RAPPORT FINAL

Sécurisation d’une infrastructure virtualisée et conteneurisée

---

Informations générales

- **Nom de l’étudiant :** AGBENONZAN KOSSIVI JACQUES JUNIOR
- **Binôme :** SANOGO SOULEYMANE
- **Système d’exploitation :** Ubuntu Server 22.04 LTS
- **Hyperviseur :** Oracle VirtualBox
- **Référentiel :** NIST Cybersecurity Framework

INTRODUCTION

Dans un contexte où les infrastructures informatiques sont de plus en plus exposées aux menaces cybernétiques, la sécurisation des systèmes, des réseaux et des applications est devenue un enjeu majeur. Ce projet a pour objectif de mettre en œuvre une infrastructure virtualisée et conteneurisée, simulant un environnement d’entreprise, tout en appliquant une démarche de sécurisation basée sur le NIST Cybersecurity Framework.

Le projet couvre l’ensemble du cycle de vie de la sécurité, depuis l’identification des actifs jusqu’à la réponse à incident et l’amélioration continue.

PHASE 0 — VIRTUALISATION & ISOLATION

Fonction NIST : IDENTIFY

Objectifs

- Comprendre le rôle de la virtualisation en sécurité
- Identifier les frontières d’isolation

Travaux réalisés

Une machine virtuelle a été déployée sur Oracle VirtualBox afin d'isoler l'environnement de travail du système hôte. Le système d'exploitation choisi est Ubuntu Server 22.04 LTS pour sa stabilité, son support long terme et sa compatibilité avec les outils de sécurité.

Ressources allouées

Ressource	Valeur
CPU	3 vCPU
RAM	4 Go
Stockage	50 Go

Intérêt sécurité

- Isolation du système hôte
- Cloisonnement des services
- Réduction de l'impact d'un incident

PHASE 1 — ARCHITECTURE RÉSEAU & CLOUD

Fonction NIST : IDENTIFY

Objectifs

- Comprendre la segmentation réseau
- Identifier les flux autorisés et interdits

Architecture mise en place

- Réseau public (NAT)
- DMZ (services Web)
- Réseau interne (LAN)

Cette segmentation permet de limiter la propagation des attaques et de contrôler les flux réseau.

Tableau des flux

Source	Destination	Port	Autorisé	Justification
Internet	Web DMZ	80	Oui	Accès public
LAN	Web DMZ	80	Oui	Accès interne
Internet	LAN	*	Non	Sécurité

PHASE 2 — SÉCURITÉ RÉSEAU

Fonction NIST : PROTECT

Objectifs

- Réduire la surface d'attaque
- Mettre en place un filtrage réseau

Actions réalisées

- Scan réseau initial avec Nmap
- Identification des ports ouverts
- Mise en place de règles iptables
- Filtrage des réseaux Docker

Résultat

Une réduction significative des ports exposés a été constatée après la mise en œuvre des règles de filtrage.

PHASE 3 — SÉCURITÉ SYSTÈME LINUX

Fonction NIST : PROTECT

Mesures appliquées

- Gestion des comptes utilisateurs
- Interdiction du login root via SSH
- Changement du port SSH
- Permissions strictes sur les fichiers sensibles
- Désactivation des services inutiles

Ces actions renforcent la sécurité du système et limitent les vecteurs d'attaque.

PHASE 4 — SÉCURITÉ WEB

Fonction NIST : PROTECT

Outils utilisés

- Nikto

- curl
- Navigateur Web

Vulnérabilités identifiées

- Headers HTTP manquants
- Répertoires accessibles
- Absence de HTTPS

Impact

Ces vulnérabilités facilitent la reconnaissance et augmentent les risques d'attaque côté client et serveur.

PHASE 5 — DÉTECTION, LOGS ET FORENSIC

Fonction NIST : DETECT

Logs analysés

- /var/log/auth.log
- Logs Nginx (access.log, error.log)

Analyse

Les journaux ont permis d'identifier des scans réseau et des tentatives d'accès non autorisées.

Timeline simplifiée

1. Scan réseau
2. Tentative d'accès
3. Rejet par le pare-feu

PHASE 6 — RÉPONSE ET AMÉLIORATION

Fonctions NIST : RESPOND & RECOVER

Plan de réponse

- Détection
- Analyse
- Confinement

- Éradication
- Rétablissement

Améliorations proposées

- Mise en place du HTTPS
- Ajout d'un IDS/IPS
- Centralisation des logs
- Audits réguliers

CONCLUSION GÉNÉRALE

Ce projet a permis de concevoir, déployer et sécuriser une infrastructure informatique virtualisée reproduisant une architecture réseau d'entreprise segmentée. L'approche méthodique basée sur le NIST Cybersecurity Framework a permis de couvrir l'ensemble du cycle de la cybersécurité, de l'identification des actifs à la réponse à incident.

Il met en évidence l'importance de la segmentation réseau, du durcissement système, de la sécurité applicative et de la surveillance continue. Les améliorations proposées ouvrent la voie à une infrastructure plus résiliente et mieux préparée face aux menaces futures.