RÉPUBLIQUE DU CAMEROUN
******
UNIVERSITÉ DE YAOUNDÉ I
******
ÉCOLE NATIONALE SUPÉRIEURE POLYTECHNIQUE
******
DÉPARTEMENT DU GÉNIE INFORMATIQUE

REPUBLIC OF CAMEROON
******
UNIVERSITY OF YAOUNDE I
******
NATIONAL ADVANCED SCHOOL OF ENGINEERING
******
DEPARTMENT OF COMPUTER ENGINEERING

RAPPORT

LAB 1 et debut du LAB 2

Réalisé par : NANTIA ZAGUE AXEL FRISKYL

Matricule : 22P105

Spécialité : Cybersécurité et Investigation Numérique (CIN)

UE : Introduction aux techniques de l'Investigations Numériques

Sous la supervision de : Mr. MINKA MI NGUIDJOI Thierry Emmanuel

Année académique : 2025/2026

Rapport de Laboratoire : Configuration Réseau et Simulation de Ransomware

Cours : Sécurité des Réseaux et Systèmes

Date : 30 octobre 2025

Résumé

Ce rapport présente les travaux réalisés dans le cadre de deux laboratoires de sécurité informatique. Le premier labo concerne la configuration d'un environnement réseau sécurisé avec GNS3, intégrant un firewall FortiGate et une DMZ. Le deuxième labo porte sur le développement et le test d'un ransomware simulé pour comprendre les mécanismes de cette menace cybernétique.

Table des matières

1 Lab 1 – Configuration d'un environnement réseau fonctionnel et sécurisé

1.1 Objectif du laboratoire

Ce laboratoire consistait à concevoir un réseau sous GNS3 incluant plusieurs machines virtuelles (Windows, Linux, Kali), un routeur, un firewall FortiGate, et la segmentation en sous-réseaux. L'objectif était de maîtriser la création d'une DMZ, le paramétrage du routage et la sécurisation par firewall, tout en maintenant la connectivité sur les services autorisés entre les différentes zones.

1.2 Architecture du réseau

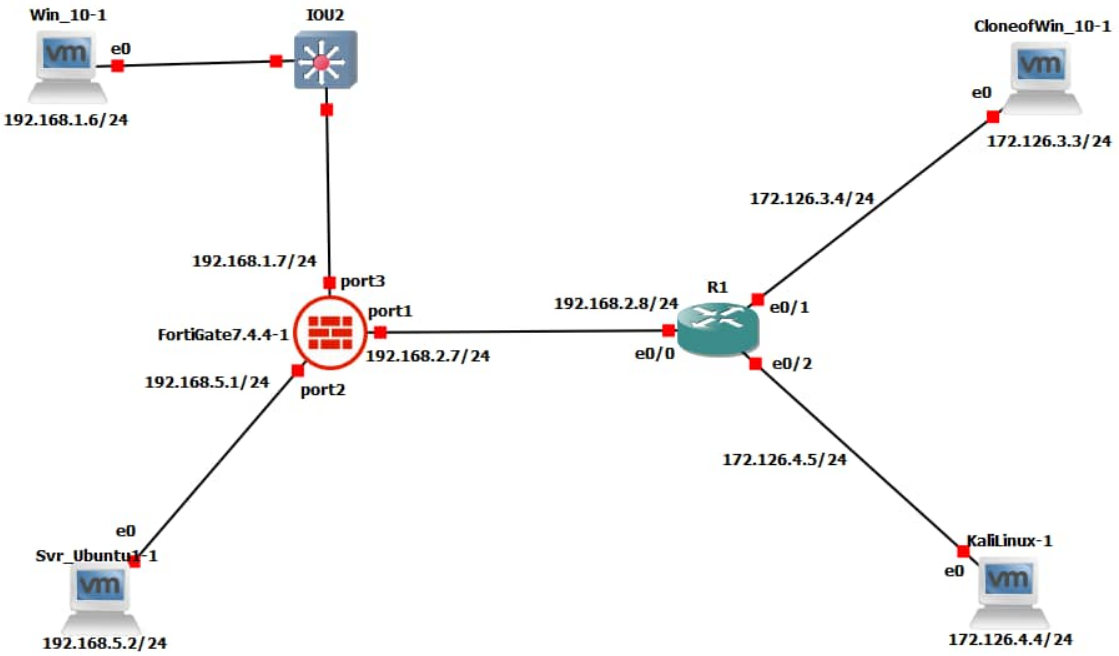

FIGURE 1 – Schéma de l'architecture réseau réalisée sous GNS3

L'architecture réalisée est fidèle à celle proposée dans l'énoncé. Elle inclut les composants suivants :

— **VM Windows 10** : 192.168.1.6/24 (réseau local)

— **Serveur Ubuntu** : 192.168.5.2/24 (DMZ)

— **Firewall FortiGate** :

  — Port1 : 192.168.2.7/24

  — Port2 : 192.168.5.1/24

  — Port3 : 192.168.1.7/24

— **Routeur R1** : Interfaces e0/0, e0/1, e0/2 pour interconnecter les zones internes et externes

— **Kali Linux** : 172.126.4.4/24 (machine d'attaque)

— **CloneWindows** : 172.126.3.3/24 (cible additionnelle)

Le schéma, bien segmenté, permet de contrôler les accès entre la DMZ, le réseau local (LAN), et les zones « extérieures », comme demandé par le lab.

1.3 Configurations et vérifications réalisées

1.3.1 Politique sur le firewall

Sur le FortiGate, chaque port a été configuré avec les règles adaptées :

— La DMZ n'est accessible que via certains services (HTTP/HTTPS)

— La VM Windows bloque tout trafic non nécessaire

— Les règles inter-zones segmentent correctement les réseaux internes, DMZ et zones d'attaque

1.3.2 Routage

Le routeur R1 a été configuré pour faire du routage entre les différents sous-réseaux. Les routes statiques ont été définies pour permettre la communication entre le LAN, la DMZ, et la zone d'attaque, tout en respectant l'isolation.

1.3.3 Adressage IP

Toutes les interfaces ont reçu des adresses IP cohérentes avec le plan d'adressage fourni. Les VLAN et sous-réseaux sont correctement séparés.

1.3.4 Tests de connectivité

Des tests ping et d'accès HTTP/HTTPS ont été menés pour valider la configuration et l'application correcte des règles de sécurité.

1.4 Conclusion du Lab 1

L'architecture réseau a été correctement implémentée avec une segmentation efficace des différentes zones de sécurité. Les règles firewall appliquées permettent un contrôle granulaire des accès tout en maintenant la fonctionnalité des services essentiels.

2 Lab 2 – Création et test d'un ransomware simulé

2.1 Objectif du laboratoire

Ce laboratoire demandait de développer sous Kali Linux un script de ransomware simulant le chiffrement (en renommant les fichiers avec une extension, par exemple ".locked"), puis de transformer ce script en exécutable Windows (.exe avec PyInstaller), et enfin de tester son

propagation sur une VM Windows soit par email, soit par téléchargement malveillant hébergé sur Kali.

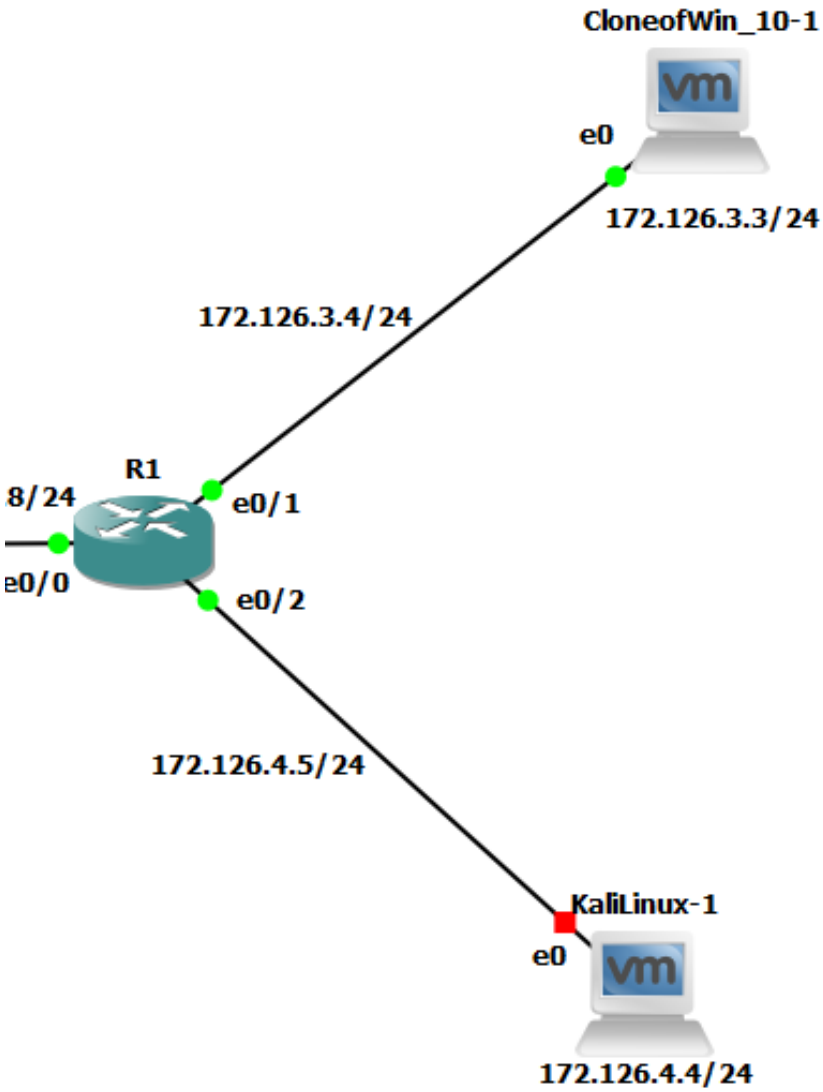

FIGURE 2 – Test du ransomware sur la VM CloneWindows

2.2 Développement du ransomware

2.2.1 Implémentation technique

Le ransomware a été développé en Python sur Kali Linux avec les caractéristiques suivantes :

— Accès à la machine cible via les informations d'authentification (nom, utilisateur, mot de passe)

— Chiffrement simulé par renommage des fichiers avec une extension ".locked"

— Génération d'un message de rançon avec instructions de paiement

— Transformation en exécutable Windows via PyInstaller

2.2.2 Résultats des tests

Le ransomware a été testé avec succès sur la VM CloneWindows :

— Le script a correctement fonctionné et a "chiffré" les fichiers cibles

— Le message de rançon a été affiché avec les informations bancaires demandées

— La simulation a permis de comprendre les mécanismes d'infection

2.3 Limitations rencontrées

— **Connectivité internet** : Impossible de réaliser la propagation par email en raison de l'absence de connectivité internet des machines virtuelles

— **Bibliothèques manquantes** : Difficultés à télécharger les dépendances nécessaires pour certaines fonctionnalités avancées

— **Fonctionnalités réduites** : Le ransomware développé reste basique comparé aux véritables menaces

2.4 Conclusion du Lab 2

Ce laboratoire a permis de comprendre les principes fondamentaux du fonctionnement des ransomwares et les défis techniques liés à leur développement. La simulation a mis en évidence l'importance des mesures de protection et de détection contre ce type de menace.

3 Conclusion générale

Les deux laboratoires ont permis d'acquérir des compétences pratiques en sécurité réseau et en analyse de menaces cybernétiques. Le premier labo a renforcé la compréhension des architectures réseau sécurisées et des politiques firewall, tandis que le deuxième a offert une perspective concrète sur le fonctionnement des ransomwares.

Ces expériences pratiques sont essentielles pour développer une approche proactive de la sécurité informatique, combinant à la fois la prévention technique et la compréhension des tactiques adverses.