

**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

## Table des matières

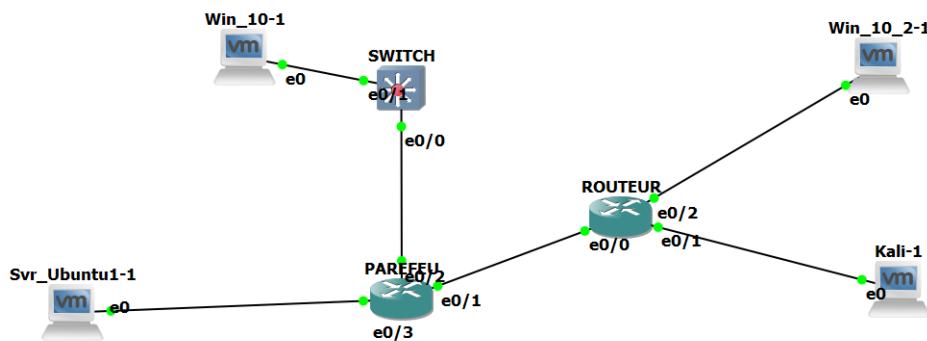
<b>Introduction</b>	<b>3</b>
<b>1 Construction de l'architecture du lab</b>	<b>4</b>
<b>2 Configuration du routeur</b>	<b>4</b>
<b>3 Configuration du parefeu</b>	<b>5</b>
<b>4 Configuration du serveur ubuntu</b>	<b>7</b>
<b>5 Configuration de la 2é machine windows</b>	<b>9</b>
<b>6 Configuration de la machine Linux</b>	<b>11</b>
<b>7 Configuration de la 1ère machine windows</b>	<b>12</b>
<b>Conclusion</b>	<b>13</b>

# 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 : constituée 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

IOU2 startup-config.cfg

```

!
!
!
!
!
!
!
interface Ethernet0/0
ip address 192.168.2.8 255.255.255.0
!
interface Ethernet0/1
ip address 172.126.4.5 255.255.255.0
!
interface Ethernet0/2
ip address 172.126.3.4 255.255.255.0
!
interface Ethernet0/3
no ip address
shutdown
!
```

Création des routes

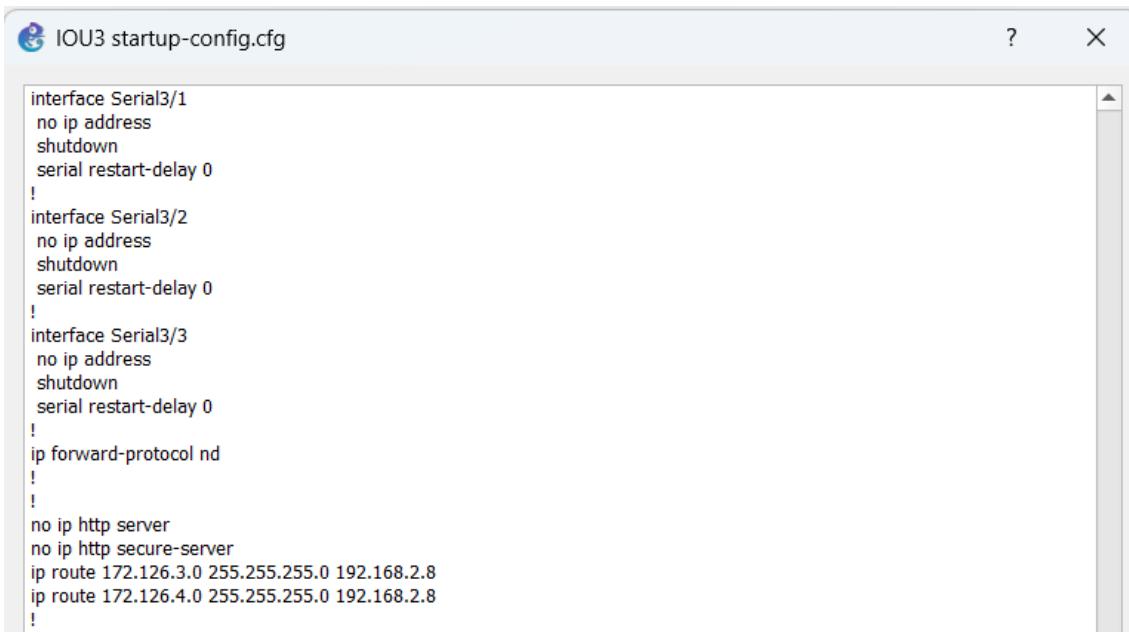
```
!IOU2 startup-config.cfg ? X
serial restart-delay 0
!
interface Serial3/1
no ip address
shutdown
serial restart-delay 0
!
interface Serial3/2
no ip address
shutdown
serial restart-delay 0
!
interface Serial3/3
no ip address
shutdown
serial restart-delay 0
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip route 192.168.1.0 255.255.255.0 192.168.2.7
ip route 192.168.5.0 255.255.255.0 192.168.2.7
!
```

### 3 Configuration du parefeu

Adressage des interfaces du parefeu conformément aux adresses données

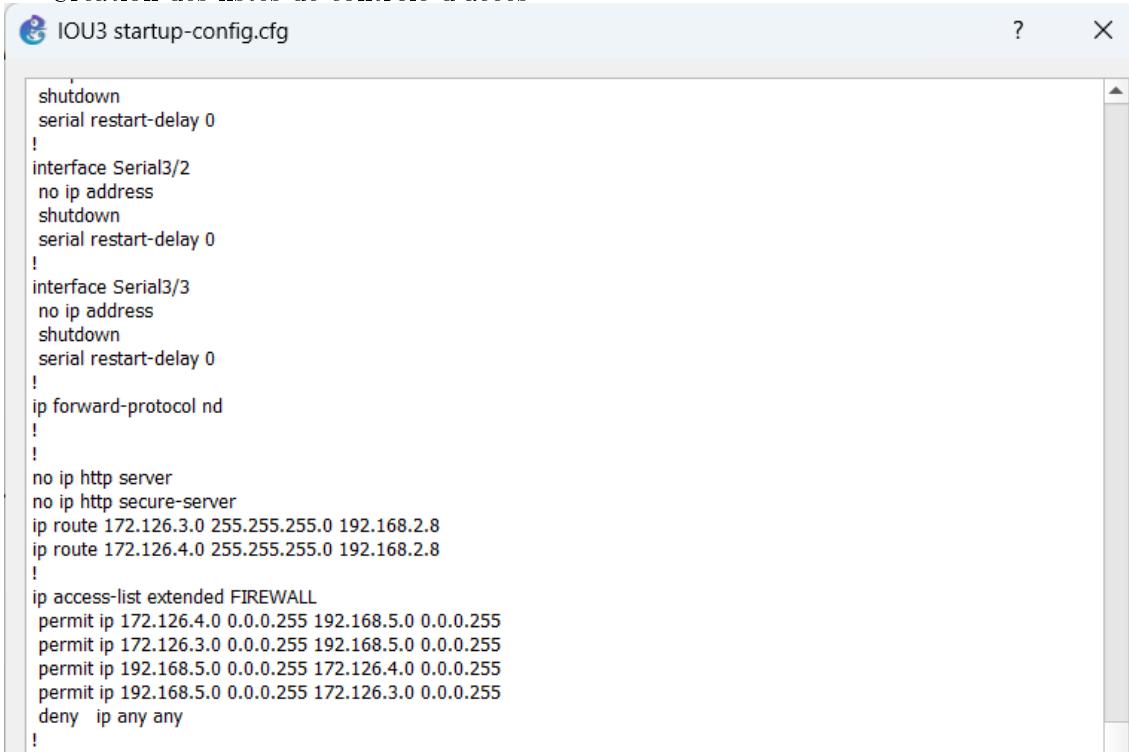
```
!  
!  
!  
!  
!  
!  
!  
!  
interface Ethernet0/0  
no ip address  
shutdown  
!  
interface Ethernet0/1  
ip address 192.168.2.7 255.255.255.0  
!  
interface Ethernet0/2  
ip address 192.168.1.7 255.255.255.0  
!  
interface Ethernet0/3  
ip address 192.168.5.1 255.255.255.0  
!  
interface Ethernet1/0  
no ip address  
shutdown
```

## Création des routes



```
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



```
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

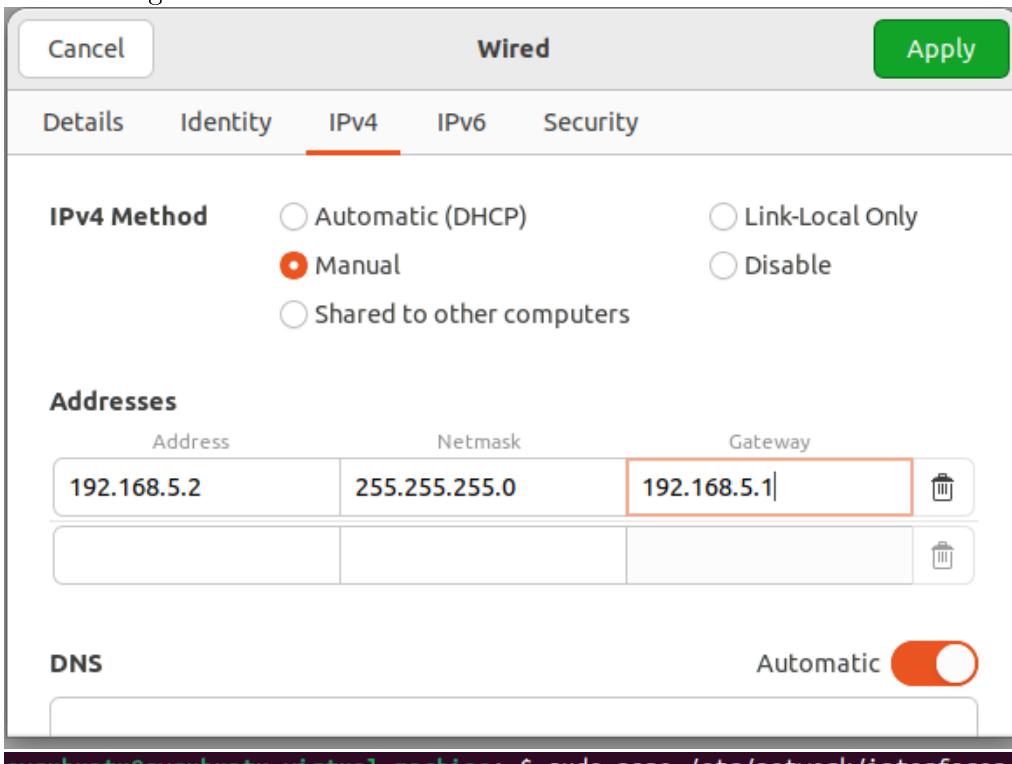
```

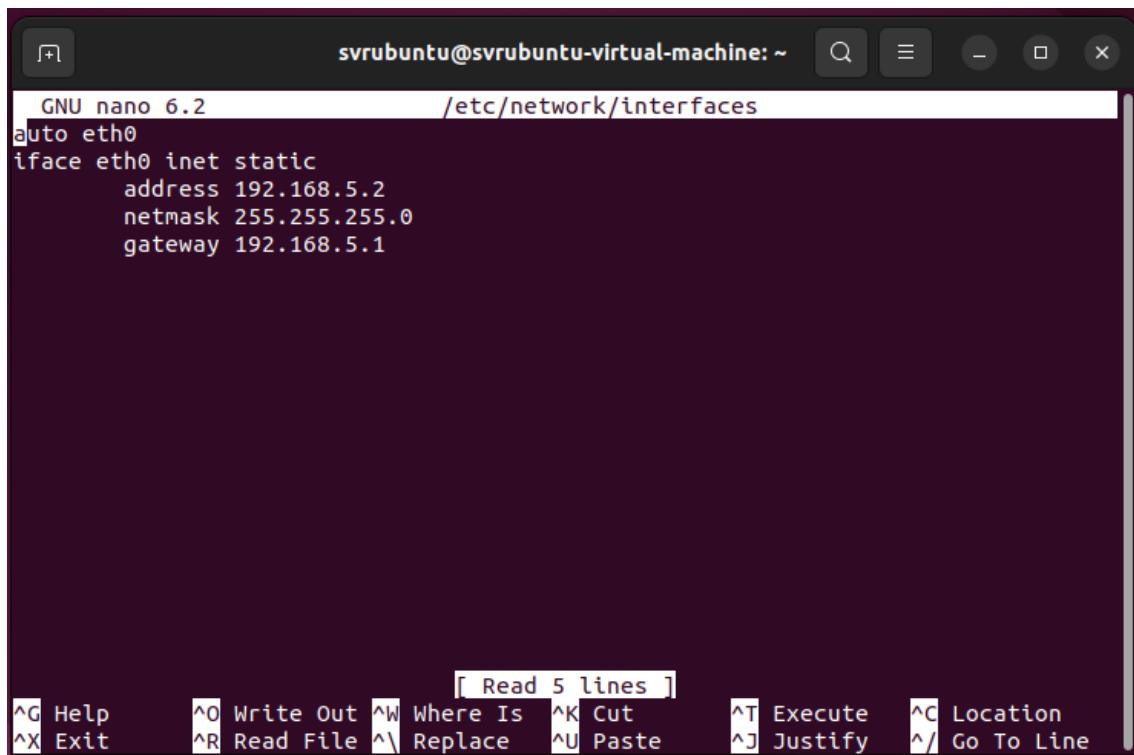
!
!
!
!
!
interface Ethernet0/0
no ip address
shutdown
!
interface Ethernet0/1
ip address 192.168.2.7 255.255.255.0
ip access-group FIREWALL in
!
interface Ethernet0/2
ip address 192.168.1.7 255.255.255.0
!
interface Ethernet0/3
ip address 192.168.5.1 255.255.255.0
ip access-group FIREWALL in
!
interface Ethernet1/0
no ip address
shutdown

```

## 4 Configuration du serveur ubuntu

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





```
GNU nano 6.2          /etc/network/interfaces
auto eth0
iface eth0 inet static
    address 192.168.5.2
    netmask 255.255.255.0
    gateway 192.168.5.1
```

[ Read 5 lines ]

**^G Help** **^O Write Out** **^W Where Is** **^K Cut** **^T Execute** **^C Location**  
**^X Exit** **^R Read File** **^\\ Replace** **^U Paste** **^J Justify** **^/ Go To Line**

Exécution du serveur web

```
svrubuntu@svrubuntu-virtual-machine:~/Desktop/projetAudit$ python3 manage.py runserver 192.168.5.2:8000
```

```
svrubuntu@svrubuntu-virtual-machine:~/Desktop/projetAudit$ python3 manage.py runserver 192.168.5.2:8000
Watching for file changes with StatReloader
Performing system checks...

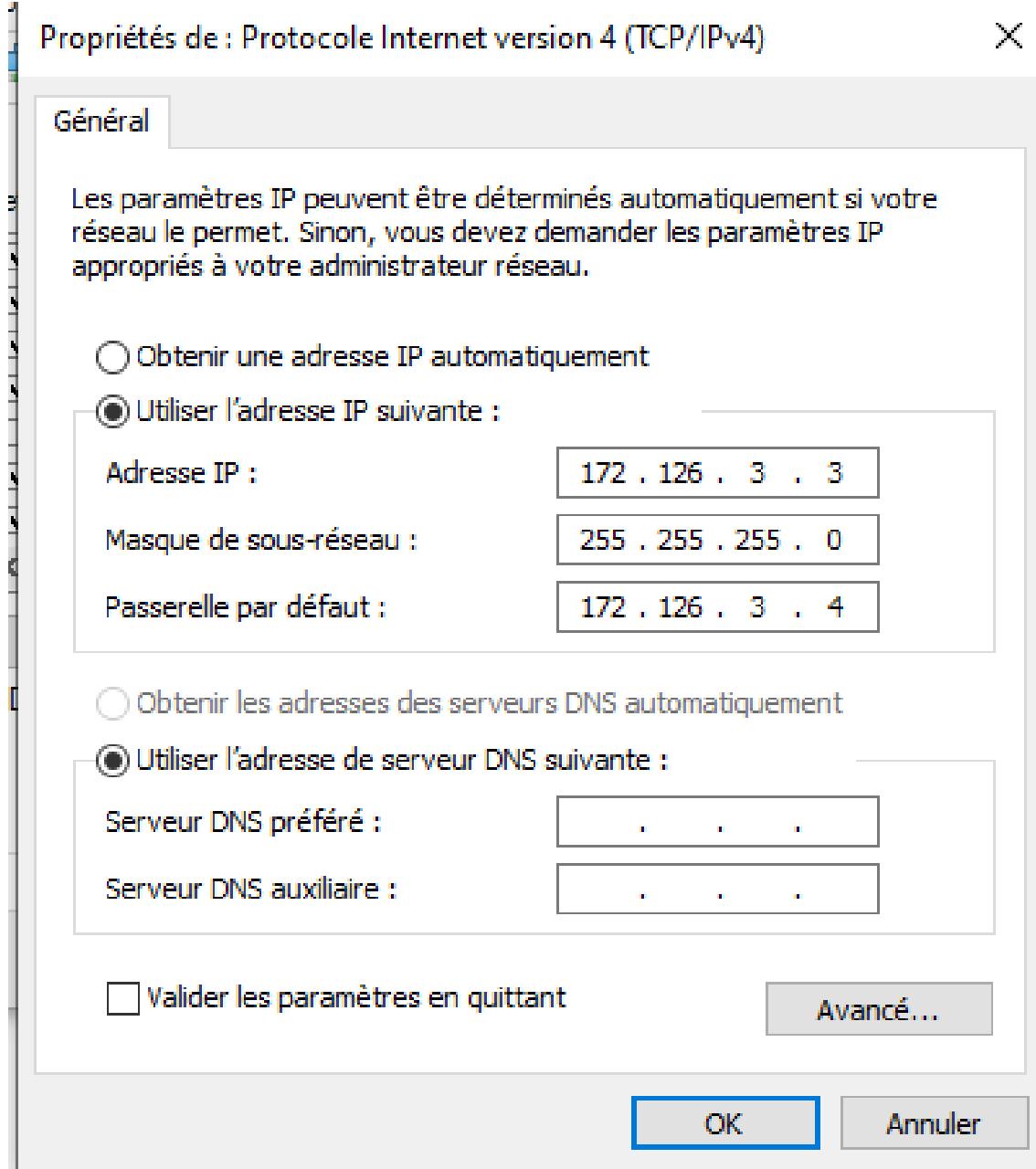
System check identified some issues:

WARNINGS:
?: (staticfiles.W004) The directory '/home/svrubuntu/Desktop/projetAudit/static' in the STATICFILES_DIRS setting does not exist.

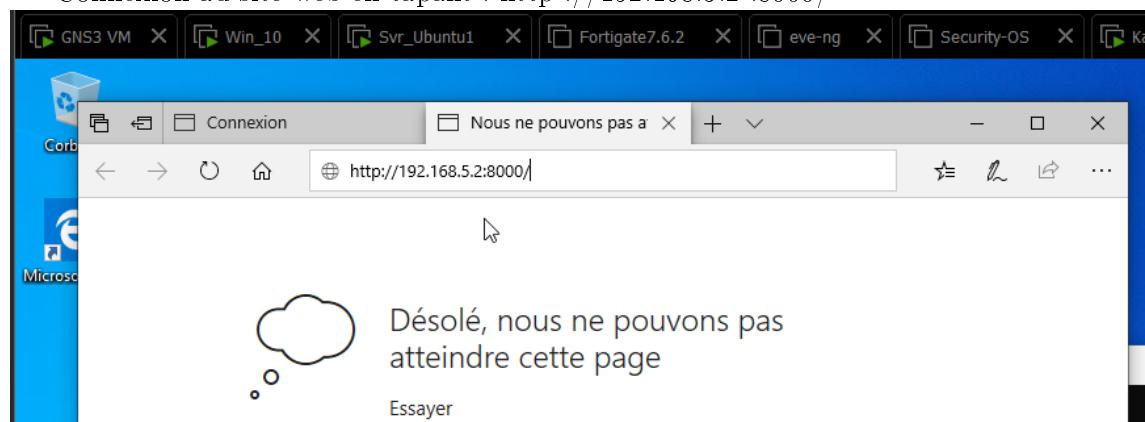
System check identified 1 issue (0 silenced).
November 04, 2025 - 23:14:56
Django version 5.1.7, using settings 'projetAudit.settings'
Starting development server at http://192.168.5.2:8000/
Quit the server with CONTROL-C.
```

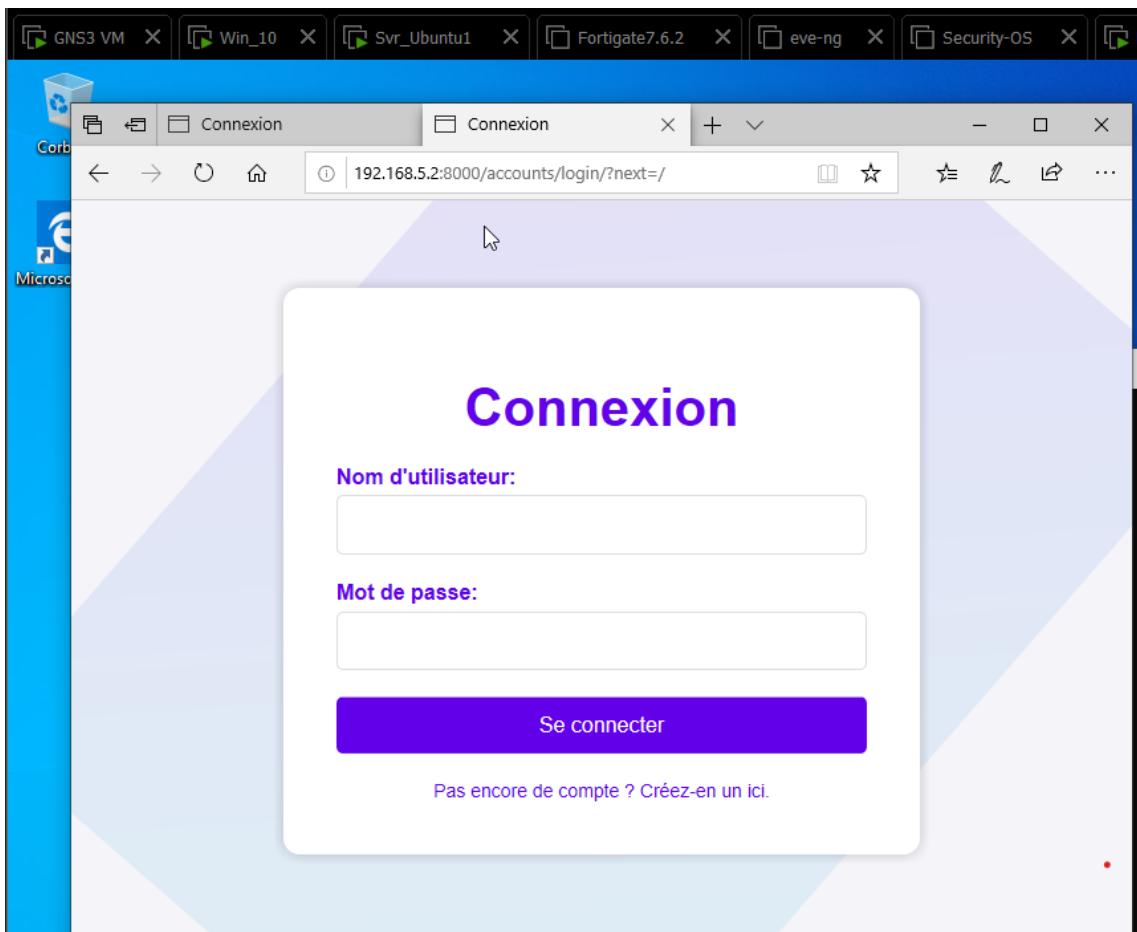
## 5 Configuration de la 2é machine windows

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



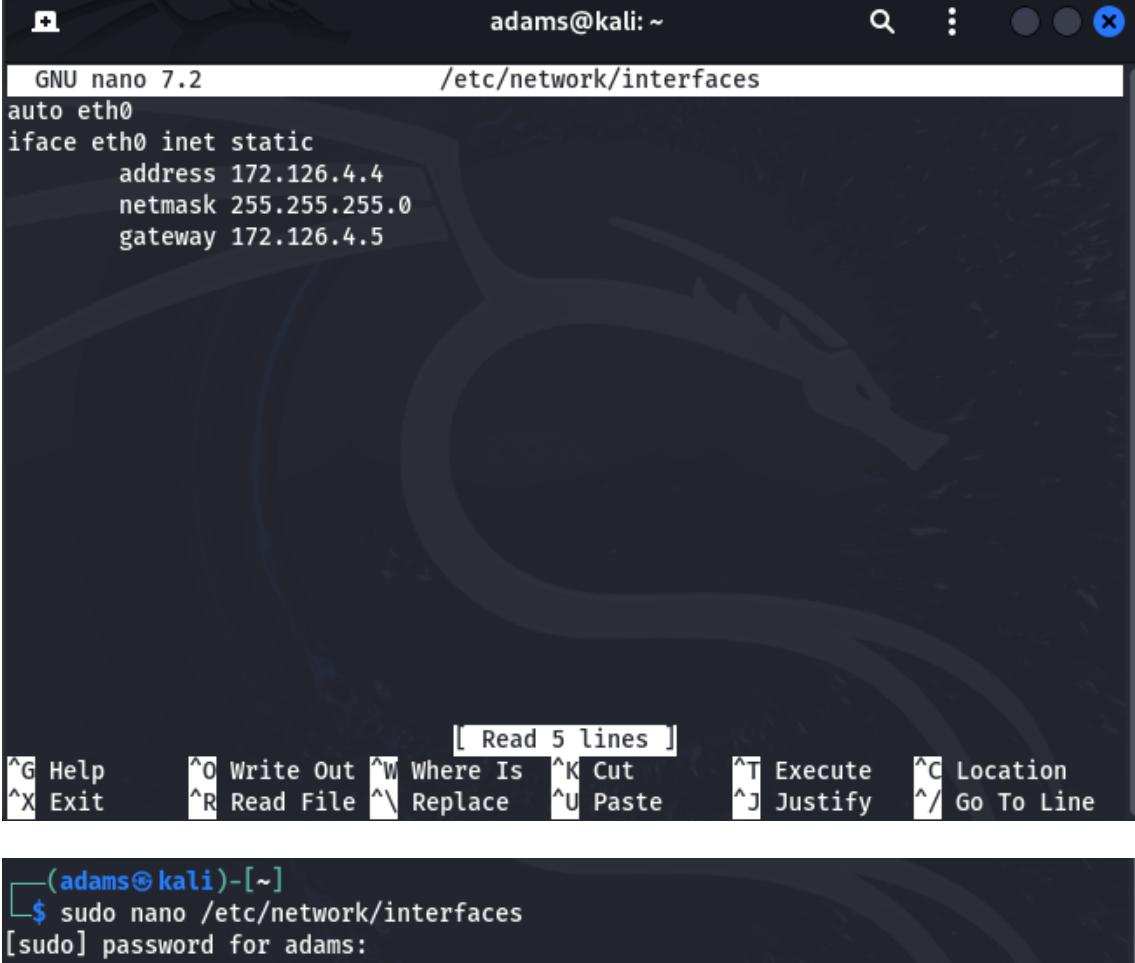
Connexion au site web en tapant : http://192.168.5.2:8000/





## 6 Configuration de la machine Linux

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

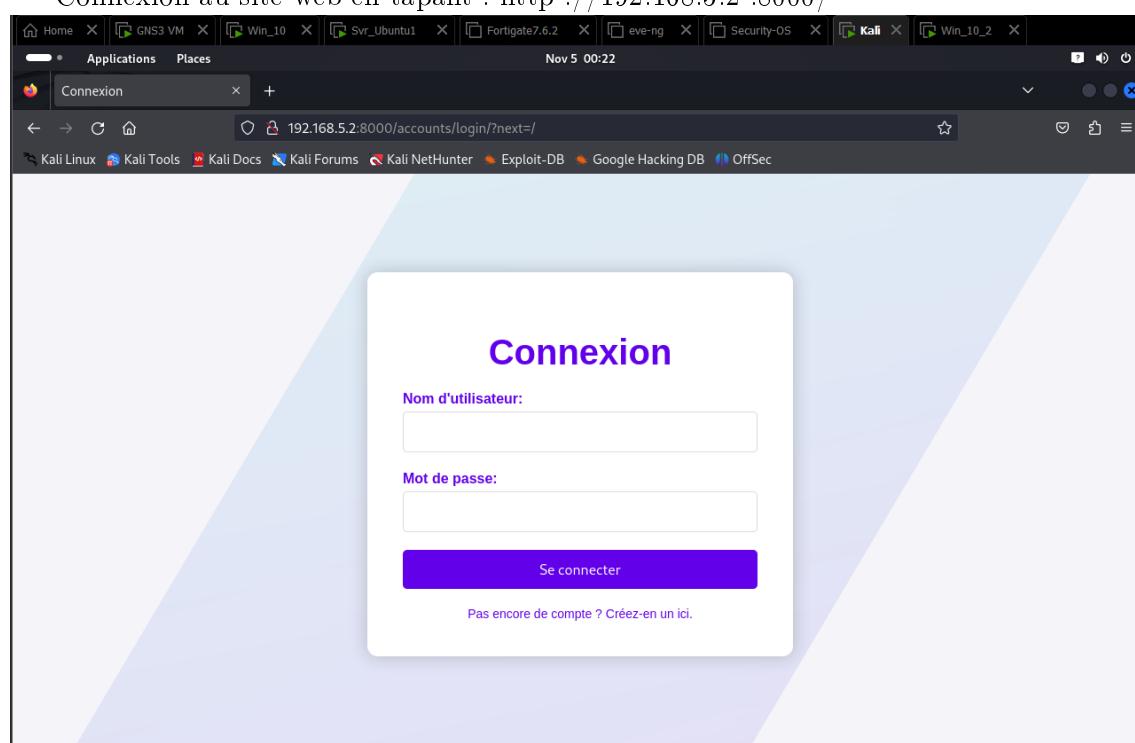


```
GNU nano 7.2          /etc/network/interfaces
auto eth0
iface eth0 inet static
    address 172.126.4.4
    netmask 255.255.255.0
    gateway 172.126.4.5

[ Read 5 lines ]
^G Help      ^O Write Out ^W Where Is  ^K Cut        ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^/ Go To Line
```

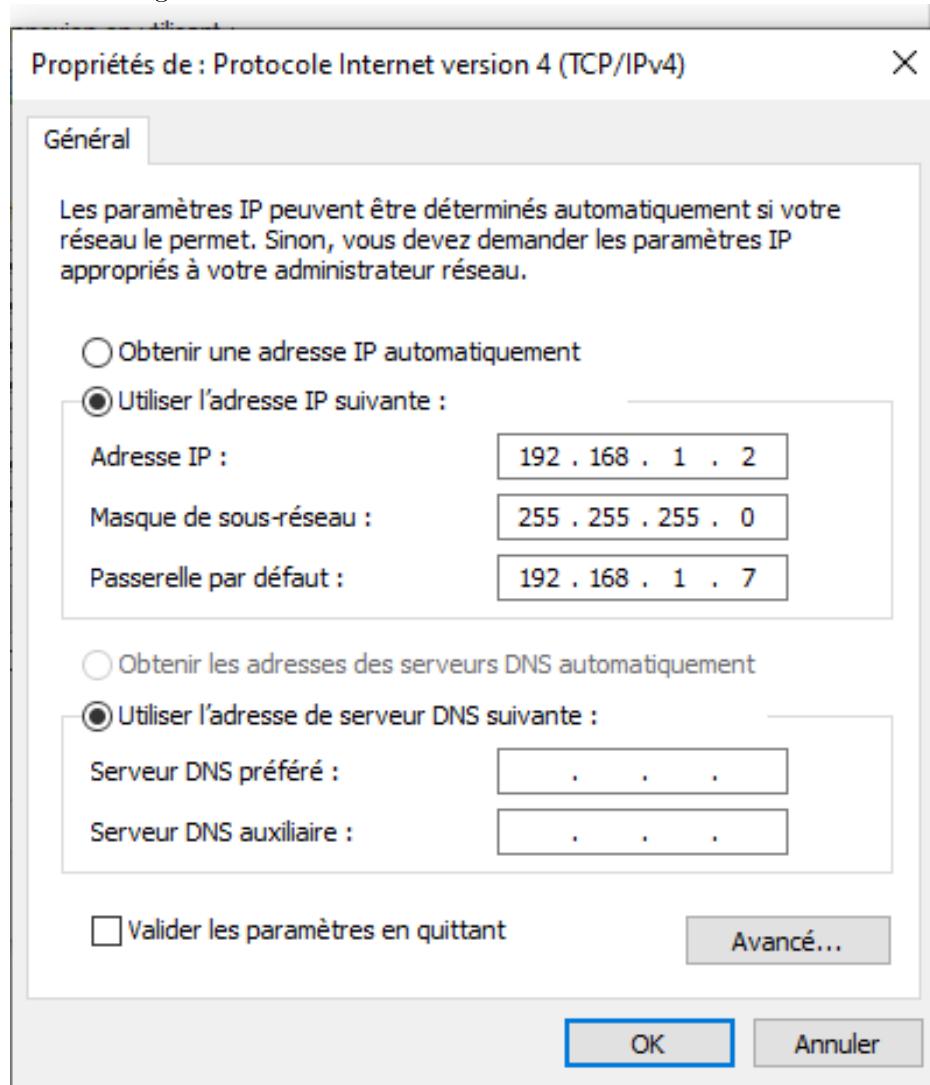
(adams@kali)-[~]\$ sudo nano /etc/network/interfaces  
[sudo] password for adams:

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 routeur 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.