**REPUBLIQUE DU CAMEROUN**
Paix – Travail – Patrie

**UNIVERSITE DE YAOUNDE I**

**ECOLE NATIONALE SUPERIEURE POLYTECHNIQUE DE YAOUNDE**

**DEPARTEMENT DE GENIE INFORMATIQUE**

**REPUBLIC OF CAMEROON**
Peace – Work – Fatherland

**UNIVERSITY OF YAOUNDE I**

**NATIONAL ADVANCED SCHOOL OF ENGINEERING OF YAOUNDE**

**DEPARTMENT OF COMPUTER SCIENCE**

# LAB SEMESTRE I

**Participant**

**Matricule :** 22P035

**Spécialité :** Cybersécurité et Investigation Numérique

**Noms :** MBETSI DJOFANG AIME LINDSEY

**Niveau :** 4

**Superviseur**

M. MINKA MI NGUIDJOI Thierry Emmanuel

**Année Scolaire : 2025–2026**

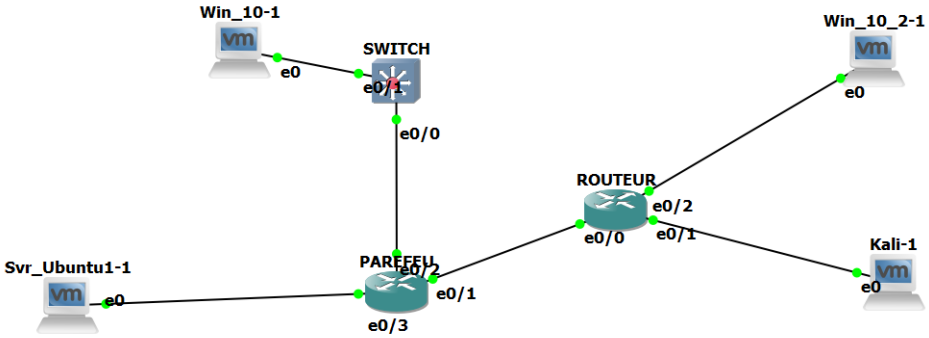
# Table des matières

# Introduction

L'univers numérique est au cœur des enjeux actuels en matière de sécurité informatique. Ce laboratoire porte sur l'introduction aux techniques d'investigation numérique, visant à comprendre et mettre en œuvre les configurations réseau essentielles pour sécuriser et analyser les architectures informatiques. Le travail réalisé inclut la construction d'une architecture réseau en DMZ composée d'un serveur web Ubuntu et d'un parefeu, ainsi que la configuration de routeurs, machines Windows et Linux, en vue de maîtriser les outils et les concepts clés en cybersécurité et investigation numérique.

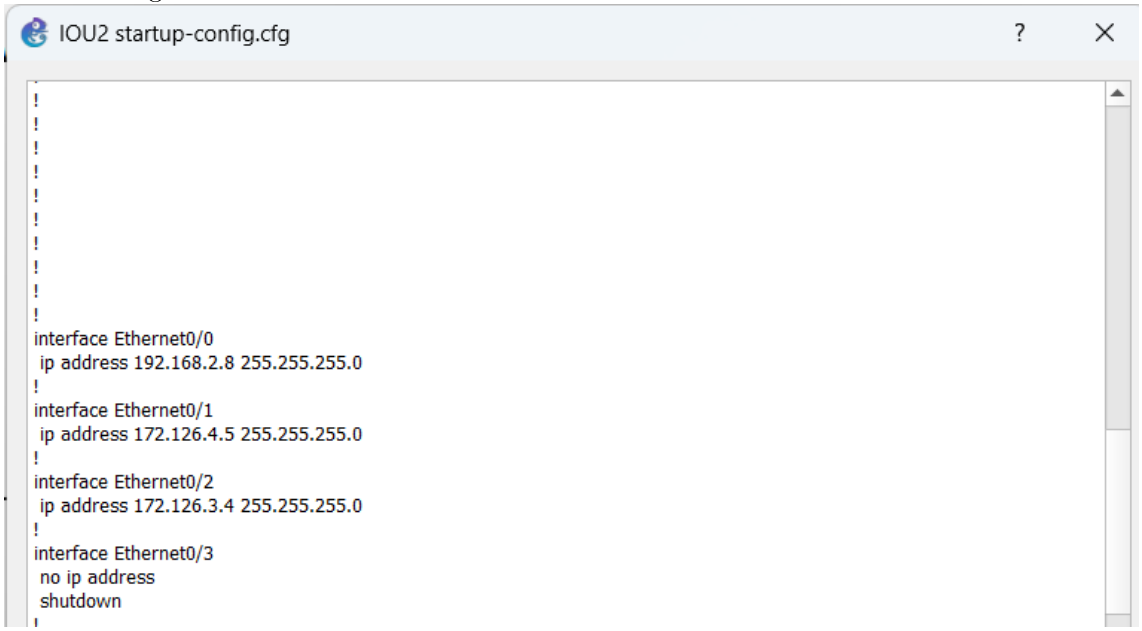
# 1 Construction de l'architecture du lab

- Une DMZ : constiuée d'un serveur web ubuntu et d'un parefeu (routeur+ACL)
- Un routeur
- 2 ordinateurs dans des réseaux ayant l'accès aux services web du serveur
- Un ordinateur dans un réseau n'ayant pas l'accès aux services web du serveur
- Un switch

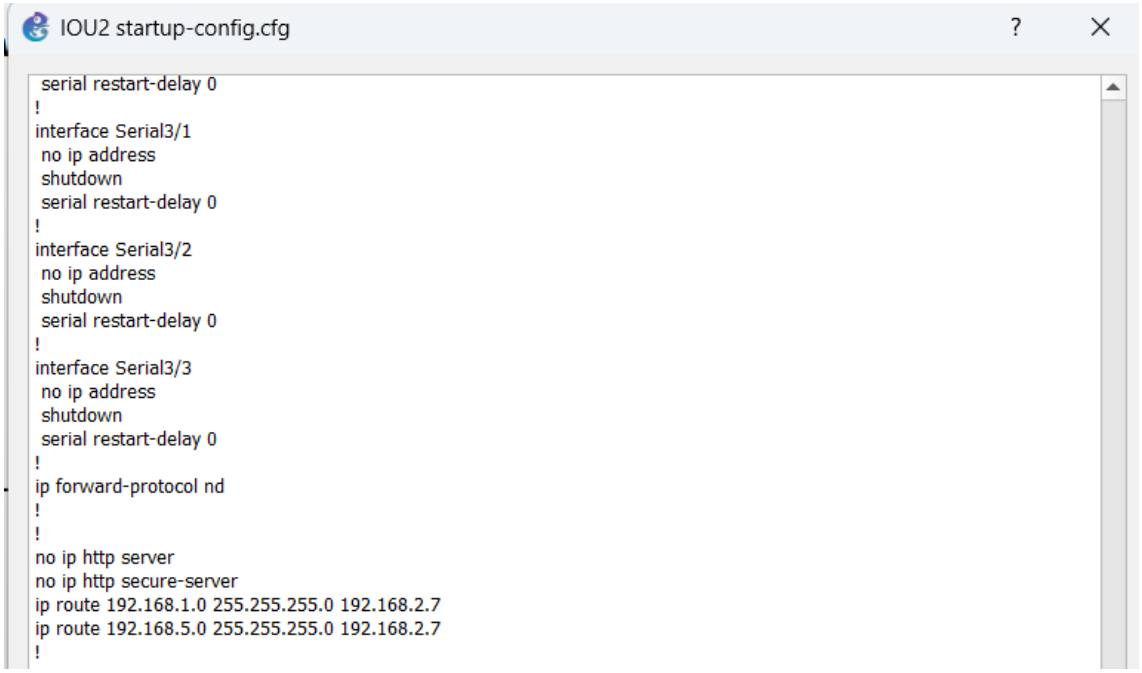



# 2 Configuration du routeur

Adressage des interfaces du routeur conformément aux adresses données

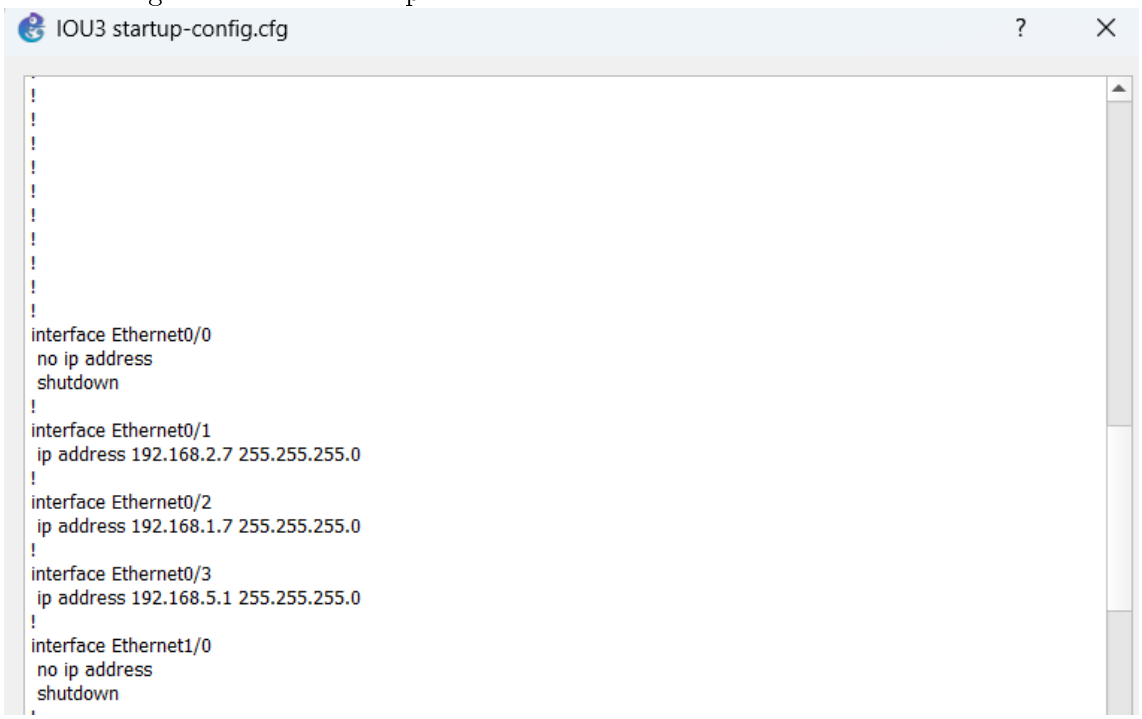



Création des routes




# 3 Configuration du parefeu

Adressage des interfaces du parefeu conformément aux adresses données




Création des routes

IOU3 startup-config.cfg

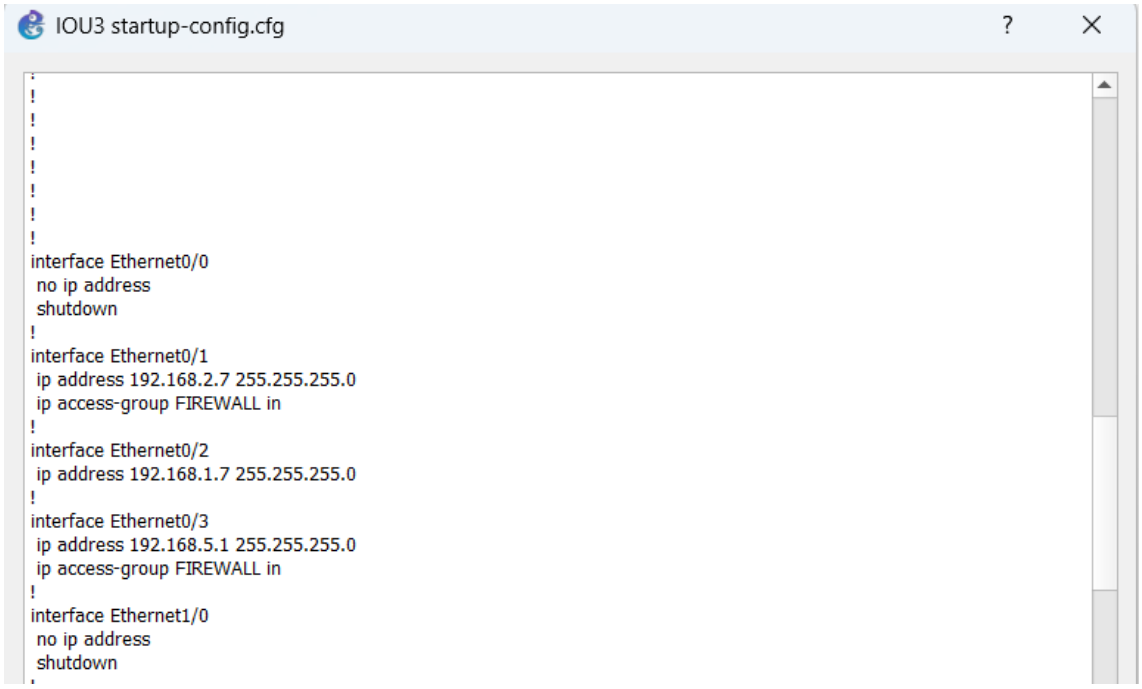
```
interface Serial3/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/3
 no ip address
 shutdown
 serial restart-delay 0
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip route 172.126.3.0 255.255.255.0 192.168.2.8
ip route 172.126.4.0 255.255.255.0 192.168.2.8
!
```

Création des listes de contrôle d'accès

IOU3 startup-config.cfg

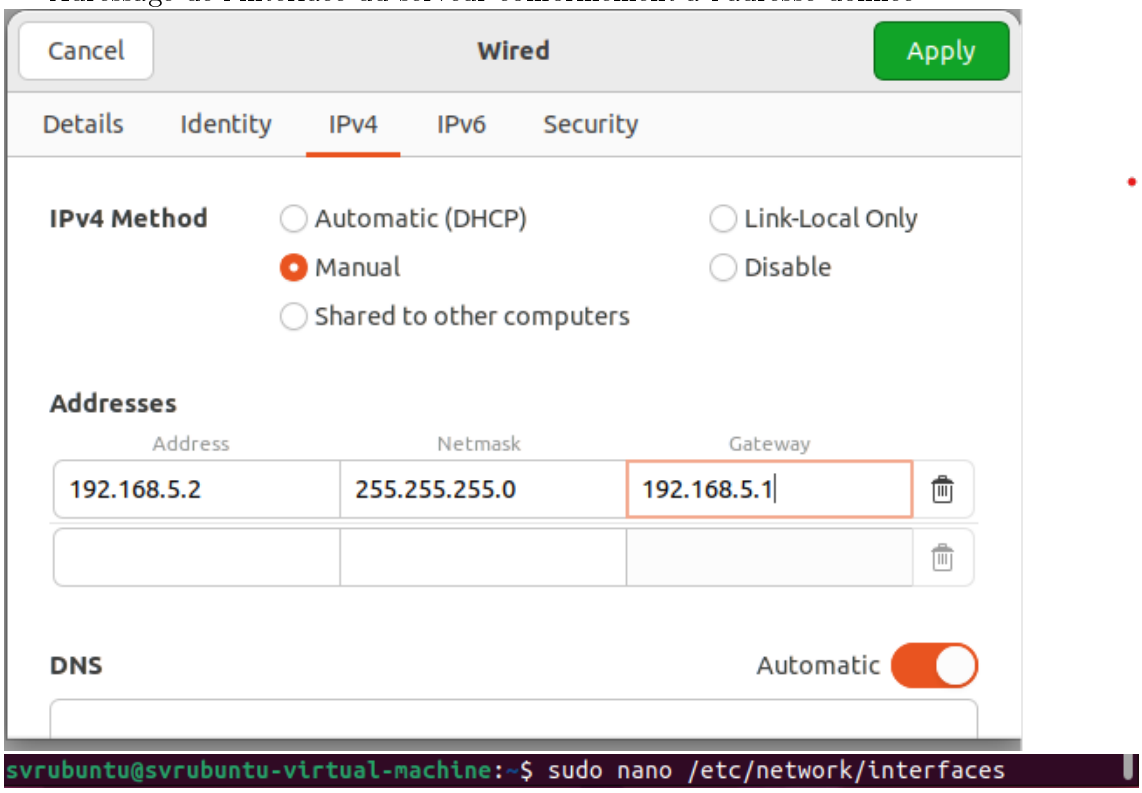
```
 shutdown
 serial restart-delay 0
!
interface Serial3/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/3
 no ip address
 shutdown
 serial restart-delay 0
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip route 172.126.3.0 255.255.255.0 192.168.2.8
ip route 172.126.4.0 255.255.255.0 192.168.2.8
!
ip access-list extended FIREWALL
 permit ip 172.126.4.0 0.0.0.255 192.168.5.0 0.0.0.255
 permit ip 172.126.3.0 0.0.0.255 192.168.5.0 0.0.0.255
 permit ip 192.168.5.0 0.0.0.255 172.126.4.0 0.0.0.255
 permit ip 192.168.5.0 0.0.0.255 172.126.3.0 0.0.0.255
 deny   ip any any
!
```

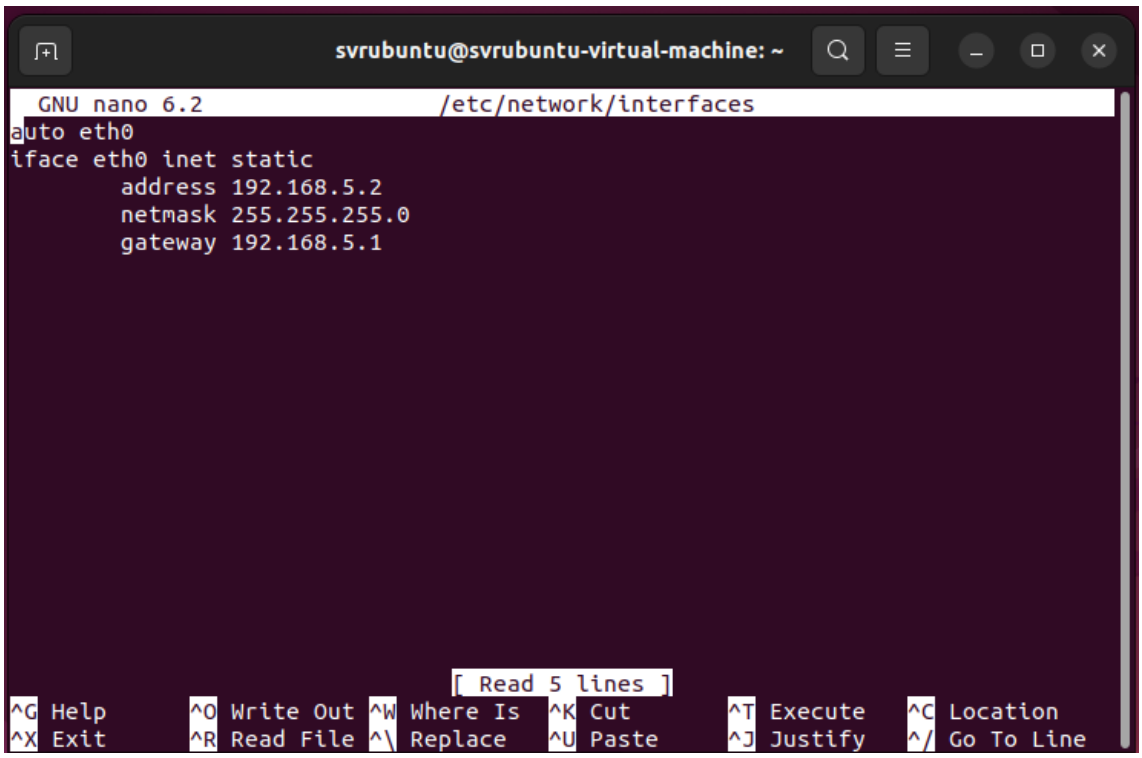
Attribution des ACL aux interfaces concernées



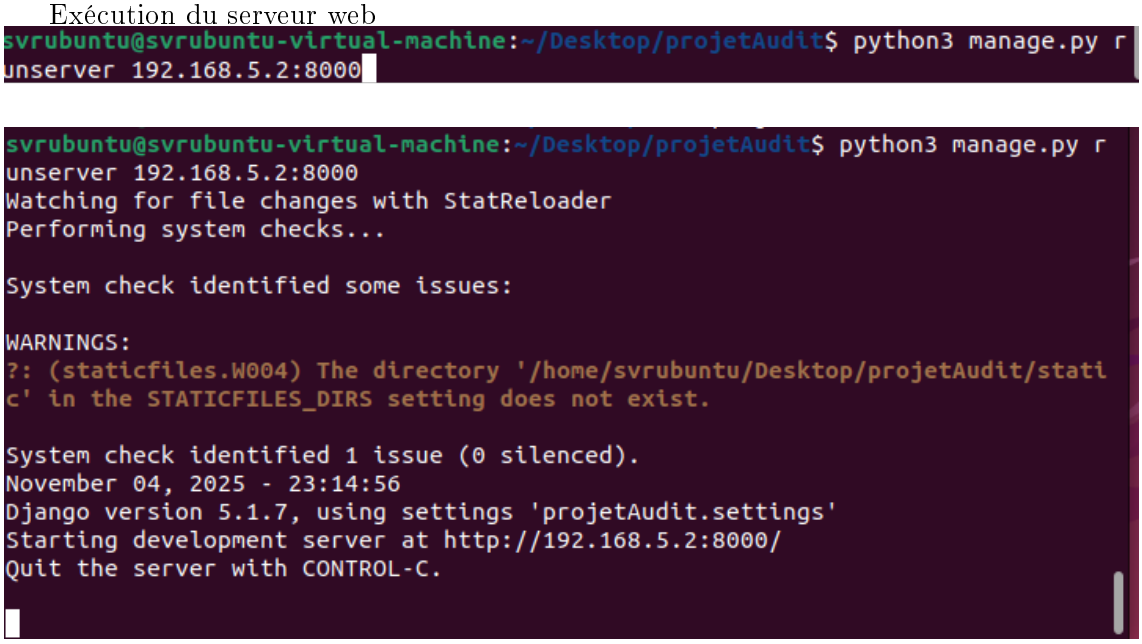

# 4 Configuration du serveur ubuntu

Adressage de l'interface du serveur conformément à l'adresse donnée



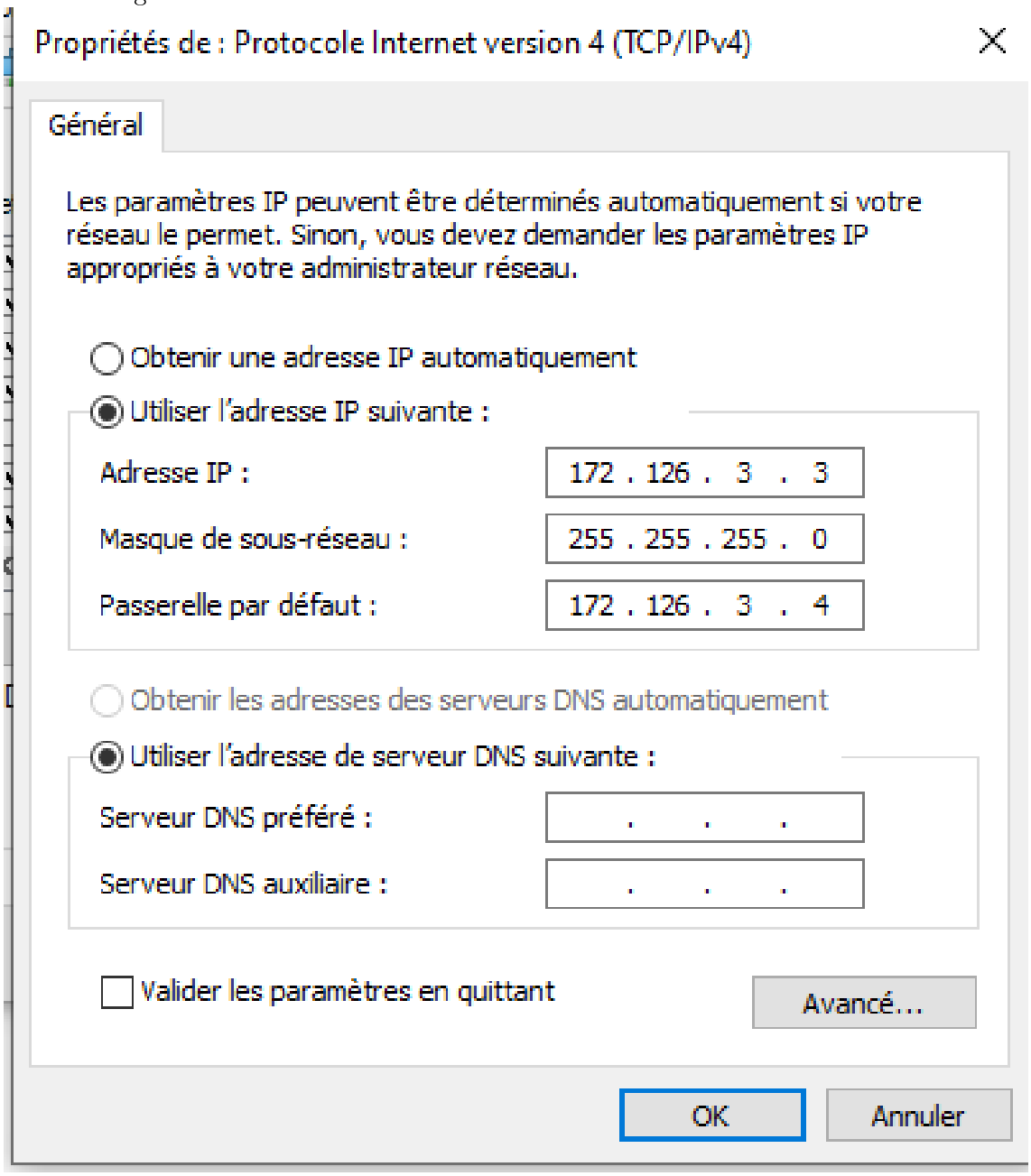



Exécution du serveur web

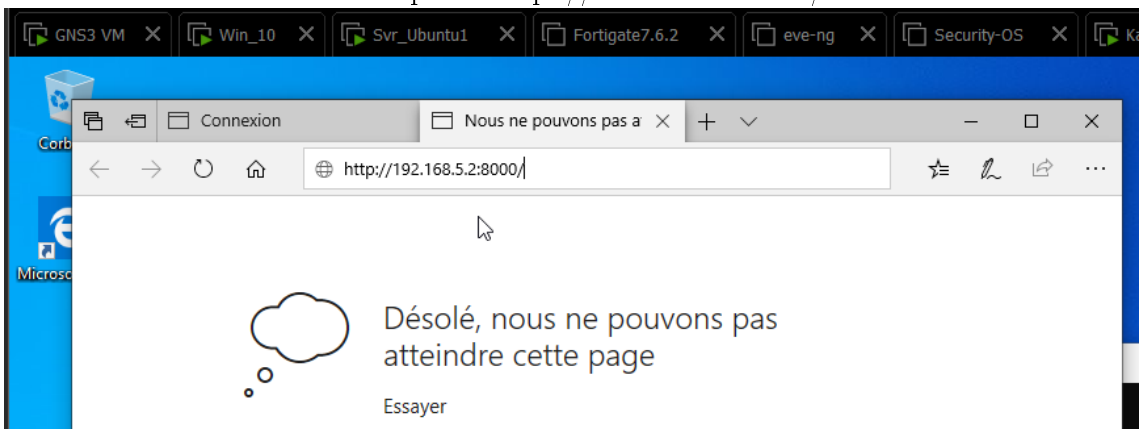


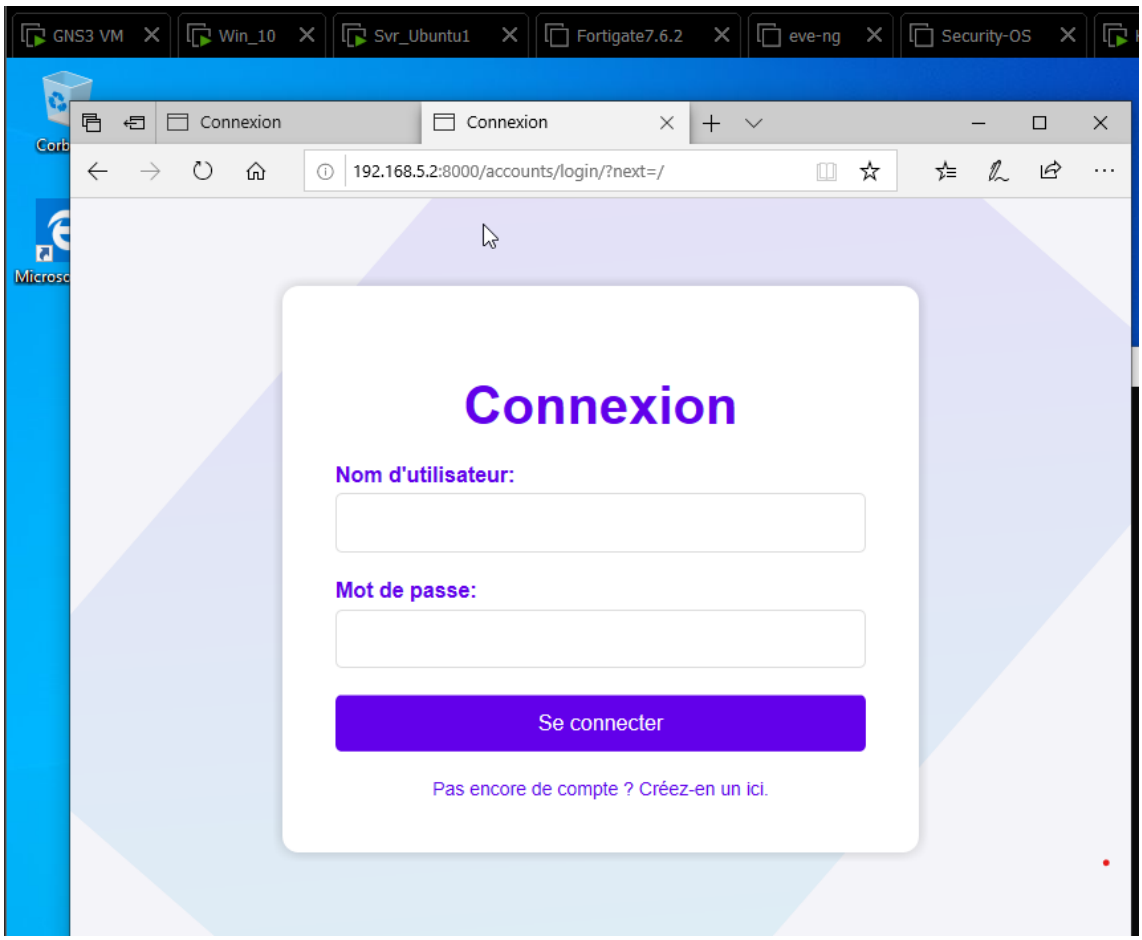
# 5 Configuration de la 2é machine windows

Adressage de l'interface du serveur conformément à l'adresse donnée



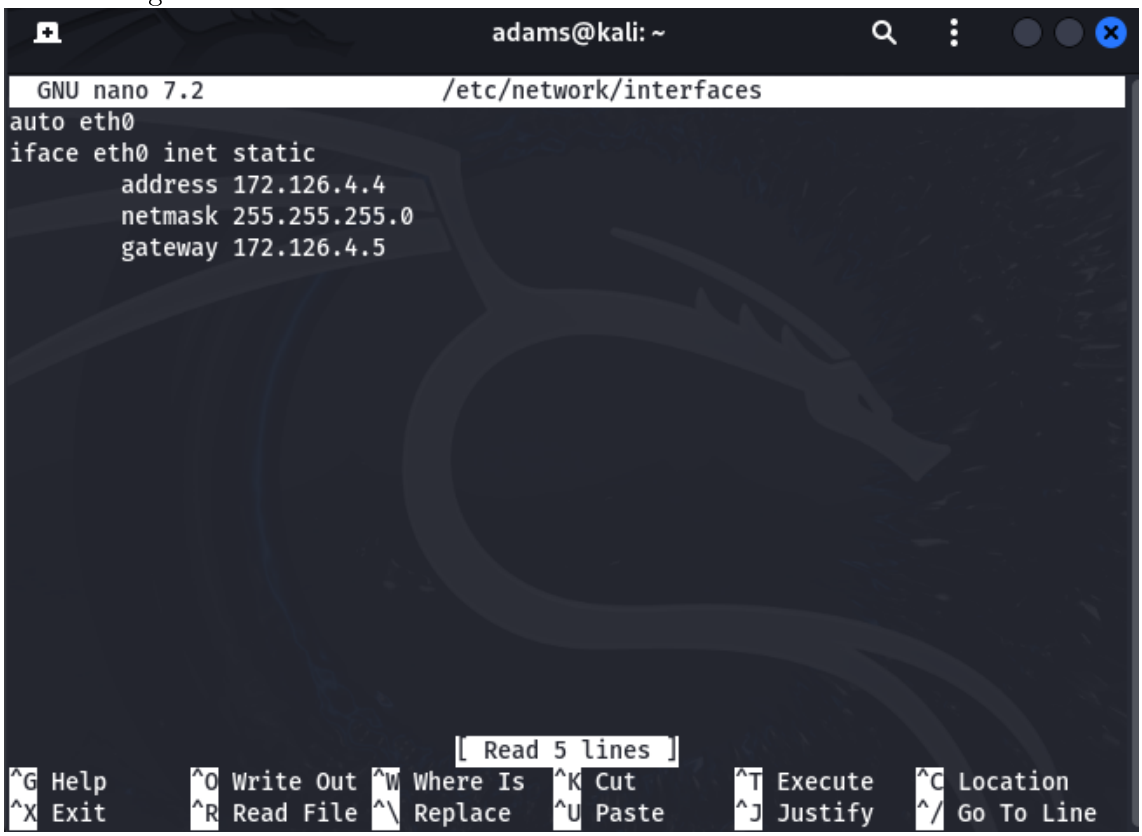

Connexion au site web en tapant : http ://192.168.5.2 :8000/

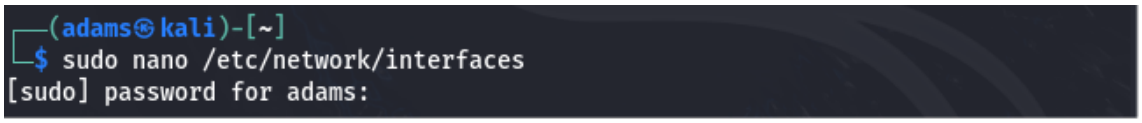



GNS3 VM
Win_10
Svr_Ubuntu1
Fortigate7.6.2
eve-ng
Security-OS
Connexion
Connexion
192.168.5.2:8000/accounts/login/?next=/
Connexion
Nom d'utilisateur:
Mot de passe:
Se connecter
Pas encore de compte ? Créez-en un ici.

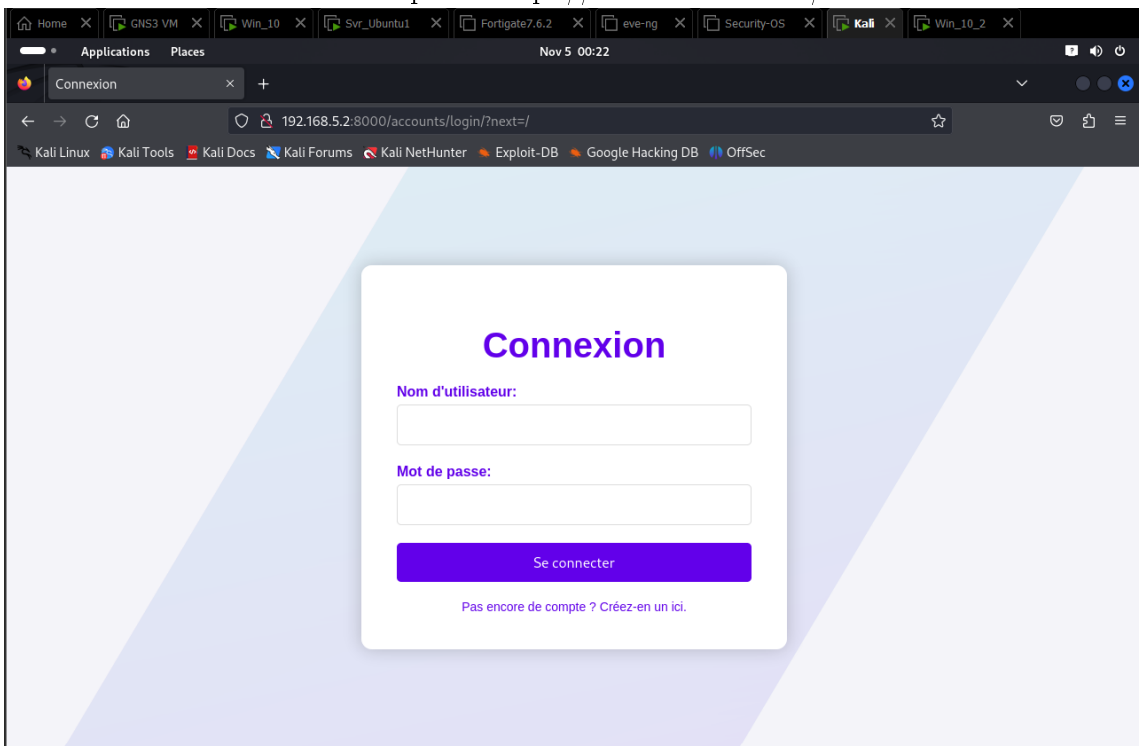
# 6 Configuration de la machine Linux

Adressage de l'interface de la machine Kali conformément à l'adresse donnée



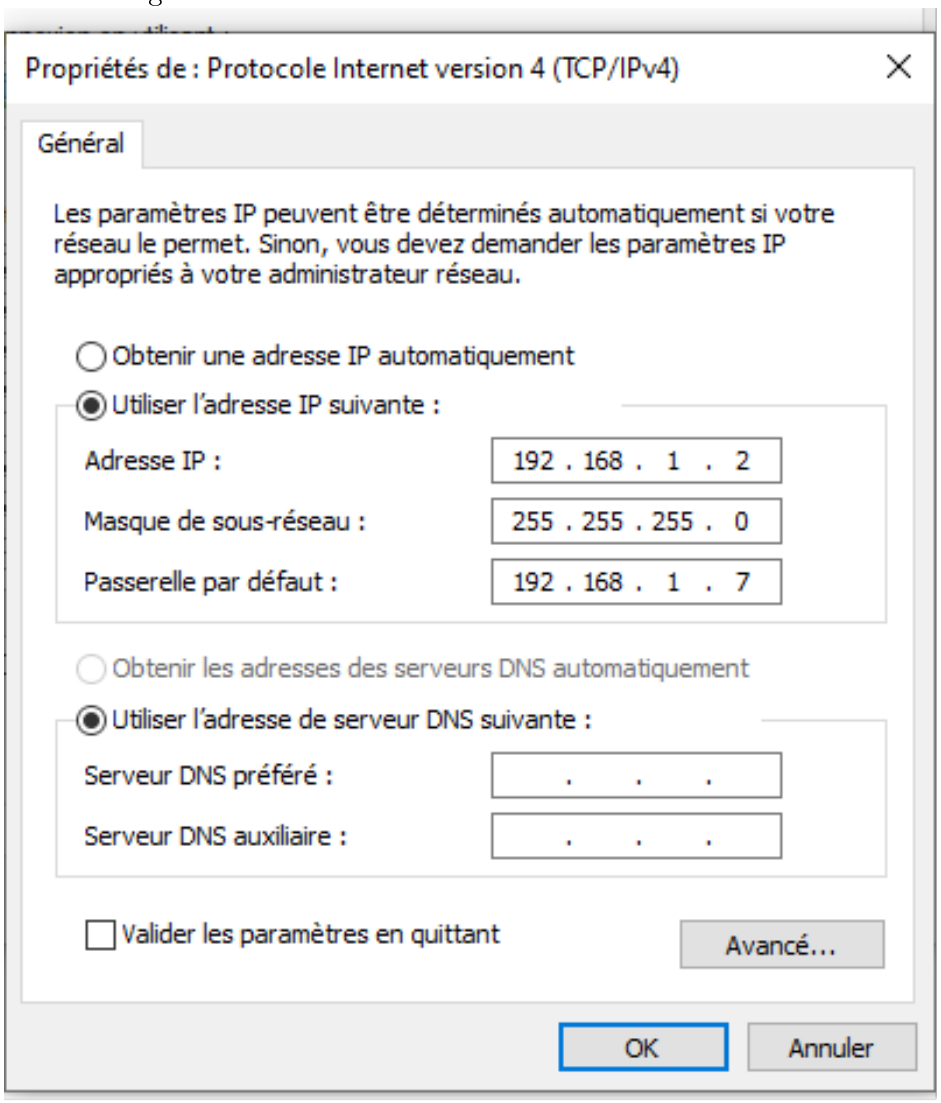




Connexion au site web en tapant : http ://192.168.5.2 :8000/



# 7 Configuration de la 1ère machine windows

Adressage de l'interface de la machine Kali conformément à l'adresse donnée




NB : Le réseau n'a pas accès au site web car il a été bloqué par les ACL configurés dans le roteur ayant le rôle de parefeu

# Conclusion

Ce laboratoire a permis de mettre en pratique les principes fondamentaux de l'investigation numérique et de la cybersécurité, notamment à travers la construction et configuration d'une architecture réseau sécurisée. L'approche adoptée, incluant la mise en place de contrôles d'accès et la configuration des différents équipements réseau, est essentielle pour garantir la sécurité des systèmes d'information. Cette expérience contribue à renforcer les compétences techniques indispensables pour identifier, analyser et contrer les menaces dans un environnement numérique sécurisé.