



**IUS**  
INSTITUT  
UNIVERSITAIRE  
DES SCIENCES

**FACULTÉ DES SCIENCES ET DES TECHNOLOGIES  
(FST)**

**Nom :**

**BYRON**

**Prénom :**

**P. D. Naguiby**

**Cours :**

**Système**

**Professeur :**

**Mr I. Saint Amour**

**Niveau :**

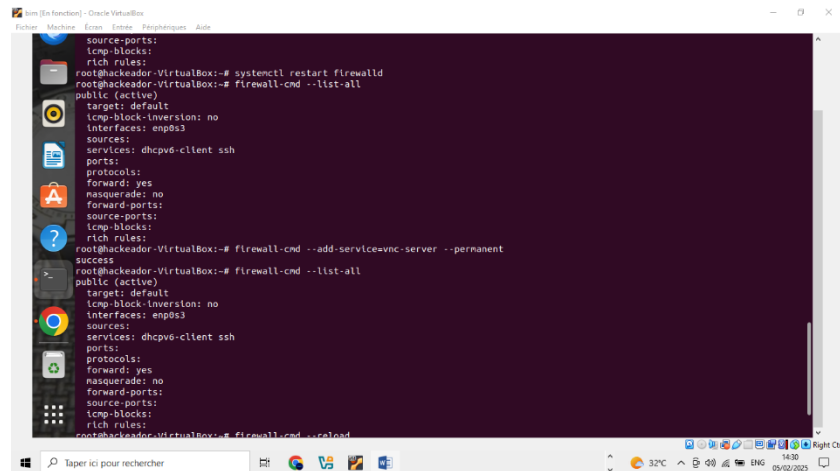
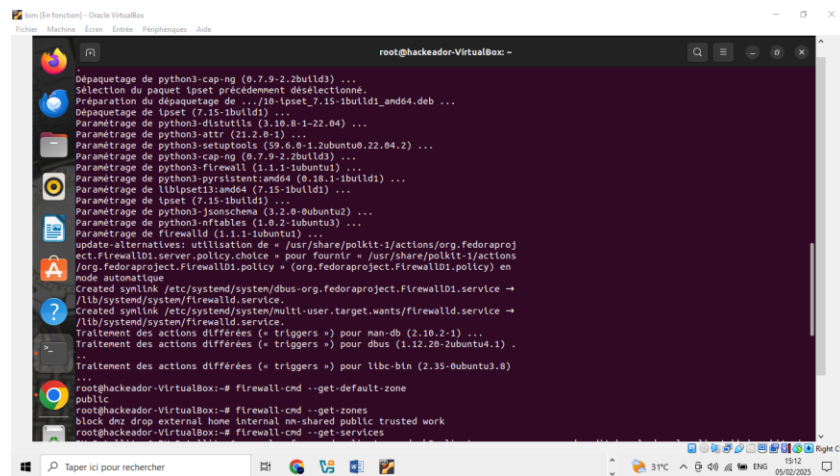
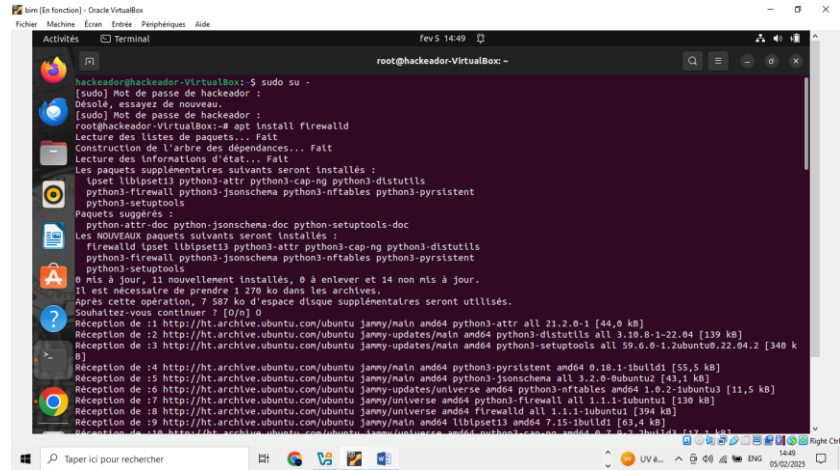
**3<sup>ième</sup> année**

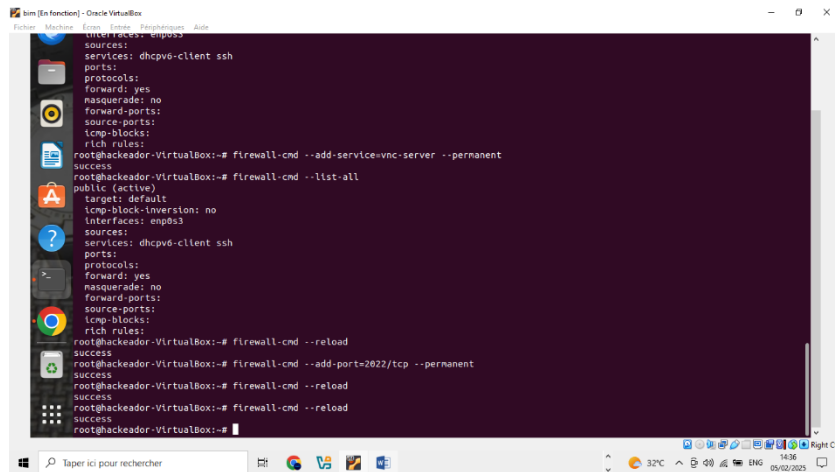
**Année :**

**2024-2025**

**Le 05/02/2025**

## Exécution du TD





```
root@hackador-VirtualBox:~# ufw status
sources:
services: dhcpv6-client ssh
ports:
protocols:
forward: yes
masquerade: no
forward-ports:
source-ports:
icmp-blocks:
rich rules:
root@hackador-VirtualBox:~# firewall-cmd --add-service=vnc-server --permanent
success
root@hackador-VirtualBox:~# firewall-cmd --list-all
public (active)
target: default
icmp-block-inversion: no
interfaces: enp0s3
sources:
services: dhcpv6-client ssh
ports:
protocols:
forward: yes
masquerade: no
forward-ports:
source-ports:
icmp-blocks:
rich rules:
root@hackador-VirtualBox:~# firewall-cmd --reload
success
root@hackador-VirtualBox:~# firewall-cmd --add-port=2022/tcp --permanent
success
root@hackador-VirtualBox:~# firewall-cmd --reload
success
root@hackador-VirtualBox:~# firewall-cmd --reload
success
root@hackador-VirtualBox:~#
```

En conclusion, ce TD nous permet d'apprendre à configurer et gérer un pare-feu sur un système Ubuntu en utilisant ufw (Uncomplicated Firewall) et iptables. Il nous permet aussi d'apprendre à créer des règles pour bloquer ou autoriser le trafic réseau en fonction de vos besoins de sécurité, de comprendre le fonctionnement de SELinux (Security-Enhanced Linux), un mécanisme de sécurité qui impose des politiques d'accès rigoureuses pour protéger les ressources du système contre les attaques.

