École Nationale Supérieure Polytechnique de Yaoundé

Cybersécurité et Investigation Numérique

Niveau 4

Rapport de Configuration d'une infrastructure reseau fonctionelle (Lab1)

Étudiant : MELONE ANDRE V.

Matricule : 22p059

Unite d'enseignement : Introduction aux techniques d'investigation numerique

Enseignant : Mr MINKA Thierry

Table des matières

Presentation du lab 1

Dans le cadre du cours d'investigation numerique, il nous est demande pour ce lab de configurer une infrastructure fonctionnelle comprenant un PC Kali, un serveur web Ubuntu, deux machines windows et un parefeu.

Pour cela, voici l'architecture pour laquelle j'ai opté

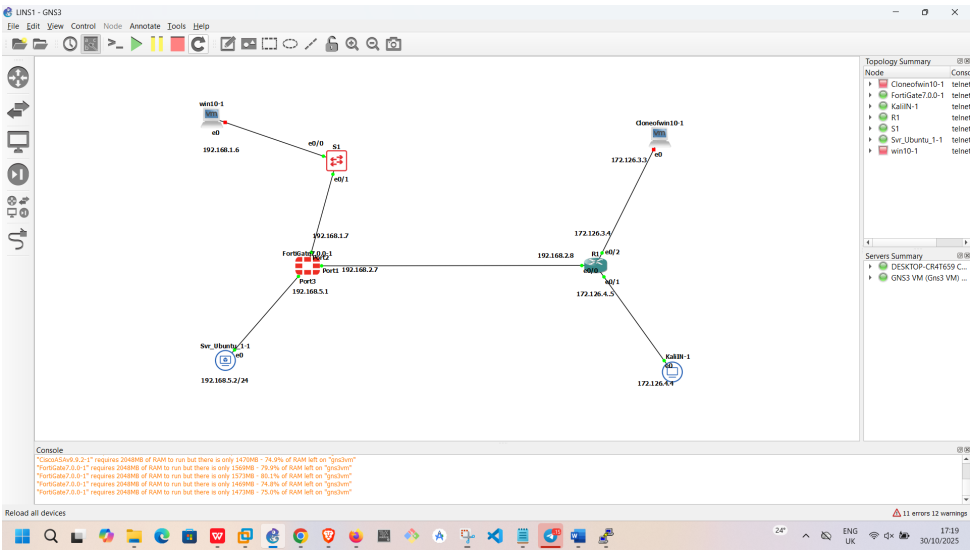

FIGURE 1 – Capture d'écran : architecture reseau pour le lab

Chapitre 1

Configuration des machines

Le tableau suivant resume les adresses ip de nos machines avec les differentes passerelles par defaut.

Machine	**Adresse IP**	**Masque de sous-réseau**	**Passerelle par défaut**
Win_10_Client1	192.168.1.6	255.255.255.0	192.168.1.7 (Fortigate)
Win_10_Client2	172.126.3.3	255.255.255.0	172.126.3.4 (R1)
Kali_1	172.126.4.4	255.255.255.0	172.126.4.5 (R1)
Svr_Ubuntu_1	192.168.5.2	255.255.255.0	192.168.5.1 (Fortigate)

Les images suivantes montrent comment jai adresse Ubuntu et Kali.

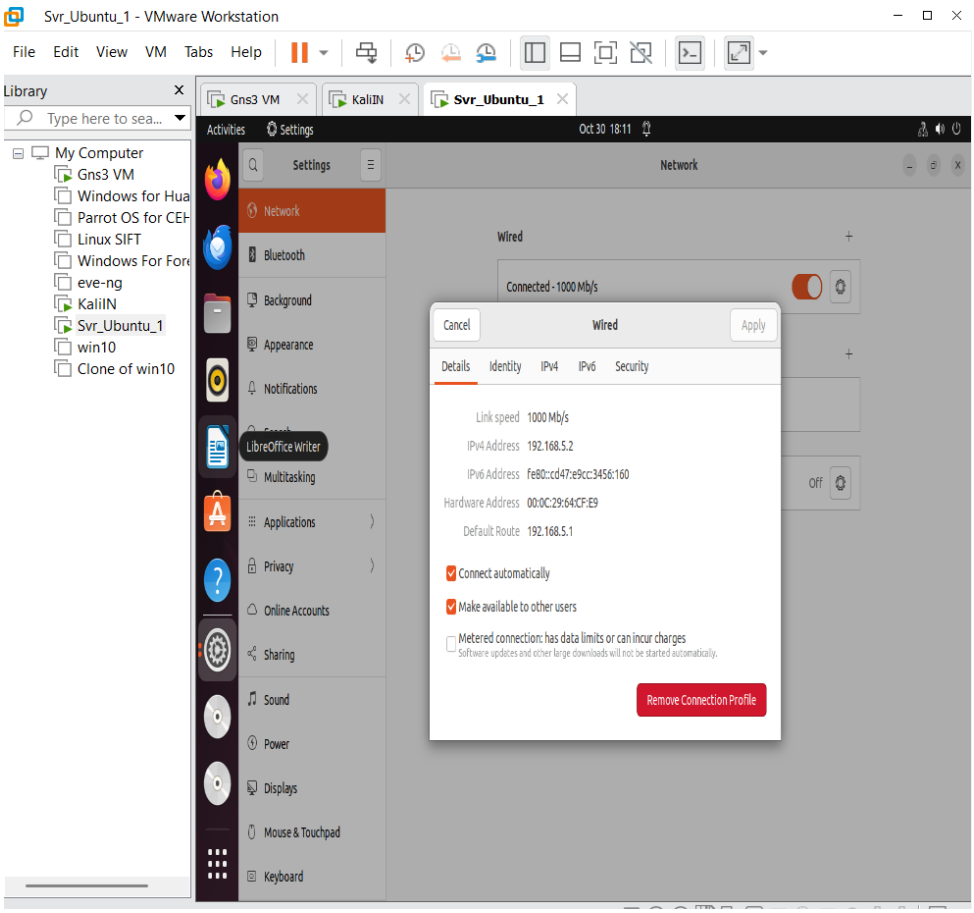

FIGURE 1.1 – Capture d'écran : adressage du serveur ubuntu

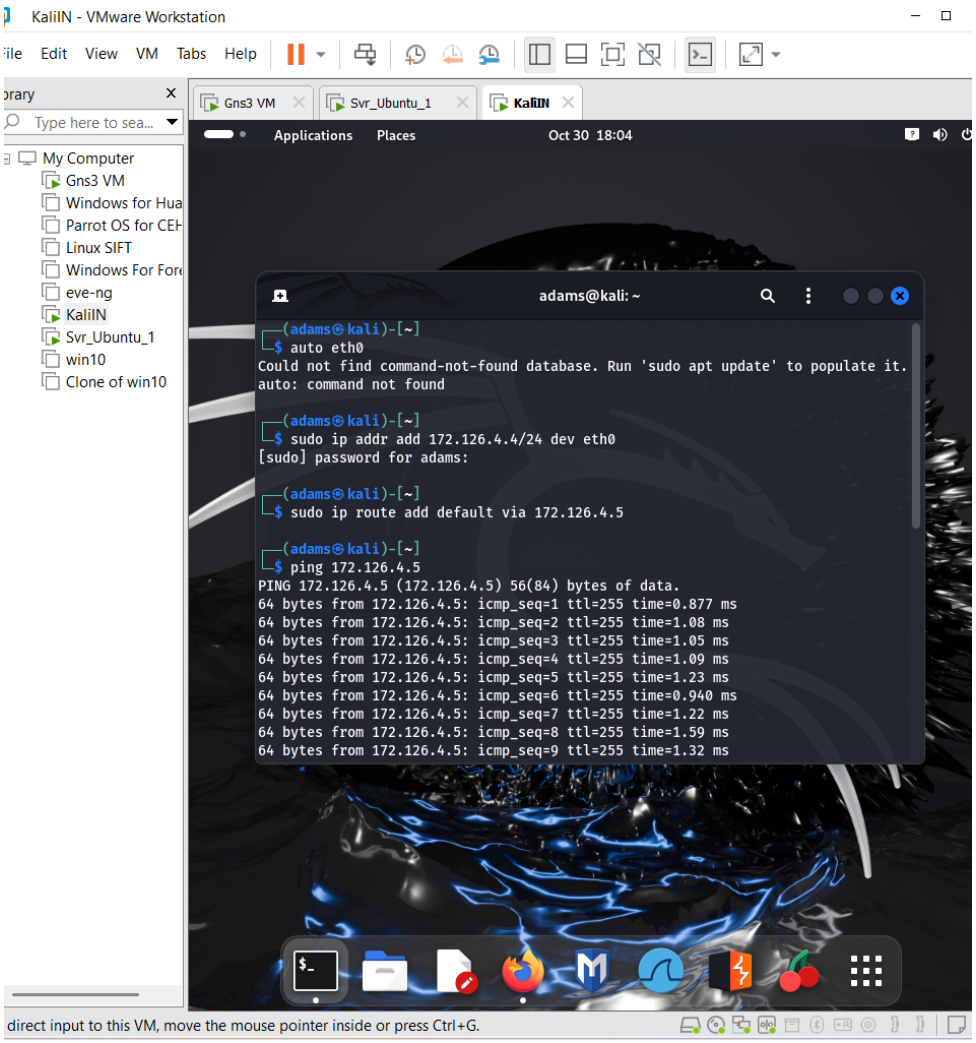

FIGURE 1.2 – Capture d'écran : adressage du PC Kali Linux et test de connectivités avec sa gateway

Chapitre 2

Configuration du routeur R1

2.1 Configuration des interfaces

Les commandes ci-dessous sont destinées à être collées dans l'interface CLI du routeur (mode privilégié) :

Listing 2.1 – Configuration des interfaces - R1

```
enable
configure terminal

interface e0/0
 ip address 192.168.2.8 255.255.255.0
 no shutdown

interface e0/1
 ip address 172.126.4.5 255.255.255.0
 no shutdown

interface e0/2
 ip address 172.126.3.4 255.255.255.0
 no shutdown

do copy running-config startup-config
end
```

2.2 Ajout de routes statiques

Ci-dessous les entrées de routage statique fournies — certains chemins semblent redondants ou comportent des erreurs typographiques (par ex. 192.158.1.0) ; laissez-les tels quels si voulu, sinon corrigez en 192.168.x.x selon l'architecture réelle.

Listing 2.2 – Routes statiques - R1

```
conf t
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
ip route 172.126.3.0 255.255.255.0 172.126.4.0
ip route 172.126.3.0 255.255.255.0 192.168.1.0
ip route 172.126.3.0 255.255.255.0 192.168.2.0
ip route 172.126.4.0 255.255.255.0 172.126.3.0
ip route 192.158.1.0 255.255.255.0 172.126.4.0
ip route 192.168.1.0 255.255.255.0 192.168.2.7
ip route 192.168.2.0 255.255.255.0 172.126.3.0
ip route 192.168.2.0 255.255.255.0 172.126.4.0
ip route 192.168.5.0 255.255.255.0 192.168.2.7
ip route 192.168.5.0 255.255.255.0 172.126.4.0

do copy running-config startup-config
end
```

Conseils

- Vérifiez la cohérence des réseaux et corrigez les éventuelles fautes de frappe (ex : `192.158.1.0` probablement doit être `192.168.1.0`).
- Pour éviter les routes contradictoires, préférez une seule route par destination avec la passerelle correcte.
- Testez la connectivité étape par étape avec `ping` et `traceroute`.

Chapitre 3

Configuration du pare-feu Fortigate

3.1 Interfaces du pare-feu

On saisit les commandes suivantes au niveau du pare-feu pour définir les interfaces :

Listing 3.1 – Configuration des interfaces - pare-feu

```
config system interface
    edit "port1"
        set mode static
        set ip 192.168.2.7 255.255.255.0
        set allowaccess ping https http ssh
    next
    edit "port2"
        set mode static
        set ip 192.168.1.7 255.255.255.0
        set allowaccess ping https http ssh
    next
    edit "port3"
        set mode static
        set ip 192.168.5.1 255.255.255.0
        set allowaccess ping https http ssh
    next
end
```

3.2 Routes statiques (pare-feu)

Listing 3.2 – Routes statiques - pare-feu

```
config router static
    edit 1
        set dst 0.0.0.0 0.0.0.0
        set gateway 192.168.2.8
        set device port1
    next
config router static
```

```
    edit 1
        set dst 172.126.3.0 255.255.255.0
        set gateway 192.168.2.8
        set device "port1"
    next
    edit 2
        set dst 172.126.4.0 255.255.255.0
        set gateway 192.168.2.8
        set device "port1"
    next
    edit 3
        set dst 192.168.1.0 255.255.255.0
        set gateway 192.168.2.8
        set device "port2"
    next
    edit 4
        set dst 192.168.5.0 255.255.255.0
        set gateway 192.168.2.8
        set device "port3"
    next
end
```

3.3 Création de services personnalisés

Définition des services ICMP et TCP/8000 :

Listing 3.3 – Services personnalisés - pare-feu

```
config firewall service custom
    edit "ICMP_ALL"
        set protocol ICMP
    next
end
config firewall service custom
    edit "TCP_8000"
        set protocol TCP
        set tcp-portrange 8000
    next
end
```

3.4 Politiques de securite du pare-feu

Les politiques ci-dessous autorisent la communication entre les ports et l'ICMP/TCP$_8$000.

Listing 3.4 – Politiques - pare-feu

```
config firewall policy
    edit 1
```

```
        set name "Port1 to Port2"
        set srcintf "port1"
        set dstintf "port2"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ICMP_ALL"
        set service "TCP_8000"
        set logtraffic all
    next
    edit 2
        set name "Port2 to Port1"
        set srcintf "port2"
        set dstintf "port1"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ICMP_ALL"
        set service "TCP_8000"
        set logtraffic all
    next
    edit 3
        set name "Port1 to Port3"
        set srcintf "port1"
        set dstintf "port3"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ICMP_ALL"
        set service "TCP_8000"
        set logtraffic all
    next
    edit 4
        set name "Port3 to Port1"
        set srcintf "port3"
        set dstintf "port1"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ICMP_ALL"
        set service "TCP_8000"
        set logtraffic all
    next
    edit 5
```

```
        set name "Port2 to Port3"
        set srcintf "port2"
        set dstintf "port3"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ICMP_ALL"
        set service "TCP_8000"
        set logtraffic all
    next
    edit 6
        set name "Port3 to Port2"
        set srcintf "port3"
        set dstintf "port2"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ICMP_ALL"
        set service "TCP_8000"
        set logtraffic all
    next
    edit 9
        set name "Allow Ping"
        set srcintf "any"
        set dstintf "any"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set service "PING"
        set schedule "always"
    next
end
```

Chapitre 4

Démarrage et test de l'application web

Cette section décrit la mise en service et la vérification de l'application web hébergée sur le serveur Ubuntu.

4.1 Lancement du serveur Django

Sur le serveur Ubuntu (`Svr_Ubuntu_1`), se placer dans le répertoire du projet puis exécuter la commande suivante :

Listing 4.1 – Commande de lancement du serveur Django

```
python3 manage.py runserver 192.168.5.2:8000
```

Le serveur démarre et affiche dans le terminal que l'application écoute sur l'adresse 192.168.5.2, port 8000.

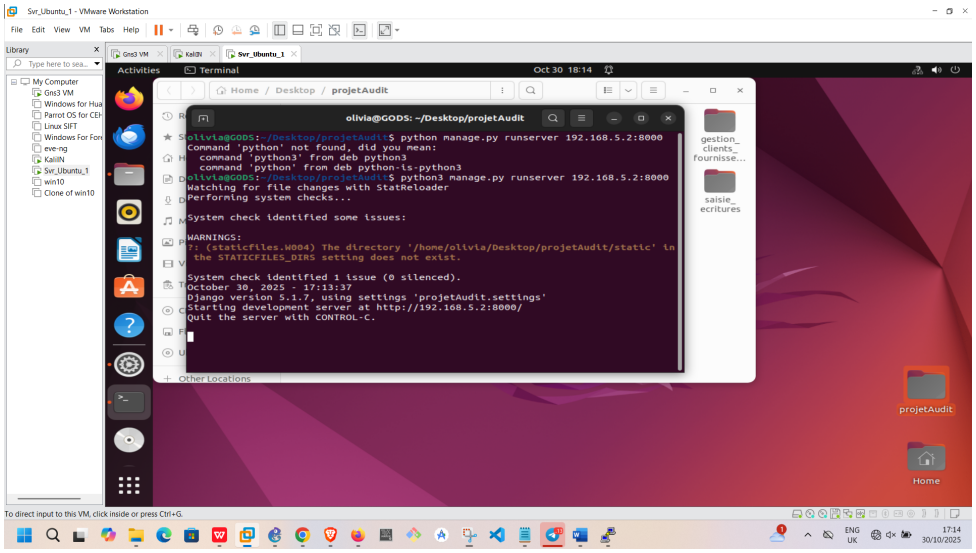

FIGURE 4.1 – Capture d'écran : Application Django démarrée sur le serveur Ubuntu

4.2 Accès depuis la machine Kali

Depuis la machine `Kali_1`, ouvrir un navigateur web et entrer l'URL suivante :

```
http://192.168.5.2:8000
```

Si l'infrastructure réseau fonctionne correctement, la page web de l'application doit s'afficher sans erreur.

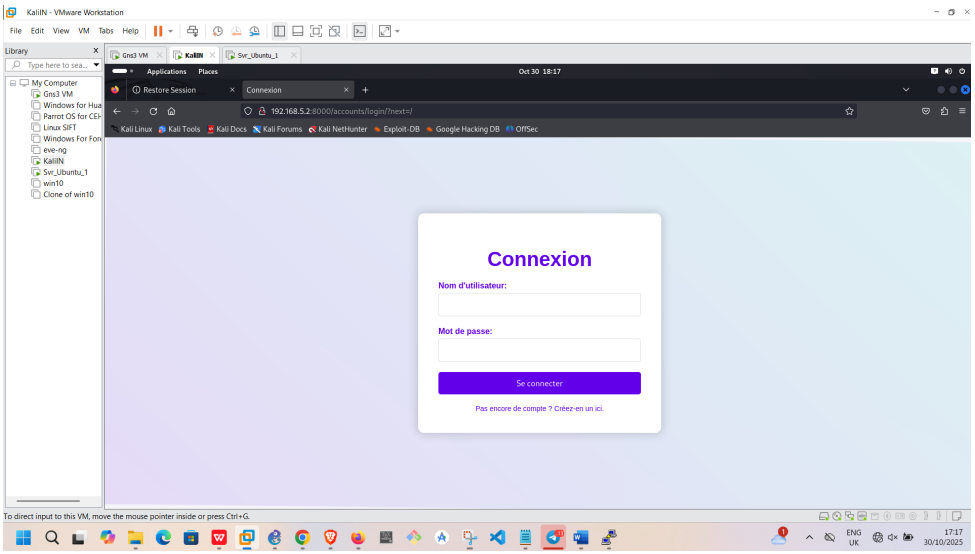

FIGURE 4.2 – Capture d'écran : Application ouverte sur Kali

Validation du test Cette démonstration prouve que les routes, les politiques du pare-feu et les interfaces sont configurées correctement. Le trafic TCP/8000 entre le serveur Ubuntu et le poste Kali est autorisé et fonctionnel.