



ÉCOLE NATIONALE SUPÉRIEURE POLYTECHNIQUE DE YAOUNDÉ

DÉPARTEMENT DE GÉNIE INFORMATIQUE

INTRODUCTION AUX TECHNIQUES D'INVESTIGATION NUMÉRIQUE

Rapport de configuration d'une infrastructure réseau fonctionnelle



MAKEU TENKU STELY BELVA
CIN-4

Superviseur : M. THIERRY
MINKA

Table des matières

Introduction	2
1 Objectif du Lab	3
2 Topologie et Description du Réseau	4
2.1 Schéma logique	4
2.2 Description des composants	4
3 Matériel et Logiciels Utilisés	6
4 Étapes de Réalisation	7
4.1 Création des Machines Virtuelles	7
4.2 Création de l'Infrastructure dans GNS3	7
4.3 Tests de Connectivité	8
5 Résultats et Vérifications	9
Conclusion	14

Introduction

Ce premier laboratoire a pour objectif de configurer une infrastructure réseau complète, fonctionnelle et sécurisée. L'environnement comprend un routeur en frontière, une zone démilitarisée (DMZ) hébergeant un serveur web sous Linux, et un réseau local (LAN) contenant un poste de travail Windows. Cette mise en place vise à fournir une base pour des activités d'investigation numérique simulant une entreprise victime d'un ransomware.

Chapitre 1

Objectif du Lab

Ce laboratoire permet de :

- Configurer un réseau fonctionnel comprenant un équipement de frontière, un LAN et une DMZ;
- Mettre en place un serveur web accessible depuis l'intérieur et l'extérieur du réseau;
- Configurer les adresses IP, les interfaces réseau et les politiques de sécurité;
- Tester la connectivité et la disponibilité des ressources.

Chapitre 2

Topologie et Description du Réseau

2.1 Schéma logique

Le réseau comporte trois segments principaux : un réseau externe (Internet), une DMZ, et un réseau local (LAN). Le schéma ci-dessous illustre l'architecture mise en œuvre.

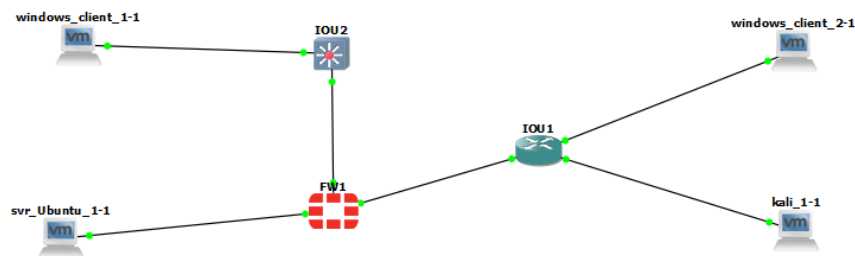


FIGURE 2.1 – Topologie du réseau dans GNS3

2.2 Description des composants

- **Routeur** : assure la connectivité entre le réseau externe et le réseau interne ;
- **Switch manageable** : permet la segmentation en sous-réseaux et la communication inter-réseaux ;
- **Pare-feu** : contrôle les flux entre le LAN et la DMZ ;
- **Serveur Linux** : héberge une application web ;

- **Poste Windows** : simule un utilisateur interne.

Chapitre 3

Matériel et Logiciels Utilisés

Composant	Logiciel / Matériel	Version	Rôle
Routeur	Cisco IOL	-	Équipement de frontière
Pare-feu	FortiGate	-	Sécurisation de la DMZ
Switch	Switch manageable IOL	-	Communication inter-réseaux
Machine virtuelle Windows	Windows 10	-	Poste client LAN
Machine virtuelle Linux	Ubuntu / Kali linux	-	Serveur Web
Logiciel de virtualisation	VMware	-	Hébergement des VM
Simulateur réseau	GNS3	-	Simulation de l'infrastructure

TABLE 3.1 – Matériel et logiciels utilisés dans le Lab

Chapitre 4

Étapes de Réalisation

4.1 Création des Machines Virtuelles

Machine Windows 10

- Disque dur : 10 Go
- RAM : 2 Go
- Données copiées : 2 Go de fichiers variés
- Rôle : Poste de travail utilisateur sur le LAN

Machine Linux (serveur web)

- Disque dur : 10 Go
- RAM : 2 Go
- Distribution : Ubuntu
- Application web déployée via Django

4.2 Création de l'Infrastructure dans GNS3

1. Installation de GNS3 et création du projet LAB1.
2. Ajout d'un routeur (équipement de frontière).
3. Configuration des interfaces :
 - R-Eth0 : Adresse publique (Internet)
 - R-Eth1 : Adresse privée (LAN)
4. Ajout d'un switch manageable connecté au routeur.
5. Configuration :
 - S-Eth0 connecté à R-Eth1

- S-Eth1 connecté au pare-feu (F-Eth0)
 - S-Eth2 connecté au poste Windows
6. Ajout d'un pare-feu :
- F-Eth0 : vers le switch (DMZ)
 - F-Eth1 : vers le serveur web Linux

4.3 Tests de Connectivité

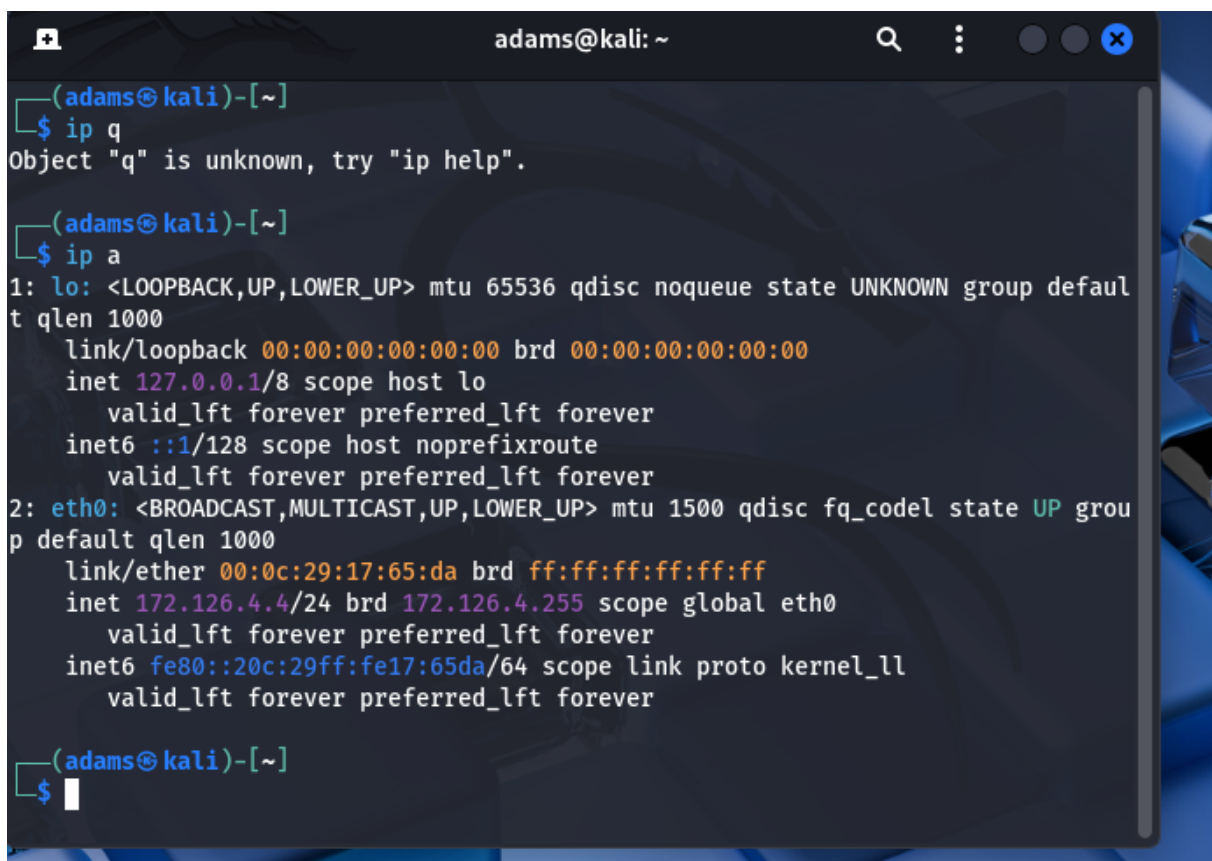
- Ping entre le poste Windows et le serveur Linux;
- Accès HTTP à l'application web depuis le LAN;
- Vérification du trafic à travers le pare-feu;
- Test de connectivité externe (Internet simulé).

Chapitre 5

Résultats et Vérifications

Les tests effectués confirment la fonctionnalité de l'infrastructure :

- Le poste Windows accède correctement à l'application web du serveur Linux ;
- Le pare-feu filtre les flux entre le LAN et la DMZ ;
- Le routage et les interfaces sont opérationnels ;
- L'application est fonctionnel sur le serveur web.

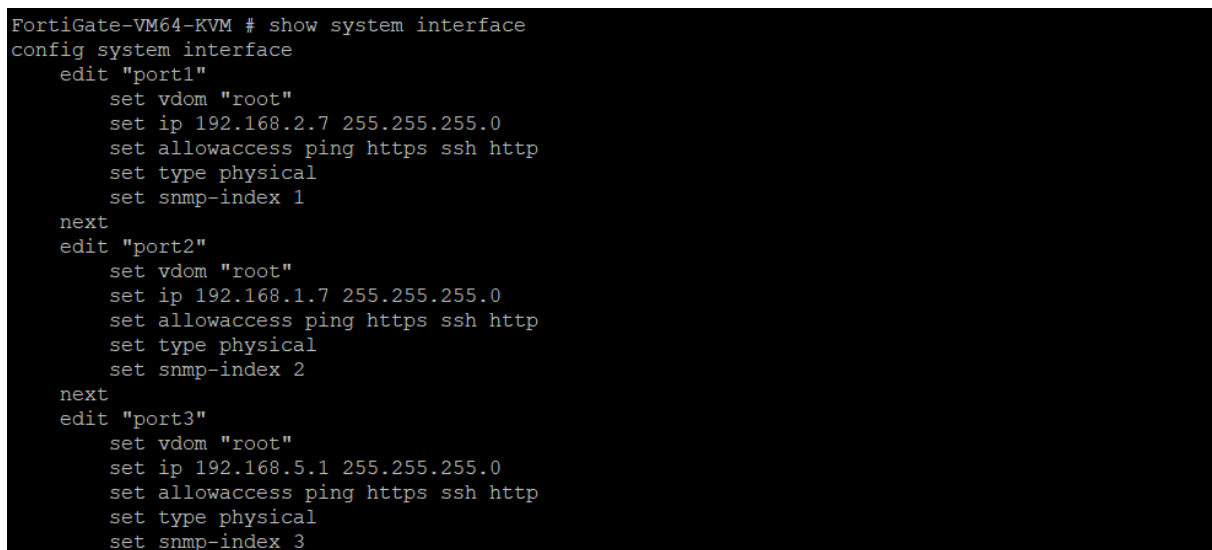


```
(adams@kali)-[~]
$ ip q
Object "q" is unknown, try "ip help".

(adams@kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:17:65:da brd ff:ff:ff:ff:ff:ff
    inet 172.126.4.4/24 brd 172.126.4.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe17:65da/64 scope link proto kernel_ll
        valid_lft forever preferred_lft forever

(adams@kali)-[~]
$
```

FIGURE 5.1 – configuration de kali



```
FortiGate-VM64-KVM # show system interface
config system interface
    edit "port1"
        set vdom "root"
        set ip 192.168.2.7 255.255.255.0
        set allowaccess ping https ssh http
        set type physical
        set snmp-index 1
    next
    edit "port2"
        set vdom "root"
        set ip 192.168.1.7 255.255.255.0
        set allowaccess ping https ssh http
        set type physical
        set snmp-index 2
    next
    edit "port3"
        set vdom "root"
        set ip 192.168.5.1 255.255.255.0
        set allowaccess ping https ssh http
        set type physical
        set snmp-index 3
```

FIGURE 5.2 – interface du parefeu

```

FortiGate-VM64-KVM # show firewall policy
config firewall policy
edit 1
    set name "Port1 to Port2"
    set uuid 8ae220b4-b278-51f0-d20c-e1f337ab14ae
    set srcintf "port1"
    set dstintf "port2"
    set action accept
    set srcaddr "all"
    set dstaddr "all"
    set schedule "always"
    set service "ICMP_ALL"
    set logtraffic all
next
edit 2
    set name "Port2 to Port1"
    set uuid 8b006290-b278-51f0-f96b-cce346ca3a81
    set srcintf "port2"
    set dstintf "port1"
    set action accept
    set srcaddr "all"
    set dstaddr "all"
    set schedule "always"
    set service "TCP 8000"
    set logtraffic all
next
edit 3
    set name "Port1 to Port3"
    set uuid 8b1cddb8-b278-51f0-8baf-e070369d4bda
    set srcintf "port1"
    set dstintf "port3"
    set action accept
    set srcaddr "all"
    set dstaddr "all"
    set schedule "always"
    set service "TCP 8000"
    set logtraffic all
next
edit 4
    set name "Port3 to Port1"
    set uuid 8b39cbd4-b278-51f0-98db-6295dd22cb98
    set srcintf "port3"
    set dstintf "port1"
    set action accept
    set srcaddr "all"
    set dstaddr "all"
    set schedule "always"
    set service "TCP 8000"

```

FIGURE 5.3 – policy du parefeu

```
olivia@G0DS:~/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/olivia/Desktop/projetAudit/static' in
the STATICFILES_DIRS setting does not exist.

System check identified 1 issue (0 silenced).
October 30, 2025 - 20:06:01
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.

[30/Oct/2025 20:06:17] "GET / HTTP/1.1" 200 3265
[30/Oct/2025 20:06:17] "GET /static/css/style.css HTTP/1.1" 200 2664
Not Found: /media/default.jpg
[30/Oct/2025 20:06:17] "GET /media/default.jpg HTTP/1.1" 404 4271
Not Found: /favicon.ico
[30/Oct/2025 20:06:18] "GET /favicon.ico HTTP/1.1" 404 4041
```

FIGURE 5.4 – serveur ubuntu

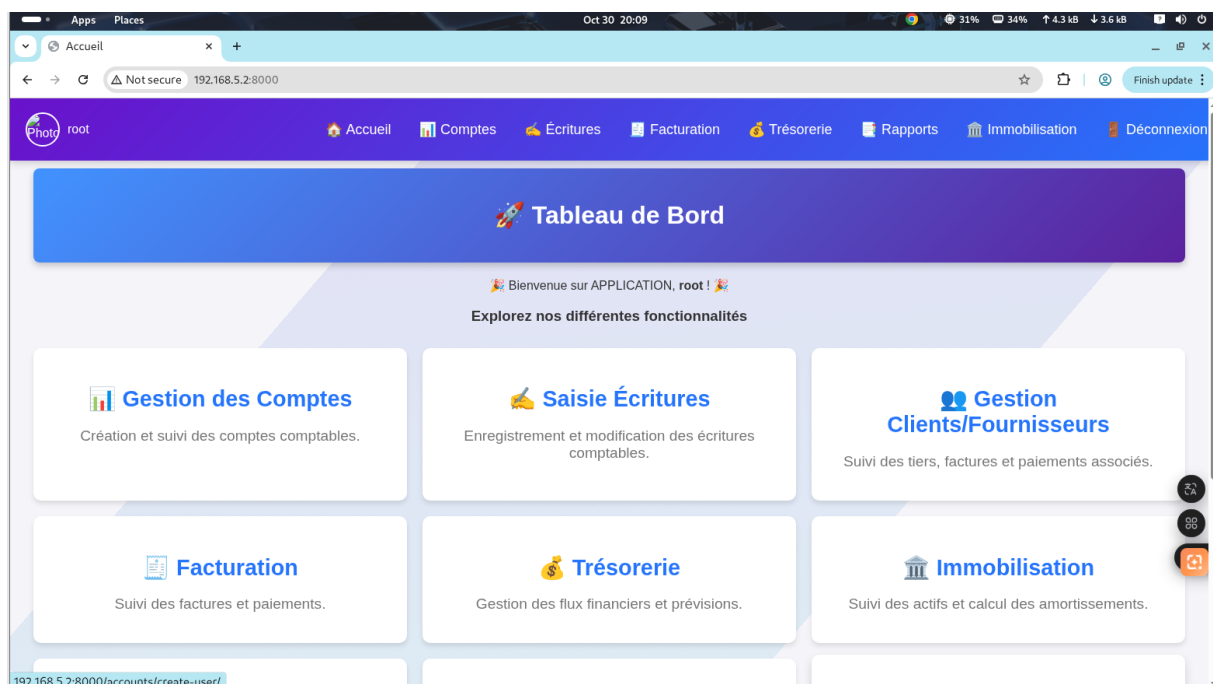


FIGURE 5.5 – application sur kali linux

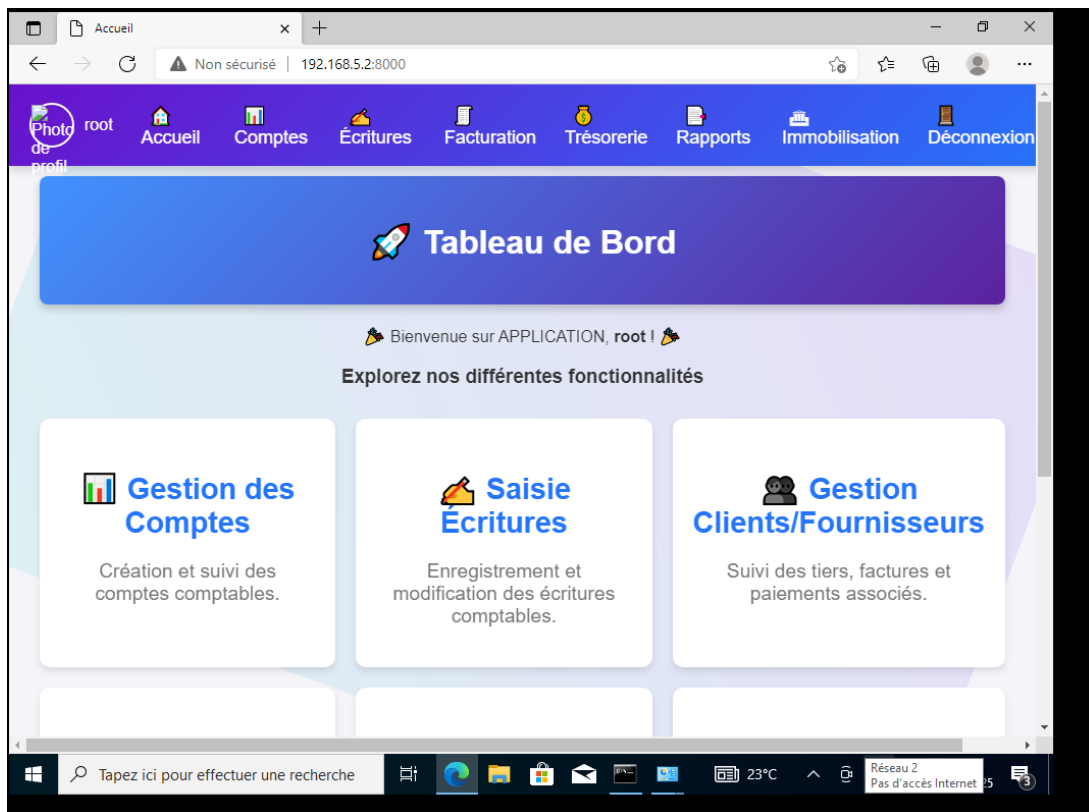


FIGURE 5.6 – Accès à l'application web depuis le poste Windows

```

C:\> Invite de commandes

Microsoft Windows [version 10.0.19045.4412]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\ADAM'S>ping 192.168.5.2

Envoi d'une requête 'Ping' 192.168.5.2 avec 32 octets de données :
Réponse de 192.168.5.2 : octets=32 temps=4 ms TTL=62
Réponse de 192.168.5.2 : octets=32 temps=3 ms TTL=62
Réponse de 192.168.5.2 : octets=32 temps=3 ms TTL=62
Réponse de 192.168.5.2 : octets=32 temps=3 ms TTL=62

Statistiques Ping pour 192.168.5.2:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 3ms, Maximum = 4ms, Moyenne = 3ms

C:\Users\ADAM'S>

```

FIGURE 5.7 – ping vers le serveur web

Conclusion

Ce laboratoire a permis de mettre en œuvre un environnement réseau complet, intégrant les notions de routage, segmentation, sécurisation et virtualisation. Cette base pourra être utilisée pour les travaux d'investigation numérique à venir, notamment la simulation d'attaques et l'analyse post-incident.