loaded	active	exited	Virtual Console Setup
tlp.service	not-found	inactive	dead	tlp.service
tuned-ppd.service	loaded	active	running	PPD-to-TuneD API Translation Daemon
tuned.service	loaded	active	running	Dynamic System Tuning Daemon
udisks2.service	loaded	active	running	Disk Manager
upower.service	loaded	active	running	Daemon for power management
user-runtime-dir@1000.service	loaded	active	exited	User Runtime Directory /run/user/1000
user-runtime-dir@42.service	loaded	active	exited	User Runtime Directory /run/user/42
user@1000.service	loaded	active	running	User Manager for UID 1000
user@42.service	loaded	active	running	User Manager for UID 42
vgauthd.service	loaded	inactive	dead	VGAuth Service for open-vm-tools
vmtoolsd.service	loaded	inactive	dead	Service for virtual machines hosted on VMware
wpa_supplicant.service	loaded	active	running	WPA supplicant
ypbind.service	not-found	inactive	dead	ypbind.service

- **Vérification des utilisateurs, groupes, permissions sensibles**

Liste des utilisateurs avec un **shell de connexion** : **root, sync, shutdown, halt, centos**

```
[root@appserv01 centos]# awk -F: '($7 != /(nologin|false)/) {print $1, $3, $7}' /etc/passwd
root 0 /bin/bash
sync 5 /bin/sync
shutdown 6 /sbin/shutdown
halt 7 /sbin/halt
centos 1000 /bin/bash
[root@appserv01 centos]#
```

Liste des comptes UID=0 (root ou autre !) : root

```
[root@appserv01 centos]# awk -F: '($3 == 0) {print $1, $3, $7}' /etc/passwd
root 0 /bin/bash
[root@appserv01 centos]#
```

Liste des comptes expirés ou verrouillés : (L : verrouillé ou expiré) (P : actif)


Accounts	Status	Date of last password change
root	P	never
centos	P	2025-04-11
bin	L	2024-10-29
daemon	L	2024-10-29
adm	L	2024-10-29
lp	L	2024-10-29
sync	L	2024-10-29
shutdown	L	2024-10-29
halt	L	2024-10-29
mail	L	2024-10-29
operator	L	2024-10-29
games	L	2024-10-29
ftp	L	2024-10-29
nobody	L	2024-10-29
tss	L	2025-04-11
dbus	L	2025-04-11
avahi	L	2025-04-11
systemd-oom	L	2025-04-11
polkitd	L	2025-04-11
rtkit	L	2025-04-11
colord	L	2025-04-11
geoclue	L	2025-04-11
sssd	L	2025-04-11
libstoragemgmt	L	2025-04-11
systemd-coredump	L	2025-04-11
wsdd	L	2025-04-11
clevis	L	2025-04-11
setroubleshoot	L	2025-04-11
pipewire	L	2025-04-11
flatpak	L	2025-04-11

```
root@appserv01:/home/centos

[root@appserv01 centos]# sudo passwd -S -a | grep ' L '
bin L 2024-10-29 0 99999 7 -1
daemon L 2024-10-29 0 99999 7 -1
adm L 2024-10-29 0 99999 7 -1
lp L 2024-10-29 0 99999 7 -1
sync L 2024-10-29 0 99999 7 -1
shutdown L 2024-10-29 0 99999 7 -1
halt L 2024-10-29 0 99999 7 -1
mail L 2024-10-29 0 99999 7 -1
operator L 2024-10-29 0 99999 7 -1
games L 2024-10-29 0 99999 7 -1
ftp L 2024-10-29 0 99999 7 -1
nobody L 2024-10-29 0 99999 7 -1
tss L 2025-04-11 -1 -1 -1 -1
dbus L 2025-04-11 -1 -1 -1 -1
avahi L 2025-04-11 -1 -1 -1 -1
systemd-oom L 2025-04-11 -1 -1 -1 -1
polkitd L 2025-04-11 -1 -1 -1 -1
rtkit L 2025-04-11 -1 -1 -1 -1
colord L 2025-04-11 -1 -1 -1 -1
geoclue L 2025-04-11 -1 -1 -1 -1
sssd L 2025-04-11 -1 -1 -1 -1
libstoragemgmt L 2025-04-11 -1 -1 -1 -1
systemd-coredump L 2025-04-11 -1 -1 -1 -1
wsdd L 2025-04-11 -1 -1 -1 -1
clevis L 2025-04-11 -1 -1 -1 -1
setroubleshoot L 2025-04-11 -1 -1 -1 -1
pipewire L 2025-04-11 -1 -1 -1 -1
flatpak L 2025-04-11 -1 -1 -1 -1
gdm L 2025-04-11 -1 -1 -1 -1
gnome-initial-setup L 2025-04-11 -1 -1 -1 -1
dnsmasq L 2025-04-11 -1 -1 -1 -1
sshd L 2025-04-11 -1 -1 -1 -1
chrony L 2025-04-11 -1 -1 -1 -1
tcpdump L 2025-04-11 -1 -1 -1 -1
gnome-remote-desktop L 2025-04-11 -1 -1 -1 -1
xterm L 2025-06-18 0 99999 7 -1
```


gdm	L	2025-04-11
gnome-initial-setup	L	2025-04-11
dnsmasq	L	2025-04-11
sshd	L	2025-04-11
chrony	L	2025-04-11
tcpdump	L	2025-04-11
gnome-remote-desktop	L	2025-04-11
xterm	L	2025-06-18

Liste des membres du groupe **wheel** (**sudoers** par défaut sur CentOS) : centos

 root@appserv01:/home/centos

```
[root@appserv01 centos]# getent group wheel
wheel:x:10:centos
[root@appserv01 centos]#
```

Liste des **sudoers** configurés dans **/etc/sudoers** : **root**, **wheel**

 root@appserv01:/home/centos

```
[root@appserv01 centos]# sudo grep -vE '^#|^$' /etc/sudoers
Defaults    !visiblepw
Defaults    always_set_home
Defaults    match_group_by_gid
Defaults    always_query_group_plugin
Defaults    env_reset
Defaults    env_keep = "COLORS DISPLAY HOSTNAME HISTSIZE KDEDIR LS_COLORS"
Defaults    env_keep += "MAIL PS1 PS2 QTDIR USERNAME LANG LC_ADDRESS LC_CTYPE"
Defaults    env_keep += "LC_COLLATE LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES"
Defaults    env_keep += "LC_MONETARY LC_NAME LC_NUMERIC LC_PAPER LC_TELEPHONE"
Defaults    env_keep += "LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET XAUTHORITY"
Defaults    secure_path = /sbin:/bin:/usr/sbin:/usr/bin
root        ALL=(ALL)        ALL
%wheel      ALL=(ALL)        ALL
[root@appserv01 centos]#
```

- **Vérification des permissions sensibles**

Fichiers en mode SUID (exécutés avec droits de leur propriétaire) :

/usr/lib/polkit-1/polkit-agent-helper-1

/usr/bin/umount

/usr/bin/fusermount3

/usr/bin/chage

/usr/bin/gpasswd

/usr/bin/newgrp

/usr/bin/passwd

/usr/bin/mount

/usr/bin/chfn

/usr/bin/chsh

/usr/bin/su

/usr/bin/pkexec


/usr/bin/crontab

/usr/bin/sudo

/usr/bin/at


```
[root@appserv01 centos]# find / -perm -4000 -type f 2>/dev/null
/usr/lib/polkit-1/polkit-agent-helper-1
/usr/bin/umount
/usr/bin/fusermount3
/usr/bin/chage
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/passwd
/usr/bin/mount
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/su
/usr/bin/pkexec
/usr/bin/crontab
/usr/bin/sudo
/usr/bin/at
/usr/bin/vmware-user-suid-wrapper
/usr/sbin/pam_timestamp_check
/usr/sbin/unix_chkpwd
/usr/sbin/grub2-set-bootflag
/usr/libexec/libgtop_server2
/usr/libexec/dbus-1/dbus-daemon-launch-helper
[root@appserv01 centos]#
```

Fichiers en mode **SGID**: /usr/bin/write /usr/bin/plocate, /usr/sbin/lockdev, /usr/libexec/utempter/utempter

 root@appserv01:/home/centos

```
[root@appserv01 centos]# find / -perm -2000 -type f 2>/dev/null
/usr/bin/write
/usr/bin/plocate
/usr/sbin/lockdev
/usr/libexec/utempter/utempter
[root@appserv01 centos]#
```

Fichiers et répertoire avec des permissions **world-writable** :


 root@appserv01:/home/centos

```
[root@appserv01 centos]# find / -xdev -type f -perm -o+w -print 2>/dev/null
[root@appserv01 centos]# find / -xdev -type d -perm -o+w -print 2>/dev/null
/tmp
/tmp/.X11-unix
/tmp/.ICE-unix
/tmp/systemd-private-5364bfba0c8945cb982ccf7f8349fb29-dbus-broker.service-jbzD3g/tmp
/tmp/systemd-private-5364bfba0c8945cb982ccf7f8349fb29-chronyd.service-Vkx8Uu/tmp
/tmp/systemd-private-5364bfba0c8945cb982ccf7f8349fb29-irqbalance.service-x4tBKF/tmp
/tmp/systemd-private-5364bfba0c8945cb982ccf7f8349fb29-polkit.service-3SyKo3/tmp
/tmp/systemd-private-5364bfba0c8945cb982ccf7f8349fb29-rtkit-daemon.service-fraVKp/tmp
/tmp/systemd-private-5364bfba0c8945cb982ccf7f8349fb29-switcheroo-control.service-DZbbqz/tmp
/tmp/systemd-private-5364bfba0c8945cb982ccf7f8349fb29-upower.service-7gjNnf/tmp
/tmp/systemd-private-5364bfba0c8945cb982ccf7f8349fb29-ModemManager.service-dM1TE6/tmp
/tmp/systemd-private-5364bfba0c8945cb982ccf7f8349fb29-colord.service-Ra2Wfe/tmp
/tmp/systemd-private-5364bfba0c8945cb982ccf7f8349fb29-systemd-logind.service-TmEzOA/tmp
/tmp/systemd-private-5364bfba0c8945cb982ccf7f8349fb29-fwupd.service-wFsZsm/tmp
/var/tmp
/var/tmp/systemd-private-5364bfba0c8945cb982ccf7f8349fb29-dbus-broker.service-7AOYKI/tmp
/var/tmp/systemd-private-5364bfba0c8945cb982ccf7f8349fb29-chronyd.service-haug7E/tmp
/var/tmp/systemd-private-5364bfba0c8945cb982ccf7f8349fb29-irqbalance.service-Bax0fb/tmp
/var/tmp/systemd-private-5364bfba0c8945cb982ccf7f8349fb29-polkit.service-JwutY0/tmp
/var/tmp/systemd-private-5364bfba0c8945cb982ccf7f8349fb29-rtkit-daemon.service-Nogi2D/tmp
/var/tmp/systemd-private-5364bfba0c8945cb982ccf7f8349fb29-switcheroo-control.service-rBg2gy/tmp
/var/tmp/systemd-private-5364bfba0c8945cb982ccf7f8349fb29-upower.service-le67td/tmp
/var/tmp/systemd-private-5364bfba0c8945cb982ccf7f8349fb29-ModemManager.service-JICymR/tmp
/var/tmp/systemd-private-5364bfba0c8945cb982ccf7f8349fb29-colord.service-7k0dlj/tmp
/var/tmp/systemd-private-5364bfba0c8945cb982ccf7f8349fb29-fwupd.service-dbkDnl/tmp
/var/tmp/systemd-private-5364bfba0c8945cb982ccf7f8349fb29-systemd-logind.service-AmkQUP/tmp
[root@appserv01 centos]#
```

```
/tmp
/tmp/.X11-unix
/tmp/.ICE-unix
/tmp/systemd-private-5364bfba0c8945cb982ccf7f8349fb29-dbus-broker.service-jbzD3g/tmp
/tmp/systemd-private-5364bfba0c8945cb982ccf7f8349fb29-chrond.service-Vkx8Uu/tmp
/tmp/systemd-private-5364bfba0c8945cb982ccf7f8349fb29-irqbalance.service-x4tBKF/tmp
/tmp/systemd-private-5364bfba0c8945cb982ccf7f8349fb29-polkit.service-3SyKo3/tmp
/tmp/systemd-private-5364bfba0c8945cb982ccf7f8349fb29-rtkit-daemon.service-fraVKp/tmp
/tmp/systemd-private-5364bfba0c8945cb982ccf7f8349fb29-switcheroo-control.service-DZbbqz/tmp
/tmp/systemd-private-5364bfba0c8945cb982ccf7f8349fb29-upower.service-7gjNnf/tmp
/tmp/systemd-private-5364bfba0c8945cb982ccf7f8349fb29-ModemManager.service-dM1TE6/tmp
/tmp/systemd-private-5364bfba0c8945cb982ccf7f8349fb29-colord.service-Ra2Wfe/tmp
/tmp/systemd-private-5364bfba0c8945cb982ccf7f8349fb29-systemd-logind.service-TmEzOA/tmp
/tmp/systemd-private-5364bfba0c8945cb982ccf7f8349fb29-fwupd.service-wFsZsm/tmp
/var/tmp
/var/tmp/systemd-private-5364bfba0c8945cb982ccf7f8349fb29-dbus-broker.service-7AOYKI/tmp
/var/tmp/systemd-private-5364bfba0c8945cb982ccf7f8349fb29-chrond.service-hauq7E/tmp
/var/tmp/systemd-private-5364bfba0c8945cb982ccf7f8349fb29-irqbalance.service-Bax0fb/tmp
/var/tmp/systemd-private-5364bfba0c8945cb982ccf7f8349fb29-polkit.service-JwutY0/tmp
/var/tmp/systemd-private-5364bfba0c8945cb982ccf7f8349fb29-rtkit-daemon.service-Nogi2D/tmp
/var/tmp/systemd-private-5364bfba0c8945cb982ccf7f8349fb29-switcheroo-control.service-
rBg2gy/tmp
/var/tmp/systemd-private-5364bfba0c8945cb982ccf7f8349fb29-upower.service-le67td/tmp
/var/tmp/systemd-private-5364bfba0c8945cb982ccf7f8349fb29-ModemManager.service-
```

- Vérification des accès **root** implicites : **centos**

```
sudo grep -r " /etc/sudoers /etc/sudoers.d/ 2>/dev/null
```

 root@appserv01:/home/centos

```
[root@appserv01 centos]# grep -E 'wheel|sudo' /etc/group
wheel:x:10:centos
[root@appserv01 centos]#
```

- Vérification d'autres accès implicites pour faire un **shutdown**: RAS

```
[root@appserv01 centos]# grep -E 'users|shutdown' /etc/group
users:x:100:
[root@appserv01 centos]# getent group users
users:x:100:
[root@appserv01 centos]#
```

- **État des services en cours**

UNIT	LOAD	ACTIVE	STATUS	DESCRIPTION
accounts-daemon.service	loaded	active	running	Accounts Service
atd.service	loaded	active	running	Deferred execution scheduler
auditd.service	loaded	active	running	Security Audit Logging Service
avahi-daemon.service	loaded	active	running	Avahi mDNS/DNS-SD Stack
chronyd.service	loaded	active	running	NTP client/server
colord.service	loaded	active	running	Manage, Install and Generate Color Profiles
cron.service	loaded	active	running	Command Scheduler
cups.service	loaded	active	running	CUPS Scheduler
dbus-broker.service	loaded	active	running	D-Bus System Message Bus
firewalld.service	loaded	active	running	firewalld - dynamic firewall daemon
fwupd.service	loaded	active	running	Firmware update daemon
gdm.service	loaded	active	running	GNOME Display Manager
hypervkvpd.service	loaded	active	running	Hyper-V KVP daemon
hypervvssd.service	loaded	active	running	Hyper-V VSS daemon
irqbalance.service	loaded	active	running	irqbalance daemon
libstoragemgmt.service	loaded	active	running	libstoragemgmt plug-in server daemon
mcelog.service	loaded	active	running	Machine Check Exception Logging Daemon
ModemManager.service	loaded	active	running	Modem Manager
NetworkManager.service	loaded	active	running	Network Manager
polkit.service	loaded	active	running	Authorization Manager
rsyslog.service	loaded	active	running	System Logging Service
rtdk-daemon.service	loaded	active	running	RealtimeKit Scheduling Policy Service
sshd.service	loaded	active	running	OpenSSH server daemon
switcheroo-control.service	loaded	active	running	Switcheroo Control Proxy service
systemd-journald.service	loaded	active	running	Journal Service
systemd-logind.service	loaded	active	running	User Login Management
systemd-udev.service	loaded	active	running	Rule-based Manager for Device Events and Files
systemd-userdbd.service	loaded	active	running	User Database Manager
tuned-ppd.service	loaded	active	running	PPD-to-Tuned API Translation Daemon

tuned.service	loaded	active	running	Dynamic System Tuning Daemon
udisks2.service	loaded	active	running	Disk Manager
upower.service	loaded	active	running	Daemon for power management
user@1000.service	loaded	active	running	User Manager for UID 1000
user@42.service	loaded	active	running	User Manager for UID 42
wpa_supplicant.service	loaded	active	running	WPA supplicant

- Identification des anomalies ou failles potentielles

✓ SERVICES NORMAUX & JUSTIFIÉS

Services	Commentaires
auditd	Important pour la journalisation sécurité
firewalld	OK (pare-feu actif, bon point)
sshd	OK, service SSH légitime
chronyd	OK, pour la synchro NTP
crond	OK, planification des tâches
rsyslog	OK, gestion classique des logs
dbus-broker, systemd-journald, systemd-logind, systemd-udev	OK, services système indispensables
polkit	OK, pour la gestion des autorisations
tuned, irqbalance	OK, optimisation des performances
NetworkManager	OK, gestion des interfaces réseau
auditd	OK, journalisation de la sécurité
sshd	OK, SSH Server
gdm	OK, car le serveur avec interface graphique GNOME
colord	Gestion des profils de couleur → inutile sur serveur sans interface graphique
hypervkvpd et hypervvssd	Outils spécifiques Hyper-V, garder seulement si serveur tourne sur Hyper-V
udisks2.service	Gestion des disques pour utilisateurs (souvent pour GUI)

⚠ SERVICES À ÉVALUER SELON LE CONTEXTE

Services	Commentaires
avahi-daemon	Découverte réseau mDNS (Zeroconf), inutile/risqué sur serveur en prod
cups.service	Impression réseau, inutile sur serveur non dédié à l'impression
fwupd.service	Mise à jour firmware, dépend du contexte, désactiver si non utilisé
ModemManager.service	Support modem 3G/4G, inutile sur serveur
upower.service	Gestion de l'énergie (utile sur laptop, inutile sur serveur)
switcheroo-control	Pour les GPU hybrides, inutile sur serveur
wpa_supplicant	Pour wifi, inutile sur serveur câblé

SERVICES QUI PEUVENT POSER RISQUE SI PAS JUSTIFIÉS

Services	Risques potentiels
avahi-daemon	Expose le service sur le réseau (multicast DNS) → surface d'attaque
cups.service	Expose un service d'impression inutile → possible point d'entrée
ModemManager.service	Expose ports pour modem → surface d'attaque réseau inutile
wpa_supplicant	Si le serveur ne fait pas de wifi → inutile

Résumé : Le serveur devant héberger l'application exécute des services non justifiés qui présentent des risques :

- avahi-daemon
- cups.service
- ModemManager.service
- upower.service
- switcheroo-control.service
- wpa_supplicant.service
- fwupd.service (si pas utilisé)

2. Corrections et durcissement

- Désactiver les services non essentiels

```
root@appserv01:/home/centos
[root@appserv01 centos]# systemctl disable avahi-daemon cups.service ModemManager.service switcheroo-control.service fwupd.service
Removed '/etc/systemd/system/sockets.target.wants/avahi-daemon.socket'.
Removed '/etc/systemd/system/sockets.target.wants/cups.socket'.
Removed '/etc/systemd/system/dbus-org.freedesktop.Avahi.service'.
Removed '/etc/systemd/system/multi-user.target.wants/avahi-daemon.service'.
Removed '/etc/systemd/system/multi-user.target.wants/ModemManager.service'.
Removed '/etc/systemd/system/multi-user.target.wants/cups.path'.
Removed '/etc/systemd/system/multi-user.target.wants/cups.service'.
Removed '/etc/systemd/system/graphical.target.wants/switcheroo-control.service'.
Removed '/etc/systemd/system/dbus-org.freedesktop.ModemManager1.service'.
Removed '/etc/systemd/system/printer.target.wants/cups.service'.
Disabling 'avahi-daemon.service', but its triggering units are still active:
avahi-daemon.socket
Disabling 'cups.service', but its triggering units are still active:
cups.socket, cups.path
[root@appserv01 centos]#
```

- Correction des permissions trop larges

RAS

```
root@appserv01:/home/centos
[root@appserv01 centos]# grep -E 'wheel|sudo' /etc/group
wheel:x:10:centos
[root@appserv01 centos]#
```




root@appserv01:/home/centos

```
[root@appserv01 centos]# getent group wheel
wheel:x:10:centos
[root@appserv01 centos]#
```

- Sécurisation des fichiers de configuration

Identification des fichiers de configuration sensibles

Emplacement	Contenu
/etc/ssh/sshd_config	Configuration SSH
/etc/passwd	Comptes utilisateurs
/etc/shadow	Hash de mots de passe
/etc/sudoers	Droits sudo
/etc/fstab	Points de montage
/etc/firewalld/	Configuration FirewallD

Vérification des permissions sur les fichiers et répertoires de configuration sensible

Fichiers/Répertoires	Permissions actuelles
/etc/fstab	-rw-r--r--. (644)
/etc/passwd	-rw-r--r--.(644)
/etc/shadow	-----.(000)
/etc/ssh/sshd_config	-rw-----.(600)
/etc/sudoers	-r--r-----.(440)
/etc/firewalld/firewalld.conf	-rw-r--r--. (644)
/etc/firewalld/helpers	drwxr-x---.(750)
/etc/firewalld/icmptypes	drwxr-x---.(750)
/etc/firewalld/ipsets	drwxr-x---.(750)
/etc/firewalld/policies	drwxr-x---.(750)
/etc/firewalld/services	drwxr-x---.(750)
/etc/firewalld/zones	drwxr-x---.(750)

Les permissions du fichier **/etc/shadow** ne sont pas normales car il reste même invisible pour l'utilisateur « root ».

Pour sécuriser d'avantage les fichiers de configurations, nous allons appliquer les permissions recommandées sur le fichier **/etc/shadow** (640).


```
root@appserv01:/home/centos
[root@appserv01 centos]# chmod 640 /etc/shadow
[root@appserv01 centos]# chown root /etc/shadow
[root@appserv01 centos]# ls -l /etc/shadow
-rw-r-----. 1 root root 1078 18 jun 14:47 /etc/shadow
[root@appserv01 centos]#
```

- **Vérification et renforcement de la configuration SSH (port, root login, authentification par clé)**

Exécution d'un petit script qui auditera les options du fichier `/etc/ssh/sshd_config` ou afin parcourir le fichier `/etc/ssh/sshd` ligne par ligne afin d'appliquer les recommandations de sécurité, ce script vérifie les lignes de configuration des options port de connexion, rootlogin, PasswordAuthentication, PubkeyAuthentication et x11Forwarding.

Script

```
#!/bin/bash

SSH_CONFIG="/etc/ssh/sshd_config"

echo "=== Vérification de la configuration SSH ==="

# Vérifier port

PORT=$(grep -i '^Port' "$SSH_CONFIG" | awk '{print $2}')

[ -z "$PORT" ] && PORT="22 (par défaut)"

echo "Port configuré : $PORT"

# Vérifier PermitRootLogin

ROOT_LOGIN=$(grep -i '^PermitRootLogin' "$SSH_CONFIG" | awk '{print $2}')

[ "$ROOT_LOGIN" == "no" ] && echo "Root login désactivé" || echo "Root login ACTIVÉ ($ROOT_LOGIN)"

# Vérifier PasswordAuthentication

PASS_AUTH=$(grep -i '^PasswordAuthentication' "$SSH_CONFIG" | awk '{print $2}')

[ "$PASS_AUTH" == "no" ] && echo "Authentification par mot de passe désactivée" || echo "Authentification par mot de passe ACTIVE ($PASS_AUTH)"

# Vérifier PubkeyAuthentication

PUBKEY_AUTH=$(grep -i '^PubkeyAuthentication' "$SSH_CONFIG" | awk '{print $2}')

[ "$PUBKEY_AUTH" == "yes" ] && echo "Authentification par clé PUBKEY activée" || echo "Authentification par clé désactivée"

# Vérifier Protocol

PROTOCOL=$(grep -i '^Protocol' "$SSH_CONFIG" | awk '{print $2}')

#[ "$PROTOCOL" == "2" ] && echo "Protocole SSH version 2 OK" || echo "Mauvais protocole SSH ($PROTOCOL)"

# Vérifier X11Forwarding

X11=$(grep -i '^X11Forwarding' "$SSH_CONFIG" | awk '{print $2}')

[ "$X11" == "no" ] && echo "X11Forwarding désactivé" || echo "X11Forwarding ACTIVÉ ($X11)"

echo "=== Vérification terminée ==="
```

```
[root@appserv01 .ssh]# /home/centos/check_ssh.sh
=== Vérification de la configuration SSH ===
Port configuré : 22 (par défaut)
/ Root login ACTIVE (prohibit-password)
/ Authentication par mot de passe ACTIVE (yes)
/ Authentication par clé désactivée
/ X11Forwarding ACTIVE (yes)
=== Vérification terminée ===
[root@appserv01 .ssh]#
```

Option	Situation actuelle	Recommandation
Port	22	À Changer
PermitRootLogin	prohibit-password	Mettre no
PasswordAuthentication	yes	Mettre no (si on privilégie clés SSH en place)
PubkeyAuthentication	yes	Mettre yes
X11Forwarding	yes	Mettre no
AllowUsers centos	Non défini	Défini les utilisateurs pouvant accéder

Application des recommandations pour renforcer la sécurité ssh : Port 2223, Restriction d'utilisateurs (Pour le moment sauf l'utilisateur **centos** est autorisé).

```
root@appserv01: ~/.ssh
[root@appserv01 .ssh]# systemctl restart sshd.service
[root@appserv01 .ssh]# cat /etc/ssh/sshd_config
# $OpenBSD: sshd_config,v 1.104 2021/07/02 05:11:21 dtucker Exp $

Include /etc/ssh/sshd_config.d/*.conf
AuthorizedKeysFile      /root/.ssh/authorized_keys
Port 2223
PermitRootLogin no
PasswordAuthentication no
PubkeyAuthentication yes
PermitEmptyPasswords no
LoginGraceTime 30
MaxAuthTries 3
MaxSessions 5
ClientAliveInterval 300
ClientAliveCountMax 2
UseDNS no
AllowAgentForwarding no
PermitTunnel no
AllowTcpForwarding no
Banner /etc/issue.net
X11Forwarding no
Subsystem sftp          /usr/libexec/openssh/sftp-server
AllowUsers centos
[root@appserv01 .ssh]#
```

```
centos@appserv01:~  
login as: centos  
Pre-authentication banner message from server:  
OS:CentOs Stream 10  
Kernel:6.12.0-66.el10.x86_64  
  
*****  
> **  
> * *  
> *  
> * AVERTISSEMENT : ACCES NON AUTORISE INTERDIT ! *  
> *  
> * *  
> *  
> * Ce système est uniquement destiné aux utilisateurs autorisés.*  
> *  
> * * Exclusif Lab.local * *  
> *  
> * Tout acces non autorisé est journalisé et auditer *  
> *  
> * *  
> *  
> *****  
> **  
End of banner message from server  
Authenticating with public key "rsa-key-20250619"  
Activate the web console with: systemctl enable --now cockpit.socket  
  
Last login: Sat Jun 21 05:08:14 2025 from 10.0.0.100  
[centos@appserv01 ~]$
```

```
[root@appserv01 .ssh]# /home/centos/check_ssh.sh  
=== Vérification de la configuration SSH ===  
Port configuré : 2223  
[x] Root login désactivé  
[x] Authentification par mot de passe ACTIVE (yes)  
[x] Authentification par clé PUBKEY activée  
[x] X11Forwarding désactivé  
=== Vérification terminée ===  
[root@appserv01 .ssh]#
```

3. Script d'audit automatisé

Un script Bash avec les fonctionnalités suivantes : Détection des fichiers SUID/SGID, Liste des permissions critiques (ex. : fichiers world-writable), Liste des utilisateurs à risque (ex. : root shells, no password), Liste des services actifs, Génération d'un rapport daté (/var/log/audit-YYYYMMDD.log).

```
root@appserv01/home/centos/Mini-Projet-DevSecOps/audit-securite  
[root@appserv01 audit-securite]# /usr/local/bin/audit.sh  
=====
```

Script d'audit de securité des services,des utilisateurs à risque, les permission sensibles

```
=====
```

Création du rapport dans /etc/log/
Temps écoulé : 00:00Le fichier rapport crée

```
=== 0. Détection des ports ouverts ===  
=== 1. Détection des fichiers SUID/SGID ===  
=== 2. Fichiers et répertoires world-writable ===  
Temps écoulé : 00:16 === 3. Utilisateurs à risque, analyse des groupes à privileges, comptes echus et permission des fichiers et repertoires sensibles ===  
Utilisateur: root      UID: 0  
=== 4. Services actifs ===  
=== 5. Verification du renforcement ssh ===  
... Vérification de la configuration SSH  
Root login désactivé  
Authentification par mot de passe désactivée  
Authentification par clé PUBKEY activée  
X11Forwarding désactivé
```

```
=== Vérification SSH terminée ===
```

Rapport généré avec succès: /var/log/audit-20250621.log
Temps total d'exécution : 00:08
[root@appserv01 audit-securite]#

Programmation automatique du script via cron à 03h00 chaque jour

Creation d'un CronJob

```
root@appserv01:/home/centos/Mini-Projet-DevSecOps/audit-securite
[root@appserv01 audit-securite]# crontab -l
0 3 * * * /usr/local/bin/audit.sh
[root@appserv01 audit-securite]#
```

4. Déploiement application web

- Installation de nginx

```
[root@appserv01 centos]# systemctl status nginx.service
● nginx.service - The nginx HTTP and reverse proxy server
   Loaded: loaded (/usr/lib/systemd/system/nginx.service; enabled; preset: disabled)
   Active: active (running) since Fri 2025-06-20 15:32:15 EDT; 3min 3s ago
  Invocation: 8d8de8de440d42189226586f4c021b87
    Process: 2751493 ExecStartPre=/usr/bin/rm -f /run/nginx.pid (code=exited, status=0/SUCCESS)
    Process: 2751494 ExecStartPre=/usr/sbin/nginx -t (code=exited, status=0/SUCCESS)
    Process: 2751496 ExecStart=/usr/sbin/nginx (code=exited, status=0/SUCCESS)
   Main PID: 2751498 (nginx)
      Tasks: 3 (limit: 22673)
     Memory: 3.3M (peak: 3.7M)
        CPU: 35ms
    CGroup: /system.slice/nginx.service
            └─2751498 "nginx: master process /usr/sbin/nginx"
              └─2751499 "nginx: worker process"
                └─2751500 "nginx: worker process"

jun 20 15:32:15 appserv01 systemd[1]: Starting nginx.service - The nginx HTTP and reverse proxy server...
jun 20 15:32:15 appserv01 nginx[2751494]: nginx: the configuration file /etc/nginx/nginx.conf syntax is ok
jun 20 15:32:15 appserv01 nginx[2751494]: nginx: configuration file /etc/nginx/nginx.conf test is successful
jun 20 15:32:15 appserv01 systemd[1]: Started nginx.service - The nginx HTTP and reverse proxy server.
[root@appserv01 centos]#
```

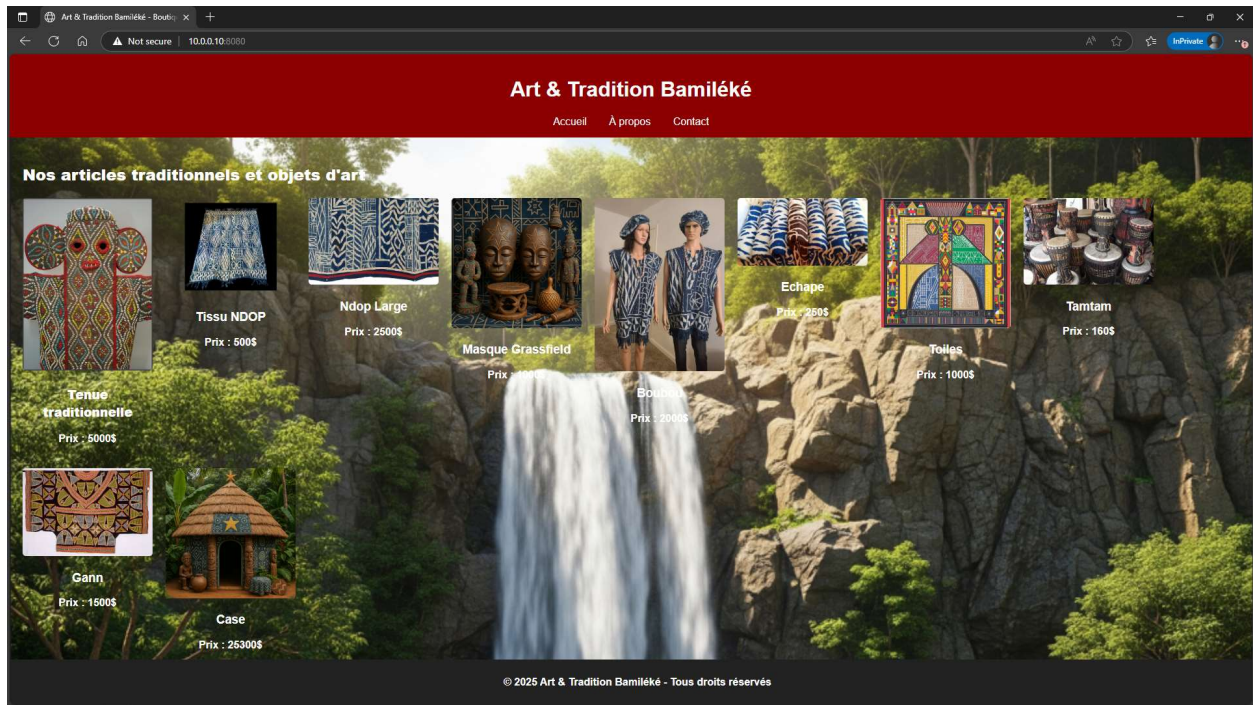
- Configuration du serveur pour faire tourner l'application sur le port 8080

```
[root@appserv01 centos]# ss -tulnp
Netid  State  Recv-Q  Send-Q  Local Address:Port  Peer Address:Port  Process
udp    UNCONN 0        0       127.0.0.1:323      0.0.0.0:*          users:(("chronyd",pid=2690407,fd=5))
udp    UNCONN 0        0       [::]:323          [::]:*             users:(("chronyd",pid=2690407,fd=6))
tcp    LISTEN 0        4096    127.0.0.1:631     0.0.0.0:*          users:(("cupsd",pid=979,fd=8))
tcp    LISTEN 0        511     0.0.0.0:8080     0.0.0.0:*          users:(("nginx",pid=2751500,fd=6),("nginx",pid=2751498,fd=6))
tcp    LISTEN 0        128     0.0.0.0:2223     0.0.0.0:*          users:(("sshd",pid=2665045,fd=7))
tcp    LISTEN 0        511     0.0.0.0:80      0.0.0.0:*          users:(("nginx",pid=2751500,fd=7),("nginx",pid=2751498,fd=7))
tcp    LISTEN 0        128     [::]:2223       [::]:*             users:(("sshd",pid=2665045,fd=8))
tcp    LISTEN 0        511     [::]:80         [::]:*             users:(("nginx",pid=2751500,fd=8),("nginx",pid=2751499,fd=8),("nginx",pid=2751498,fd=8))
tcp    LISTEN 0        4096    [::]:631        [::]:*             users:(("cupsd",pid=979,fd=7))
```

- Vérification du bon fonctionnement local via curl ou navigateur

```
[root@appserv01 centos]# curl http://localhost:8080
<html>
<head><title>404 Not Found</title></head>
<body>
<center><h1>404 Not Found</h1></center>
<hr><center>nginx/1.26.3</center>
</body>
</html>
```

Pour le test demo de notre application web sécurisé, nous avons déployé un site statique d'exposition d'objet d'art et culture hébergé dans le repertoire /www/var/html/



- Restriction de l'accès à certaines IPs et mise en place d'une authentification simple

Étape 1 : La restriction de l'accès se fait en spécifiant les IP autorisées dans le fichier /etc/nginx/conf.d/myapp.conf au niveau de la section **location**

```
root@appserv01:/home/centos
GNU nano 8.1 /etc/nginx/conf.d/myapp.conf
server {
    listen 8080;

    server_name _; # ou un nom de domaine si tu en as un

    root /var/www/html; # ton dossier application
    index index.php index.html index.htm;

    location / {
        allow 10.0.0.100;
        deny all;
        try_files $uri $uri/ =404;
    }

    location ~ \.php$ {
        include fastcgi_params;
        fastcgi_pass 127.0.0.1:9000; # selon ta config PHP-FPM
        fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
    }
}
```

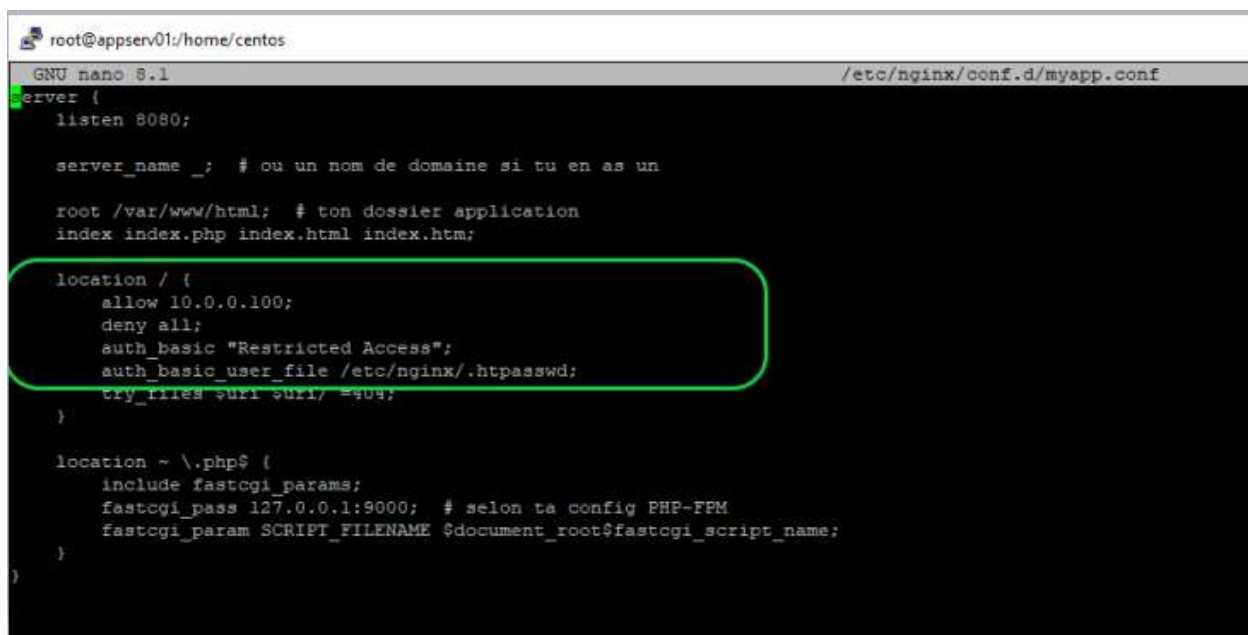
Étape 2 : Installer le paquet qui permet de générer un fichier de mot de passe httpd-tools

```
[root@appserv01 centos]# systemctl restart nginx.service
[root@appserv01 centos]# sudo dnf install httpd-tools
Dernière vérification de l'expiration des métadonnées effectuée il y a 1:06:37 le ven 20 jun 2025 14:48:39.
Dépendances résolues.
```

Étape 3 : Créer le fichier de mot de passe et création de l'utilisateur **webuser**


```
[root@appserv01 centos]# htpasswd -c /etc/nginx/.htpasswd webuser
New password:
Re-type new password:
Adding password for user webuser
```

Étape 4 : Ajouter cette configuration dans ton bloc location



```
root@appserv01:/home/centos
GNU nano 8.1 /etc/nginx/conf.d/myapp.conf
server {
    listen 8080;

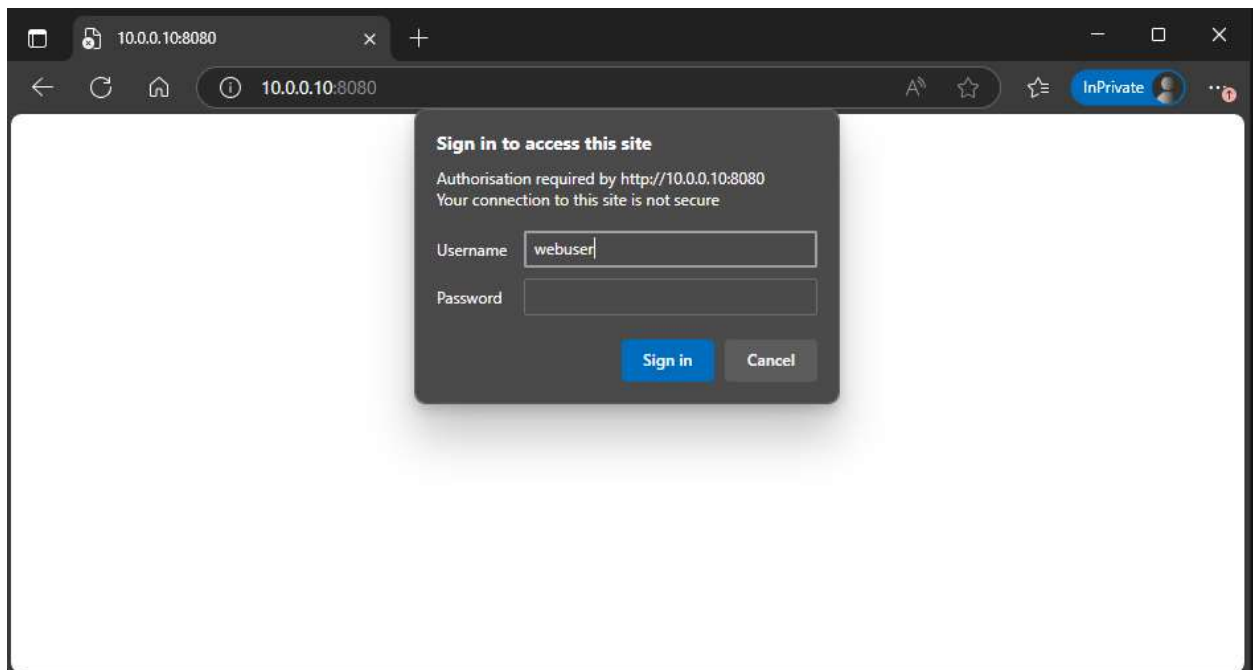
    server_name _; # ou un nom de domaine si tu en as un

    root /var/www/html; # ton dossier application
    index index.php index.html index.htm;

    location / {
        allow 10.0.0.100;
        deny all;
        auth_basic "Restricted Access";
        auth_basic_user_file /etc/nginx/.htpasswd;
        try_files $uri $uri/ =404;
    }

    location ~ \.php$ {
        include fastcgi_params;
        fastcgi_pass 127.0.0.1:9000; # selon ta config PHP-FPM
        fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
    }
}
```

Test : Demande d'authentification pour accéder à l'application depuis une ip autorisé



5. Documentation

a. État initial

Le serveur devant héberger notre application sécurisée est un serveur fonctionnant sous OS Linux CentOS stream 10 dont la version du noyau est **6.12.0-66.el10.x86_64** avec les services de sécurités de base Firewalld, Auditd et SELinux activé. Le serveur présente une configuration d'accès à distance basique avec un certains nombres de ports (9090, 5353), des services actifs non essentiels pour le besoin de l'application web, une configuration ssh basique exposant certains accès distant sur son port par défaut. Il existe en dehors du compte root, l'utilisateur nommé « CentOS » détenant un rôle privilégié avec un accès au Shell de connexion et des comptes de services restreints. Outre le serveur dispose de plusieurs fichiers et répertoires world-writable, plusieurs fichiers SUID, SGID et un fichier de configuration sensible /etc/shadow dont la permission n'est pas normale.

b. Les problèmes identifiés et leurs impacts

❖ Services non justifiés

Problèmes:

- Multiplication de la surface d'attaque (plus de failles possibles)
- Failles non maîtrisées (services oubliés ou jamais mis à jour)
- Incohérence avec le besoin réel (principe de "moindre privilège" violé)

Impact:

- Portes dérobées ouvertes (même par erreur)
- Compromission du serveur via un service superflu (scan, brute force, exploit...)

❖ **Ports ouverts non nécessaires**

Problèmes :

- Chaque port accessible depuis l'extérieur est une cible pour les scans et attaques
- Certains ports peuvent utiliser des protocoles non chiffrés
- Certains ports ne sont pas surveillés, risque de passer inaperçu

Impact :

- Exposition à des exploits réseaux (DoS, MITM...)
- Communication non autorisée vers/depuis le serveur (data exfiltration possible)
- Contournement des firewalls ou WAF

❖ **Configuration basique SSH (non durcie)**

Problèmes :

- Port 22 standard = cible directe pour brute-force
- Accès root SSH possible = prise de contrôle totale si le mot de passe est deviné
- Authentification par mot de passe autorisée (vs clé SSH) = moins sécurisé

Impact :

- Compromission SSH = perte de contrôle du serveur
- Mouvements latéraux vers d'autres machines si les clés privées sont compromises
- Persistance d'attaquants sur le serveur

❖ **Comptes utilisateurs ou comptes de service disposant d'un shell de connexion**

Problèmes:

- Si un compte de service obtient un shell, possibilité de l'utiliser pour exécuter des commandes
- Utilisateurs inactifs ou oubliés = comptes fantômes (potentiellement compromis)
- Trop de comptes avec un shell bash, difficile à surveiller

Impact:

- Multiplication des points d'accès
- Risques d'escalade de privilège via des comptes oubliés
- Exécution de code non contrôlée par des comptes non légitimes

❖ Fichiers et répertoires world-writable

Problèmes :

- Tout le monde peut écrire dedans; y compris des utilisateurs non privilégiés
- Fichiers de config modifiables; exécution de code malveillant possible
- Attaques par injection de fichier, ou persistance via modification de fichiers systèmes

Impact :

- Altération de l'application web
- Déploiement de malwares
- Persistance après une attaque; re-compromission du serveur

❖ Présence de nombreux fichiers SUID/SGID

Problèmes :

- SUID = exécution avec les droits root; dangereux si binaire vulnérable
- SGID = exécution avec droits du groupe
- Beaucoup de SUID/SGID = difficile de surveiller les bons usages

Impact :

- Escalade de privilèges (privilege escalation)
- Transformation d'un compte simple en compte root via un binaire mal protégé
- Ciblage par des scripts d'attaques automatisés

❖ Tableau Récapitulatif

Faibles possibles	Impacts réels
Services non justifiés	Compromission réseau, faille logicielle, pivot interne
Ports ouverts	Exposition aux scans, attaque brute-force, exploitation réseau

SSH non durci	Prise de contrôle du serveur
Shells inutiles	Mouvement latéral, commande non autorisée
World-writable	Injection de malwares, perte d'intégrité
SUID/SGID	Escalade de privilèges, contrôle root

c. Détails des mesures correctives

❖ Problèmes : surface d'attaque inutile (Services non justifiés)

- Auditer les services
- identifier les services inutiles, les stopper & désactiver

❖ Problèmes: ports d'attaque réseau

- Liste des ports ouverts
- Fermer les ports au firewall
- Modifier la config du service nginx pour n'écouter que sur un port précis

❖ Problèmes : vulnérabilités SSH (SSH non durci)

- Modifier le fichier `/etc/ssh/sshd_config` pour appliquer les configurations recommandées.

Option	Situation actuelle	Recommandation
Port	22	À Changer
PermitRootLogin	prohibit-password	Mettre no
PasswordAuthentication	yes	Mettre no (si on privilégie clés SSH en place)
PubkeyAuthentication	yes	Mettre yes
X11Forwarding	yes	Mettre no
AllowUsers centos	Non défini	Défini les utilisateurs pouvant accéder

- Redémarrer le service sshd
- Activer et configurer SELinux en mode enforcing

❖ Problèmes: comptes oubliés / détournés (Comptes à shell non nécessaires)

- Lister les comptes shell
- Désactiver les comptes inutiles
- Supprimer les comptes inutiles

❖ Problèmes : modification non autorisée (Fichiers et répertoire world-writable)

- Identifier les fichiers/répertoires world-writable
- Corriger les droits
- Si pertinent, changer le propriétaire ou le groupe pour restreindre

❖ Problèmes: escalade de privileges

- Lister les SUID / SGID
- Identifier les binaires légitimes (vs suspects)
- Désactiver SUID/SGID si inutile
- Mettre à jour régulièrement les paquets système pour patcher les vulnérabilités

d. Recommandations supplémentaires pour renforcer la sécurité

Quelques recommandations supplémentaires :

- Vérifier les scans réseau internes / externes (nmap)
- Installer fail2ban pour protéger contre les brute-force
- Mettre à jour régulièrement les paquets système pour patcher les vulnérabilités
- Garder le système à jour
- Sauvegardes régulières des configs sensibles (sous le répertoire /etc)
- Activer les logs centralisés et la surveillance des accès
- Activer auditd si cela n'est pas le cas pour surveiller les changements critiques

```
root@appserv01:/home/centos/Mini-Projet-DevSecOps/audit-securite
[root@appserv01 audit-securite]# /usr/local/bin/audit.sh
=====
-Script d'audit de sécurité des services,des utilisateurs à risque, les permission sensibles-
=====
Temps écoulé : 00:00=====
Création du rapport dans /etc/log/
Le fichier rapport crée
=== 0. Détection des ports ouverts ===
=== 1. Détection des fichiers SUID/SGID ===
=== 2. Fichiers et répertoires world-writable ===
Temps écoulé : 00:18 === 3. Utilisateurs à risque, analyse des groupes à privilèges, comptes echus et permission des fichiers et répertoires sensibles ===
Utilisateur: root          UID: 0
=== 4. Services actifs ===
=== 5. Verification du renforcement ssh ===
... Vérification de la configuration SSH
Root login désactivé
Authentification par mot de passe désactivée
Authentification par clé PUBKEY activée
X11Forwarding désactivé

=== Vérification SSH terminée ===

Rapport généré avec succès: /var/log/audit-20250621.log
Temps total d'exécution : 00:09
[root@appserv01 audit-securite]# crontab -l
0 3 * * * /usr/local/bin/audit.sh
[root@appserv01 audit-securite]#
```

6. Livrables

- ❖ Compte rendu des exercices 1 à 3

(Voir compte rendu en PJ ou sur le repos <https://github.com/nguewou/Mini-projet-DevSecOps.git>).

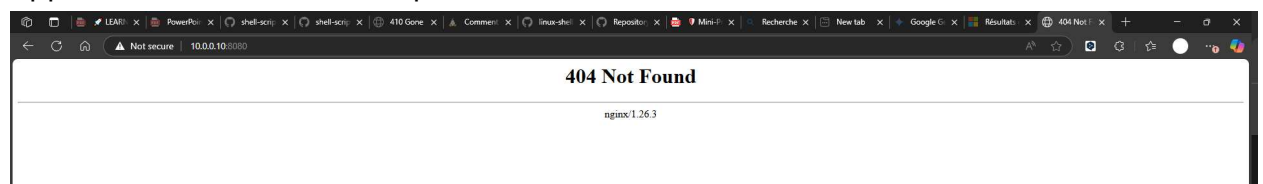
- ❖ Script Bash documenté (audit.sh) : télécharger via le lien ci-dessous

<https://github.com/nguewou/Mini-projet-DevSecOps/blob/main/audit-securite/audit.sh>

- ❖ Rapport d'audit automatisé généré : télécharger via le lien ci-dessous

<https://github.com/nguewou/Mini-projet-DevSecOps/blob/main/audit-20250621.log>

- ❖ Application fonctionnelle sur port 8080



- ❖ Document final de synthèse (PDF et Markdown) : Voir ce rapport et téléchargeable sur github

<https://github.com/nguewou/Mini-projet-DevSecOps.git>