

**Institut Universitaire des Sciences (IUS)**  
**FACULTÉ DES SCIENCES ET DES TECHNOLOGIES (FST)**

**PRESENTATION DU LAB 6**

*Systèmes d'Exploitation Linux*

Étudiant : Wendy COLAS  
Niveau : L3

2024

## 1. Reproduction des tâches du td

```
wendy@wendy-VirtualBox:~$ sudo apt update
[sudo] Mot de passe de wendy :
Ign :1 http://ht.archive.ubuntu.com/ubuntu jammy InRelease
Ign :2 https://packages.microsoft.com/repos/code stable InRelease
Ign :3 http://security.ubuntu.com/ubuntu jammy-security InRelease
Ign :4 http://ht.archive.ubuntu.com/ubuntu jammy-updates InRelease
Ign :5 http://ht.archive.ubuntu.com/ubuntu jammy-backports InRelease
Ign :1 http://ht.archive.ubuntu.com/ubuntu jammy InRelease
Ign :2 https://packages.microsoft.com/repos/code stable InRelease
Ign :3 http://security.ubuntu.com/ubuntu jammy-security InRelease
Ign :4 http://ht.archive.ubuntu.com/ubuntu jammy-updates InRelease
Ign :5 http://ht.archive.ubuntu.com/ubuntu jammy-backports InRelease
Ign :1 http://ht.archive.ubuntu.com/ubuntu jammy InRelease
Ign :2 https://packages.microsoft.com/repos/code stable InRelease
Ign :3 http://security.ubuntu.com/ubuntu jammy-security InRelease
Ign :4 http://ht.archive.ubuntu.com/ubuntu jammy-updates InRelease
Ign :5 http://ht.archive.ubuntu.com/ubuntu jammy-backports InRelease
Err :1 http://ht.archive.ubuntu.com/ubuntu jammy InRelease
    Erreur temporaire de résolution de « ht.archive.ubuntu.com »
Err :2 https://packages.microsoft.com/repos/code stable InRelease
    Erreur temporaire de résolution de « packages.microsoft.com »
Err :3 http://security.ubuntu.com/ubuntu jammy-security InRelease
    Erreur temporaire de résolution de « security.ubuntu.com »
Err :4 http://ht.archive.ubuntu.com/ubuntu jammy-updates InRelease
wendy@wendy-VirtualBox:~$ 
W: Impossible de récupérer https://packages.microsoft.com/repos/code/dists/stable/InRelease Erreur temporaire de résolution de « packages.microsoft.com »
W: Le téléchargement de quelques fichiers d'index a échoué, ils ont été ignorés, ou les anciens ont été utilisés à la place.
wendy@wendy-VirtualBox:~$ sudo apt install ufw
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
ufw est déjà la version la plus récente (0.36.1-4ubuntu0.1).
ufw passé en « installé manuellement ».
0 mis à jour, 0 nouvellement installés, 0 à enlever et 211 non mis à jour.
wendy@wendy-VirtualBox:~$ sudo ufw status verbose
État : inactif
wendy@wendy-VirtualBox:~$ sudo ufw enable
Le pare-feu est actif et lancé au démarrage du système
wendy@wendy-VirtualBox:~$ sudo ufw status verbose
État : actif
Journalisation : on (low)
Par défaut : deny (incoming), allow (outgoing), disabled (routed)
Nouveaux profils : skip
wendy@wendy-VirtualBox:~$ sudo ufw allow 80/tcp
La règle a été ajoutée
La règle a été ajoutée (v6)
wendy@wendy-VirtualBox:~$ 
```

```
La règle a été ajoutée
La règle a été ajoutée (v6)
wendy@wendy-VirtualBox:~$ sudo ufw allow 22/tcp
La règle a été ajoutée
La règle a été ajoutée (v6)
wendy@wendy-VirtualBox:~$ sudo ufw deny 23
La règle a été ajoutée
La règle a été ajoutée (v6)
wendy@wendy-VirtualBox:~$ sudo ufw status numbered
État : actif

      Vers          Action     De
      ----          -----   --
[ 1] 80/tcp       ALLOW IN  Anywhere
[ 2] 22/tcp       ALLOW IN  Anywhere
[ 3] 23           DENY IN   Anywhere
[ 4] 80/tcp (v6)  ALLOW IN  Anywhere (v6)
[ 5] 22/tcp (v6)  ALLOW IN  Anywhere (v6)
[ 6] 23 (v6)     DENY IN   Anywhere (v6)

wendy@wendy-VirtualBox:~$ sudo ufw allow 23
La règle a été mise à jour
La règle a été mise à jour (v6)
wendy@wendy-VirtualBox:~$ sudo ufw status numbered
```

```
État : actif

      Vers          Action     De
      ----          -----   --
[ 1] 80/tcp       ALLOW IN  Anywhere
[ 2] 22/tcp       ALLOW IN  Anywhere
[ 3] 23           ALLOW IN  Anywhere
[ 4] 80/tcp (v6)  ALLOW IN  Anywhere (v6)
[ 5] 22/tcp (v6)  ALLOW IN  Anywhere (v6)
[ 6] 23 (v6)     ALLOW IN  Anywhere (v6)

wendy@wendy-VirtualBox:~$ sudo ufw delete allow 80/tcp
La règle a été supprimée
La règle a été supprimée (v6)
wendy@wendy-VirtualBox:~$ sudo ufw status numbered
État : actif

      Vers          Action     De
      ----          -----   --
[ 1] 22/tcp       ALLOW IN  Anywhere
[ 2] 23           ALLOW IN  Anywhere
[ 3] 22/tcp (v6)  ALLOW IN  Anywhere (v6)
[ 4] 23 (v6)     ALLOW IN  Anywhere (v6)
```

```
wendy@wendy-VirtualBox: ~
[ 2] 23                      ALLOW IN    Anywhere
[ 3] 22/tcp (v6)              ALLOW IN    Anywhere (v6)
[ 4] 23 (v6)                 ALLOW IN    Anywhere (v6)

wendy@wendy-VirtualBox:~$ sudo ufw allow 80/tcp
La règle a été ajoutée
La règle a été ajoutée (v6)
wendy@wendy-VirtualBox:~$ sudo ufw status numbered
État : actif

      Vers          Action      De
      ---          ----
[ 1] 22/tcp        ALLOW IN    Anywhere
[ 2] 23           ALLOW IN    Anywhere
[ 3] 80/tcp        ALLOW IN    Anywhere
[ 4] 22/tcp (v6)  ALLOW IN    Anywhere (v6)
[ 5] 23 (v6)      ALLOW IN    Anywhere (v6)
[ 6] 80/tcp (v6)  ALLOW IN    Anywhere (v6)

wendy@wendy-VirtualBox:~$ sudo ufw disable
Le pare-feu est arrêté et désactivé lors du démarrage du système
wendy@wendy-VirtualBox:~$ sudo ufw status verbose
État : inactif
wendy@wendy-VirtualBox:~$
```

```
wendy@wendy-VirtualBox: ~
wendy@wendy-VirtualBox:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ufw-before-logging-input  all  --  anywhere             anywhere
ufw-before-input   all  --  anywhere             anywhere
ufw-after-input   all  --  anywhere             anywhere
ufw-after-logging-input all  --  anywhere             anywhere
ufw-reject-input  all  --  anywhere             anywhere
ufw-track-input   all  --  anywhere             anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
ufw-before-logging-forward all  --  anywhere             anywhere
ufw-before-forward  all  --  anywhere             anywhere
ufw-after-forward  all  --  anywhere             anywhere
ufw-after-logging-forward all  --  anywhere             anywhere
ufw-reject-forward all  --  anywhere             anywhere
ufw-track-forward all  --  anywhere             anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ufw-before-logging-output all  --  anywhere             anywhere
ufw-before-output   all  --  anywhere             anywhere
ufw-after-output   all  --  anywhere             anywhere
```

```
wendy@wendy-VirtualBox: ~
target      prot opt source          destination
Chain ufw-reject-input (1 references)
target      prot opt source          destination
Chain ufw-reject-output (1 references)
target      prot opt source          destination
Chain ufw-track-forward (1 references)
target      prot opt source          destination
Chain ufw-track-input (1 references)
target      prot opt source          destination
Chain ufw-track-output (1 references)
target      prot opt source          destination
wendy@wendy-VirtualBox:~$ sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
wendy@wendy-VirtualBox:~$ sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT
wendy@wendy-VirtualBox:~$ sudo iptables -A INPUT -p tcp --dport 23 -j REJECT
wendy@wendy-VirtualBox:~$ sudo iptables-save > /etc/iptables/rules.v4
bash: /etc/iptables/rules.v4: Aucun fichier ou dossier de ce nom
wendy@wendy-VirtualBox:~$ sudo iptables -A INPUT -p tcp --dport 23 -j ACCEPT
wendy@wendy-VirtualBox:~$ sudo iptables -F
wendy@wendy-VirtualBox:~$
```

```
wendy@wendy-VirtualBox: ~
wendy@wendy-VirtualBox:~$ sestatus
La commande « sestatus » n'a pas été trouvée, mais peut être installée avec :
sudo apt install policycoreutils
wendy@wendy-VirtualBox:~$ sudo apt-get update
[Atteint :1 http://ht.archive.ubuntu.com/ubuntu jammy InRelease
Réception de :2 http://ht.archive.ubuntu.com/ubuntu jammy-updates InRelease [128 kB]
Réception de :3 http://security.ubuntu.com/ubuntu jammy-security InRelease [129 kB]
Réception de :4 https://packages.microsoft.com/repos/code stable InRelease [3 58 9 B]
Réception de :5 http://ht.archive.ubuntu.com/ubuntu jammy-backports InRelease [1 27 kB]
Réception de :6 https://packages.microsoft.com/repos/code stable/main armhf Packages [17,8 kB]
Réception de :7 https://packages.microsoft.com/repos/code stable/main amd64 Packages [17,5 kB]
Réception de :8 https://packages.microsoft.com/repos/code stable/main arm64 Packages [17,7 kB]
Réception de :9 http://ht.archive.ubuntu.com/ubuntu jammy-updates/main amd64 DEP-11 Metadata [103 kB]
Réception de :10 http://ht.archive.ubuntu.com/ubuntu jammy-updates/restricted arm64 DEP-11 Metadata [212 B]
Réception de :11 http://ht.archive.ubuntu.com/ubuntu jammy-updates/universe amd64
```

```
l 098 ko réceptionnés en 6s (175 ko/s)
lecture des listes de paquets... Fait
wendy@wendy-VirtualBox:~$ sudo apt-get install selinux-basics
lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  binutils binutils-common binutils-x86-64-linux-gnu checkpolicy gawk
  libauparse0 libbinutils libctf-nobfd0 libctf0 libgfortran5 liblapack3
  libquadmath0 libsigsegv2 m4 make policycoreutils policycoreutils-dev
  policycoreutils-python-utils python3-audit python3-decorator
  python3-networkx python3-numpy python3-selinux python3-semanage
  python3-sepolgen python3-sepolicy python3-setools selinux-policy-default
  selinux-policy-dev selinux-utils semodule-utils setools
Paquets suggérés :
  binutils-doc gawk-doc m4-doc make-doc python-networkx-doc python3-gdal
  python3-matplotlib python3-pydot python3-pygraphviz python3-scipy gcc
  gfortran python-numpy-doc python3-dev python3-pytest logcheck syslog-summary
  setools-gui
Les NOUVEAUX paquets suivants seront installés :
  binutils binutils-common binutils-x86-64-linux-gnu checkpolicy gawk
  libauparse0 libbinutils libctf-nobfd0 libctf0 libgfortran5 liblapack3
  libquadmath0 libsigsegv2 m4 make policycoreutils policycoreutils-dev
  policycoreutils-python-utils python3-audit python3-decorator
```

```
wendy@wendy-VirtualBox:~$ sudo apt-get install selinux-policy-default
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
selinux-policy-default est déjà la version la plus récente (2:2.20210203-10).
selinux-policy-default passé en « installé manuellement ».
0 mis à jour, 0 nouvellement installés, 0 à enlever et 211 non mis à jour.
wendy@wendy-VirtualBox:~$ sudo apt-get install auditd
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Paquets suggérés :
  audispd-plugins
Les NOUVEAUX paquets suivants seront installés :
  auditd
0 mis à jour, 1 nouvellement installés, 0 à enlever et 211 non mis à jour.
Il est nécessaire de prendre 212 ko dans les archives.
Après cette opération, 707 ko d'espace disque supplémentaires seront utilisés.
Réception de :1 http://ht.archive.ubuntu.com/ubuntu jammy/main amd64 auditd amd64 1:3.0.7-1build1 [212 kB]
212 ko réceptionnés en 1s (172 ko/s)
Sélection du paquet auditd précédemment désélectionné.
(Lecture de la base de données... 183030 fichiers et répertoires déjà installés.
)
```

```
wendy@wendy-VirtualBox: ~
Sélection du paquet auditd précédemment désélectionné.
(Lecture de la base de données... 183030 fichiers et répertoires déjà installés.
)
Préparation du dépaquetage de .../auditd_1%3a3.0.7-1build1_amd64.deb ...
Dépaquetage de auditd (1:3.0.7-1build1) ...
Paramétrage de auditd (1:3.0.7-1build1) ...
Created symlink /etc/systemd/system/multi-user.target.wants/auditd.service →/lib/systemd/system/auditd.service.
Traitement des actions différées (« triggers ») pour man-db (2.10.2-1) ...
wendy@wendy-VirtualBox:~$ sudo selinux-activate
Activating SE Linux
Sourcing file `/etc/default/grub'
Sourcing file `/etc/default/grub.d/init-select.cfg'
Generating grub configuration file ...
Found linux image: /boot/vmlinuz-6.8.0-40-generic
Found initrd image: /boot/initrd.img-6.8.0-40-generic
Found memtest86+ image: /boot/memtest86+.elf
Found memtest86+ image: /boot/memtest86+.bin
Warning: os-prober will not be executed to detect other bootable partitions.
Systems on them will not be added to the GRUB boot configuration.
Check GRUB_DISABLE_OS_PROBER documentation entry.
done
SE Linux is activated. You may need to reboot now.
wendy@wendy-VirtualBox:~$
```

```
wendy@wendy-VirtualBox: ~
wendy@wendy-VirtualBox:~$ set enforce 1
wendy@wendy-VirtualBox:~$ sudo nano /etc/selinux/config
wendy@wendy-VirtualBox:~$ set enforce 0
wendy@wendy-VirtualBox:~$ sudo nano /etc/selinux/config
wendy@wendy-VirtualBox:~$ sestatus
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:              default
Current mode:                   permissive
Mode from config file:          permissive
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Memory protection checking:    actual (secure)
Max kernel policy version:     33
wendy@wendy-VirtualBox:~$ getentforce
La commande « getentforce » n'a pas été trouvée, voulez-vous dire :
  commande « getenforce » du deb selinux-utils (3.3-1build2)
Essayez : sudo apt install <nom du deb>
wendy@wendy-VirtualBox:~$ sudo apt install selinux-utils
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
selinux-utils est déjà la version la plus récente (3.3-1build2).
```

/etc/nginx(.*)?	all files	system_u:o
bject_r:httpd_config_t:s0	regular file	system_u:o
/etc/ngircd\.conf	regular file	system_u:o
bject_r:ircd_etc_t:s0	regular file	system_u:o
/etc/ngircd\.motd	regular file	system_u:o
bject_r:ircd_etc_t:s0	regular file	system_u:o
/etc/nohotplug	regular file	system_u:o
bject_r:etc_runtime_t:s0	regular file	system_u:o
/etc/nologin	regular file	system_u:o
bject_r:shutdown_etc_t:s0	regular file	system_u:o
/etc/nologin.*	regular file	system_u:o
bject_r:etc_runtime_t:s0	regular file	system_u:o
/etc/nsd(.*)?	all files	system_u:o
bject_r:nsd_conf_t:s0	regular file	system_u:o
/etc/nsd/nsd\.db	regular file	system_u:o
bject_r:nsd_db_t:s0	all files	system_u:o
/etc/nsd/primary(.*)?	all files	system_u:o
bject_r:nsd_zone_t:s0	all files	system_u:o
/etc/nsd/secondary(.*)?	all files	system_u:o
bject_r:nsd_zone_t:s0	regular file	system_u:o
/etc/nss-ldapd\.conf	regular file	system_u:o
bject_r:nslcd_conf_t:s0	all files	system_u:o
/etc/ntop.*	all files	system_u:o
bject_r:ntop_etc_t:s0	all files	system_u:o

```
wendy@wendy-VirtualBox: ~
Équivalence fcontext de distribution SELinux

/bin = /usr/bin
/lib = /usr/lib
/lib32 = /usr/lib
/lib64 = /usr/lib
/libx32 = /usr/lib
/sbin = /usr/sbin
/etc/init.d = /etc/rc.d/init.d
/etc/systemd/system = /usr/lib/systemd/system
/lib/systemd = /usr/lib/systemd
/run/lock = /var/lock
/usr/lib32 = /usr/lib
/usr/lib64 = /usr/lib
/usr/libx32 = /usr/lib
/usr/local/lib32 = /usr/lib
/usr/local/lib64 = /usr/lib
/usr/local/lib = /usr/lib
/var/lib/private = /var/lib
/var/cache/private = /var/cache
/var/log/private = /var/log
/var/run = /run
wendy@wendy-VirtualBox:~$
```

```
wendy@wendy-VirtualBox: ~
m="cached_setup_fo" name="console-setup" dev="tmpfs" ino=939 scontext=system_u:s
ystem_r:udev_t:s0-s0:c0.c1023 tcontext=system_u:object_r:initrc_runtime_t:s0 tcl
ass=dir permissive=1
    Was caused by:
        Unknown - would be allowed by active policy
        Possible mismatch between this policy and the one under which th
e audit message was generated.

            Possible mismatch between current in-memory boolean settings vs.
permanent ones.

type=AVC msg=audit(1741276610.687:64): avc: denied { setattr } for pid=383 co
mm="systemd-resolve" name="/" dev="cgroup2" ino=1 scontext=system_u:system_r:sys
temd_resolved_t:s0 tcontext=system_u:object_r:cgroup_t:s0 tclass=filesystem perm
issive=1
    Was caused by:
        Unknown - would be allowed by active policy
        Possible mismatch between this policy and the one under which th
e audit message was generated.

            Possible mismatch between current in-memory boolean settings vs.
permanent ones.

type=AVC msg=audit(1741276610.689:65): avc: denied { search } for pid=383 com
```

```
wendy@wendy-VirtualBox: ~
his access.

type=AVC msg=audit(1741277460.035:1076): avc: denied { read } for pid=3908
mm="modprobe" name="blacklist-oss.conf" dev="sda3" ino=2098993 scontext=system
:system_r:kmod_t:s0 tcontext=system_u:object_r:modules_conf_t:s0 tclass=lnk_fi
permisse=1
    Was caused by:
        Missing type enforcement (TE) allow rule.

            You can use audit2allow to generate a loadable module to allow
his access.

type=AVC msg=audit(1741277513.175:1080): avc: denied { setattr } for pid=41
comm="systemd-tmpfile" name="/" dev="cgroup2" ino=1 scontext=system_u:system_
systemd_tmpfiles_t:s0 tcontext=system_u:object_r:cgroup_t:s0 tclass=filesystem
ermisse=1
    Was caused by:
        Missing type enforcement (TE) allow rule.

            You can use audit2allow to generate a loadable module to allow
his access.

wendy@wendy-VirtualBox:~$ sudo audit2allow -M mypolicies
```

```
mas 6 11:52
wendy@wendy-VirtualBox:~$ sudo systemctl status apparmor
[sudo] Mot de passe de wendy :
○ apparmor.service - Load AppArmor profiles
    Loaded: loaded (/lib/systemd/system/apparmor.service; enabled; vendor pres>
    Active: inactive (dead)
      Condition: start condition failed at Thu 2025-03-06 11:27:43 EST; 4min 19s ago
        Docs: man:apparmor(7)
              https://gitlab.com/apparmor/apparmor/wikis/home/
mas 06 11:27:43 wendy-VirtualBox systemd[1]: Condition check resulted in Load A>
wendy@wendy-VirtualBox:~$ sudo apt update
Atteint :1 https://packages.microsoft.com/repos/code stable InRelease
0% [Connexion à ht.archive.ubuntu.com] [Connexion à security.ubuntu.com]
```

```
mas 6 11:34
wendy@wendy-VirtualBox:~$ sudo apt install apparmor
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
App
Lecture des informations d'état... Fait
Les paquets suivants ont été installés automatiquement et ne sont plus nécessair
es :
  checkpolicy libauparse0 libgfortran5 liblapack3 libquadmath0 m4
  python3-audit python3-decorator python3-networkx python3-numpy
  python3-selinux python3-semanage python3-sepolgen python3-sepolicy
  python3-setools semodule-utils setools
Veuillez utiliser « sudo apt autoremove » pour les supprimer.
Paquets suggérés :
  apparmor-profiles-extra apparmor-utils
Les paquets suivants seront mis à jour :
  apparmor
  1 mis à jour, 0 nouvellement installés, 0 à enlever et 210 non mis à jour.
Il est nécessaire de prendre 598 ko dans les archives.
Après cette opération, 4 096 o d'espace disque supplémentaires seront utilisés.
Réception de :1 http://ht.archive.ubuntu.com/ubuntu jammy-updates/main amd64 app
armor amd64 3.0.4-2ubuntu2.4 [598 kB]
598 ko réceptionnés en 12s (51,4 ko/s)
Préconfiguration des paquets...
(Lecture de la base de données... 181826 fichiers et répertoires déjà installés.
```

```
mas 6 11:34
wendy@wendy-VirtualBox: ~
Traitement des actions différées (« triggers ») pour man-db (2.10.2-1) ...
wendy@wendy-VirtualBox:~$ sudo apt install apparmor-utils
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets suivants ont été installés automatiquement et ne sont plus nécessaires :
  checkpolicy libauparse0 libgfortran5 liblapack3 libquadmath0 m4
  python3-audit python3-decorator python3-networkx python3-numpy
  python3-selinux python3-semanage python3-sepolgen python3-sepolicy
  python3-setools semodule-utils setools
Veuillez utiliser « sudo apt autoremove » pour les supprimer.
Les paquets supplémentaires suivants seront installés :
  python3-apparmor python3-libapparmor
Paquets suggérés :
  vim-addon-manager
Les NOUVEAUX paquets suivants seront installés :
  apparmor-utils python3-apparmor python3-libapparmor
0 mis à jour, 3 nouvellement installés, 0 à enlever et 210 non mis à jour.
Il est nécessaire de prendre 170 ko dans les archives.
Après cette opération, 1 186 ko d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [0/n] o
Réception de :1 http://ht.archive.ubuntu.com/ubuntu jammy-updates/main amd64 python3-libapparmor amd64 3.0.4-2ubuntu2.4 [29,5 kB]
```

```
wendy@wendy-VirtualBox: ~
paramétrage de apparmor-utils (3.0.4-2ubuntu2.4) ...
Traitement des actions différées (« triggers ») pour man-db (2.10.2-1) ...
wendy@wendy-VirtualBox:~$ sudo systemctl enable apparmor
Synchronizing state of apparmor.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable apparmor
wendy@wendy-VirtualBox:~$ sudo systemctl start apparmor
wendy@wendy-VirtualBox:~$ sudo systemctl status apparmor
● apparmor.service - Load AppArmor profiles
   Loaded: loaded (/lib/systemd/system/apparmor.service; enabled; vendor pres>
   Active: inactive (dead)
     Docs: man:apparmor(7)
           https://gitlab.com/apparmor/apparmor/wikis/home/

mas 06 11:27:43 wendy-VirtualBox systemd[1]: Condition check resulted in Load A>
mas 06 11:35:16 wendy-VirtualBox systemd[1]: Condition check resulted in Load A>
wendy@wendy-VirtualBox:~$ sudo apparmor_status
apparmor module is loaded.
apparmor filesystem is not mounted.
wendy@wendy-VirtualBox:~$ sudo aa-enforce /etc/apparmor.d/usr.bin.something
Profile for /etc/apparmor.d/usr.bin.something not found, skipping
wendy@wendy-VirtualBox:~$
```

```
wendy@wendy-VirtualBox:~$ sudo su-
[sudo] Mot de passe de wendy :
sudo: su- : commande introuvable
wendy@wendy-VirtualBox:~$ sudo su -
root@wendy-VirtualBox:~# apt install firewalld
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets suivants ont été installés automatiquement et ne sont plus nécessaires :
  checkpolicy libauparse0 libgfortran5 liblapack3 libquadmath0 m4
  python3-audit python3-decorator python3-networkx python3-numpy
  python3-selinux python3-semanage python3-sepolgen python3-sepolicy
  python3-setools semodule-utils setools
Veuillez utiliser « apt autoremove » pour les supprimer.
Les paquets supplémentaires suivants seront installés :
  ipset libipset13 python3-attr python3-cap-ng python3-distutils
  python3-firewall python3-jsonschema python3-nftables python3-pkg-resources
  python3-persistent python3-setuptools
Paquets suggérés :
  python-attr-doc python-jsonschema-doc python-setuptools-doc
Les NOUVEAUX paquets suivants seront installés :
  firewalld ipset libipset13 python3-attr python3-cap-ng python3-distutils
  python3-firewall python3-jsonschema python3-nftables python3-persistent
  python3-setuptools
Les paquets suivants seront mis à jour :
```

```
wendy@wendy-VirtualBox:~$ sudo su-
[sudo] Mot de passe de wendy :
sudo: su- : commande introuvable
wendy@wendy-VirtualBox:~$ sudo su -
root@wendy-VirtualBox:~# apt install firewalld
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets suivants ont été installés automatiquement et ne sont plus nécessaires :
  checkpolicy libauparse0 libgfortran5 liblapack3 libquadmath0 m4
  python3-audit python3-decorator python3-networkx python3-numpy
  python3-selinux python3-semanage python3-sepolgen python3-sepolicy
  python3-setools semodule-utils setools
Veuillez utiliser « apt autoremove » pour les supprimer.
Les paquets supplémentaires suivants seront installés :
  ipset libipset13 python3-attr python3-cap-ng python3-distutils
  python3-firewall python3-jsonschema python3-nftables python3-pkg-resources
  python3-persistent python3-setuptools
Paquets suggérés :
  python-attr-doc python-jsonschema-doc python-setuptools-doc
Les NOUVEAUX paquets suivants seront installés :
  firewalld ipset libipset13 python3-attr python3-cap-ng python3-distutils
  python3-firewall python3-jsonschema python3-nftables python3-persistent
  python3-setuptools
Les paquets suivants seront mis à jour :
```

```
wendy@wendy-VirtualBox:~$ sudo su -  
[sudo] Mot de passe de wendy :  
root@wendy-VirtualBox:~# firewall-cmd --get-defaults-zone  
usage: see firewall-cmd man page  
firewall-cmd: error: unrecognized arguments: --get-defaults-zone  
root@wendy-VirtualBox:~# firewall-cmd --get-default-zone  
public  
root@wendy-VirtualBox:~# firewall-cmd --get-zones  
block dmz drop external home internal nm-shared public trusted work  
root@wendy-VirtualBox:~# firewall-cmd --get-services  
RH-Satellite-6 RH-Satellite-6-capsule afp amanda-client amanda-k5-client amqp am  
qps apcupsd audit bacula bacula-client bb bgp bitcoin bitcoin-rpc bitcoin-testne  
t bitcoin-testnet-rpc bittorrent-lsd ceph ceph-mon cfengine cockpit collectd con  
dor-collector ctdb dhcp dhcpcv6 dhcpcv6-client distcc dns dns-over-tls docker-regi  
stry docker-swarm dropbox-lansync elasticsearch etcd-client etcd-server finger f  
oreman foreman-proxy freeipa-4 freeipa-ldap freeipa-ldaps freeipa-replication fr  
eeipa-trust ftp galera ganglia-client ganglia-master git grafana gre high-availa  
bility http http3 https imap imaps ipp ipp-client ipsec irc ircs iscsi-target is  
ns jellyfin jenkins kadmin kdeconnect kerberos kibana klogin kpasswd kprop kshel  
l kube-api kube-apiserver kube-control-plane kube-controller-manager kube-schedu  
ler kubelet-worker ldap ldaps libvirt libvirt-tls lightning-network llmnr llmnr-  
tcp llmnr-udp managesieve matrix mdns memcache minidlna mongodb mosh mountd mqtt  
mqtt-tls ms-wbt mssql murmur mysql nbd netbios-ns nfs nfs3 nmea-0183 nrpe ntp n  
ut openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole plex pmcd pmproxy
```

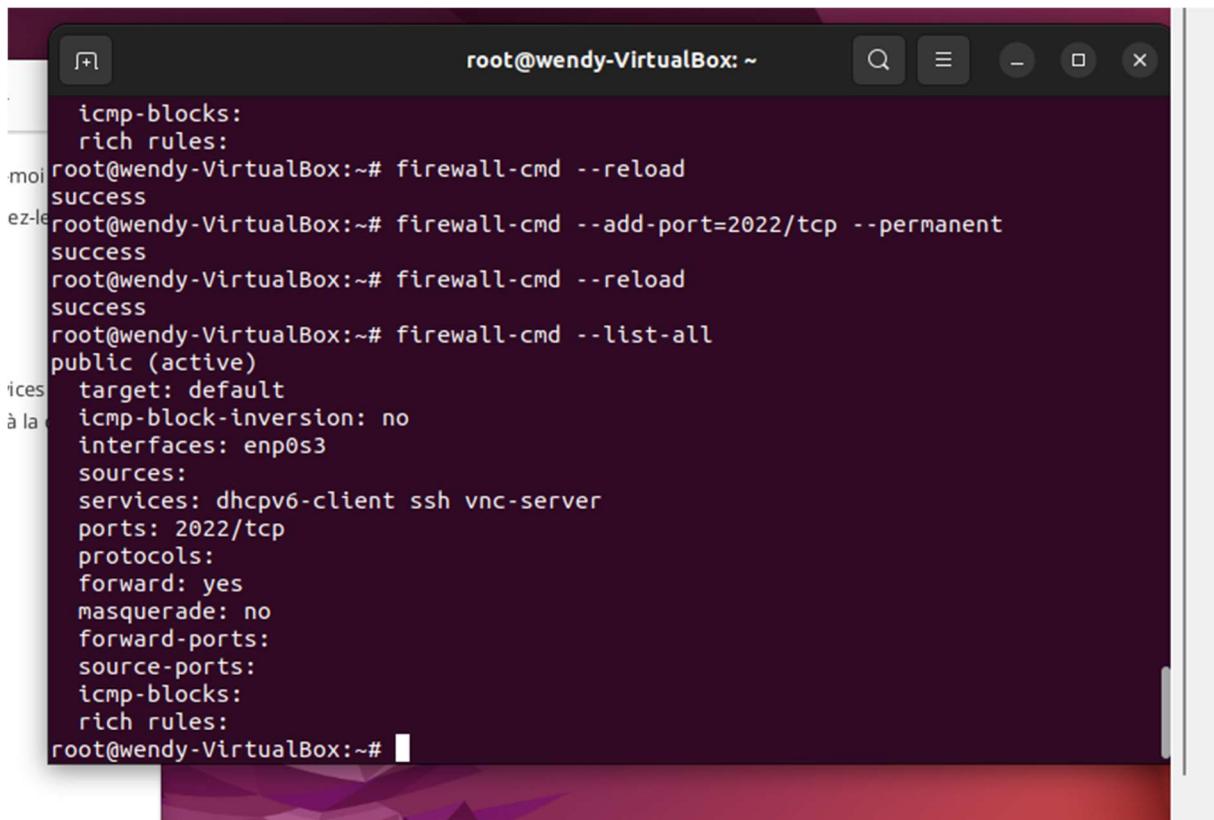
```
root@wendy-VirtualBox:~# firewall-cmd --list-services  
dhcpcv6-client ssh  
root@wendy-VirtualBox:~# firewall-cmd --list-all  
public (active)  
  target: default  
  icmp-block-inversion: no  
  interfaces: enp0s3  
  sources:  
  services: dhcpcv6-client ssh  
  ports:  
  protocols:  
  forward: yes  
  masquerade: no  
  forward-ports:  
  source-ports:  
  icmp-blocks:  
  rich rules:  
root@wendy-VirtualBox:~# firewall-cmd --list-all --zone=public  
public (active)  
  target: default  
  icmp-block-inversion: no  
  interfaces: enp0s3  
  sources:  
  services: dhcpcv6-client ssh
```

```
root@wendy-VirtualBox:~# firewall-cmd --list-all --zone=public
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: dhcpcv6-client ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
root@wendy-VirtualBox:~# firewall-cmd --add-service=vnc-server
success
root@wendy-VirtualBox:~#
```

```
root@wendy-VirtualBox:~# firewall-cmd --list-all --zone=public
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: dhcpcv6-client ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
root@wendy-VirtualBox:~# systemctl restart firewalld
root@wendy-VirtualBox:~# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: dhcpcv6-client ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
root@wendy-VirtualBox:~#
```

```
root@wendy-VirtualBox:~# firewall-cmd --add-service=vnc-server --permanent
success
root@wendy-VirtualBox:~# firewall-cmd --add-service=vnc-server --permanent
Warning: ALREADY_ENABLED: vnc-server
success
root@wendy-VirtualBox:~# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: dhcpcv6-client ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
root@wendy-VirtualBox:~# systemctl restart firewalld
root@wendy-VirtualBox:~# firewall-cmd --list-all
public (active)
```

```
root@wendy-VirtualBox:~# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: dhcpcv6-client ssh vnc-server
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
root@wendy-VirtualBox:~# systemctl restart firewalld
root@wendy-VirtualBox:~# firewall-cmd --list-all
public (active)
```



A screenshot of a terminal window titled "root@wendy-VirtualBox: ~". The terminal displays the following command-line session:

```
root@wendy-VirtualBox:~# firewall-cmd --reload
success
root@wendy-VirtualBox:~# firewall-cmd --add-port=2022/tcp --permanent
success
root@wendy-VirtualBox:~# firewall-cmd --reload
success
root@wendy-VirtualBox:~# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: dhcpcv6-client ssh vnc-server
  ports: 2022/tcp
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
root@wendy-VirtualBox:~#
```

## Conclusion

Ce td m'a permis de maîtriser la configuration des pare-feu sur linux Ubuntu. Je sais comment bloquer ou autoriser le trafic entrant ou sortant, ou encore comment bloquer ou autoriser l'usage d'un port et tant d'autres choses.