République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université A.MIRA-BEJAIA
Faculté des Sciences Exactes
Département Informatique

Mémoire de Master
En
Informatique
Option
Administration et Sécurité des Réseaux

Thème

Audit du système d'informations pour le référentiel ISO 27000
Cas : L'Entreprise Portuaire de Béjaia (EPB)

Réalisé par :

M^{lle} AMEDDAH Siham
M^{lle} AMOKRANE Lidya

Devant le jury composé de :

Président : M. FARAH Zoubeyr	Université de Béjaia.
Examinatrice : M^{me} SABRI Salima	Université de Béjaia.
Encadrant : M. AMROUN Kamal	Université de Béjaia.
Co-Encadrant : M. ELSAKAAN Nadim	Université de Béjaia.

U. A/M Béjaia, Septembre 2022.

Remerciements

Avant tout, Il semble approprié d'entamer ce mémoire par des remerciements, d'abord au bon Dieu de nous avoir accordé la force et le courage de mener à terme ce modeste travail.

Toute notre reconnaissance et toute notre gratitude vont vers nos encadrants, M^r AMROUN Kamal et M^r ELSAKAAN Nadim, qui nous ont aidés et accompagnés tout au long de cette expérience professionnelle avec beaucoup de patience et d'enthousiasme.

Un grand merci pour l'organisme d'accueil EPB, en particulier notre encadrant M^r BEDAOUCHE Belal pour sa patience, et son aide.

Nous remercions également les membres du jury d'avoir accepté d'examiner et de juger notre travail.

Que tous ceux qui, de près ou de loin ont contribué, par leurs conseils ; leurs encouragements ou leur amitié à l'aboutissement de ce travail ; Trouve ici l'expression de notre profonde reconnaissance.

Pour leur encouragement, leur soutien moral et la patience qu'ils nous ont manifesté durant toute l'année,

Nous remercions fortement tous les membres de nos familles.

Dédicaces

Ce modeste travail est dédié :

A nos chers parents qui nous ont soutenus et encouragés durant toute notre scolarité,

A nos frères et soeurs

A nos enseignants

A nos ami(e)s

A toutes les personnes qui nous ont apportés de l'aide.

Siham & Lidya

Table des matières

Liste des figures

Liste des tableaux

Liste des Abréviations

AD	Active Directory
ARP	Address Resolution Protocol
BAM	Business Activity Monitoring
CDP	Cisco Discovery Protocol
CLUSIF	Club de la Sécurité de l'Information Français
CMMI	Capability Maturity Model Integration
COBIT	Control Objectives For Information and Related Technology
CPU	Central Processing Unit
CRM	Customer Relationship Management
CS	Certificate Services
DHCP	Dynamic Host Configuration
DNS	Domain Name System
DS	Domain Services
DSI	Direction des Systèmes d'Information
EAP	Extensible Authentification Protocol
EDS	Évaluation, Direction et Surveillance
ERP	Entreprise Ressource Planning
EPB	Entreprise Portuaire de Béjaia
GED	Gestion Électronique des Documents
GNS	Graphical Network Simulator
IEEE	International Electronical and Electronics Engineers
IEC	International Electrotechnical Commission
IETF	Internet Engineering TASK Force
IMC	Intelligence, Modélisation et Choix
IP	Internet Protocol
ISO	International Organization for Standardization
IT	Information Technology
ITIL	Information Technology Infrastructure Library
LAN	Local Area Network
MARION	Méthode d'Analyse de Risques Informatiques Optimisée par Niveau
MEHARI	Méthode Harmonisée d'Analyse des Risques
MELISA	Méthode d'Evaluation de la vulnérabilité résiduelle des Systèmes d'information
MERISE	Méthode d'Etude et de Réalisation Informatique pour les Systèmes d'Entrepeise
NAS	Network Access Server
NPS	Network Policy Server
OBJ	Objectif
OM	Objets Métiers
OSI	Open Systems Interconnection

PCT	Plan de Continuité de Travail
PING	Packet Internet/Inter-Network Groper
PRET	Plan de Reprise dans l'Environnement de Travail
QoS	Quality Of Service
RADIUS	Remote Authentification Dial-In User Service
RH	Ressources Humaines
SGBD	Système de Gestion de Base de Données
SI	Système d'Informations
SQL	Structured Query Language
SSH	Secure Shell
SWOT	Strengths, Weaknesses, Opportunities and Threats
TELNET	Telecommunications Network
TIC	Technologies de l'Information et de la Communication
UML	Unified Modeling Language
Val IT	Value from IT Investments
VLAN	Virtual Local Area Network
VM	Virtual Machine
WEB	World Wide Web

INTRODUCTION GÉNÉRALE

L'environnement de travail de nos jours est confronté à un environnement technologiques de plus en plus développée et en évolution permanente caractérisée par le numérique. Ce qui impose aux entreprises d'étudier un changement, du fait que le digitale est un domaine surtout vise le service client.
Comme ça sont alors les outils numériques intégrés dans les domaines professionnels apportant un bénéfice qui est tout simplement internet et un enjeu d'anticipation de ces changements.

Quand on parle de la technologie informatique en entreprise on cite effectivement le système d'informations, car on est d'accord que c'est une valeur ajoutée étant donné qu'il traite l'information (l'élément majeur de toutes entreprises).
Pour cela, la performance et la conformité aux règles de gestion de cette structure de système est classée vitale.

Notre travail sur le terrain consiste en une mission d'audit de sécurité du système d'informations mené par nous même au sein de la Direction Digitalisation et Numérique de l'Entreprise Portuaire de Béjaia (EPB) pour objectif de mesurer l'alignement de son système d'informations aux réglementations de la norme ISO/IEC 27000.

Et parce qu'un audit de sécurité offre la possibilité de trouver les failles de son système, identifier les vulnérabilités et classer le niveau de gravité des risques en effectuant un état des lieux complet et en réalisant une roadmap d'urbanisation.

Selon la norme de sécurité de l'information ISO/IEC 27000, un questionnaire d'audit est réalisé puis étudié selon les méthodes MEHARI pour l'analyse des risques et COBIT5 pour l'analyse de la gouvernance qui vont permettre d'évaluer la structure informatique supposée protéger les données de l'entreprise, identifier ces risques et d'obtenir des solutions pour les réduire.

Ce travail est organisé en quatre (04) chapitres :

Le premier chapitre sera consacré à une introduction des systèmes d'informations numériques, réparti en deux sections : dont la première portera sur la définition de ce dernier, ces modèles, normes en bref et quelques d'autres termes relatifs, puis la seconde sur une présentation de l'organisme d'accueil.

Le second chapitre est dédié à « Rapport d'audit et roadmap » dans lequel nous analyserons le système d'informations de l'EPB selon les deux méthodes citées ci-dessus.

Dans le troisième chapitre qui concerne les recommandations proposés, nous passerons à l'émulation d'un réseau afin de pouvoir appliquer les recommandations sur un environnement

virtuel puis procéder à une analyse comparative des résultats obtenus et de l'état des lieux initial.

On termine par le chapitre 04 « Évaluation de la solution et tests fonctionnels » qui portera sur différents examens unitaires et fonctionnels.

Chapitre 1

Introduction aux systèmes d'informations numériques

Section 1

1.1 Introduction

Une entreprise est un acteur économique produisant des biens et des services, évoluant dans un contexte évolutif et compétitif. Afin de continuer à produire de la valeur elle doit rester à l'affût des développements technologiques et métiers. Pour ce faire elle est appelée à collecter, traiter des données et d'en tirer des informations décisionnelles.

De nos jours, vu le grand nombre de ressources et des fichiers dans les entreprises. Il est indispensable de mettre en œuvre des mécanismes et du matériel pour renforcer la sécurité des systèmes d'informations.

Dans notre premier chapitre, nous allons définir les systèmes d'informations, décrire le modèle en couche d'un SI, ainsi quelques normes ISO de la série 27000.

Ensuite, nous allons aborder la notion de la sécurité des SI, et présenter quelques mécanismes de politique de sécurité et d'analyse des risques. Nous passerons ensuite à l'urbanisation et l'audit des systèmes d'informations, Et ce dans la première partie de notre chapitre.

Nous abordons dans la deuxième partie la présentation de l'organisme d'accueil en détails. Enfin, on termine par une conclusion sur ce que a été décrit précédemment dans ce chapitre.

1.2 Qu'est-ce qu'un système d'informations

Depuis le début des années 1970, le concept de système d'informations a évolué en fonction de la diffusion croissante de l'informatique dans les activités des organisations et des entreprises. Il existe cependant plusieurs définitions qui font référence.

En général, les systèmes d'informations sont un outil qu'une entreprise utilise pour guider, piloter et mesurer ses processus de production et ses processus auxiliaires [12].

Selon R. Reix, le SI est définit comme "un ensemble organisé de ressources : matériel, logiciel, personnel, données, procédures permettant d'acquérir, traiter, stocker, communiquer des informations (sous forme de données, textes, images, sons, etc.) dans les organisations"

O'Brien écrit que "un système d'informations utilise des ressources humaines (utilisateur final et informaticiens), du matériel (machine et supports) et des logiciels (programmes et

procédures) pour accomplir des fonctions de saisie, de traitement, de sortie, de stockage et de contrôle qui servent à converti en produit informatif des ressources en donné" [11].

Donc on peut dire qu'un système d'informations est un élément central du fonctionnement d'une organisation, et qui peut être défini comme un ensemble de ressources permettant la collecte, le stockage, la gestion, l'échange et la diffusion des informations au sein de cette dernière. [8].

D'après la définition *complexe* donnée précédemment, il est primordial de différencier système d'informations et système informatique. l'informatique fait partie du SI et lui fournit des outils qui réalise l'infrastructure d'un système d'informations, alors qu'un SI est une vue fonctionnelle de l'informatique [13].

1.3 Le modèle en couches d'un système d'informations

Ce sont les étapes de description et de construction pour la mise en place d'une démarche d'urbanisation. A partir des objectifs stratégiques bien identifiées puis des fonctions et des informations bien détaillées, une implémentation sera réalisée.

Ce modèle de cartographie est un outil central pour l'urbanisation du SI, basé sur quatre visions (couches) successives : [13]

1. Couche infrastructure : L'un des objectifs du système d'informations est la représentation des activités de l'entreprise par la spécification des objets métiers (OM) en répondant à la question 'quoi ?'.

   L'infrastructure une partie de la couche métier qui désigne le matériel, système et réseau de l'entreprise, qui a pour but de fournir de la puissance informatique nécessaire en fonction des activités de l'entreprise : CPU, bande passante et réseau, modes d'accès aux réseaux, applicatifs..., divisé principalement en 3 catégories : [3]
   - le parc matériel : est l'ensemble des serveurs, postes de travail, équipements réseaux, moyens d'impression,...
   - le parc système ou logiciel : systèmes d'exploitations, applications (logiciels, progiciels etc.) et bases de données.
   - le parc réseau : concernant l'administration et la gestion de l'environnement réseau.

2. Couche fonctionnelle : Elle décrit les fonctions mises en œuvre pour réaliser les activités décrites dans la couche métier.

   L'architecture fonctionnelle est découpée en Zones, elles mêmes redécoupées en Quartier puis Îlots ou Blocs fonctionnels indépendants et autonomes pour une organisation modulaire.

   Le découpage fonctionnelle définie par des règles d'urbanisation consiste premièrement à séparer les zones de référentiels (données), d'échange (communication avec l'extérieur), de gestion interne (finance, RH, informatique...), de stratégie et règles de décision, et les zones opérationnelles (métier). [13]

3. Couche Application : L'objectif est la distribution et la réutilisation des fonctions applicatives. Elle représente la partie dynamique du système d'informations décrit dans la couche fonctionnelle. Parmi les modèles et diagrammes utiles à la description de l'architecture applicative : UML et Merise. [13]

4. La couche décisionnelle : Pour gérer une entreprise, les managers font en permanence des choix. L'un des rôles les plus importants d'un système d'informations est de faciliter la prise de décision qui est un processus complexe avec des modèles d'analyses comme celui de H.Simon (le modèle IMC) et des outils d'aide a la décision comme l'analyse SWOT (un outil de stratégie d'entreprise) ou également la business intelligence (aussi connu sous le nom de l'informatique décisionnelle, un ensemble de stratégies, concepts et méthodologies ayant pour objectif la clarification des données afin de prendre des décisions) [7]

1.4 Les normes des systèmes d'informations : ISO 27000 en bref

La nature immatérielle des systèmes d'informations rend leurs traitement plus redoutable, de plus l'absence de maîtrise des risques associée à la sécurité de l'information peut entraîner des conséquences négatives.

Pour résoudre ce problème, des méthodes et normes sont apparues. En matière de sécurité, la série de normes ISO/IEC 27000 de la catégorie des **"Technologies de l'information - Techniques de sécurité"** et ces normes relatives : [2]

NF ISO/IEC 27000 (publiée en février 2011)
Technologies de l'information - Techniques de sécurité - Systèmes de management de la sécurité de l'information - Vue d'ensemble et vocabulaire.

NF ISO/IEC 27001 (publiée en décembre 2007)
Technologies de l'information - Techniques de sécurité - Systèmes de management de la sécurité de l'information - Exigences.

ISO/IEC 27002 :2005 (publiée en juin 2005)
Technologies de l'information - Techniques de sécurité - Code de pratique pour la gestion de sécurité de l'information (ISO/CE/ 17799 :2005 et rectificatif 1 de 2007).

IEC 27003 :2010 (publiée en février 2010)
Technologies de l'information - Techniques de sécurité - Lignes directrices pour la mise en œuvre du système de management de la sécurité de l'information.

IEC 27003 :2010 (publiée en décembre 2009)
Technologies de l'information - Techniques de sécurité - Management de la sécurité de l'information - Mesurage.

ISO/IEC 27005 (publiée en juin 2011)
Technologies de l'information - Techniques de sécurité - Gestion des risques liés à la sécurité de l'information.

IEC 27006 :2011 (publiée en mars 2007 et un projet de nouvelle norme en septembre 2011)
Technologies de l'information - Techniques de sécurité - Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management de la sécurité de l'information.

IEC 27011 :2008 (publiée en décembre 2008)
Technologies de l'information - Techniques de sécurité - Lignes directrices pour le management de la sécurité de l'information pour les organismes de télécommunications sur la base de l'ISO/IEC 27002.

1.5 La sécurité des systèmes d'informations

Vu le grand nombre de ressources, de fichiers et des systèmes d'informations dans les entreprises, il est indispensable d'éviter les menaces ou les attaques qui peuvent nuire à la confidentialité de ces dernières.
C'est pour cela on a eu recours à la sécurité informatique qui est devenue de nos jours un point primordial dans la gestion des systèmes d'informations dans les entreprises.

1.5.1 Le protocole RADIUS

RADIUS pour Remote Authentication Dial-In User une norme de l'IETF (Internet Engineering TASK Force), C'est un protocole basé sur un système Client/Serveur pour les accès à distance à un réseau.

Principe de fonctionnement

RADIUS repose principalement sur : [9]

— un serveur appelé serveur RADIUS relié à une base d'identification (base de données, Active Directory, annuaire LDAP, etc.) et qui peut fonctionner aussi comme un serveur proxy, c'est-à-dire transmettre les requêtes du client à d'autres serveurs RADIUS.

— un client RADIUS, appelé NAS (Network Access Server) l'intermédiaire entre l'utilisateur final et le serveur. L'ensemble des transactions entre ces deux équipements est chiffré.

Le client RADIUS qui peut être un équipement ou bien une solution logicielle est capable d'envoyer des demandes de connexion (requêtes) et des messages à un serveur RADIUS. Il peut interpréter les réponses du serveur RADIUS et de ce fait valider ou non une authentification et/ou obtenir des autorisations.

Par la suite, ces informations sont transmises au poste de travail souhaitant accéder à la ressource informatique.

Traitement des requêtes de connexion avec RADIUS

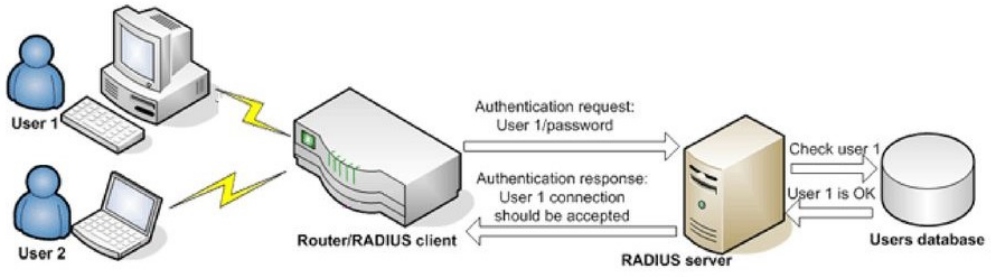


FIGURE 1.1 – Traitement des requêtes de connexion avec RADIUS

1.5.2 Analyse des risques MEHARI (Méthode Harmonisée d'Analyse des Risques)

Partons de la théorie du flacon de neige, chaque entreprise est associée à des risques différents qui peuvent endommager son système. En plus, de la complexité des risques qui est proportionnelle à la complexité croissante des technologies et des organisations elles-mêmes, fait d'un audit de sécurité un atout important vu obligatoire qui devait être effectué de façon régulière.

Une solution issue des deux approches de MELISA et MARION (Méthode d'analyse de risques informatiques optimisée par niveau) développé par le CLUSIF (Club de la sécurité de l'information français).MEHARI est liée à la sécurité de l'information d'une entreprise ou d'un organisme. Elle permet une gestion directe et individuelle des risques en spécifiant un certains nombre de principes fonctionnels qu'on peut résumer en : [5]

- Appréciation des risques
- Traitement des risques
- Gestion des risques

1.6 De l'urbanisation à l'audit

1.6.1 Audit ou urbanisation ?

un organisme devant réaliser un audit doit d'abord évaluer les risques liés a son système d'informations afin de déterminer quel audit doit être réalisé. En effet, la façon dont les audits sont définies joue un grand rôle dans l'efficacité globale de la fonction d'audit des SI.

la direction générale responsable de ce programme doit tenir compte de quelques aspects concernant l'étendue de l'audit qui doit être basé sur la taille et la nature de l'organisation auditée, ainsi que sur la nature, la fonctionnalité, la complexité et le niveau de maturité du système de management.

Limités par les contraintes temporelles, le budget,... et pour un contrôle plus approfondi, les chargés du projet emploient des outils (accélérateurs d'audits) en vue d'accroître l'efficience et l'efficacité de l'audit comme par exemple : les logiciels d'analyses et les outils de piratage.[14]

Relativement, l'élaboration d'une démarche d'urbanisation revient a l'utilisation d'une cartographie fondée sur un modèle en quatre couches de manière à cartographie l'existant et la cible du SI et d'identifier les perspectives de changements et les étapes stables.

Sa finalité consiste a organiser les niveaux du SI dans un objectif de flexibilité et réactivité, décliner et intégrer progressivement les demandes d'évolution du SI par une approche rationnelle (éviter les redondances, partage de composants et la maîtrise d'intégration de nouveaux composants).[13]

1.6.2 Les fondamentaux du COBIT 5

En vue de réaliser une inspection d'un SI, les auditeurs informatiques cherchent à avoir une meilleure gouvernance par le biais des référentiels d'audit (COBIT, Val IT, Risk IT, ...).

COBIT pour "Control Objectives for Information and related Technology", est un référentiel de bonnes pratiques d'audit informatique et de gouvernance des systèmes d'informations, qui :

- Fournit à l'ensemble des gestionnaires, auditeurs et utilisateurs des TIC, des services pratiques pour aider à maximiser les avantages issus des techniques informatiques.
- Constitue une structure de relations (cadre de référence ou framework) visant à un pilotage des techniques informatiques par le management de l'entreprise pour atteindre ses objectifs.
- Élabore de la gouvernance et du contrôle d'une entreprise, leurs faire comprendre leurs systèmes informatiques et déterminer le niveau de sécurité.[15]

Sa version 5 disponible depuis avril 2012 demeure le seul référentiel qui est orienté business pour la Gouvernance et la Gestion des Systèmes d'informations de l'entreprise, représente une évolution majeure et le plus adapté.

Cette nouvelle version combine les dernières réflexions en matière de gouvernance d'entreprise et techniques de gestion. Elle fournit des principes, des pratiques, des outils et des modèles analytiques, universelles, qui aident à améliorer la sécurité dans le Système d'Informations et sa valeur pour l'entreprise.

COBIT 5 complète COBIT 4.1 en intégrant d'autres cadres majeurs et standards, il s'agit d'un véritable référentiel intégrateur [4].

Il s'applique à :

- La sécurité de l'information
- La gestion des risques
- La gouvernance et la gestion du système d'informations de l'entreprise
- Les activités d'audit
- La conformité avec la législation et la réglementation
- Les opérations financières ou les rapports sur la responsabilité sociale de l'entreprise.

les principes du fonctionnement du COBIT 5, regroupés en 5 catégories, sont illustrés dans la figure suivante :

FIGURE 1.2 – Principes de fonctionnement du référentiel CobiT 5.

Section 2 : Présentation de l'organisme d'accueil

1.7 Introduction

Dans la partie précédente, nous avons montré que les risques liés au SI d'une entreprise peuvent affecter sa capacité à atteindre ses objectifs en raison des dommages qu'ils engendrent.

Il convient alors dans ce chapitre, de faire une étude empirique, pour faire un lien entre ce que nous avons vu précédemment et ce qui existe sur le terrain afin de vérifier nos hypothèses.

Ainsi, nous avons choisi l'EPB (Entreprise Portuaire de Béjaia). Pour mener à bien cette étude, nous avons jugé nécessaire de consacrer cette partie à la présentation de ladite entreprise, son infrastructure, applications et processus métiers puis la présentation des résultats de notre mission d'audit.

1.8 Présentation de l'organisme d'accueil

L'Entreprise Portuaire de Béjaia, est un port algérien, situé dans la ville de Béjaia, dans la région de la Kabylie. Il a été créé le 14 Août 1982 suite au décret n°82-285, joue un rôle très important dans les transactions internationales vu sa place et sa position stratégique.

Aujourd'hui, l'EPB est classé 2ème port d'Algérie en marchandises générales et 3ème port pétrolier. Il est également le 1er port du bassin méditerranéen certifié ISO 9001.2000 pour l'ensemble de ses prestations, et à avoir ainsi installé un système de management de la qualité.

Cela constitue une étape dans le processus d'amélioration continue de ses prestations au grand bénéfice de ses clients.

L'Entreprise Portuaire a connu d'autres succès depuis, elle est notamment certifiée à la Norme ISO 14001 :2004 et au référentiel OHSAS 18001 :2007, respectivement pour l'environnement et l'hygiène et sécurité au travail.

Principale tournante du commerce, il constitue l'accès privilégié aux différentes industries, parce qu'il offre à ses clients des terminaux convenables et compétitifs ainsi que des équipements modernes et performants, tous dédiés pour l'accueil et le traitement de tous types de marchandises.[6]

1.9 État des lieux

L'EPB est organisée selon des directions fonctionnelles et opérationnelles dirigées par une Direction Générale qui est chargée de concevoir, coordonner et contrôler les actions liées à la gestion et au développement de l'entreprise (voir figure 1.3).[6]

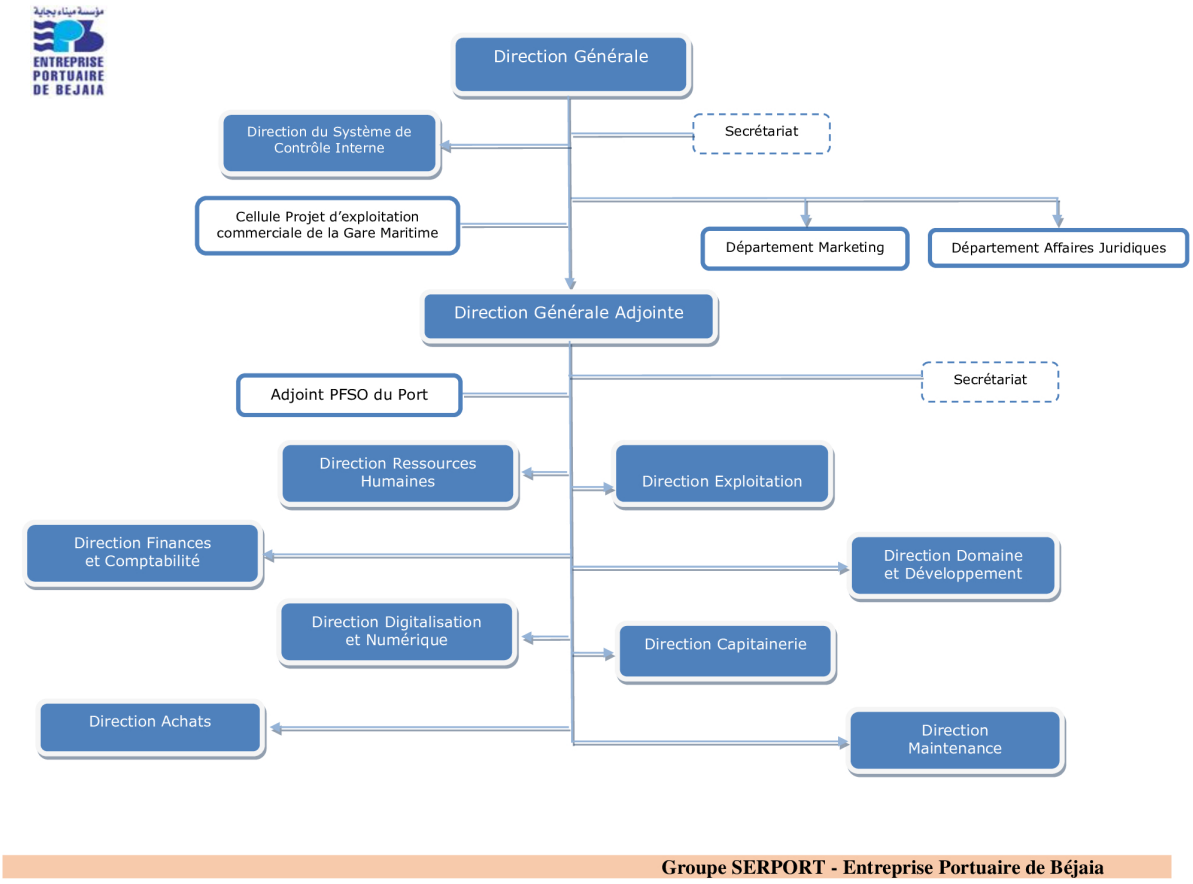


FIGURE 1.3 – Organigramme de l'état des lieux de l'EPB.

1.10 Infrastructures

Le réseau local de l'EPB permet aux différents postes de travail de s'échanger des informations, de se connecter vers l'extérieur et d'utiliser des applications hébergées en interne nécessaires à l'exécution des tâches quotidiennes des employées, il s'étend du port pétrolier n°16 aux ports n°13 & 18 (parc à bois).

Les salles machines de ce réseau contiennent principalement une armoire de brassage et une autre armoire optique de grande taille (de 09 à 42 Unités) contenant les serveurs, les onduleurs et l'ensemble des accessoires réseaux : switchs, les convertisseurs, les jarretières, les panneaux de brassage, etc. Ces deux armoires servent à relier les différents sites de l'entreprise avec le département informatique. [6]

Les équipements sont désignés dans le tableau 1.1. Et les tableaux 1.2 et 1.3 décrivent quelques exemples des serveurs baies de stockage et serveurs physiques et virtuels qu'utilise l'entreprise.

Désignation	Quantité
Ordinateurs	300
Imprimantes	200
Onduleures	300
Serveurs	13
Baies de stockage	03
Armoires de brassage	41

TABLE 1.1 – Équipements Informatiques et Réseau

Serveurs	Modèle	Caractéristiques
Baie Stockage NAS	Synology Diskstation DS1512	Processeurs : 2 CPU * 2.13 GHz Type de processeur : Intel Atom D2700 à 2.13 GHz (Dual-Core) RAM : 1 Go Disque Dur (Raid 1) : 17.9 To (7.16 To en Raid 1 + 3.58 en To en basic)
Baie Stockage SAN	HP MSA 2050 SAN Dual Controller SFF	Baie de Disques : 24 Disque Durs : 24 * 1.2 To
Baie Stockage SAN	HP MSA 2060 SAN	Baie de Disques : 24 Disque Durs : 24 * 2.4 To

TABLE 1.2 – Serveurs (Baies de Stockage)

Serveurs	Modèle	Caractéristiques	Serveur Virtuels sur ce serveur	Système d'exploitation	Description
Serveur 1	HP Proliant DL380 Gen 9	Processeurs : 12 CPU x 2,397 Ghz Type de Processeurs : Intel(R) Xeon(R) CPU E5-2620 v3 @ 2,40 GHz RAM : 4Go Disques Durs (RAID) : 3,188 To	Vm DC2 Vm system info Vm gest proi Vm ged Vm dev	Windows Server Linux Ubuntu Linux Windows Server Windows Server	Contrôleur de Domaine/ DNS/ DHCP/ partage global Serveur Web Apache Gestion de Projet Gestion électronique de documents Serveur de Développement
Serveur 2 (Serveur Hotspot)	ASUS B150	Processeurs : 1 CPU x 2,40 Ghz Type de Processeurs : Intel(R) Xeon(R) CPU E5620 v3@ 2,40 GHz RAM : 8 Go Disques Durs (RAID) : 500 Go	System Hotspot	PfSense	Pare feu et portail captif (hot spot) destiné pour les usagers de la gare maritime

TABLE 1.3 – Inventaire de quelques serveurs physiques et virtuels

1.11 Applications

Les applications métiers sont des programmes qui exécutent des tâches spécifiques liées aux activités de l'entreprise.

L'EPB parmi les plus grandes entreprises de l'Algérie, jouant un rôle très important et sensible dans les transactions internationales facilite la gestion de ses activités soit par le développement d'applications métiers, soit se dirige vers l'achat de progiciels standards avec des applications bien définies, qui ont pour but de répondre aux besoins spécifiques des utilisateurs en leurs permettant d'automatiser et de les assister dans la réalisation des tâches liées à leurs métier.

Quelques applications métiers utilisés par l'entreprise : [6]

- LogiMAC [Manutention et acconage]. (développé en interne) : Tout ce qui concerne les opérations de chargement et déchargement des navires, affectation des engins, des effectifs,...
- Application de gestion des conteneurs.
- Application de gestion des escales des navires.
- Application de gestion des opérations de remorquage.
- Logiciel de gestion du centre de transit des marchandises dangereuses.
- Logiciel de gestion de la maintenance.
- Logiciel de gestion de l'infrastructure portuaire.
- Logiciel de facturation des prestations portuaires.
- La GED [Gestion Électronique des Documents] (achetée et intégrée).
- Le SIP (développé en interne sous forme d'un site web) : consultable en local qui retrace les différentes activités du port sous forme de tableaux statistiques et rapports.
- ERP fonctionnel [Enterprise Ressource Planning] ou [Progiciel de gestion intégré] (achetée et intégrée) : fonctionne a base du SGBD SQL SERVER constitué des logiciels suivants :
  - Logiciel de comptabilité générale.
  - Logiciel de comptabilité analytique.
  - Logiciel de gestion financière.
  - Logiciel de gestion du budget.
  - Logiciel de gestion des ressources humaines.
  - Logiciel de gestion de la paie.
  - Gestion des stocks.
  - Logiciel de gestion des réclamations clients.
  - Logiciel de traitement des sondages clients.

1.12 Processus métiers

La figure (Figure 4) illustre les principaux processus métiers (Missions, Activités et Objectifs) identifiés durant notre stage effectué au sein de l'EPB.[6]

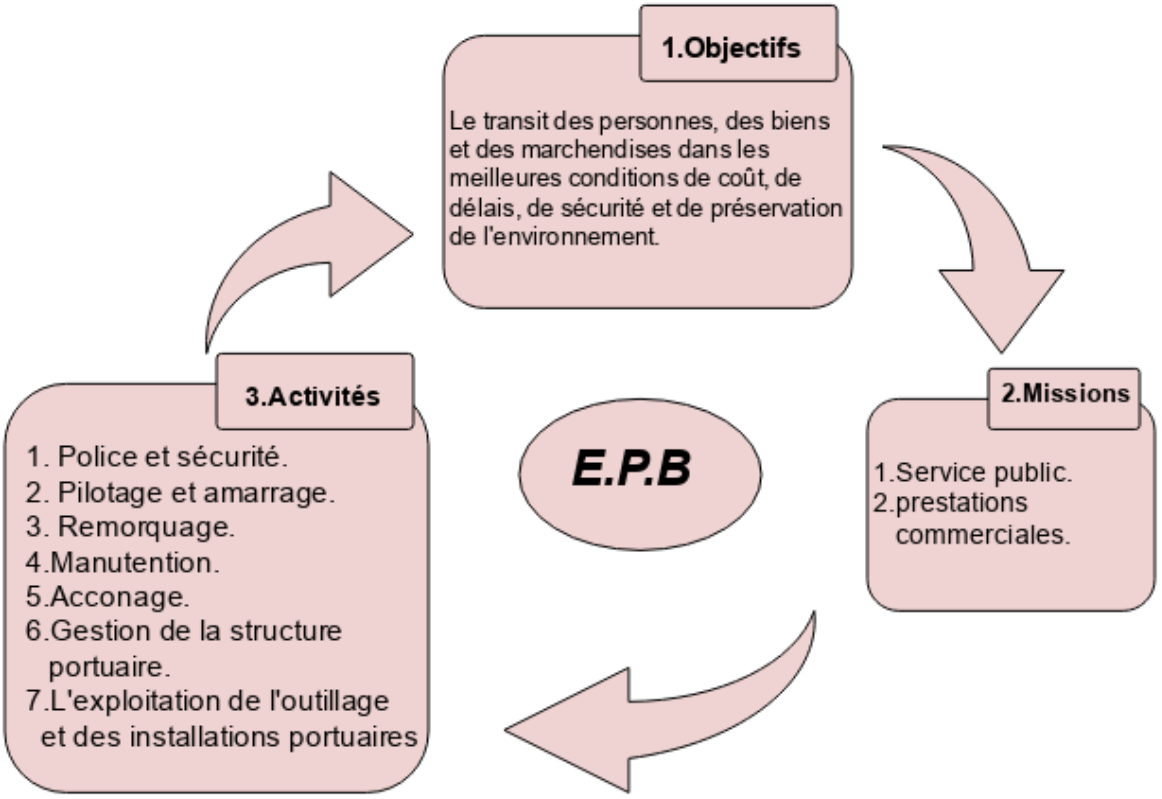


FIGURE 1.4 – Les principaux processus métiers de l'EPB

1.13 Problématiques

Plus de 10 ans sans mission d'audit de sécurité informatique dans le port de Béjaia et avec la transformation numérique qui touche tous ses services et secteurs d'activités, les risques liés à son système d'informations augmentent.

- De ce fait, quelles sont les déviations par rapport à la norme de sécurité ISO 27000 ?
- Quels sont les risques encourus par l'entreprise du fait de son SI ?
- Et si un évènement survient quel serait l'impact ?

1.14 Objectifs

Afin d'étudier la conformité du système d'informations de l'Entreprise Portuaire de Béjaia et déterminer son alignement par rapport aux bonnes pratiques (Référentiel adopté : Norme ISO 27000). Un audit de sécurité a été proposé à la direction digitalisation et numérique de l'EPB.

Le rapport fournira à la direction les points essentiels de l'analyse effectuée et soulignera les actions d'amélioration du niveau de sécurité de leur système.

1.15 Conclusion

A l'issu de ce chapitre, nous avons abordés des notions et des concepts importants sur les SI, ainsi que la sécurité dans les entreprises, et ce pour se familiariser au thème de ce mémoire.

Puis on a entamé une étude détaillée de l'organisme d'accueil, ce qui nous a permis de maîtriser ses différentes structures, ensuite une problématique est rédigée sous forme de points techniques qui nous a permis de tracer le plan d'audit.

Le chapitre suivant va porté plus de détails en réalisant un rapport d'audit et une roadmap.

Chapitre 2

Rapport d'audit et roadmap

Partie 1

2.1 Introduction

Dans le présent chapitre on va présenter la mission d'audit de la sécurité du système d'information de l'entreprise Portuaire de Béjaia réalisé en Avril-Juin 2022.

Cette mission évalue par rapport aux exigences de la norme ISO 27000 et a adopté la méthode MEHARI pour analyser les risques ainsi que COBIT5 pour analyser la gouvernance.

On expose ensuite la synthèse d'évaluation du niveau de sécurité qui a été obtenue par rapport aux référentiels de sécurité ainsi qu'un ensemble de recommandations.

2.2 Analyse des risques MEHARI

En ce qui suit, un tableau récapitulatif de la phase d'appréciation de risques qui comprend les 3 étapes d'Identification, Estimation et Évaluation ensuite dans le plan d'action on verra les solutions proposées à mettre en oeuvre et les contrôles permettant de piloter la gestion de ces risques.

Processus d'évaluation

1. **Identification des risques :**
   La 1re et la 2e colonnes du tableau sont respectivement des références aux domaines de sécurité évaluées par un questionnaire et une liste de risques possibles. (Voir les annexes A et B)

2. **Estimation des risques :**
   Réalisé selon les deux (02) critères : **Impact** et **Potentialité**.
   Qu'on a **classé** en 4 niveaux (vu que c'est une estimation et non de 'mesure' ce qui semble bon) et **évalué** en prenant en compte plusieurs facteurs :
   D'impact :
   — *la disponibilité des mesures de sécurité*
   — *l'estimation du personnels concerné de l'entreprise.*
   — *etc...*

De potentialité :
— *La localisation et l'environnement de l'entreprise, pour les risques naturels*
— *probabilité qu'un acte volontaire cible spécifiquement l'entreprise.*
— *etc...*

Échelle d'impact :
— Niveau 4 (Impact très grave) : Aucune prise des mesures de sécurité et sous-estimation totale des dirigeants.
— Niveau 3 (Impact grave) : Prises insuffisantes des mesures de sécurité et sous-estimation des dirigeants.
— Niveau 2 (Impact Important) : Prises des mesures de sécurité nécessaires avec/sans estimation.
— Niveau 1 (Impact Non significatif) : Prises satisfaisante des mesures de sécurité.

Échelle de potentialité :
— Niveau 4 (Très probable) : probabilité élevée de survenance du risque.
— Niveau 3 (Probable) : risque probable.
— Niveau 2 (improbable) : risque improbable.
— Niveau 1 (Très improbable) : risque très improbable.

3. **Évaluation des risques :**
La dernière phase d'appréciation de risques est l'évaluation qui permet de déterminer le niveau de gravité (acceptabilité) en utilisant la grille de gravité standard de MEHARI où :
— G = 4 : Risques insupportables, qui devraient faire l'objet de mesures d'urgence.
— G = 3 : Risques inadmissibles, qui devraient être réduis ou éliminés à une échéance à déterminer.
— G = 2 ou 1 : Risques tolérés.

I = 4	G = 2	G = 3	G = 4	G = 4
I = 3	G = 2	G = 3	G = 3	G = 4
I = 2	G = 1	G = 2	G = 2	G = 3
I = 1	G = 1	G = 1	G = 1	G = 2
	P = 1	P = 2	P = 3	P = 4

TABLE 2.1 – Grille standard d'acceptabilité des risques de MEHARI

Exemple d'évaluation

Domaine 07 : Gestion des incidents liés à la sécurité de l'information

1. Par les questions qui le compose nous identifions les ressources que touche ce domaine (le parc informatique, les données,...), puis utilisons la liste de risques possible et déterminons les risques pouvant être engendré.
2. Ensuite l'estimation de risques exige de calculer l'impact et la potentialité (toujours pour chaque question) qui déterminerons le niveau d'acceptabilité (ou niveau de gravité) puis on calcule la moyenne pour le domaine complet.

2.2.1 Tableau récapitulatif et analytique

Identification des risques		Estimation des risques		Évaluation des risques (Acceptabilité)
ID Domaine	ID Risques	Impact	Potentialité	Gravité
D01	R01/ R02	2	3	2
D02	R01/ R08/ R10/ R12/ R13	2.33	3.17	2.5 (3)
D03	R01/ R02/ R03/ R04/ R05/ R06/ R07/ R09	3	3.2	3
D04	R01	1	3	1
D05	R01/ R04/ R06	2.33	3	2.33 (3)
D06	R01/ R02/ R06 R07/ R11/ R12/ R13	2	3	2
D07	R01/ R02/ R05 R06/ R07/ R12 R13	3	3.5	3
D08	R01/ R02/ R03/ R04/ R05/ R06 R07/ R08/ R09/ R10/ R11/ R13	2.6	3.2	2.6 (3)
D09	R01/ R02/ R14	2.2	3	2.2 (3)
D10	R01/ R02/ R10/ R13	2.5	3	2.5 (3)
D11	R01/ R04/ R05/ R06	2	3	2
D12	R01/ R02/ R04/ R05/ R06/ R07/ R12/ R13/ R14	2.33	3	2.33 (3)
D13	R01/ R02/ R06/ R07/ R11/ R12/ R13/ R14	2.67	3	2.67 (3)
D14	R01/ R02/ R05/ R06/ R07/ R09/ R11/ R12/ R13	3	3.25	3

TABLE 2.2 – Tableau récapitulatif et analytique

Rosace de gravité et synthèse

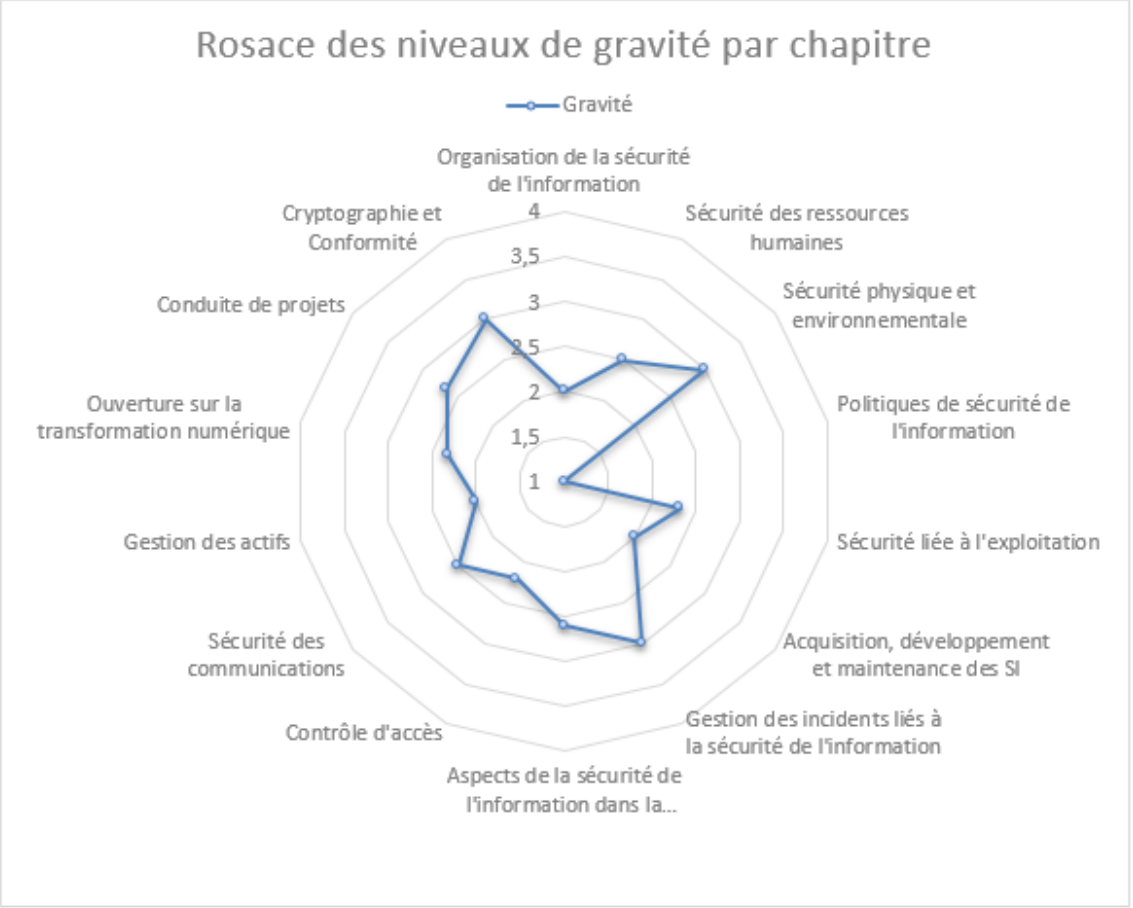


FIGURE 2.1 – Rosace des niveaux de gravité par chapitre.

L'interprétation des calculs en termes du périmètre audité de l'EPB montre :
Seulement un seul domaine qui prend la borne inférieure dans l'intervalle [1-4] alors que les restes sont entre 2 et 3 indiquant des risques **importants** et **graves** ainsi des mesures de sécurité urgentes devront être mise en oeuvre.

L'appréciation du risque utilisée par MEHARI permet à la structure auditée d'identifier ses risques et de quantifier l'effort à fournir en matière de sécurité des SI pour être conforme aux bonnes pratiques de sécurité.

2.2.2 Plan d'action

Dans la gestion des risques, le plan d'action consiste à déterminer les recommandations à mettre en œuvre, leurs niveaux d'urgence et de contrôler l'implémentation.

Seulement cela est affecté par les décisions des responsables de l'entreprise qui vont étudier selon plusieurs critères économiques, niveau de gravité des risques, nombre de risques à traités... de transformer ou non ces solutions en projets à déployer.

Approche de mise en œuvre

Ce travail a abouti à des résultats qui peuvent déceler des défaillances pouvant causer des dégâts indésirables dans l'interface de sécurité des systèmes d'informations.

Voici donc un total de 15 recommandations pertinentes proposées :

N	Recommandations	Références à des questions	Niveau d'urgence
1	Faciliter la mise en place des programmes d'auto-évaluation des contrôles de la sécurité des SI (Control-Self Assessment).	Q13/ Q18/ Q21/ Q24/ Q26	Urgent
2	Former les utilisateurs à détecter les anomalies qui pourraient révéler des tentatives d'ingénierie sociale.	Q04	Urgent
3	Faire collaborer des personnes de générations et de compétences différentes pour garantir le fonctionnement et l'évolution du SI (faire appel aux Freelancer au cas de manque de main d'oeuvre).	Q05/ Q24/ Q26/ Q43/ Q48	Urgent
4	Renforcer les mesures de sécurité physique relative à l'accès à la salle serveur	Q24	Urgent
5	Mettre en place une pointeuse à double authentification.	Q12	Urgent
6	Planifier des mises à jour périodiques sur les documents de politique de sécurité.	Q18/ Q21/ Q24/ Q26/ Q48	Urgent
7	Vérifier et lister les services en activité sur les stations, serveurs en exploitation, de décider à propos de leur utilité et s'assurer périodiquement de l'absence de failles.	Q16/ Q17/ Q18	Préférable
8	Mettre en place une veille de sécurité : Evaluation et controles du SI régulièrement en regard des risques (failles de sécurité, cyberattaques, fraudes et les risques liés à la transformation numérique).	Q13/ Q18/ Q26/ Q48	Urgent
9	Améliorer la sécurité opérationelle par la séparation des focntions de développement, de tests et d'exploitation.	Q18	Urgent
10	Planifier la réalisation d'un audit de sécurité, au moins une fois par an.	Q13/ Q24/ Q48	Urgent
11	Effectuer régulièrement des mises à jours des anti-virus et appliquer les correctifs de sécurité et les mises à jour des systèmesd'exploitation.	Q23/ Q25	Normale
12	Accorder une attention particulière aux consultants ou spécialistes pour un poste stable affecté uniquement à l'audit des systèmes.	Q43/ Q48	Urgent
13	Fournir un soutien technique ou des stages sur les audits informatique aux personnels qualifiés de la DSI.	Q43	Préférable
14	Segmenter et séparer l'information.	Q18	Urgent
15	Privilégier le stockage des données sur un espace commun sur le réseau.	Q27	Préférable

TABLE 2.3 – Tableau des recommandations proposées

Modalités de contrôle et de gestion

On définit ici en 2 étapes, les contrôles permettant de piloter la gestion des risques : [1]

1. Vérifier les solutions de sécurité proposées qu'ils correspondent bien aux niveaux de qualité de service (QoS) par un questionnaire.
   Cela veut dire que, les auditeurs devront convaincre le personnel concerné de l'entreprise de leurs solutions apportées. Ce qui conduit, à la nécessité d'une base d'expertise ou base d'audit.

2. Un contrôle de mise en oeuvre des services de sécurité
   Des contrôles devront être effectués au cas de déploiement incomplet des mesures de sécurité, d'en rédiger un rapport,...

2.3 Cadrage de la gouvernance de projets

La gouvernance SI est un concept fondamental qui permet le pilotage et l'amélioration des systèmes d'informations, a pour objectif la création de la valeur c'est à dire : la réalisation des bénéfices, l'optimisation des ressources et l'optimisation des risques de l'entreprise.

Cette 2^{e} partie de ce présent chapitre est donc consacré à l'analyse de la gouvernance du SI-EPB. L'étude se base sur le référentiel Cobit5 définit dans le chapitre précédant.

Processus d'évaluation

En plus des objectifs, selon Cobit5 les principaux éléments constituant cette analyse sont les processus de gouvernance et les facilitateurs.

Les Processus : divisés selon les deux fonctions de gouvernance et de gestion où on retrouve 5 dans la gouvernance qui définissent des pratiques d'évaluation, de direction et de surveillance (EDS).

EDS01 Assurer la définition et l'entretien d'un référentiel de gouvernance.

EDS02 Assurer la livraison des bénéfices.

EDS03 Assurer l'optimisation du risque.

EDS04 Assurer l'optimisation des ressources.

EDS05 Assurer aux parties prenantes la transparence.

Les facilitateurs : sont des éléments qui influencent les activités d'une entreprise et influencés par les objectifs TI définissent ce que les différents facilitateurs devraient permettre d'atteindre.

F01 Structure organisationnelle et règles de gestion.

F02 Processus métiers..

F03 Gouvernance de l'information et des données..

F04 Les services, l'infrastructure et les applications..

F05 Compétences et culture digitale..

Les objectifs : En terme de gouvernance du SI-EPB, voici les 16 objectifs TI de l'entreprise :

Obj 01 Valeur pour les parties prenantes.

Obj 02 Gestion de produits et services concurrentiels.

Obj 03 Gestion de risques (Protection des actifs).

Obj 04 Conformité aux lois et à la réglementation.

Obj 05 Culture de services orienté client.

Obj 06 Continuité et disponibilité des services d'affaires.

Obj 07 Faciliter l'agilité de l'entreprise en évolution.

Obj 08 Prise de décision stratégique basé sur l'information.

Obj 09 Optimisation des coûts de livraison des services.

Obj 10 Optimisation de la fonctionnalité des processus d'affaires.

Obj 11 Optimisation des coûts des processus d'affaires.

Obj 12 Productivité opérationnelle et productivité personnelle.

Obj 13 Conformité aux politiques interne.

Obj 14 Personnes qualifiés et motivés.

Obj 15 Culture d'innovation des produits et des affaires.

Obj 16 Objectifs sur la sécurité des SI.

L'évaluation : est en 2 niveaux
— **1er Niveau** : Évaluation des questions. (Voir Annexe C)
— **2e Niveau** : Évaluation des Processus et Facilitateurs.

Indicateurs d'évaluation :
— **P** : Primaire.
Ou
— **S** : Secondaire.

Exemple d'évaluation

Processus EDS01 : Assurer la définition et l'entretien d'un référentiel de gouvernance

1. Nous identifions dans le 1er niveau les objectifs cibles pour chaque question par rapport à la réponse obtenue, puis estimer un degré pour chacun des objectifs.

2. Ensuite, dans le 2e niveau, on estime le degré globale pour le processus en basant sur les degrés partiels.

Ci-dessous la grille finale de la gouvernance du SI-EPB :

Objectifs/ Processus et Facilitateurs	Obj 01	Obj 02	Obj 03	Obj 04	Obj 05	Obj 06	Obj 07	Obj 08	Obj 09	Obj 10	Obj 11	Obj 12	Obj 13	Obj 14	Obj 15	Obj 16
EDS01	P			P		P		P				S	P			
EDS02	P		S		S		P		P	P		S			S	
EDS03		S	S	S	S	S										
EDS04	S	S	S								P	S				
EDS05	P	P			P										P	
F01	P	S	S	S				S					P	S	S	S
F02	S		S			P	S			S	S				S	S
F03					P	P	P	S				S				
F04			P	P		P										P
F05	S		S			S	S					S		S	S	

TABLE 2.4 – Grille d'évaluation des processus et facilitateurs par rapport aux objectifs de la gouvernance du SI-EPB.

Analyse critique des résultats de l'audit de la gouvernance

L'évaluation de la gouvernance de l'information revêt une grande importance dans les entreprises. Toutefois, ce sujet est peu exploré dans la recherche.

D'après les résultats que montre le tableau ci-dessus, on remarque que la plupart des objectifs sont atteints en degré secondaire et donc une négligence de gestion de leurs part ou/et domaine en cours de développement

Pour réussir le projet de gouvernance des SI, voici quelques bonnes pratiques à suivre :[10]

- Bien mesurer son projet car un bon travail ne se fond pas seulement sur des réunions et des réflexions initiales.
- Établir des tableaux de bord afin d'assurer l'efficacité.
- L'importance de la gestion des risques n'a plus besoin de justification, elle est obligatoire dans la gestion des SI.
- Assurer la transparence et éviter de se cacher derrière les barreaux de *confidentialité et sécurité* pour justifier l'inaction, il faudra donc indiquer les niveaux de sécurité nécessaire.

2.4 Conclusion

Au cours de ce chapitre, nous avons analysés, par le biais d'un questionnaire, les différents domaines liés à la sécurité des SI en adoptant la démarche MEHARI qui nous a permis de mener à bien l'audit. Ensuite nous avons présentées les différentes recommandations qui permettent de remédier aux différents problèmes et failles de sécurité constatées.
En fin nous avons terminé avec une analyse de la gouvernance et quelques bonnes pratiques concernant.

On ce qui suit, la partie pratique de ce thème mémoire.

Chapitre 3

Applications des recommandations

3.1 Introduction

Notre projet s'inscrit dans le domaine de la sécurité informatique, il consiste en une mise en oeuvre d'un audit de sécurité pour le système d'informations de l'Entreprise Portuaire de Béjaia.

Ce chapitre est consacré à l'application d'une solution proposée après l'audit qui porte sur l'authentification des utilisateurs et s'appuie sur le protocole radius.

3.2 Émulation des composants infrastructures et applications du système d'informations

3.2.1 Émulation du réseau sur GNS3

Après avoir importé les machines virtuelles représentées dans la figure 3.2, installées et configurées préalablement dans VMware Workstation, nous avons choisie d'émulés ce réseau interne :

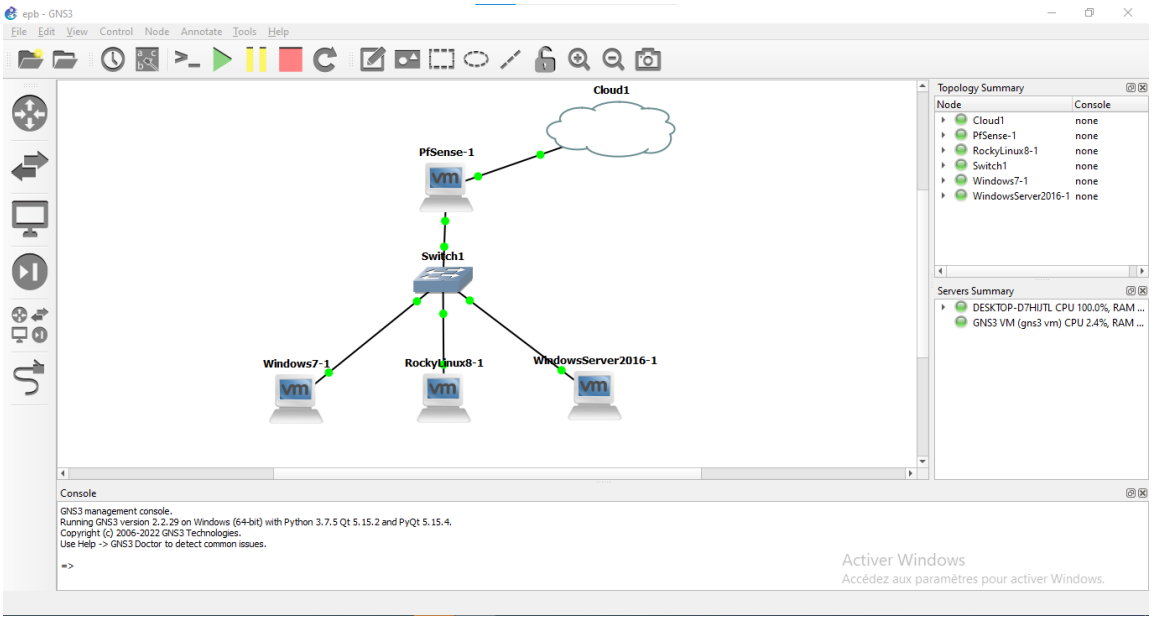


FIGURE 3.1 – Émulation d'un réseau interne sous GNS3.

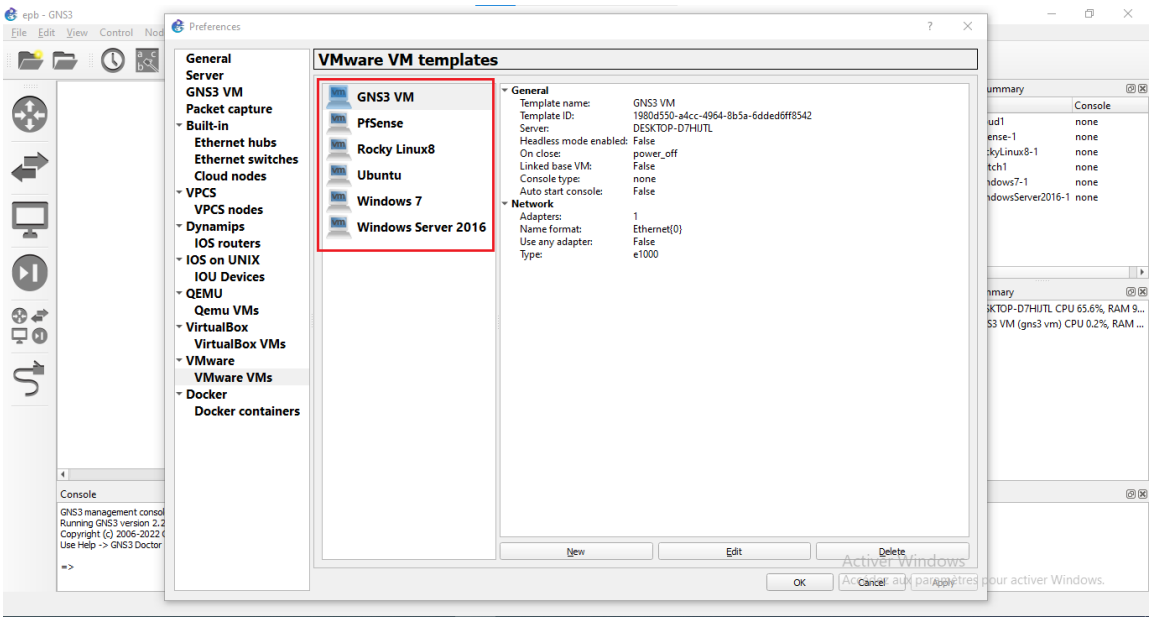


FIGURE 3.2 – Ajout des machines virtuelles sous GNS3.

Afin d'assurer la communication entre ces machines, la réussite des **pings** est obligatoire. Voici le résultat de connectivité entre quelques unes :

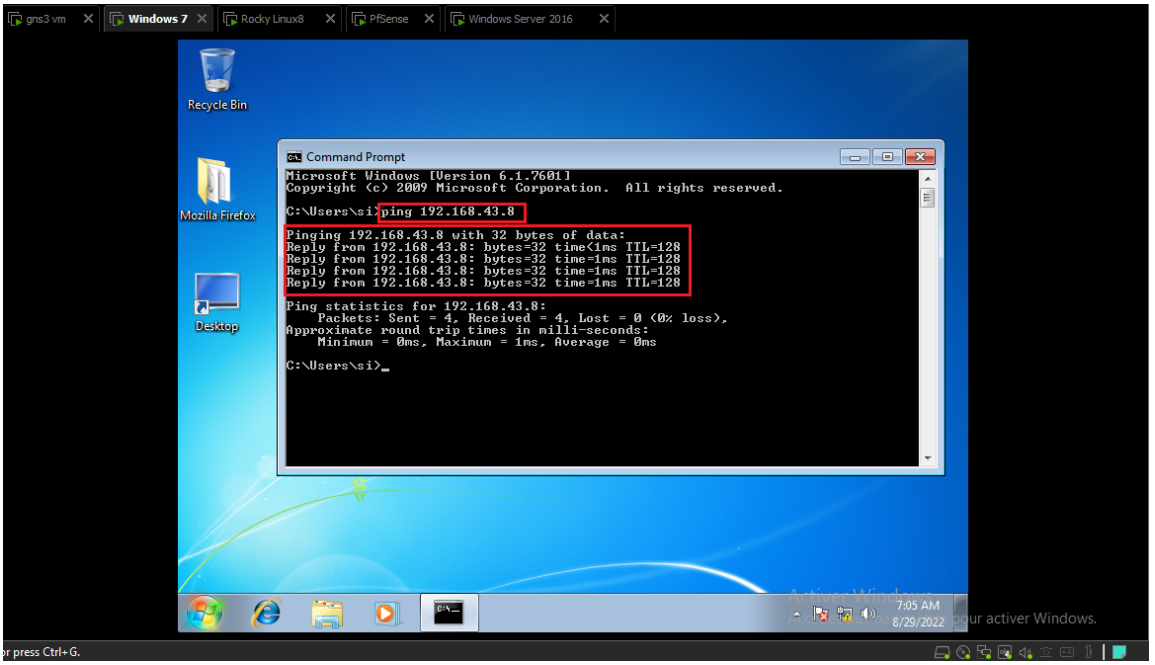


FIGURE 3.3 – Ping Windows 7 - Windows Server 2016.

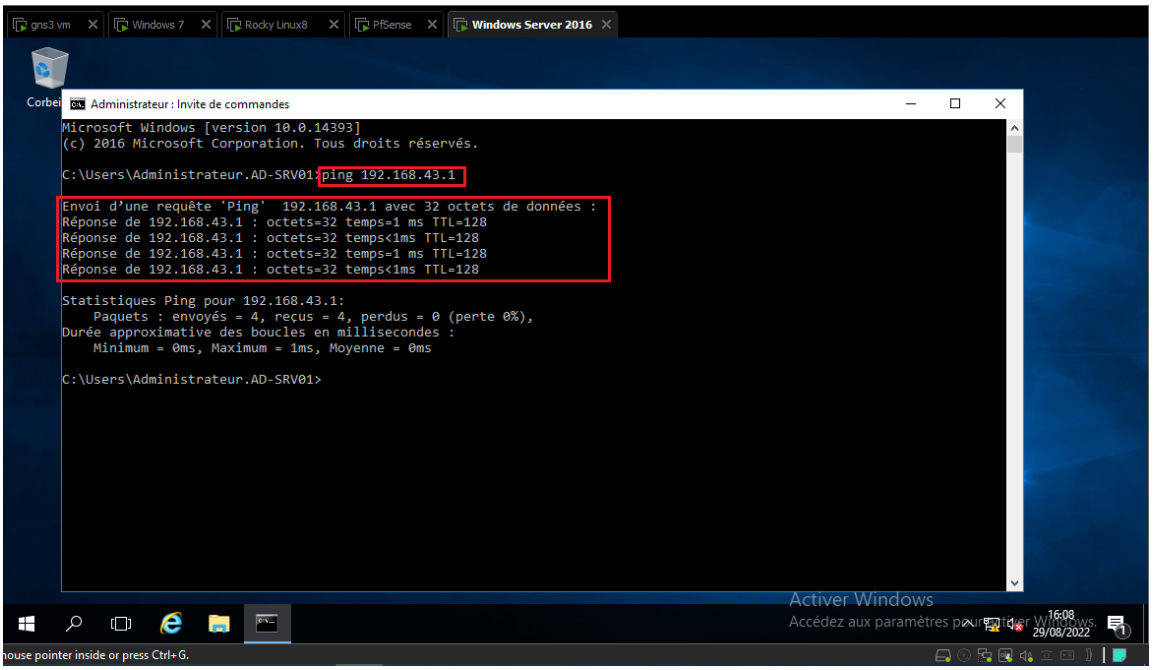


FIGURE 3.4 – Ping Windows Server 2016 - pfSense.

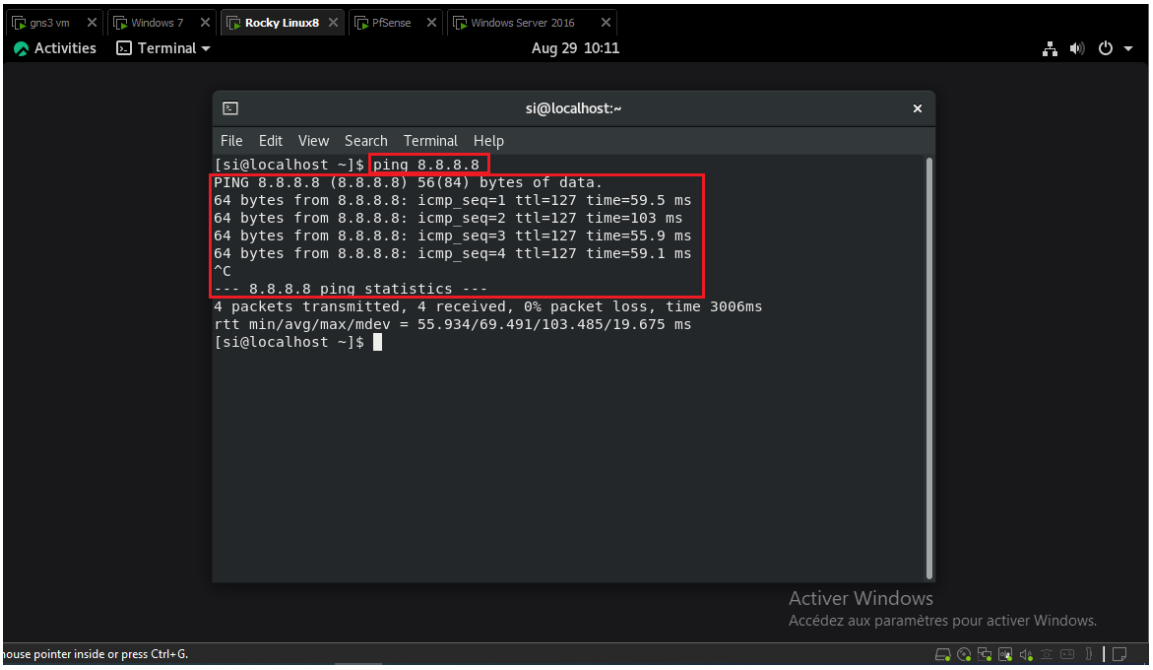


FIGURE 3.5 – Ping Rocky - Internet.

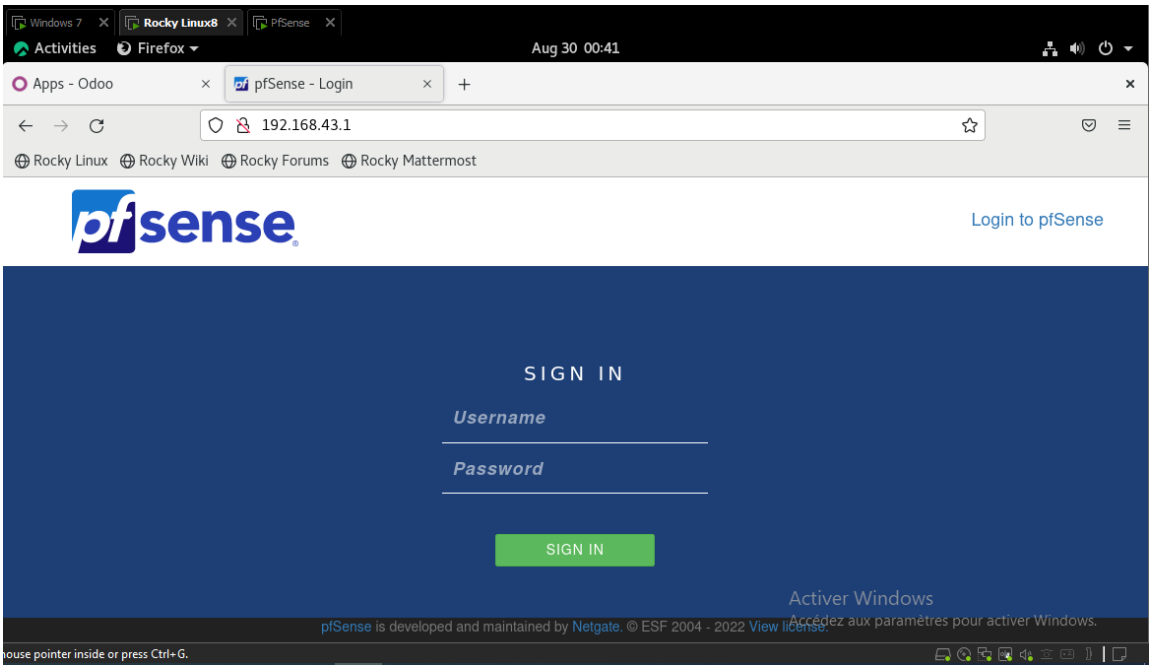
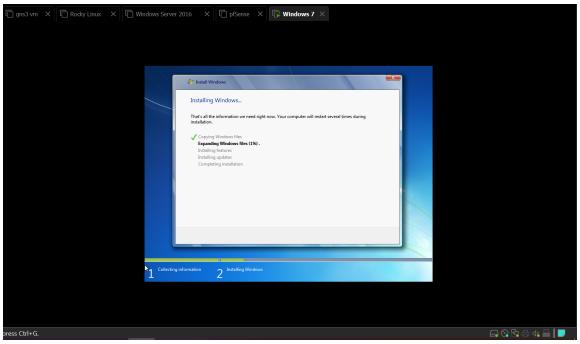


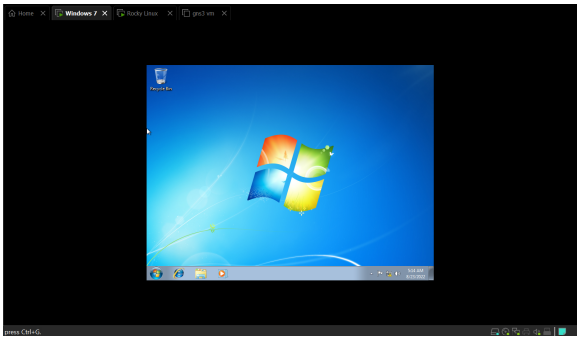
FIGURE 3.6 – Connexion à distance de Rocky à pfSense.

3.2.2 Virtualisation des systèmes

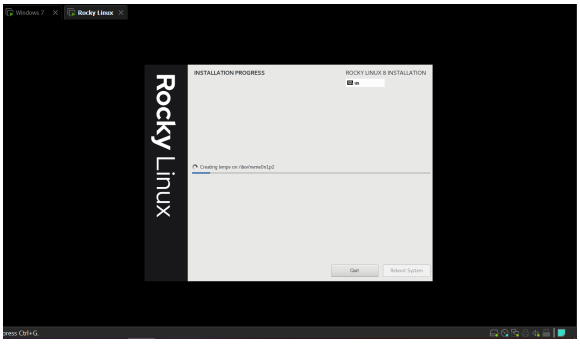
Dans cette sous partie, on mit en évidence les différentes machines installées dans le logiciel de virtualisation **VMware Workstation** :



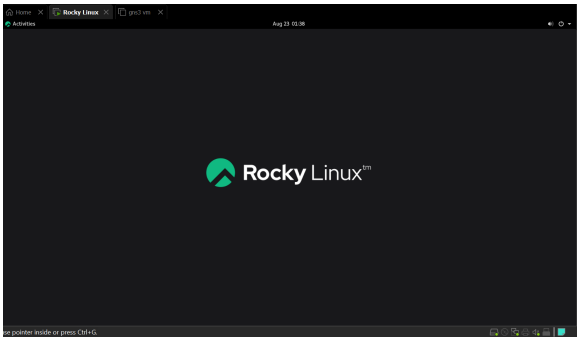
(a) Installation de Windows 7



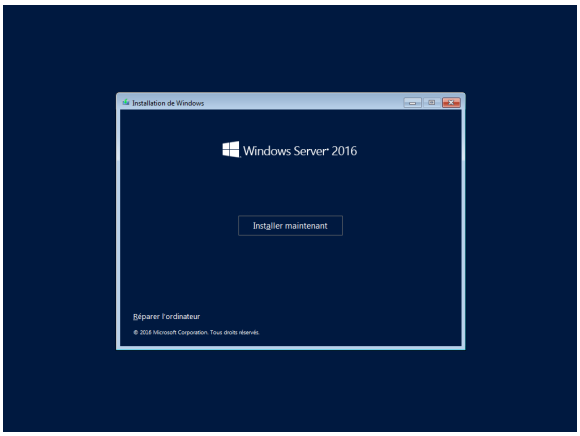
(b) Windows 7



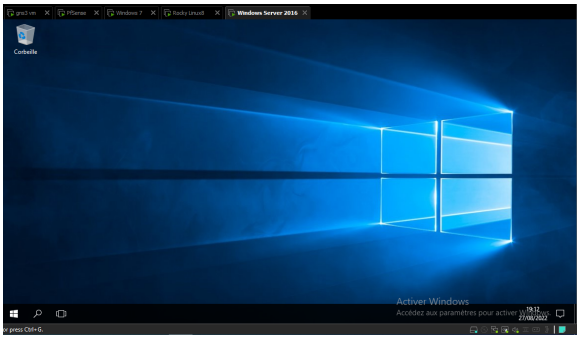
(a) Installation de Rocky Linux 8



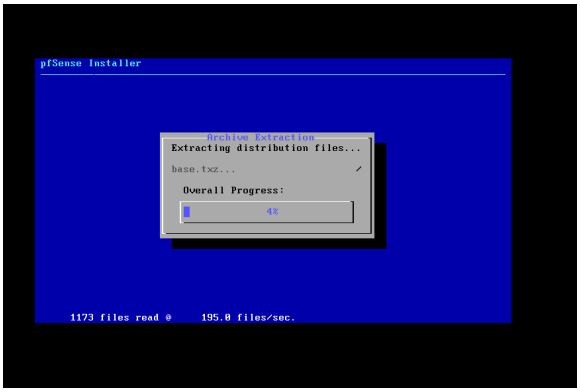
(b) Rocky Linux 8



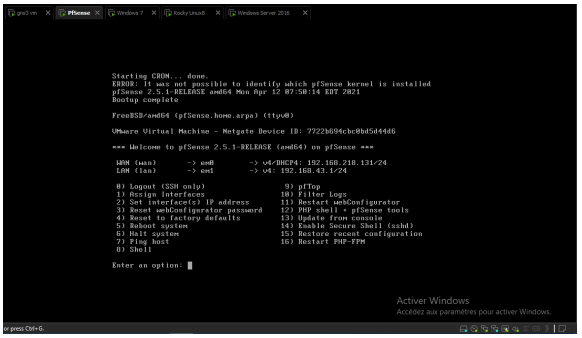
(a) Installation de Windows Server 2016



(b) Windows Server2016



(a) Installation de pfSense



(b) pfSense

3.2.3 Installation des composants logiciels et applications métiers

Parce que qu'il est un excellent outil et meilleur logiciel ERP pour une gestion personnalisé d'une entreprise, on a choisi d'installer dans cette section le progiciel open source de Odoo SA : **Odoo14**.

Pour une meilleure expérience, l'installation était réalisée sous Rocky Linux 8 suivant les étapes ci-dessus :

Mise à jour des packages et installation de la commande 'sudo'

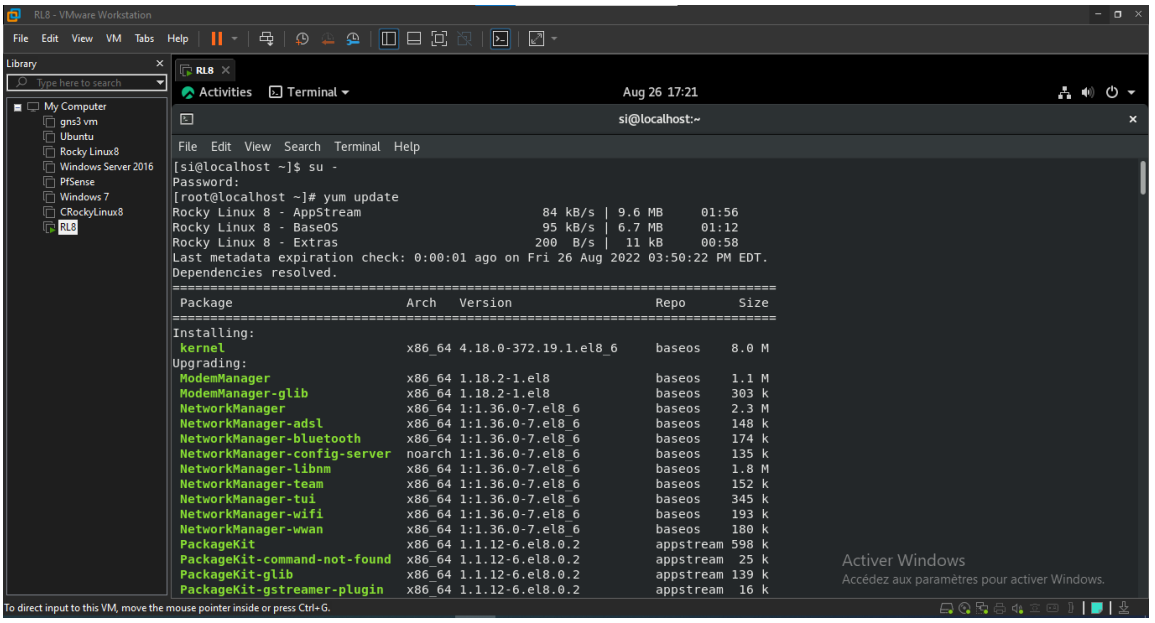


FIGURE 3.11 – Mise à jour des packages et installation de la commande 'sudo'.

Installation du référentiel EPEL

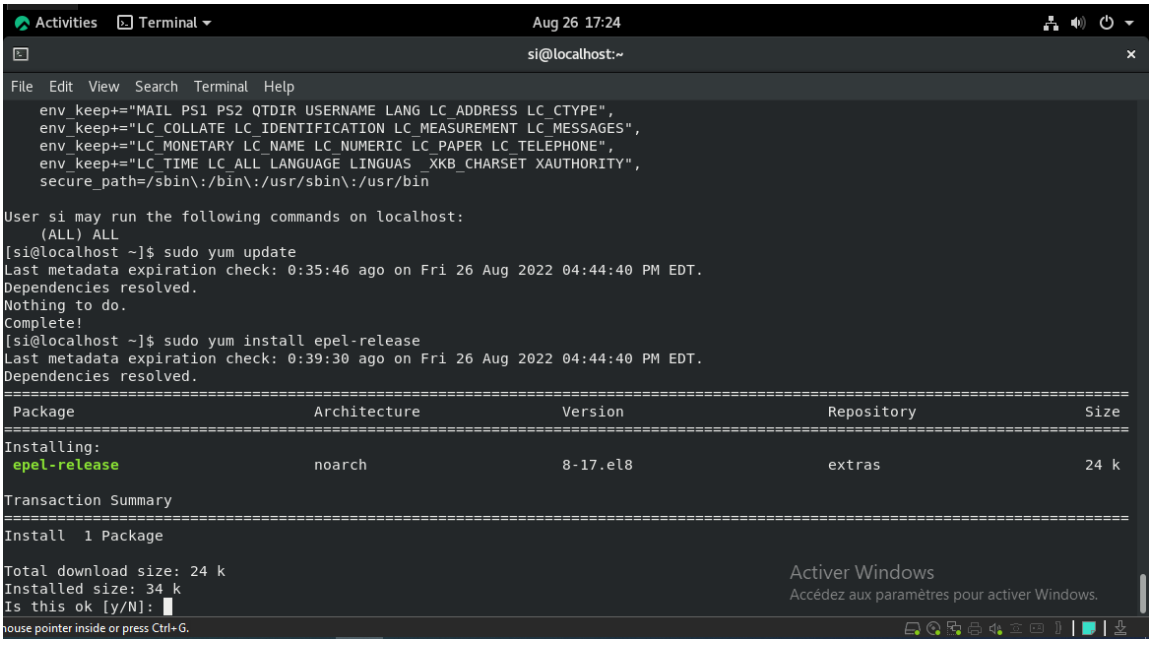


FIGURE 3.12 – Installation du référentiel EPEL.

Installation des dépendances Python et Odoo

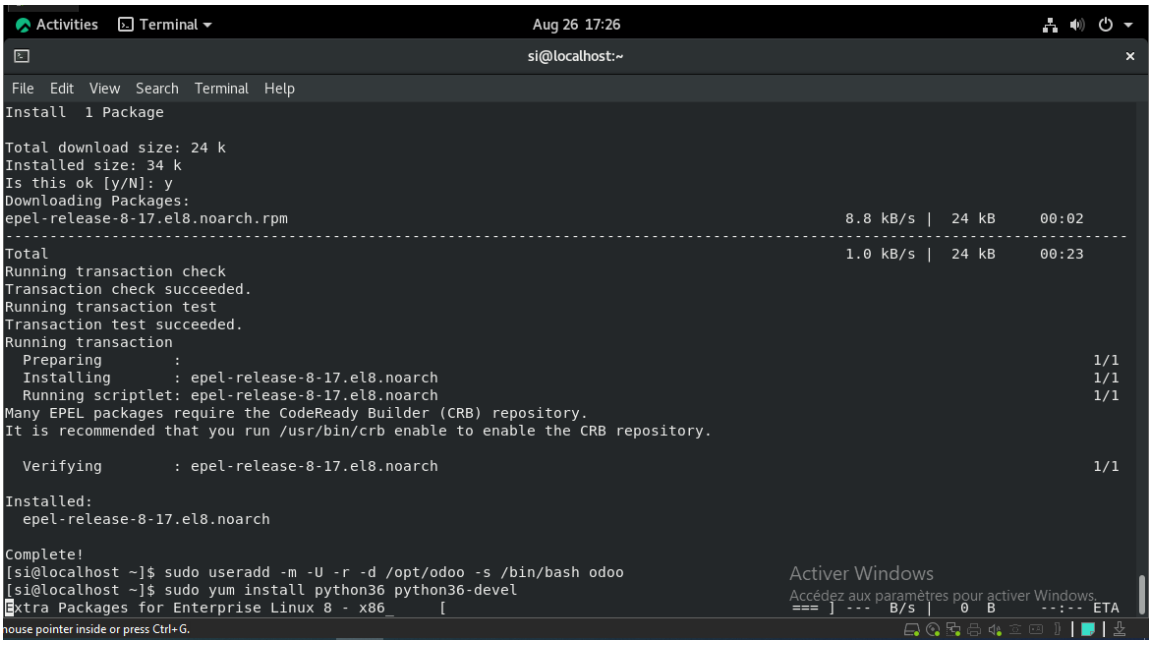


FIGURE 3.13 – Installation des dépendances Python et Odoo

Installation PostgreSQL

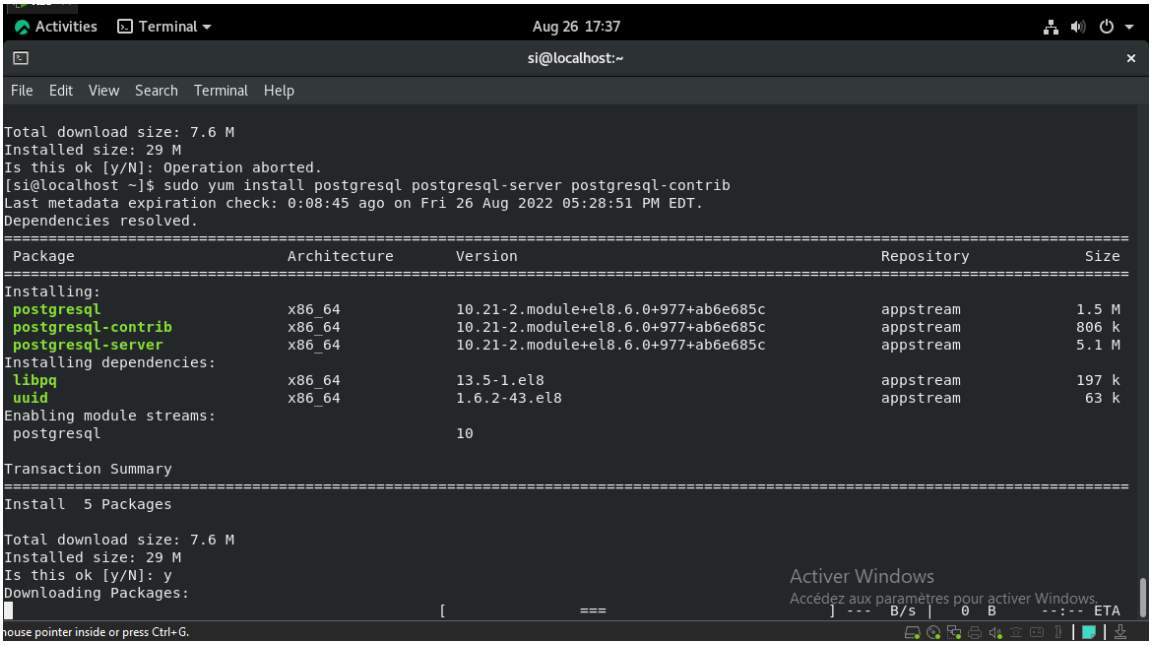


FIGURE 3.14 – a. Installation de PostgreSQL.

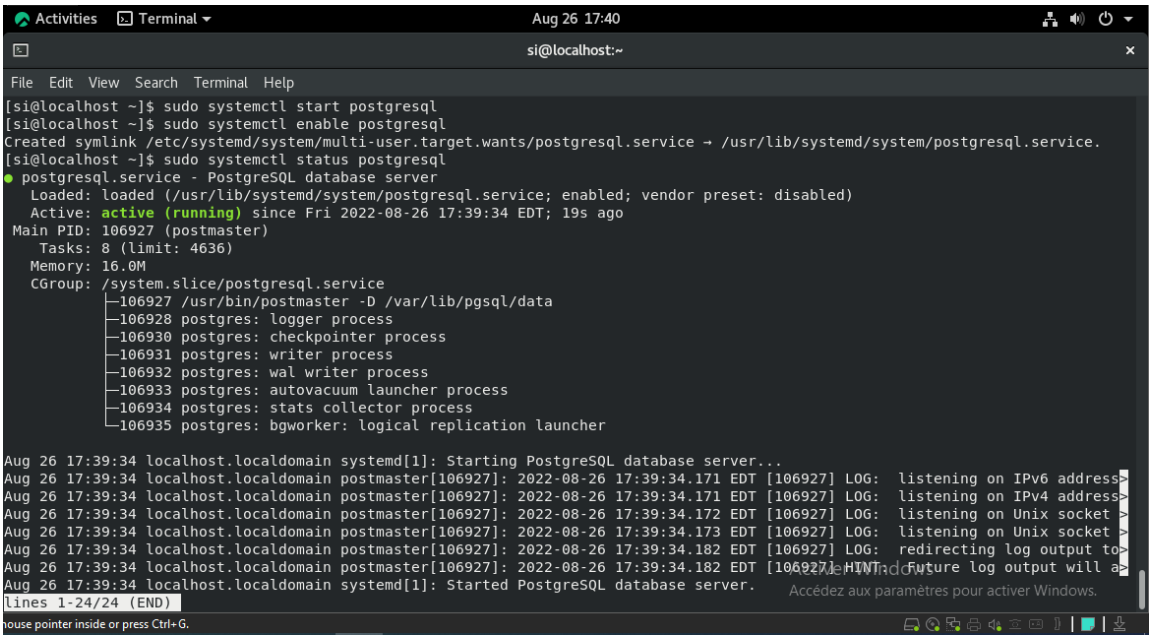


FIGURE 3.15 – b. Installation de PostgreSQL(Active).

Installation Wkhtmltopdf

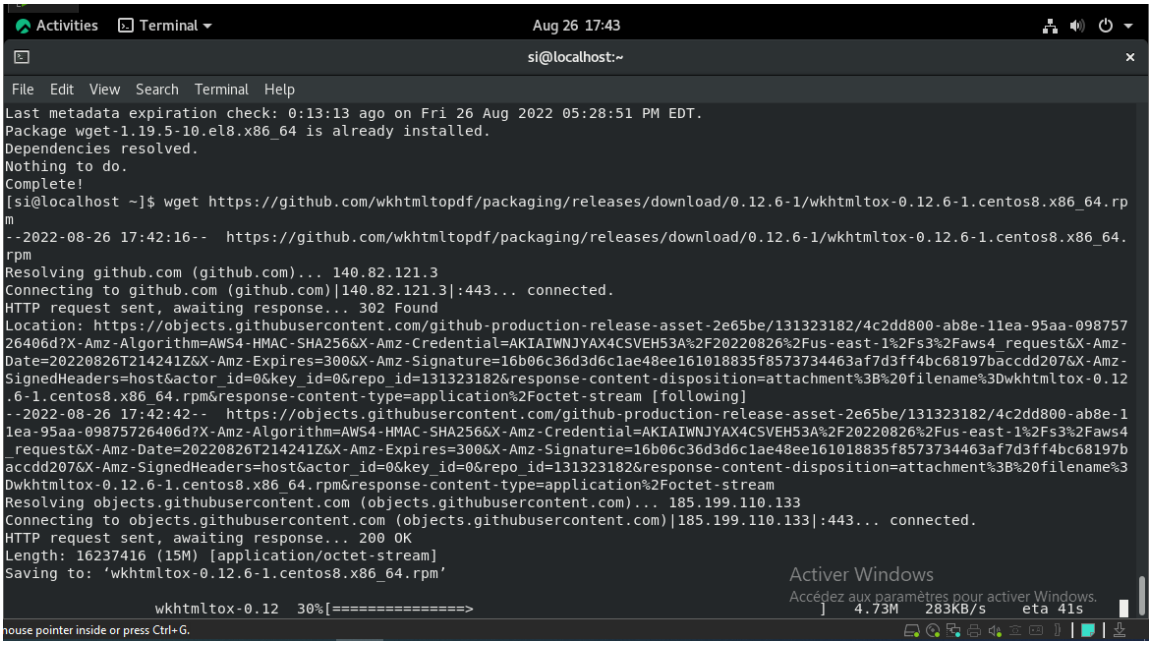


FIGURE 3.16 – Installation Wkhtmltopdf.

Téléchargement Odoo14 et Configuration de l'environnement Python

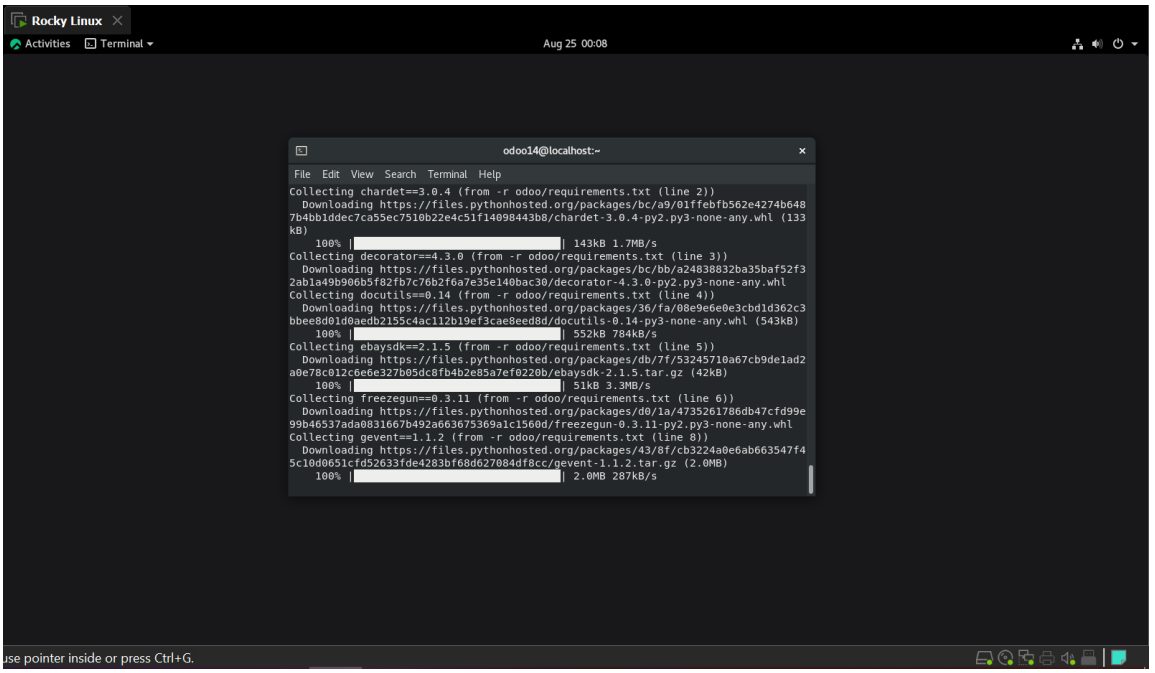


FIGURE 3.17 – Téléchargement Odoo14 et Configuration de l'environnement Python.

Création des répertoires pour les addons personnalisés et les journaux Odoo

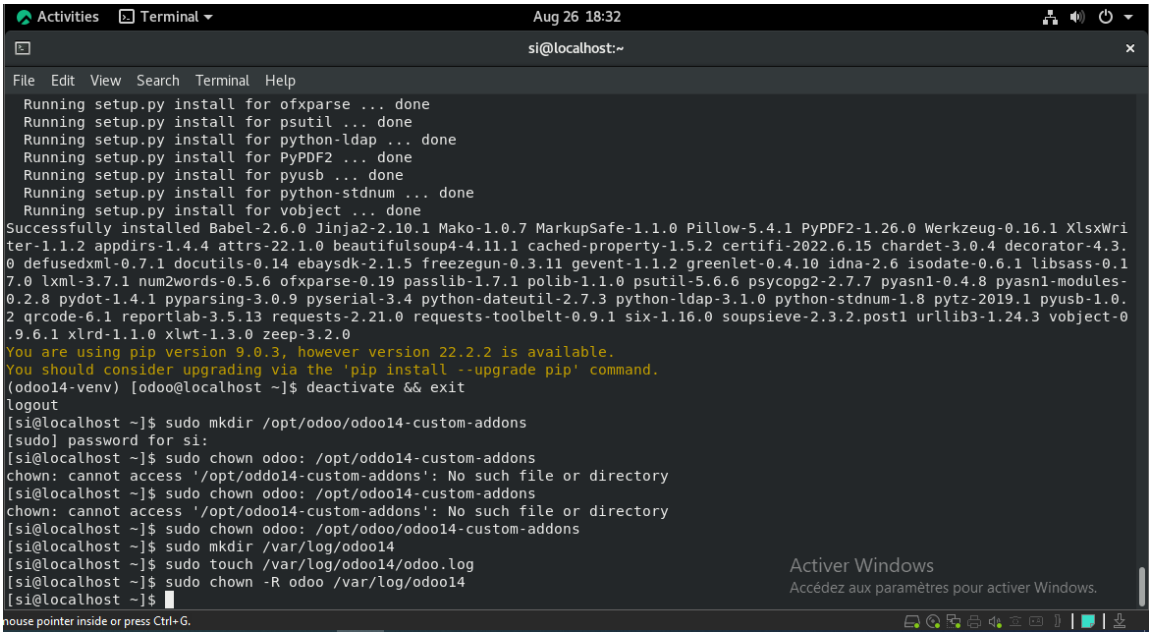


FIGURE 3.18 – Création des répertoires pour les addons personnalisés et les journaux Odoo.

Configuration de l'instance Odoo

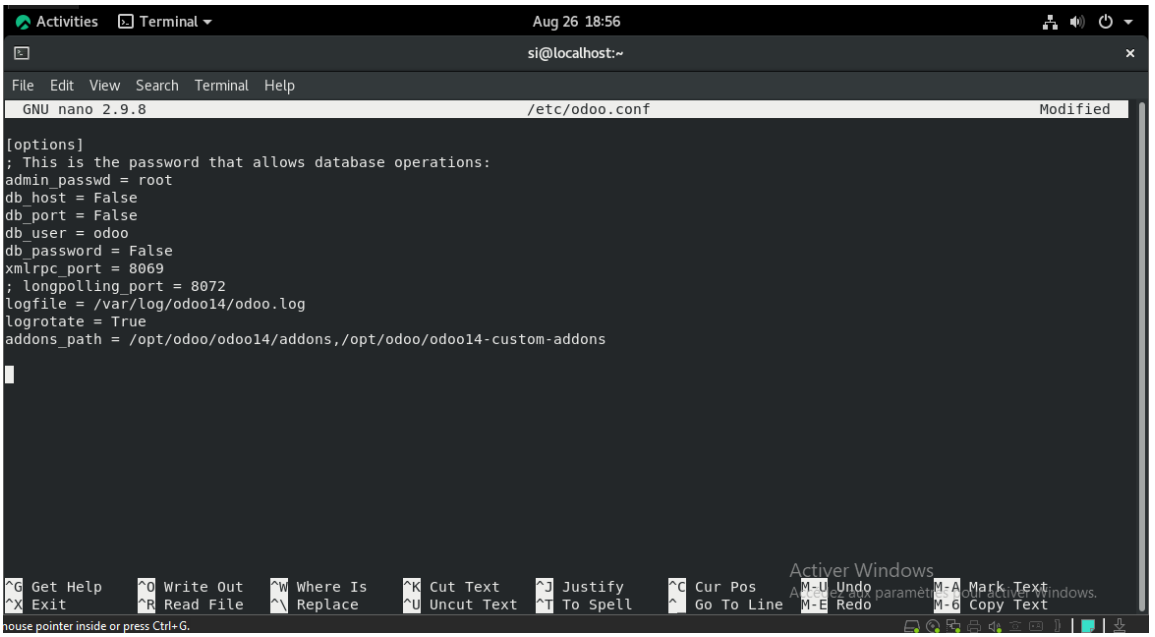


FIGURE 3.19 – Configuration de l'instance Odoo.

Activation d'Odoo

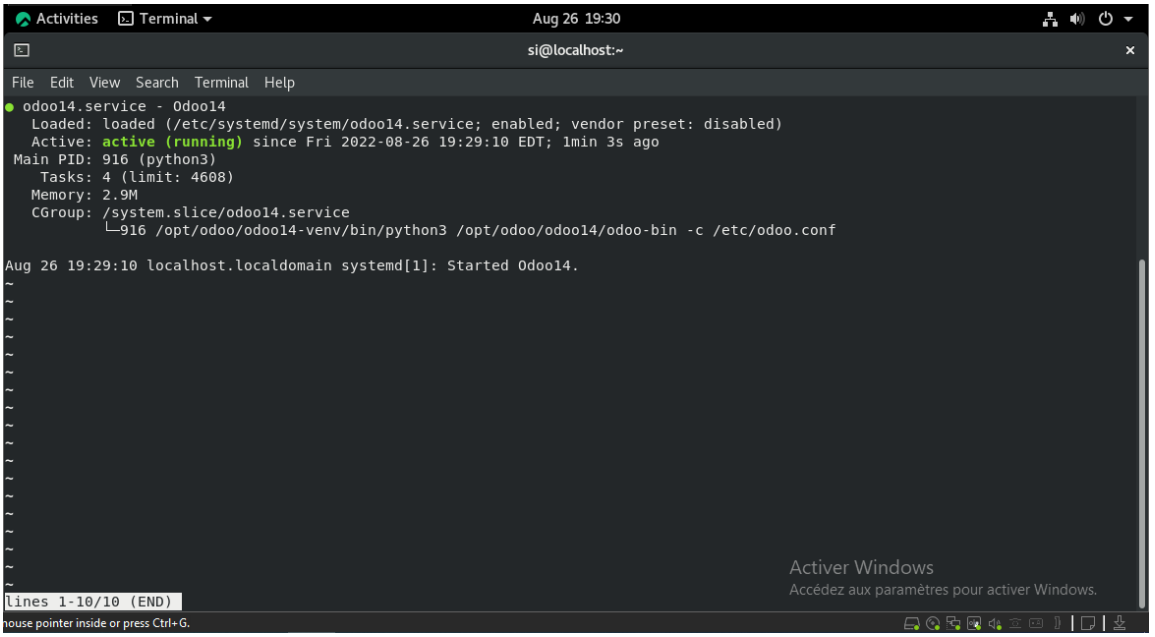


FIGURE 3.20 – Odoo active.

Interfaces Odoo

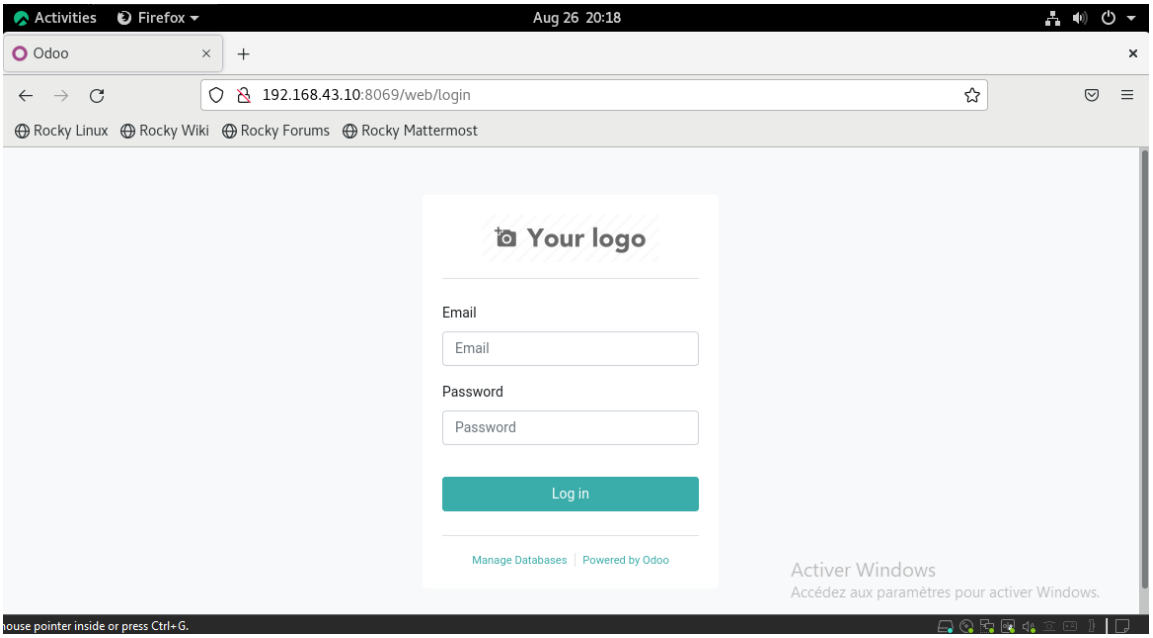


FIGURE 3.21 – a. Interface web Odoo14 (Page d'authentification).

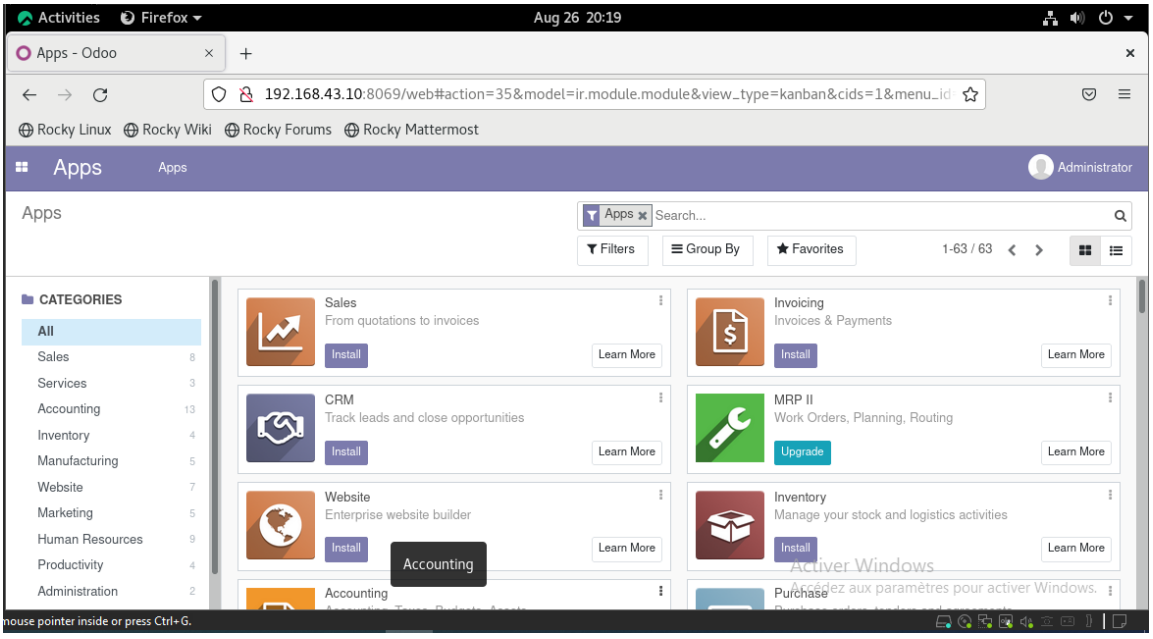


FIGURE 3.22 – b. Interface de connexion Odoo14.

3.2.4 Simulation de quelques processus métiers critiques

A la suite d'installation de Odoo14, passant maintenant à l'installation de quelques processus métiers, par exemple : CRM (Customer Relationship Management), Manufacturing et le processus Sales.

Dans l'environnement interne de Odoo14, on clique simplement sur **Install** du processus concerné :

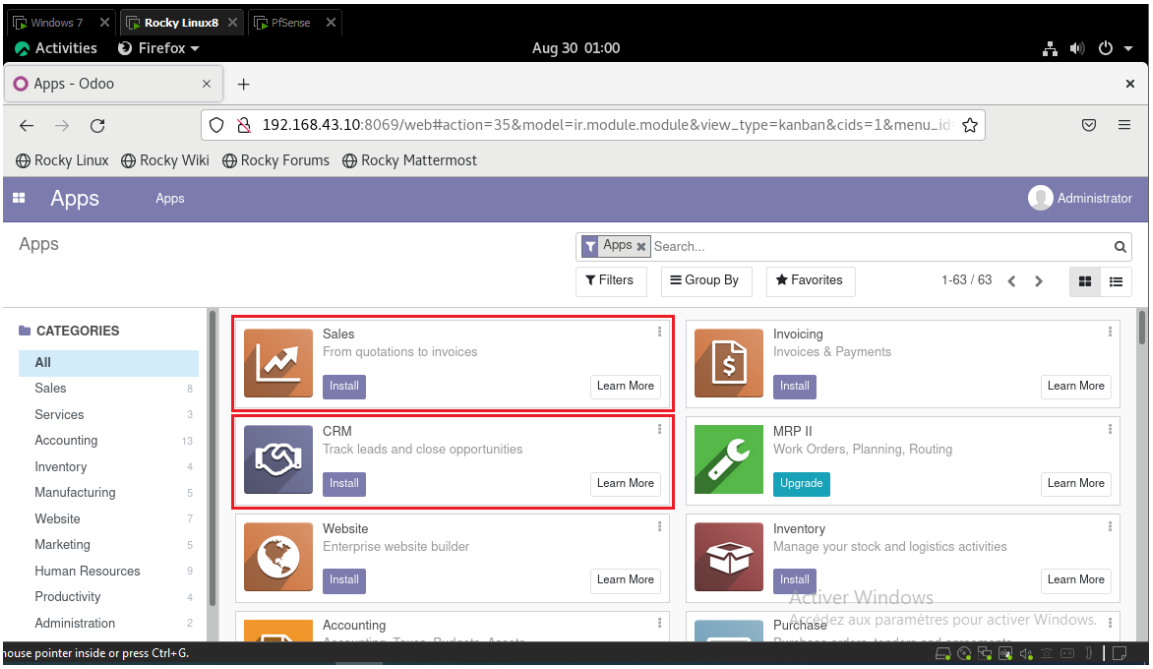


FIGURE 3.23 – Installation des processus CRM et Sales.

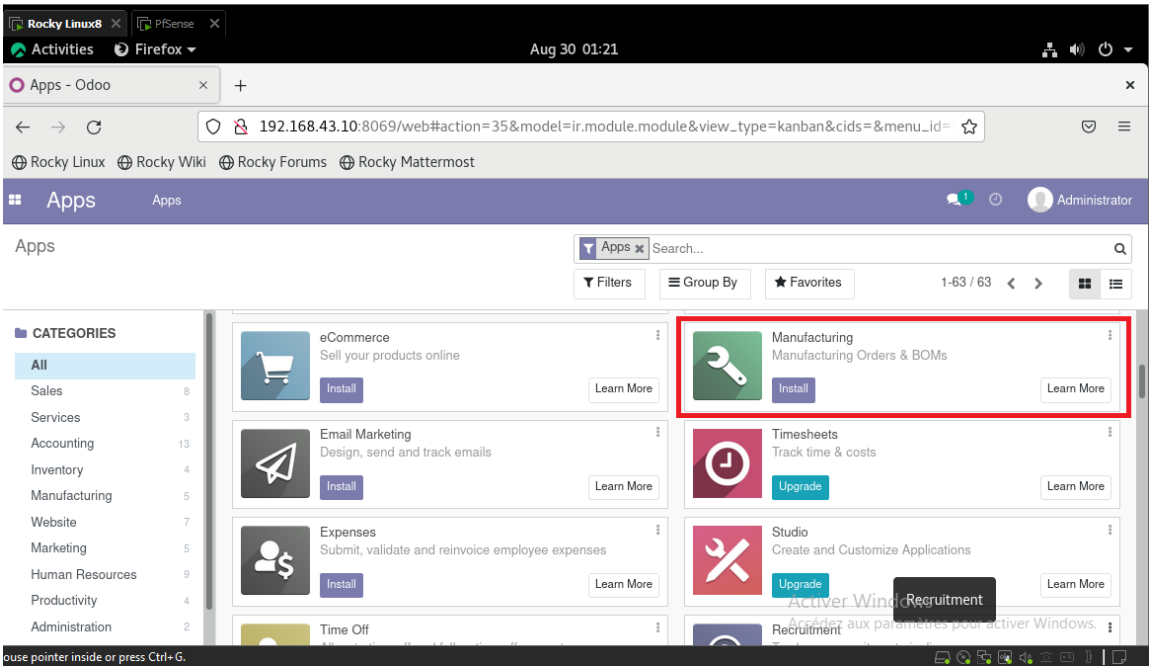


FIGURE 3.24 – Installation du processus Manufacturing.

Ce qui donne les résultats suivants :

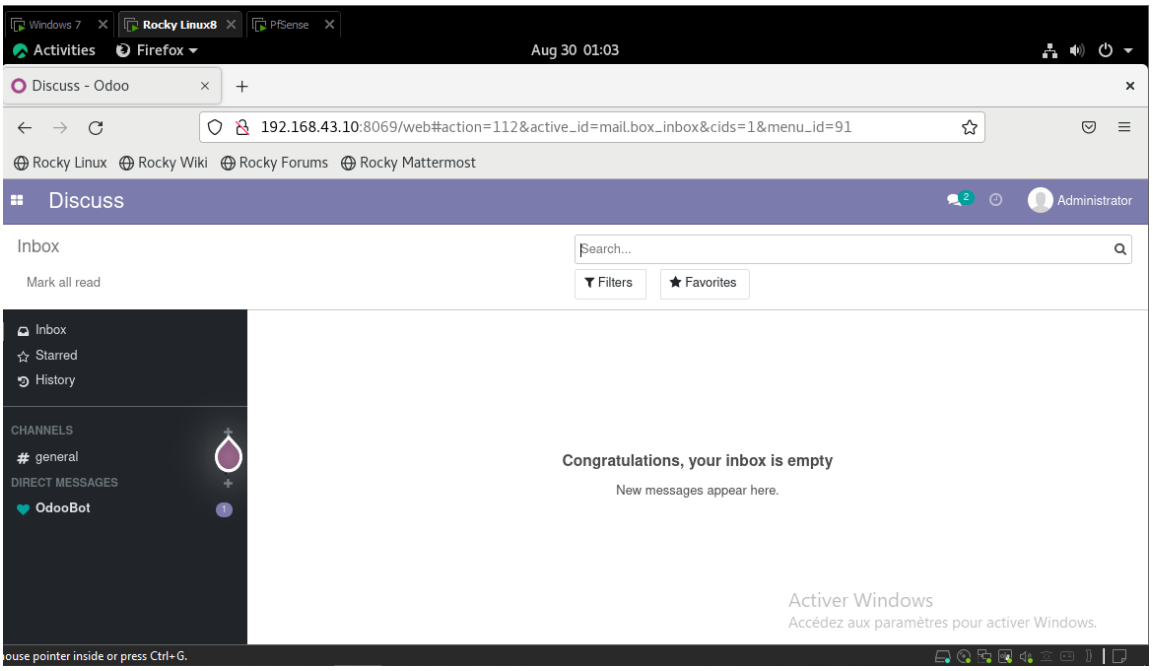


FIGURE 3.25 – Fenêtre de CRM.

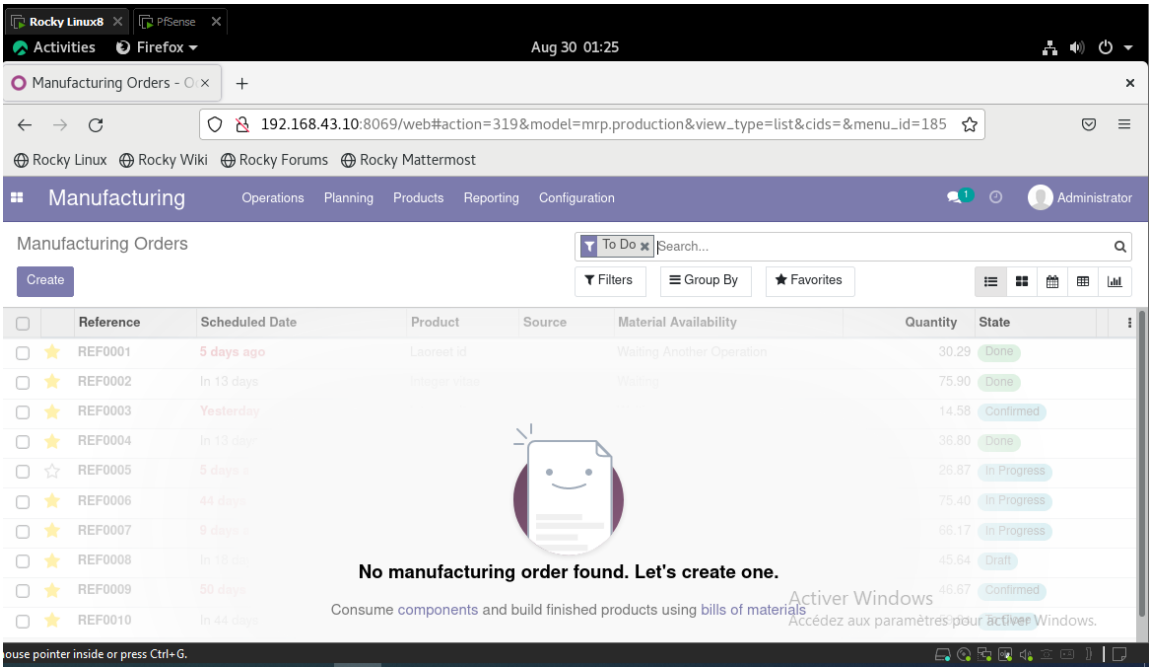


FIGURE 3.26 – Fenêtre de Manufacturing.

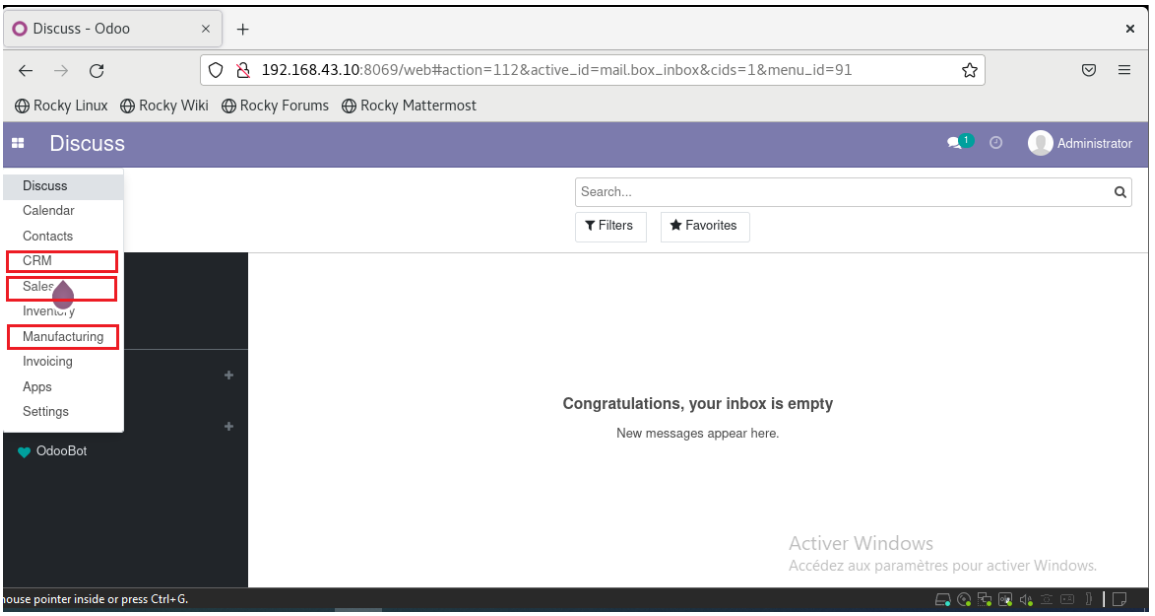


FIGURE 3.27 – Processus métiers installés.

3.3 Application des recommandations sur l'environnement virtuel

3.3.1 Création du Domaine Active Directory, Serveur de noms de domaine (DNS), les Services de Certificats Active Directory et le service Stratégie et d'accès réseau

Les captures qui suivent montrent la création du domaine Active Directory (AD) et le Serveur de noms de domaine (DNS) :

Dans **Gestionnaire de serveur** sur Windows Server 2016, on ajoute les fonctionnalités nécessaires en cliquant sur **Gérer** puis **Ajouter des rôles et des fonctionnalités**.

La même procédure pour les Services de Certificats Active Directory (Service de certificats Active Directory) et le Service Stratégie et d'Accès Réseau (Network Policy and Access Services)

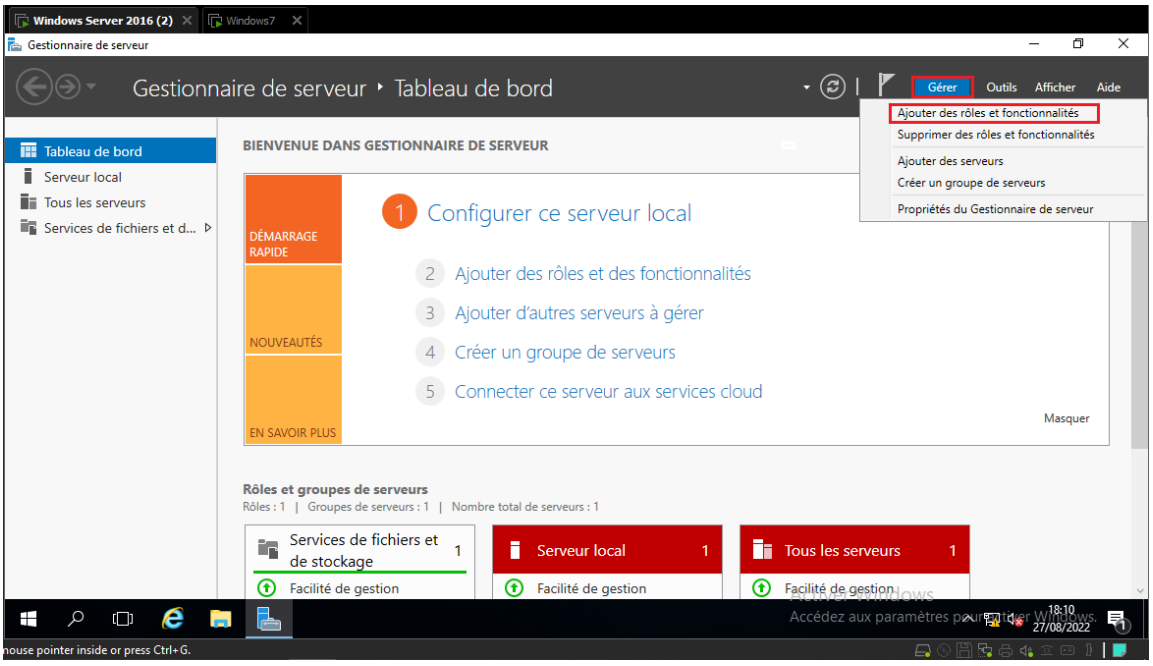


FIGURE 3.28 – Étape 1 Ajout des rôles et fonctionnalités

Suivant le processus et la sélection des deux services DNS et AD DS, comme montré dans la figure 4.2 :

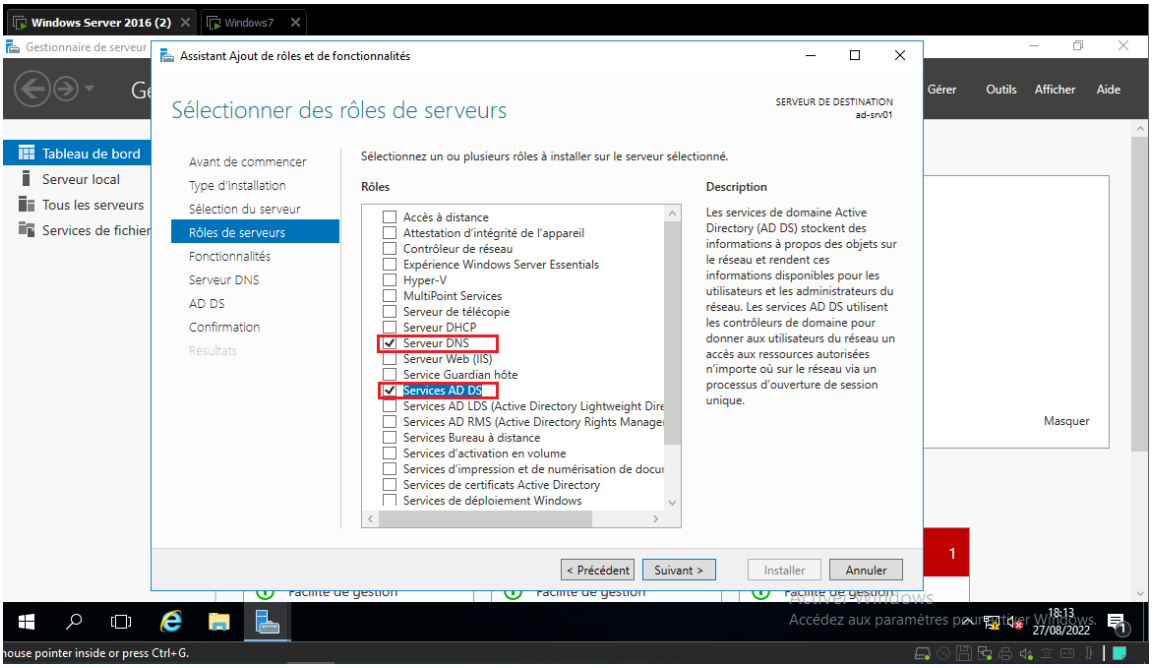


FIGURE 3.29 – Étape 2 Ajout des services DNS et AD DS

Puis les services s'installent :

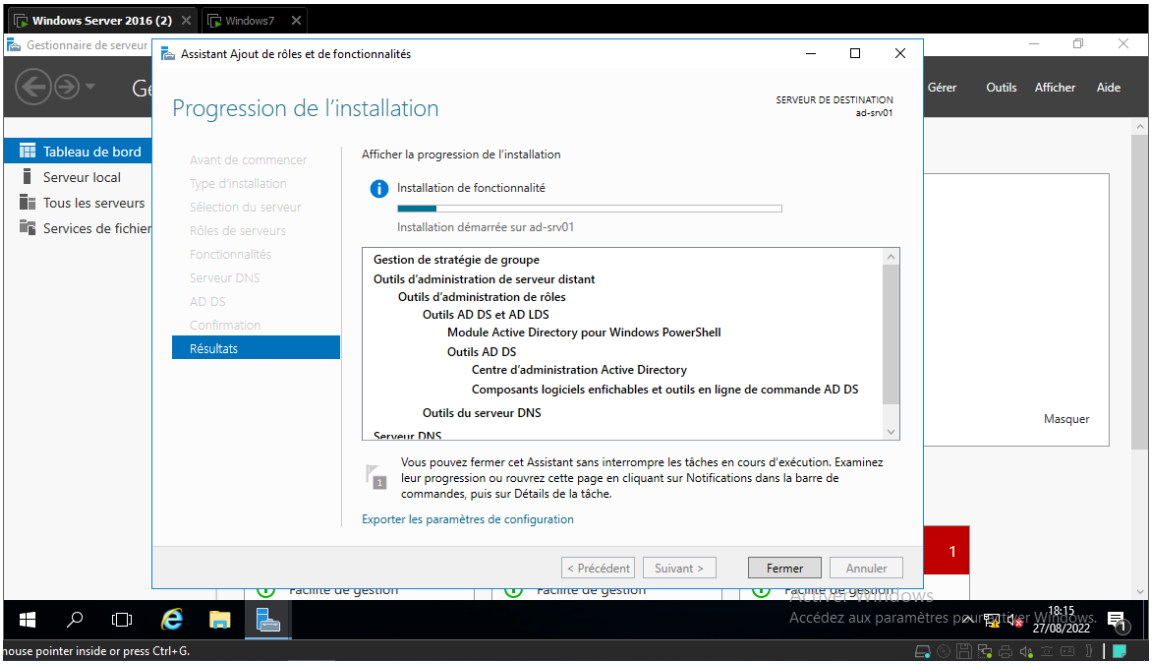


FIGURE 3.30 – Étape 3 Installation des fonctionnalités

Ensuite, pour promouvoir le serveur en contrôleur de domaine : dans **Notifications** on clique sur **Promouvoir le serveur en contrôleur de domaine**.

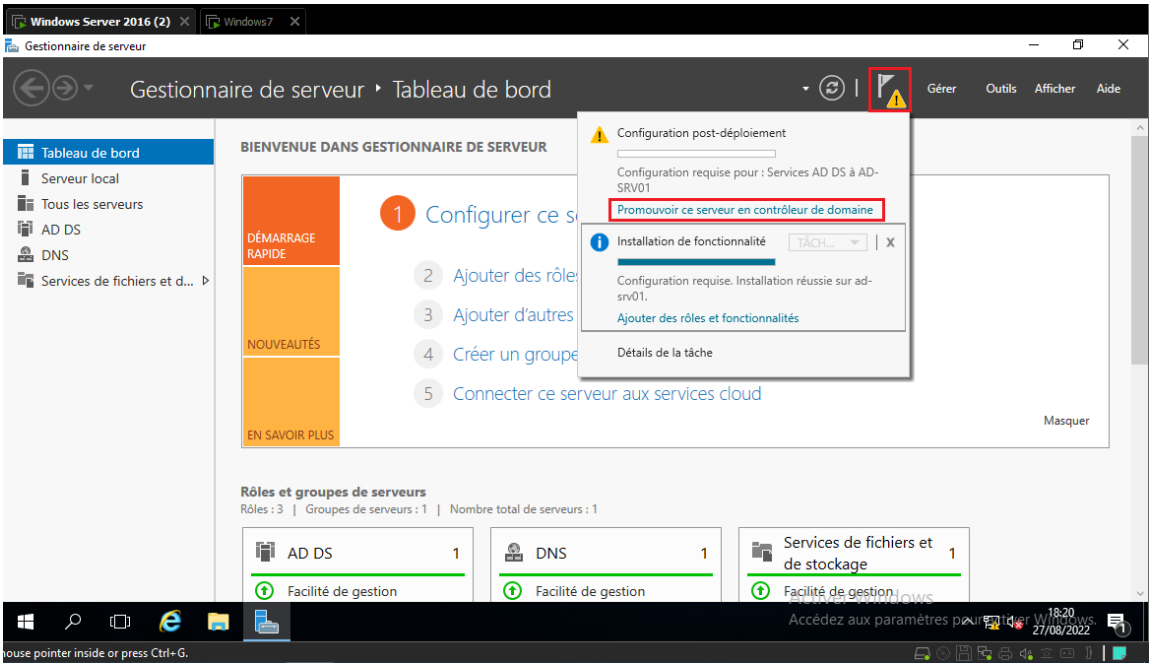


FIGURE 3.31 – Étape 4 Promouvoir ce serveur en contrôleur de domaine

On configure ensuite le nom et le mot de passe comme représenté dans les captures 4.5 et 4.6 :

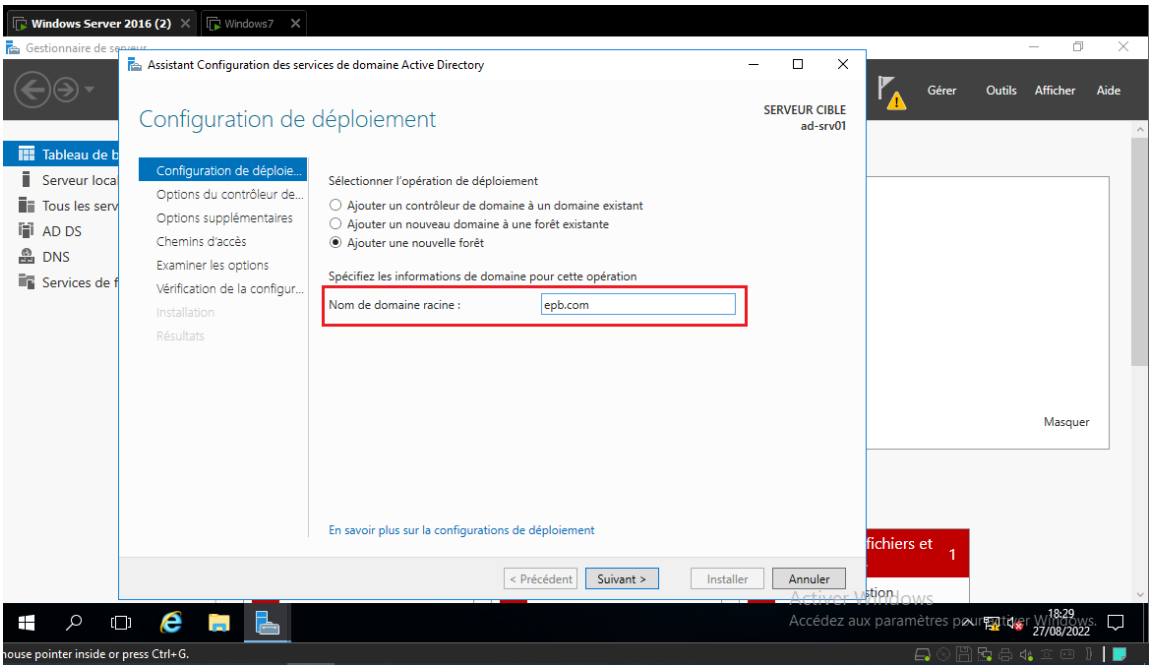


FIGURE 3.32 – Étape 5.1 Configuration du nom de domaine

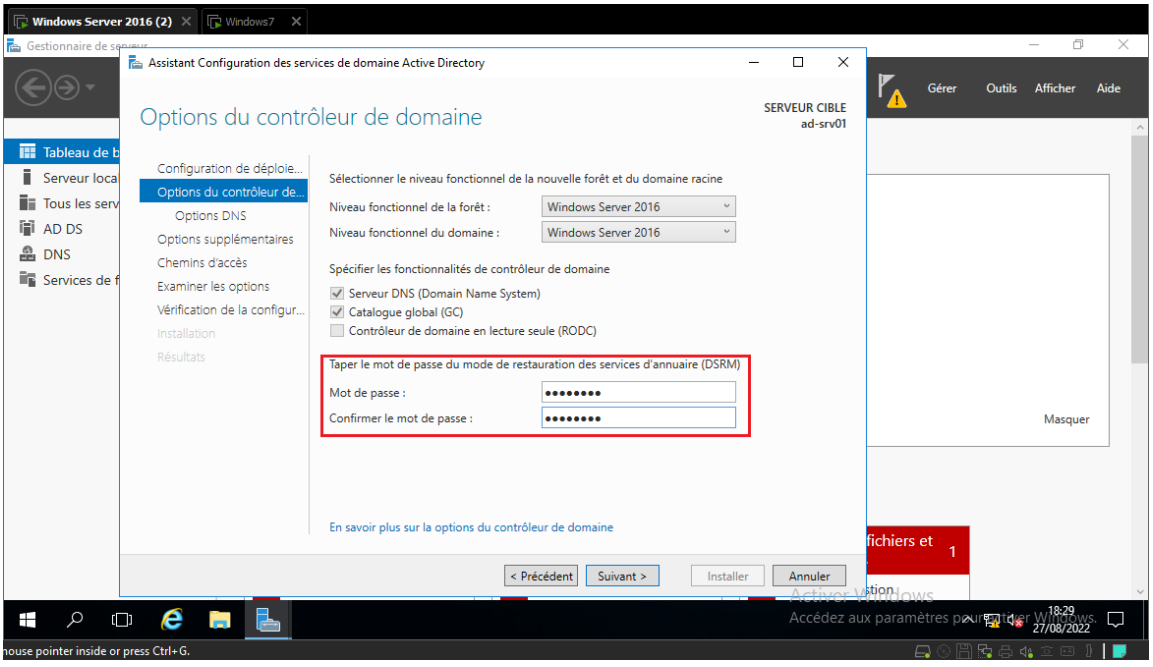


FIGURE 3.33 – Étape 5.2 Configuration du mot de passe

Ainsi, le domaine EPB.com est crée :

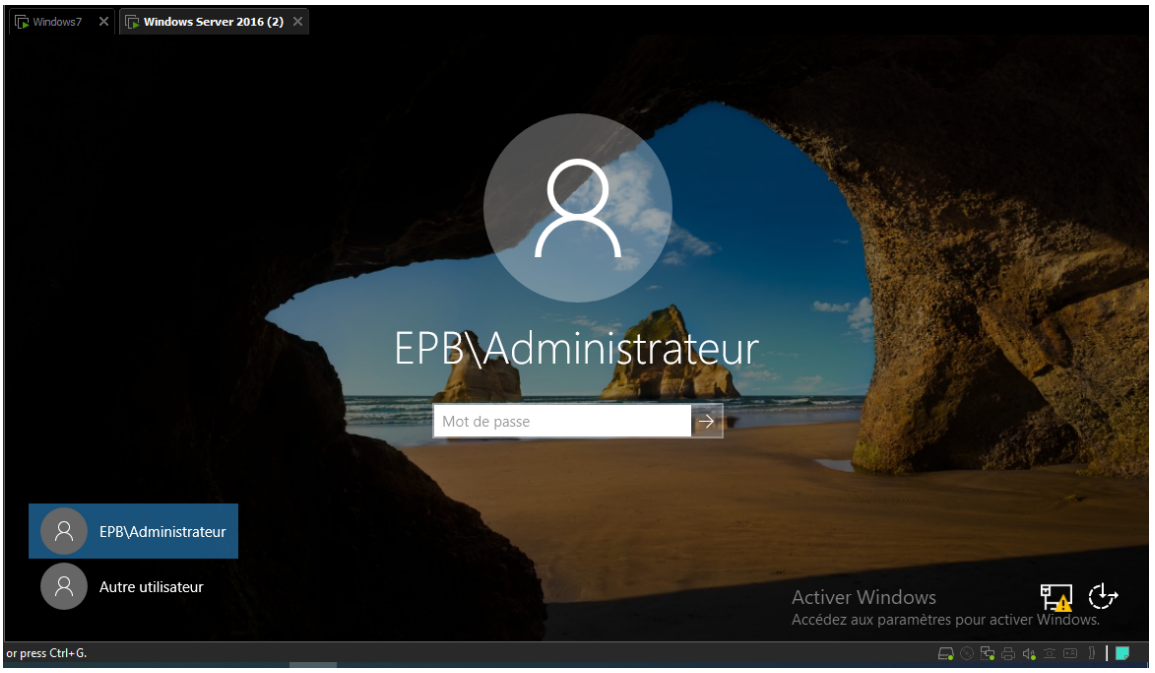
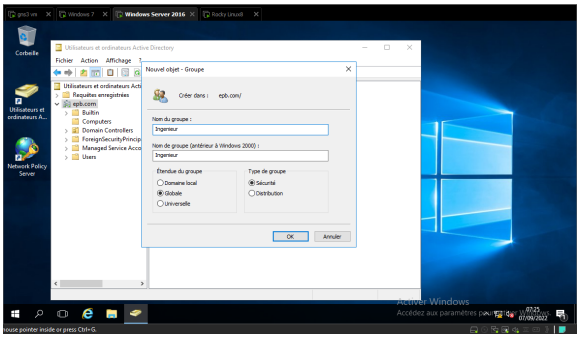


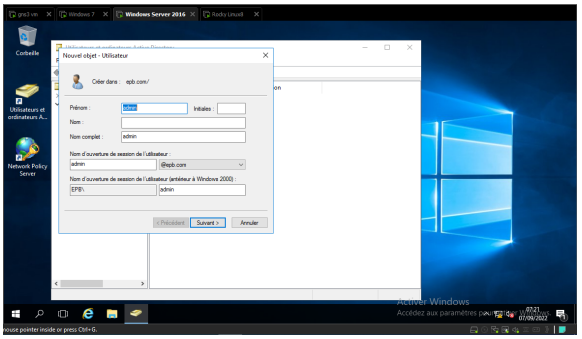
FIGURE 3.34 – Capture de la session Domaine Utilisateur

3.3.2 Création du groupe et utilisateur sur Active Directory

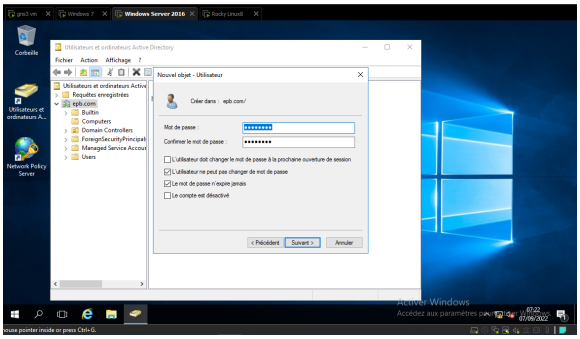
La mise en place du service radius nécessite la création des utilisateurs et un groupe d'utilisateurs sur l'annuaire AD afin de donner et contrôler l'accès aux ressources du réseau.



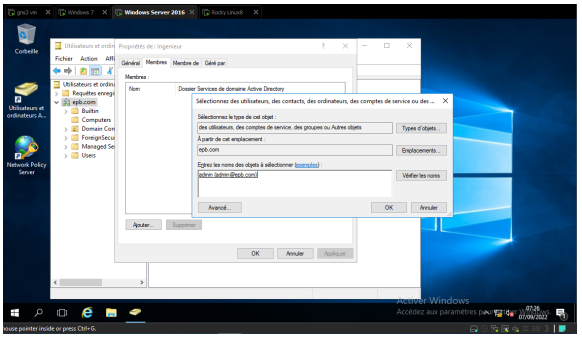
(a) Création d'un groupe



(b) Création d'un utilisateur



(a) Mot de passe de l'utilisateur



(b) Ajout de l'utilisateur au groupe

3.3.3 Configuration de 'NPS'

Les services de stratégie et d'accès réseau permettent de définir des stratégies d'accès réseau, d'authentification et d'autorisation à l'aide du serveur NPS (Network Policy Server)

On va donc déployer NPS comme un **Serveur RADIUS** (Remote Authentication Dial-In User Service) en l'inscrivant en premier lieu dans Active Directory :

Clic droit sur **NPS (local)** puis **Inscrire un serveur dans Active Directory**, ce qui nous permet d'accéder aux informations d'identifications et aux propriétés d'accès distant des comptes d'utilisateurs dans les services du domaine Active Directory.

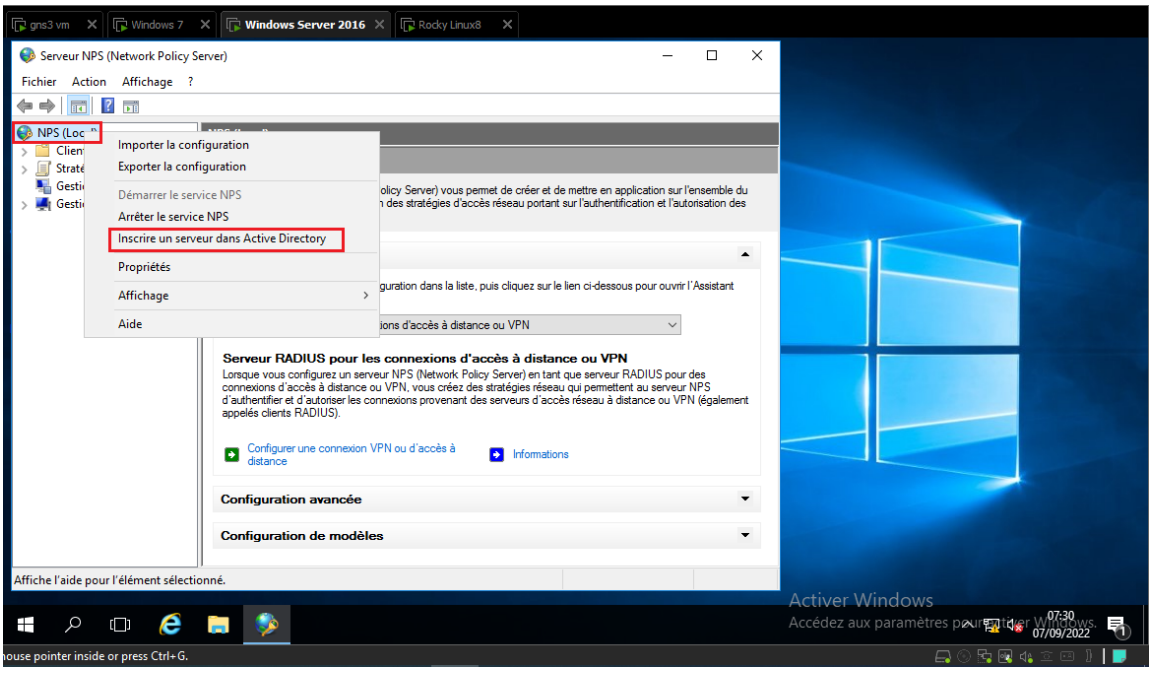


FIGURE 3.37 – Inscription du serveur NPS dans l'Active Directory

Configuration de 'NPS' en tant que Client Radius

Pour la configuration du client Radius qui est la machine autorisée à demander l'authentification auprès du serveur, voici les étapes :

Clic droit sur **Clients RADIUS** après **Nouveau client** et puis l'insertion des données comme le montre la figure ci-dessous :

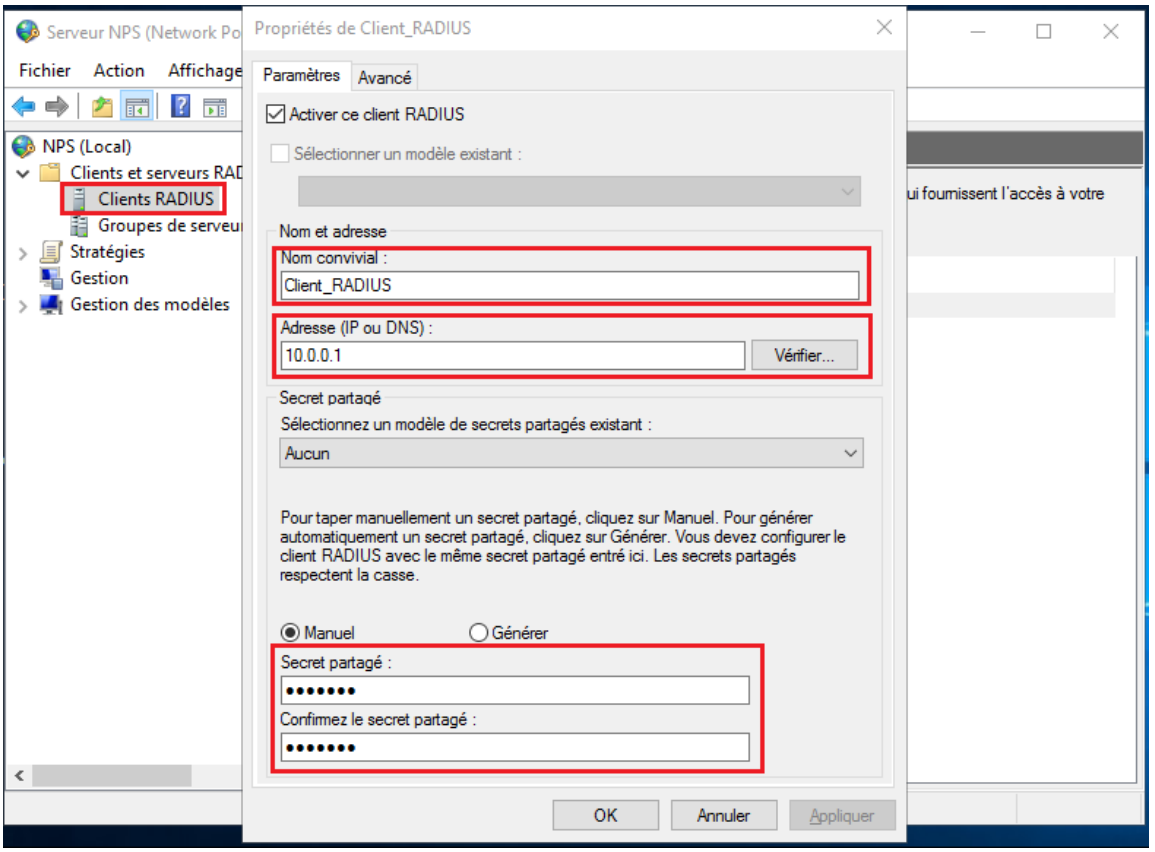
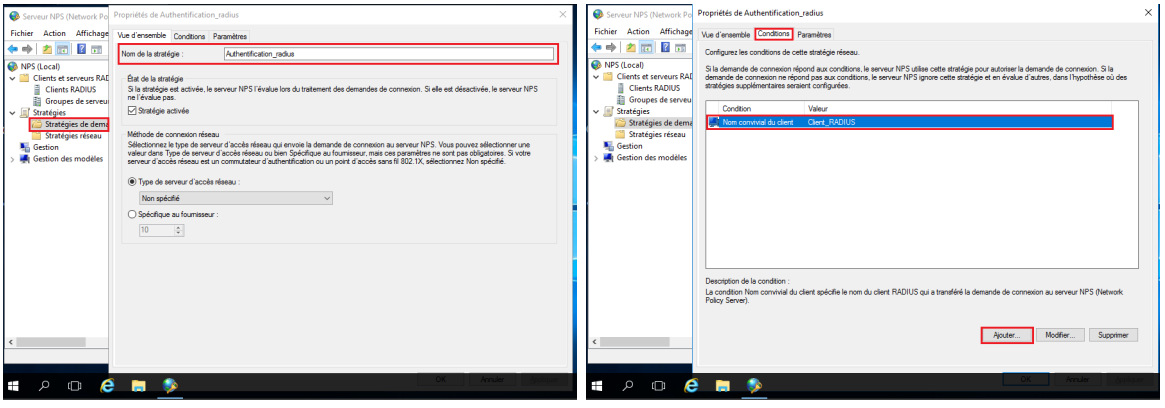


FIGURE 3.38 – création du client radius

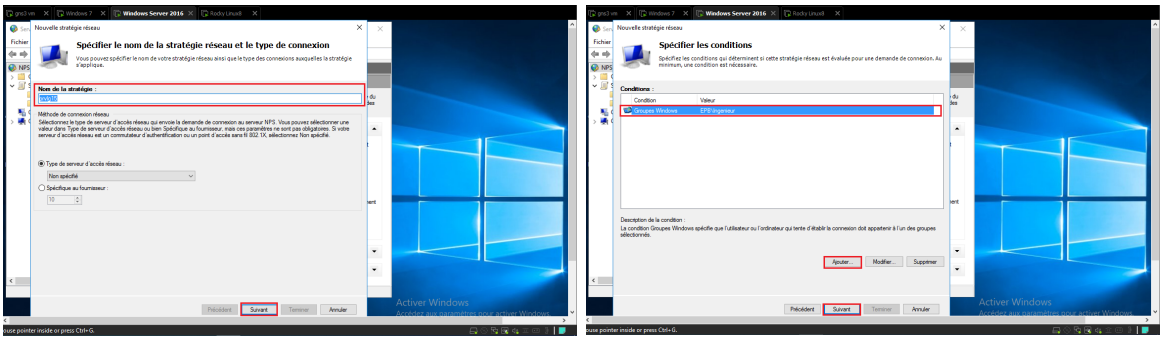
Création d'une nouvelle stratégie réseau pour l'authentificateur

Afin de déterminer si les requêtes de connexion des clients radius sont autorisés ou non, les stratégies réseau sont utilisées.

Nous allons créer ici une nouvelle stratégie pour authentifier les utilisateurs lors de la connexion à notre équipement 'Client_RADIUS' :



(a) Configuration de la demande de connexion (b) Avec spécifications des conditions



(a) Création de la connexion (b) Spécification des conditions de connexion

3.3.4 Configuration du Serveur Windows 2016

Consiste à l'attribution de l'adresse IP et DNS au serveur :

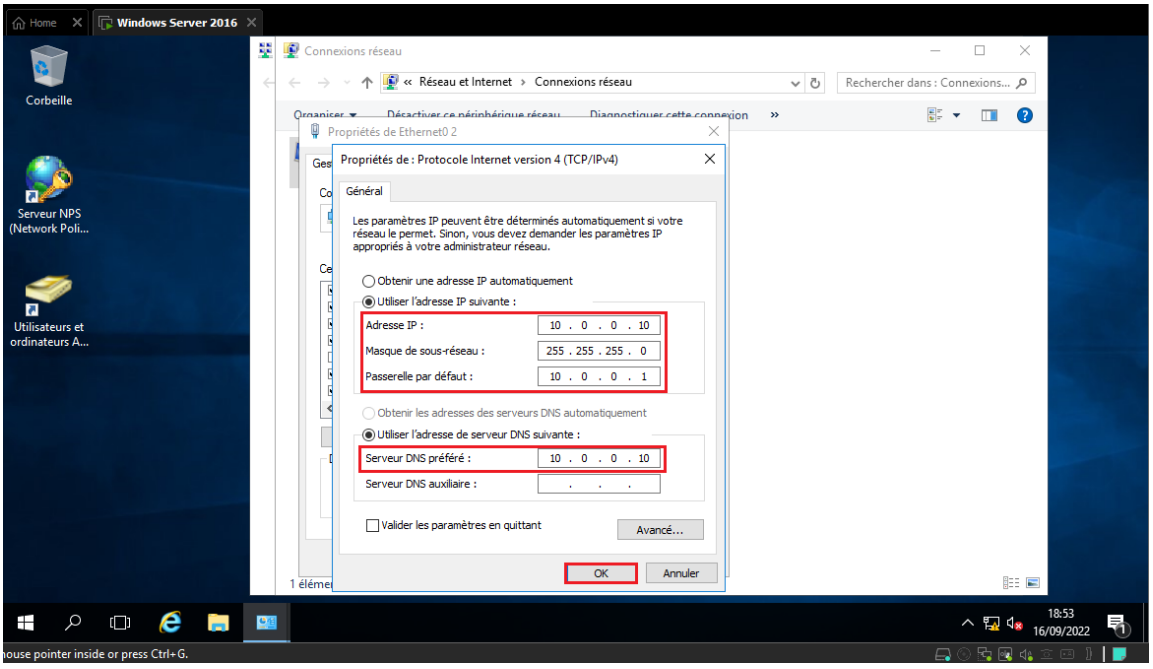


FIGURE 3.41 – Configuration du Serveur Windows 2016

3.3.5 Configuration du Client Windows 7

Ceci est une attribution de l'adresse IP à Windows 7 et l'ajout de l'adresse DNS qui est l'adresse du serveur :

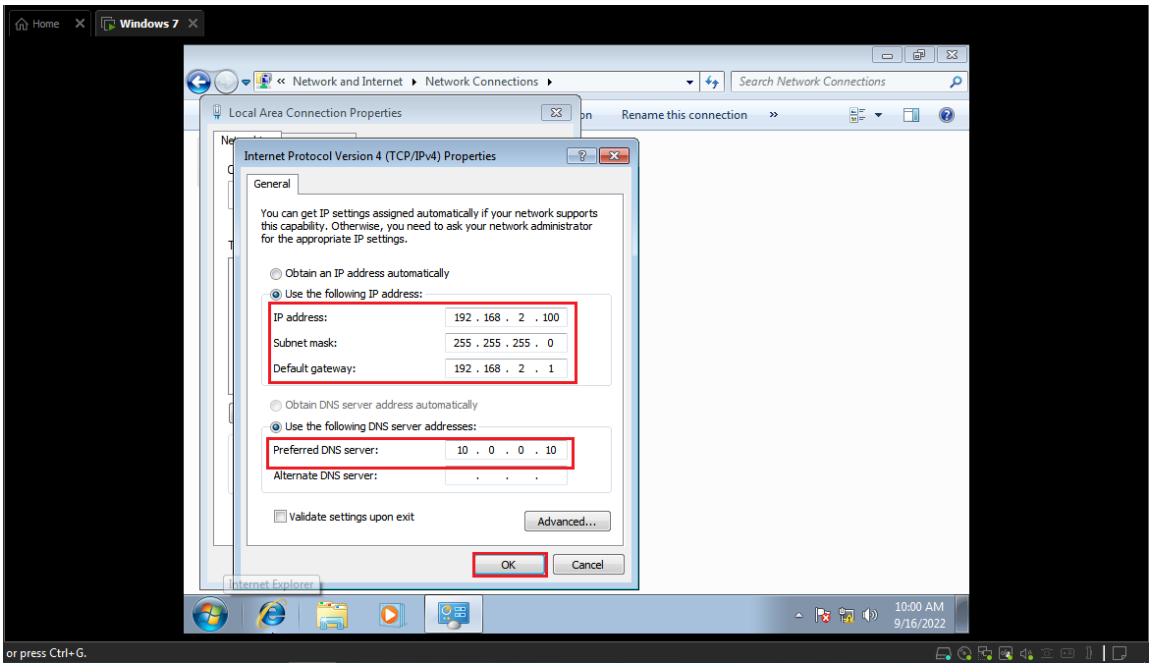


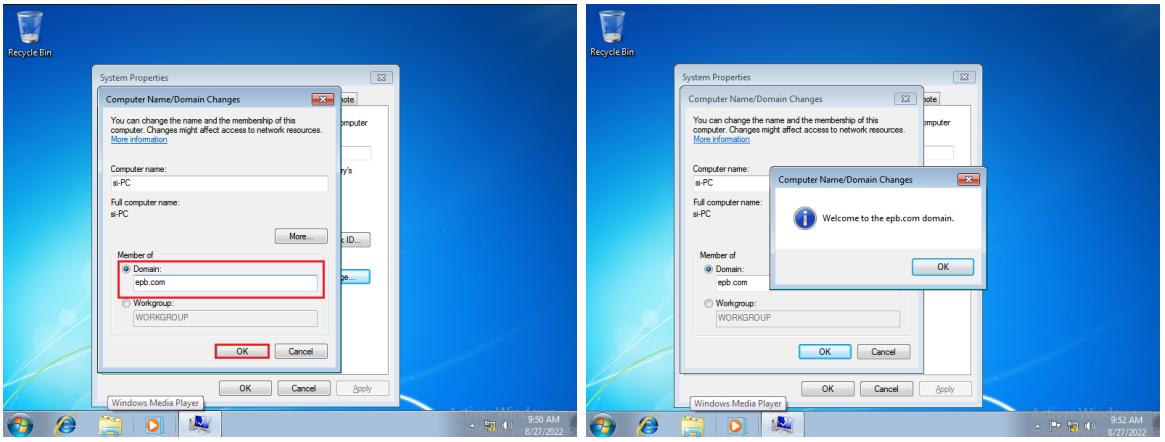
FIGURE 3.42 – Configuration Windows 7

Ajout de la machine au domaine AD

Maintenant pour faire joindre la machine virtuelle **Windows 7** au domaine EPB.COM, l'ajout de l'adresse DNS du serveur à la machine est obligatoire.

Dans la barre des recherches, on tape **Join Domain** ou **Joindre domaine** : coucher **Domain** puis le taper.

A la suite, saisir le nom et le mot de passe du compte à qui le droit et si tout est bien, une fenêtre de bienvenue s'affiche :



(a) Joindre le PC au domaine epb.com (b) Fenêtre de bienvenue

3.3.6 Architecture Réseau proposée

Dans le but de mettre en évidence les étapes nécessaires à l'installation de Radius, nous avons choisi ce réseau :

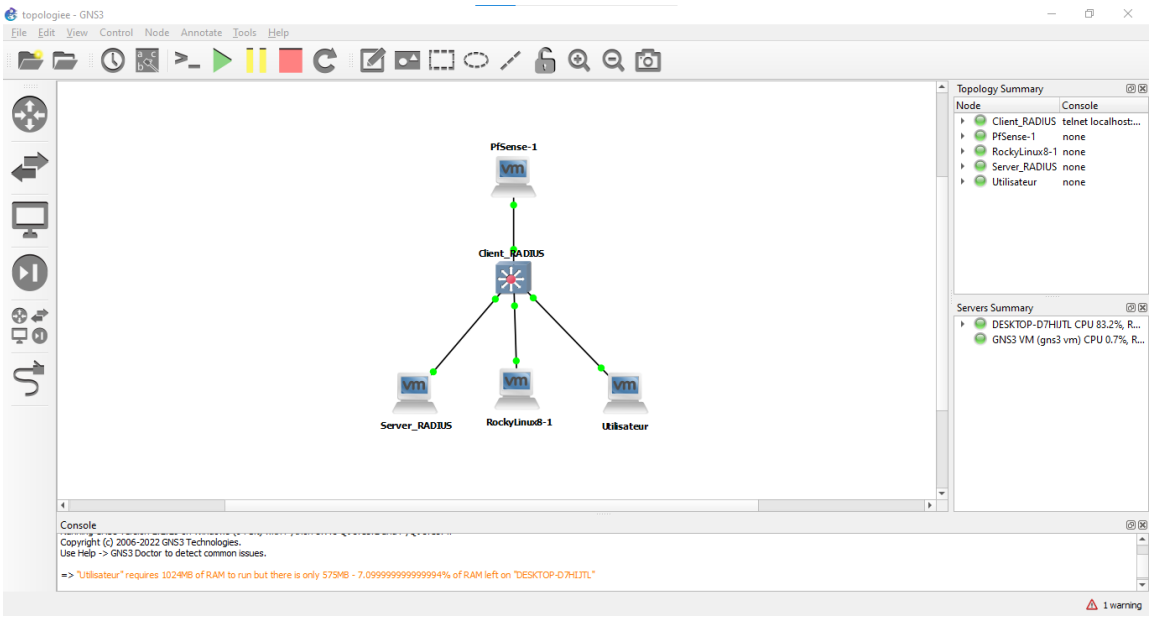


FIGURE 3.44 – Architecture réseau

3.3.7 Configuration du réseau

Configuration pfSense

Une configuration de base qui consiste à attribuer les adresses IP aux interfaces :

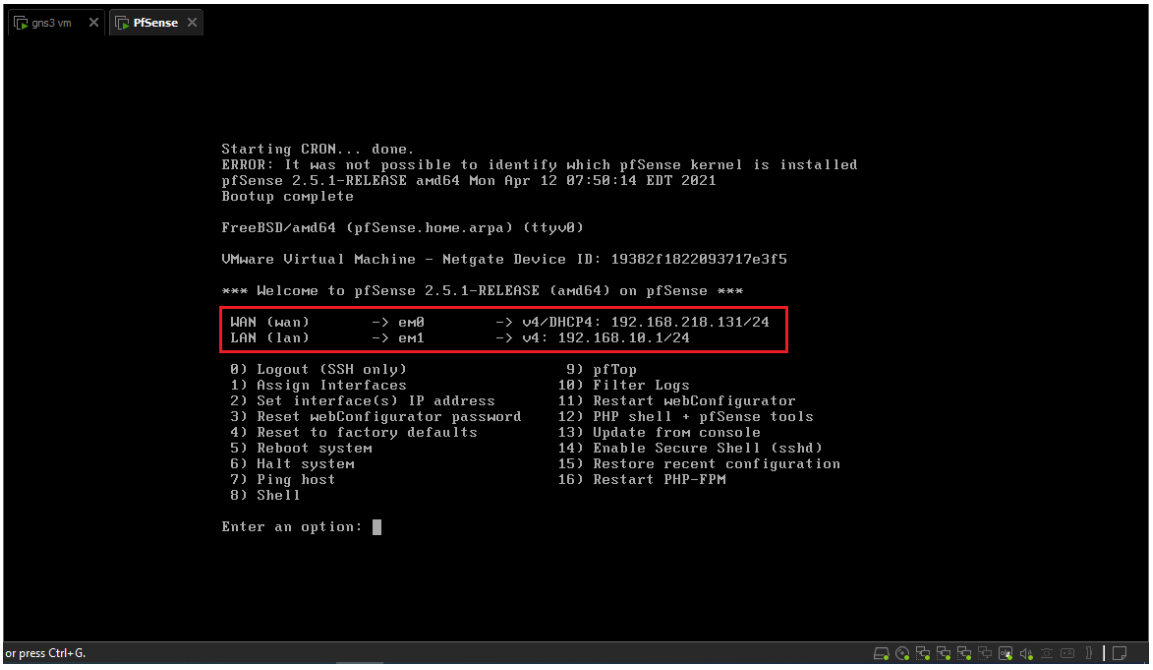


FIGURE 3.45 – Configuration pfSense

Configuration de l'équipement authentificateur

Les captures suivantes montrent :
— La configuration de base.
— Les tests de connexions.
— L'implémentation des règles d'authentification.
— L'activation du protocole SSH.

```
Client_RADIUS#SH IP INT BRIEF
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        10.0.0.1        YES NVRAM  up                    up
FastEthernet1/0        192.168.2.1     YES NVRAM  up                    up
FastEthernet2/0        unassigned      YES NVRAM  administratively down down
FastEthernet2/1        unassigned      YES NVRAM  administratively down down
Client_RADIUS#
Client_RADIUS#
Client_RADIUS#PING 192.168.2.100
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.100, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/13/24 ms
Client_RADIUS#PING 10.0.0.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/14/20 ms
Client_RADIUS#
```

FIGURE 3.46 – Configuration et Pings

Configuration de l'authentification sur Client_RADIUS

```
Client_RADIUS#CONF T
Enter configuration commands, one per line.  End with CNTL/Z.
Client_RADIUS(config)#aaa new-model
Client_RADIUS(config)#aaa authentication login default group radius local
Client_RADIUS(config)#aaa authorization exec default group radius local
Client_RADIUS(config)#aaa accounting exec default start-stop group radius
Client_RADIUS(config)#radius server NPS_Rad
Client_RADIUS(config-radius-server)#$0 auth-port 1812 acct-port 1813
Client_RADIUS(config-radius-server)#key Rad@123
Client_RADIUS(config-radius-server)#END
Client_RADIUS#
*Sep 15 17:26:24.431: %SYS-5-CONFIG_I: Configured from console by console
Client_RADIUS#test aaa group radius admin Hamza2020 legacy
Attempting authentication test to server-group radius using radius
User was successfully authenticated.

Client_RADIUS#
```


FIGURE 3.47 – Authentification Radius

```
ESW1(config)#hostname Client_RADIUS
Client_RADIUS(config)#ip domain-name EPB.com
Client_RADIUS(config)#crypto key generate rsa
The name for the keys will be: Client_RADIUS.EPB.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

Client_RADIUS(config)#
*Mar  1 00:19:01.591: %SSH-5-ENABLED: SSH 1.99 has been enabled
Client_RADIUS(config)#ip ssh version 2
Client_RADIUS(config)#ip ssh logging events
Client_RADIUS(config)#ip ssh time-out 60
Client_RADIUS(config)#ip ssh authentication-retries 3
Client_RADIUS(config)#service password-encryption
```

FIGURE 3.48 – Activation du protocole SSH

3.4 Analyse comparative des résultats obtenus et de l'état des lieux initial

Revenant à l'émulation réalisée dans la 1ère partie :
De Windows 7 vers Rocky ou de Rocky vers Serveur, la connexion n'est pas protégée vu l'utilisation d'un switch ordinaire sans défense qui peut générer des risques d'attaques interne comme le ARP Spoofing ou le DHCP Spoofing.

En revanche, dans la solution proposée :
On conseil un Switch niveau 3 avec la configuration d'un VLAN d'une part et l'impélementation du protocole radius de l'autre afin :

— d'éviter d'avoir un réseau encombré, et des périphériques plus lents et de garantir des performances optimales vu que les VLANs séparent logiquement des départements ou des directions sans pour autant qu'ils soient séparés physiquement.

— un autre avantage lié essentiellement à la sécurité par l'impélementation d'un protocole de contrôle d'accès via le Serveur Radius.
Le Serveur d'authentification Radius non seulement constitue une solution pour des connexions plus sécurisées et des données protégées, il présente aussi l'avantage d'être simple à installer.

3.5 Conclusion

A la fin de ce chapitre, nous avons émulé un réseau de l'état des lieux de l'entreprise avec l'installation d'un progiciel de gestion intégré Odoo14. Ensuite, nous avons passé à l'émulation du réseau proposé avec l'application d'une solution de sécurité suivi d'une analyse comparative des résultats obtenus et de l'état des lieux initial.

Chapitre 4

Évaluation de la solution et tests fonctionnels

4.1 Introduction

Ce dernier chapitre dédié à exposer les différents tests et manipulations appliqués entre les machines du réseau.

Ainsi, nous présentons tout d'abord un test de connexion de Windows 7 vers le client radius capturée par Wireshark et on termine avec une connexion à distance de Windows 7 à Odoo14 sous Rocky Linux 8.

4.2 Les différents tests unitaires et fonctionnels

4.2.1 Wireshark

On utilise Wireshark pour capturer et analyser le trafic réseau, pour l'ouvrir il suffit un clic droit sur les bulles vertes des interfaces sous GNS3, puis sur **Start Wireshark** .
Cela nous permet de suivre et d'analyser les paquets échangés entre le client Radius et le serveur Radius.
La fenêtre qui s'ouvre nous affiche les différents paquets circulant entre ces deux noeuds (protocoles CDP, Loop,...etc), on peut trier les paquets Radius en insérant **Radius** dans la barre de filtrage :

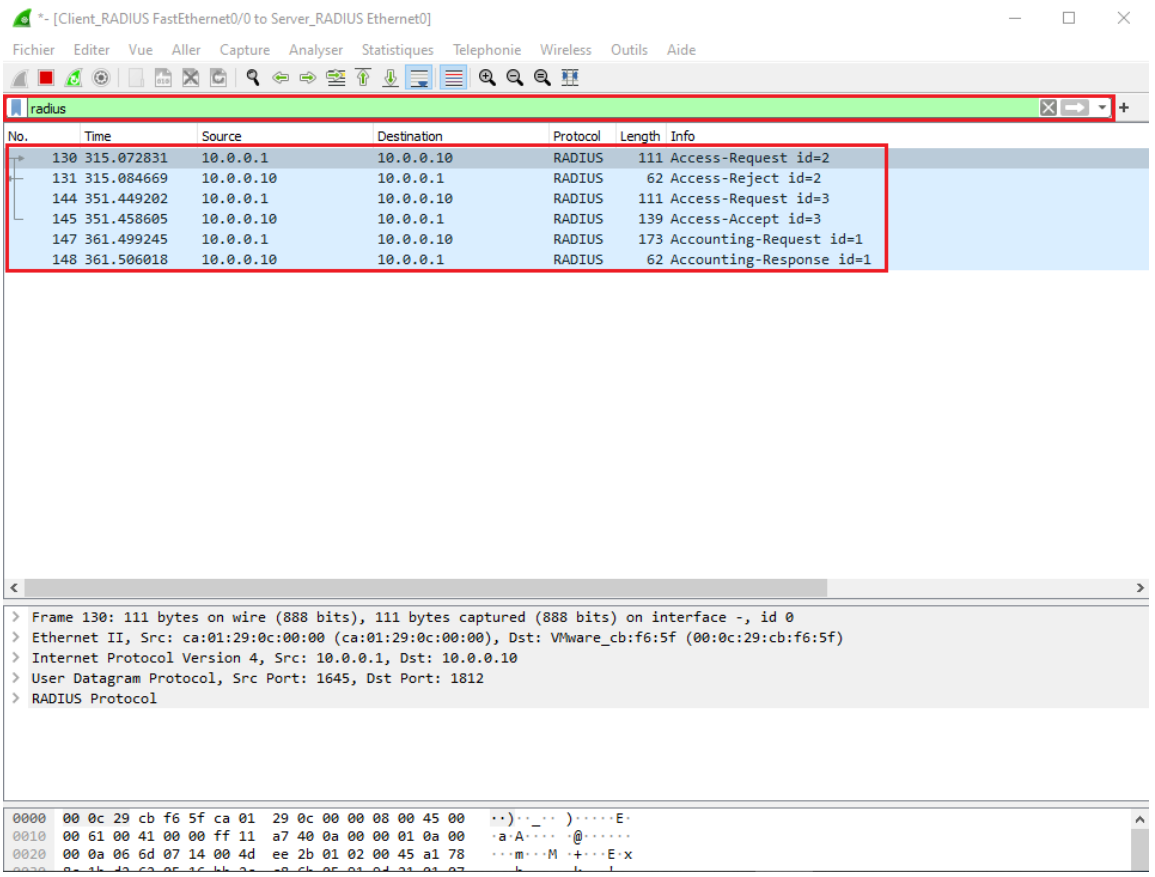


FIGURE 4.1 – Analyse du trafic entre Client Radius et Serveur Radius

4.2.2 Authentification d'un utilisateur au serveur radius

Au niveau du serveur Radius on vérifie la traçabilité de l'utilisateur, C'est à dire, vérifier les informations des utilisateurs qui sont connectés et authentifiés par le serveur, en utilisant **l'observateur d'évènements** (ou **Event viewer**) et en cliquant sur **rôles de serveurs** (**Server Roles**) et puis sur **services de stratégie et d'accès réseau** (**Network Policy and Access Services**) :
On obtient plusieurs informations concernant l'utilisateur connecté comme la date, l'heure, le nom d'utilisateur, le nom du domaine,...etc.

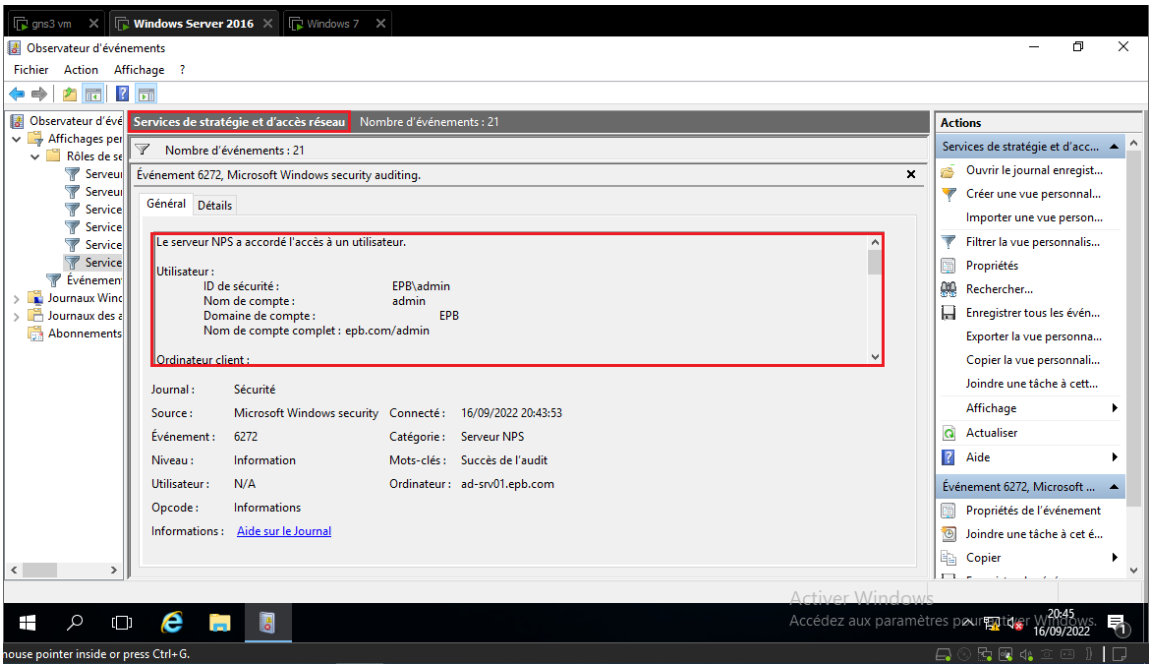


FIGURE 4.2 – Traçabilité de l'utilisateur connecté au serveur Radius

4.2.3 Test de connexion à partir de la machine Utilisateur avec PuTTy au serveur d'accès

L'utilisateur sous Windows 7 utilise le logiciel **PuTTy** en SSH pour accéder à son équipement réseau désiré.

PuTTy est un émulateur de terminal pour Windows permettant la connexion à une machine distante par protocole SSH ou Telnet, et permet en particulier d'ouvrir un Shell à distance sur le client d'accès.

On introduit l'adresse IP du client Radius et on choisit le type de connexion puis on clique sur **Open** (ou **Ouvrir**) comme le montre la figure suivante :

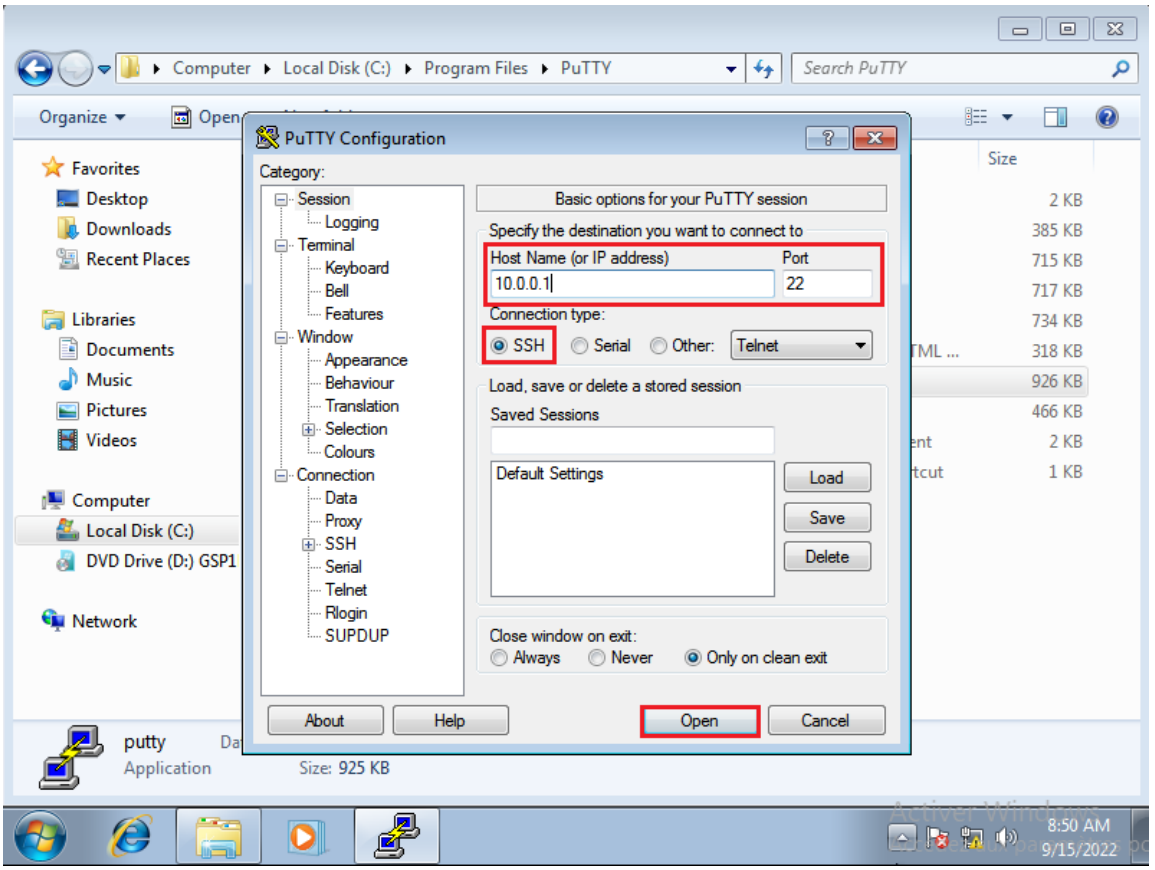


FIGURE 4.3 – L'accès au client Radius à distance avec SSH

Maintenant on introduit le nom d'utilisateur et le mot de passe pour y accéder au client Radius. Radius permet la gestion des connexions d'utilisateurs à des services distants, il permet qu'aux utilisateurs authentifiés d'accéder à ces services :

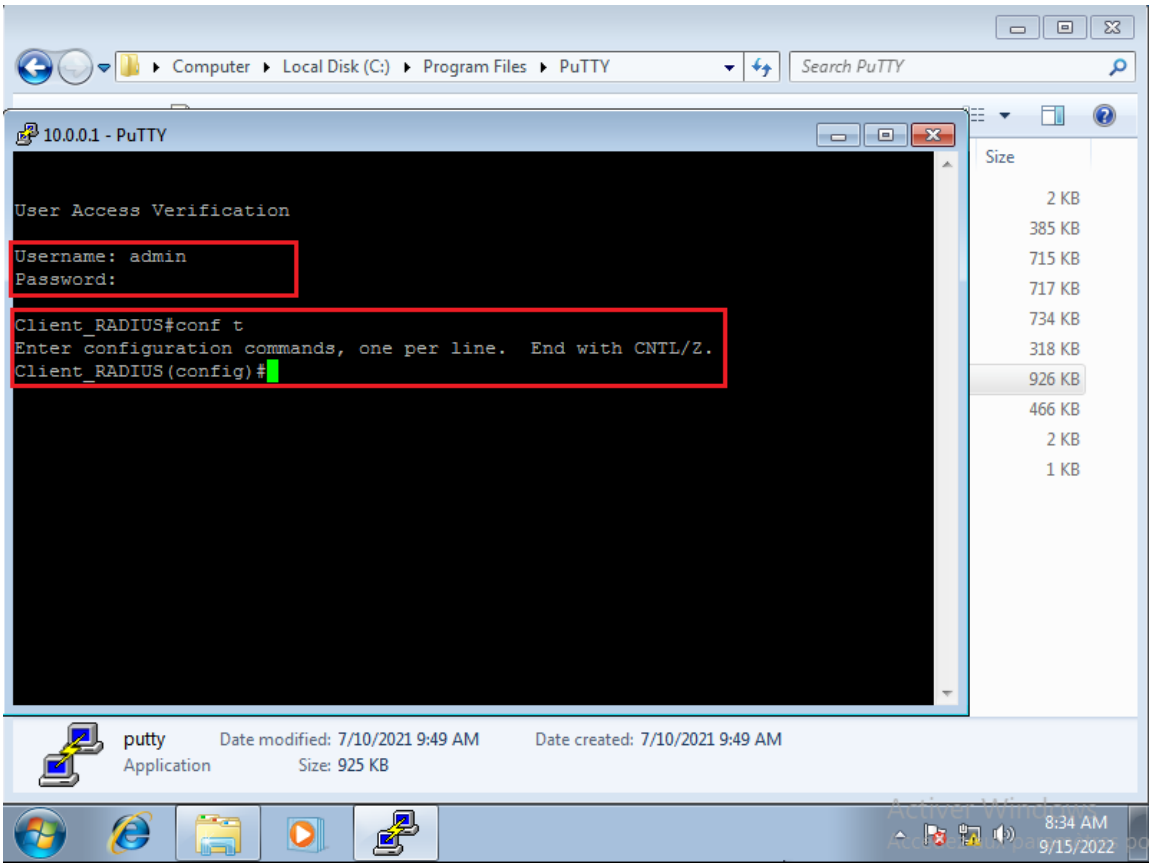


FIGURE 4.4 – L'accès à l'authentificateur avec nom d'utilisateur et mot de passe

4.2.4 Accès à l'équipement authentificateur après configuration radius et ajout d'une interface

Après avoir configurer Radius, on test l'accès sur l'équipement lui même et on rajoute les interfaces qui manquaient :

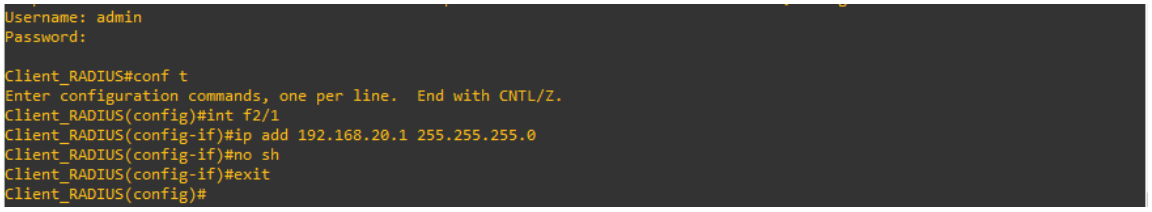


FIGURE 4.5 – Ajout d'une interface après la configuration radius

4.2.5 Connexion à distance de Windows 7 à Odoo14 sous Rocky Linux 8

Comme dernier test, on essaye de se connecter à distance de Windows 7 au progiciel Odoo14 installé auparavant dans Rocky Linux 8.

Alors pour cela, dans windows 7 on ouvre le navigateur Firefox et on tape l'adresse IP de la machine destinatrice suivi du numéro de port Odoo qui est par défaut : **8069**.

Si y a un échec de connexion, vérifier les pare-feux de vos machines qu'ils sont bien désactivés.

Le résultat de la connexion est montré dans la figure 4.5 :

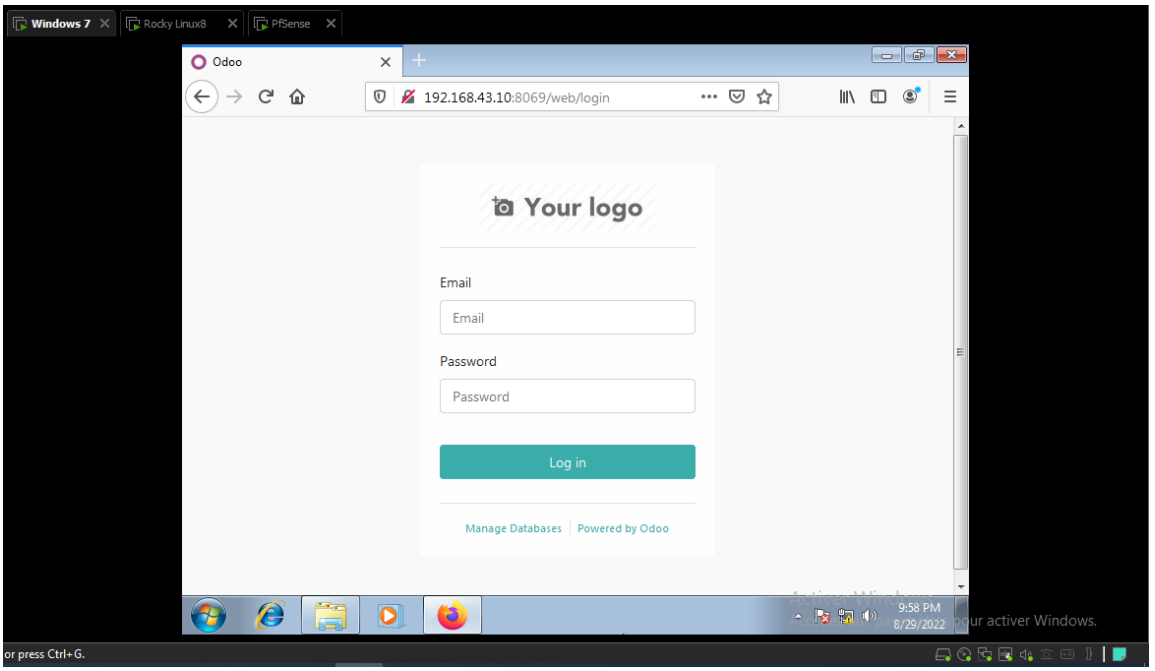


FIGURE 4.6 – Connexion à distance de Windows 7 à Odoo dans Rocky Linux 8

On saisit les coordonnées et on se connecte, pour ensuite accéder aux processus métiers.

Accès réussi :

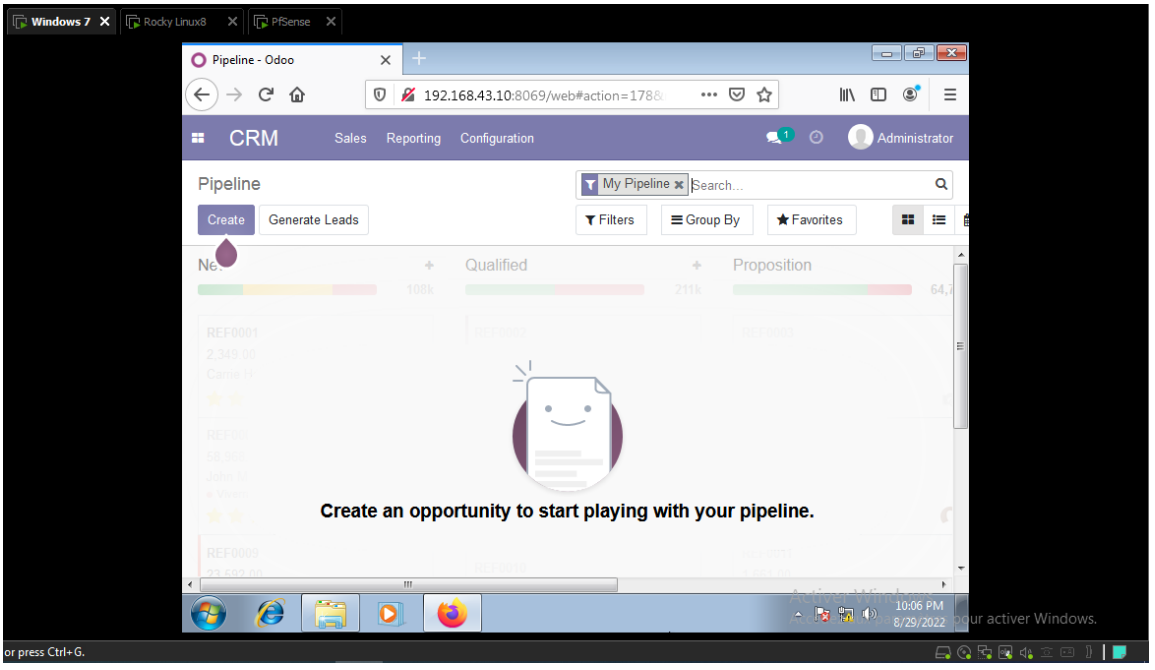


FIGURE 4.7 – Connexion à distance de Windows 7 au CRM de Odoo14 sous Rocky Linux

4.3 Conclusion

A travers ce chapitre, nous avons pu réaliser quelques manipulations sur les différentes machines indiquant ainsi une connexion sécurisé par la présence du serveur RADIUS et le protocole SSH.

Au final on termine par une conclusion générale.

CONCLUSION GÉNÉRALE

Ce travail est réalisé dans le cadre du projet de fin d'étude pour l'obtention d'un diplôme Master professionnel en Administration et Sécurité des Réseaux (ASR), nos efforts se sont concentrés sur un contrôle de sécurité d'un système d'informations pour le référentiel ISO/IEC 27000.

Dans une mission d'audit, l'objectif n'est pas de faire discréditer l'entreprise ou de les obliger à appliquer les solutions proposées ni de changer son système. Au contraire, son rôle est de protéger et détecter toutes failles ou vulnérabilités qui peuvent nuire à sa structure.

Ce rôle s'éclaircit, durant notre stage, suite à l'exécution d'une mission d'audit au sein de l'Entreprise Portuaire de Béjaia (EPB) en interviewant le personnel de la Direction Digitalisation et Numérique ainsi que la responsable de la Direction des Ressources Humaines suivant un plan d'audit et un questionnaire d'analyse. Cela afin d'évaluer et de faire des recommandations aux faiblesses détectées dans un rapport détaillé remis à l'encadrant de stage et rédigé ici sous forme d'un mémoire de fin d'étude.

Suite à cela, nous avons remarqué qu'un audit pour les dirigeants des entreprises est loin d'être appliqué non seulement en raison des coûts qu'engendre mais aussi l'audit est souvent mal jugé avec l'idée de révéler ce qui ne va pas bien.

Par conséquent, l'analyse faite à détecter quelques déviations qui peuvent facilement être contrôlées par l'entreprise qui gère quand même à un niveau acceptable la sécurité de son système informatique.

Pour conclure, l'apport de la conformité aux normes de sécurité informatique a pour objet de fournir des documents de références comportant des solutions à des problèmes autant liés à des éléments techniques qu'humains qui exposent un système d'informations aux risques accidentels et intentionnels.

Ainsi, la mise en œuvre d'un système de contrôle interne fiable et maîtrisé, qui comprend un groupe d'auditeurs formés et spécialisés peut être une solution efficace pour le management des risques et le suivie de leurs évolutions.

Dans l'avenir, on espère que cette étude sera un bénéfice pour le chercheur qui s'intéresse aux audits de sécurité informatique et pourra lui servir comme référence dans la réalisation de ses recherches et d'autre part que l'effet de la technologie à son tour va renforcer le champ d'action de ce domaine et lui ouvrir de nouvelles perspectives.

ANNEXES

Annexe A. Liste de risques possibles

ID	Risques
R01	Indisponibilité/ altération ou divulgation des éléments immatériels (logiciels, données,...) a. Accident provoqué par erreur humaine. b. Malveillance (attaques, suppression volontaire, falsification des données, rejoue de transactions,...)
R02	Pannes logicielles (bug bloquant, saturation,...)
R03	Évènement naturel accidentel dû à l'environnement (inondation, pollution,...)
R04	Accident matériel provoqué erreur humaine (perte, oubli,...)
R05	Malveillance matériels (vol, modification de câblage,...)
R06	Pannes matérielles
R07	Saturation accidentelle (réseau, système,...)
R08	Action volontaire du personnel : a. Démission collective massive b. Mouvement social avec arrêt de travail (grève)
R09	Accident touchant le personnels et/ou l'entreprise (intoxication, pandémie, accident de travail)
R10	Démotiver le personnel et perdre des compétences
R11	Perte de réputation d'image
R12	Manque de capacité de l'entreprise à faire face aux risques numériques (technologies et cyber) sur les applications majeurs, les infrastructures et les données critiques
R13	Coûts financiers et/ou baisse du chiffre d'affaires
R14	Gaspiller les ressources de l'entreprise sur des projets peu contributifs, ou mal cadrés voir accroître les coûts

Annexe B. Questionnaire d'analyse des risques du SI-EPB.

Métrique des réponses :

- R : Réponse
  - 1 : Oui
  - 0 : Non
- I : Impact
- P : Potentialité
- A : Acceptabilité

n°	Questions	R	ID Risques	I	P	A
D01 Organisation et management de la sécurité de l'information						
1	Disposez-vous des outils qui sont déployés pour détecter l'accès des appareils mobiles et étrangers au SI de l'organisme et limiter leurs accès conformément à une politique ?	1	R01/ R02	2	3	2
2	Est-ce-que des mesures de sécurité adéquate sont en place pour la protection de l'information sur des sites de télétravail ?	1	R01/ R02	2	3	2
D02 Sécurité des ressources humaines						
3	Le processus disciplinaire en cas de manquement aux règles de sécurité ou de violation de procédure est-il formalisé ?	1	R01	1	3	1
4	Existe-t-il un programme de sensibilisation du personnel aux risques d'accidents, d'erreurs et de malveillances relatifs au traitement de l'information ?	0	R01/ R12	4	4	4
5	Vous faites face à un manque de main d'oeuvre ?	1	R08/ R10	3	3	3
6	Face à de nouvelles technologies et la transformation digitale, le personnel recevaient-ils des formations particulières adaptées ?	1	R01/ R12	2	3	2
7	Durant la pandémie du COVID-19, y a-t-il eu un plan de licenciements dans l'entreprise ?	0	R08/ R10 R13	1	2	1
8	Vous obligez les employés à travailler dans des délais serrés ?	1	R08/ R10	3	4	4
D03 Sécurité physique et environnementale						
9	Les moyens de traitement de l'information gérés par l'organisme sont-ils séparés physiquement de ceux gérés par des tiers ?	1	R01/ R02 R04/ R05 R06/ R07	2	3	2
10	Si les services généraux tels que : l'électricité, les télécommunications, l'alimentation en eau, le gaz, l'évacuation des eaux usées, la ventilation et la climatisation sont : 1. Conformes aux spécifications du fabricant du matériel et aux exigences légales locales. 2. Font l'objet d'une évaluation régulière pour vérifier leur capacité à répondre à la croissance de l'organisme et aux interactions avec les autres services généraux. 3. Sont examinés et testés de manière régulière pour s'assurer de leur fonctionnement correct.	1	R01/ R02 R03/ R04 R05/ R06	3	3	3
11	Existe-t-il une salle de caméras de surveillance ?	1	R03/ R04 R05	2	3	2
12	La pointeuse est-elle à double authentification ?	0	R01/ R05 R06/ R09	4	3	4
13	Avez-vous déjà pensé aux conséquences d'un mauvais câblage informatique au sein de votre entreprise ?	0	R01/ R02 R06	4	4	4

D04 Politique de sécurité de l'information						
14	Existe-t-il des documents de politiques de sécurité de l'information, qui sont approuvées par la direction, publiées et communiquées à tous les utilisateurs du SI ?	1	R01	1	3	1
15	La politique de sécurité passe-elle en revue par un comité de sécurité à intervalles planifiés, ou si des changements importants se produisent pour s'assurer qu'elles sont toujours pertinentes, adéquates et efficaces ?	1	R01	1	3	1
D05 Sécurité liée à l'exploitation						
16	Existe-t-il un suivi régulier de la performance des serveurs et des équipements réseaux ?	1	R01/ R04 R06	2	3	2
17	Les serveurs sont pourvus de dispositifs de protection contre les codes malveillants ?	1	R01	2	3	2
18	Les fonctions de développements, de tests et d'exploitation sont-elles séparées ?	0	R01	3	3	3
D06 Acquisition, développement et maintenance des sytèmes d'information						
19	Une analyse des risques de sécurité de l'information est-elle réalisée dès la phase de conception des nouveaux systèmes d'information ou leurs améliorations ?	1	R01/ R02 R07	2	3	2
20	Un programme des tests détaillée comprenant des taches et des données de test d'entrée, avec les résultats attendus en sortie sous un certain nombre de conditions est élaboré et met en oeuvre ?	1	R01	2	3	2
21	Existe-t-il un document d"finissant les règles générales à appliquer en ce qui concerne les développements informatiques ?	0	R01/ R02	3	3	3
22	Avant tout développement ou toute acquisition de logiciel, les avantages et inconvénients respectifs de l'acquisition ou de la réalisation d'un système spécifique sont-elles analysées ?	1	R01/ R02 R12	1	3	1
D07 Gestion des incidents liés à la sécurité de l'information						
23	Un système de détection d'intrusion et d'anomalies est-il utilisé ?	1	R01/ R02 R06/ R07 R12	2	3	2
24	Est-ce-que vous évaluer l'exposition du SI aux risques d'une manière périodique ?	0	R01/ R02 R05/ R06 R12/ R13	4	4	4
25	Les failles constatées dans la sécurité de l'information sont-elles traitées ?	1	R01/ R02 R05/ R06 R12	2	3	2
26	Si des procédures permettant de prendre des mesures appropriées à des éventuelles attaques informatiques sont définies ?	0	R01/ R02 R12/ R13	4	4	4
D08 Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité						
27	Une solution de secours (systèmes redondants) est-elle mise en place pour pallier l'indisponibilité de tout équipement ou de toute liaison critique ?	1	R01/ R02 R03/ R04 R05/ R06 R07	2	3	2

28	Avez-vous élaboré un Plan de Continuité de Travail (PCT) et un Plan de Reprise dans l'environnement de Travail (PRET) lors de la pandémie du COVID-19 ?	1	R09/ R10 R11	2	3	2
29	Existe-t-il un plan de crise, en fonction de divers symptômes, les noms et coordonnées des personnes à prévenir pour qu'elles puissent effectuer un premier diagnostic et les actions urgentes à mener ?	0	R01 jusqu'à R09 R11/R13	4	4	4
30	Un plan d'action est-il élaboré pour lutter contre la congestion portuaire ?	1	R02/ R03 R04/ R07 R09/ R11 R13	2	3	2
31	Vous étiez déjà certifié ISO 9001 et non conforme lors du prochain contrôle dû a une absence de suivi des recommandations, Est-ce-que vous envisagez effectuer une mission de suivi à nouveau ?	0	R11	3	3	3
D09 Contrôle d'accès						
32	Les droits d'accès des utilisateurs sont définis ?	1	R01	2	3	2
33	L'un de vos futur projets le système RADIUS, vous l'avez commencé ? et depuis quand ?	1	R14	3	3	3
34	L'attribution des droits d'accès se fait-elle selon la règle : 1. Aucun accès sauf autorisations explicites. 2. Accès à tout sauf interdictions explicites.	1	R01	2	3	2
35	Les postes de travail se verrouillent-ils automatiquement après quelques minutes d'inutilisation ?	1	R01	2	3	2
36	Les journaux de connexion sont-ils examinés régulièrement (1) ou par échecs de connexion (0) ?	1	R01/ R02	2	3	2
D10 Sécurité des communications						
37	Disposez-vous d'une messagerie interne ?	1	R01	2	3	2
38	Vous souffrez des problèmes de connexion ?	1	R02/ R10 R13	3	3	3
D11 Gestion des actifs						
39	Un inventaire ou registre est maintenu pour tous les actifs en possession des employés ?	1	R04/ R05 R06	2	3	2
40	Si la restitution des actifs en possession des salariés et des utilisateurs tiers au terme de la période de l'emploi ou de l'accord est documentée ?	1	R04/ R05 R06	2	3	2
41	Avez-vous défini un niveau de classification des informations et ressources reflétant le besoin de protection de ces derniers en prenant en compte les critères Disponibilité, Intégrité et Confidentialité ?	1	R01	2	3	2
D12 Ouverture sur la transformation numérique						
42	L'entreprise a-t-elle mis en place un projet de transformation numérique ?	1	R01/ R02 R12/ R13 R14	2	3	2
43	L'entreprise est-elle accompagné dans ses projets de transformation par des experts interne ?	0	R01/ R12	3	3	3

44	Les évolutions numériques intègrent les exigences de gestion des risques, de contrôle et d'audit en lien avec les pratiques réglementaires et éthiques ?	1	R01/ R02 R04/ R05 R06/ R07 R12/ R13 R14	2	3	2
D13 Conduite de projets						
45	Y a-t-il eu des projets réalisés puis abandonnés ?	1	R13/ R14	3	3	3
46	Les dates cibles de livraison des projets sont "toujours" prévus et respectées ?	0	R11/ R13 R14	3	3	3
47	Des stratégies de tests sont-ils planifiées ?	1	R01/ R02 R06/ R07	2	3	2
D14 Cryptographie et conformité						
48	Un audit de sécurité des systèmes d'informations était déjà effectué ? [Réponse eu : 'Pas pendant ces 10 dernières années']	0	R01/ R02 R06/ R07 R11/ R12	4	4	4
49	Une politique d'utilisation des moyens cryptographiques est-elle élaborée et mise en oeuvre ?	1	R01/ R11 R12	2	3	2
50	Lorsque des non-conformités sont identifiées, l'organisation a-elle établi des processus appropriés pour les gérer et mettre en place des actions correctives ?	0	R01/ R02 R05/ R06 R07/ R09 R11/ R12 R13	4	3	4
51	Des tests périodiques de pénétration du réseau sont réalisés ?	1	R01/ R02 R07/ R12	2	3	2

Annexe C. Questionnaire d'analyse de la Gouvernance du SI-EPB.

N	Questions	R	Objectifs	Degré	Degré Global
EDS01 Assurer la définition et l'entretien d'un référentiel de gouvernance					
01	Existe-t-il un référentiel pour le management de votre SI ? 01. Oui 02. Non	01	Obj04 Obj08 Obj12 Obj13	P P S P	Obj04 (P) Obj12 (S) Obj08 (P) Obj13 (P) Obj01 (P) Obj06 (P)
02	Dans un contexte économique, le système gouvernemental facilite-t-il le processus d'acquisition de la technologie dont l'organisation à besoin ? 01. Oui 02. Non	01	Obj01 Obj03 Obj04 Obj05 Obj06 Obj12	P P P P P S	
EDS02 Assurer la livraison des bénéfices					
03	Vous rencontrez des problèmes à fournir des services ? Par exemple : une incapacité constante à répondre aux niveaux de service convenus (manque d'espace de stockage..) 01. Oui 02. Non	01	Obj01 Obj03 Obj05 Obj12	S S S S	Obj01 (P) Obj03 (S) Obj05 (S) Obj07 (P) Obj09 (P) Obj10 (P) Obj12 (S) Obj15 (S)
04	Des obstacles vous limitent sur l'innovation et l'agilité de l'entreprise ? Exemple : la législation et le numérique 01. Oui 02. Non	02	Obj01 Obj03 Obj12 Obj07 Obj15	P S S P S	
05	Il y avait des changements liés aux TI qui n'ont pas respectés les besoins de l'entreprise et livrés en retard ou dépassés les budgets ? 01. Oui 02. Non	02	Obj01 Obj03 Obj05 Obj09 Obj10	P S S P P	
EDS03 Assurer l'optimisation du risque					
06	Pendant ces dernières années, y a-t-il eu des incidents importants liés aux risques des TI, comme une perte de données ou l'échec d'un projet ? 01. Oui 02. Non	01	Obj01 Obj03 Obj05 Obj06	S S S S	Obj02 (S) Obj03 (S) Obj04 (S) Obj05 (S) Obj06 (S)
07	Des contrôles de prévention des risques s'effectuent-t-ils périodiquement ? 01. Oui 02. Non	01	Obj03 Obj04 Obj06 Obj13	P P P P	
08	Les risques liés aux services fournis aux clients et aux processus associés sont-ils connus et maîtrisés ? 01. Non. 02. Référencés par processus mais non suivis. 03. Référencés, suivis et contrôlés par processus.	03	Obj02 Obj03 Obj04 Obj05 Obj06 Obj10 Obj11	S S S S S S S	

N	Questions	R	Objectifs	Degré	Degré Global
	04. Référencés, contrôlés, maîtrisés et anticipés par processus. 05. Référencés, contrôlés, maîtrisés, anticipés pour l'ensemble des processus avec une gouvernance des risques intégrée au pilotage des processus.				
EDS04 Assurer l'optimisation des ressources					
09	Est ce que ça vous arrive de faire des dépenses inutiles et indésirables en TI ? 01. Oui 02. Non	02	Obj01 Obj03 Obj09 Obj10 Obj11	P P P P P	Obj01 (S) Obj02 (S) Obj03 (S) Obj11 (P) Obj12 (S)
10	Est ce que vous jugez insuffisant les ressources en TI ? 01. Oui 02. Non	01	Obj01 Obj02 Obj03 Obj06 Obj11 Obj12	S S S S P S	
EDS05 Assurer aux parties prenantes la transparence					
11	Les produits et services fournis par l'entreprise répondent-ils aux attentes des clients ? 01. Sont fournis, mais parfois avec des problèmes. 02. Fonctionnent de manière satisfaisante et s'améliorent progressivement. 03. Rapport coûts/qualité et fonctionnement jugés satisfaisants par les clients. 04. En avance sur les concurrents. 05. Font référence sur le marché et sont plébiscités par les clients.	02 04	Obj01 Obj02 Obj05 Obj06	P P P P	Obj01 (P) Obj02 (P) Obj05 (P) Obj15 (P)
12	L'entreprise a-t-elle une culture de l'écoute et de la satisfaction client ? 01. Non. 02. Partiellement. 03. Oui et les dysfonctionnements sont systématiquement corrigés. 04. Oui et les problèmes et les attentes clients sont exploités en source d'innovation. 05. Oui et l'écoute client est génératrice d'innovation et de différenciation.	02 04	Obj01 Obj05 Obj15	P P P	
F01 Structure organisationnelle et règles de gestion					
13	Existe-t-il des systèmes de résolution de conflits ? 01. Oui 02. Non 03. Je ne sais pas	03	Obj03 Obj04 Obj08 Obj13	S S S S	Obj01 (P) Obj02 (S) Obj03 (S) Obj04 (S) obj08 (S)
14	L'absence d'un poste dédié a une fonction d'audit de système d'information à l'interne de l'entreprise, est une conséquence de :	02	Obj01 Obj03 Obj14	S S S	

N	Questions	R	Objectifs	Degré	Degré Global
	01. L'absence d'une conviction de la direction supérieure ? 02. L'absence de ressources qualifiées sur le marché : moyens, outils et support nécessaire ? 03. Le coût qu'engendre les audits ?				
15	Dans le contexte actuel de votre organisation, est-ce que vous jugez les objectifs de contrôle des SI (les objectifs de sécurité des SI) sont compris suffisamment par la direction supérieure ? 01. Oui 02. Non	01	Obj01 Obj03 Obj16 Obj13	P P P P	Obj01 (S) Obj02 (S) Obj03 (S) Obj11 (P) Obj12 (S)
16	L'organisation fonctionne-t-elle dans un marché concurrentiel ? Une stratégie est mise en place pour faire face ? 01. Oui 02. Non	01 02	Obj01 Obj02 Obj15	P S S	
17	La structure organisationnelle porte-t-il sur une période cohérente (cycle de vie) avec la mission et l'environnement dans lequel elle œuvre ? 01. Oui 02. Non	01	Obj04 Obj08 Obj13	P P P	
F02 Processus métiers					
18	L'entreprise, a-t-elle mis en pilotage quelques processus (les plus stratégiques, les plus critiques) ou l'ensemble des processus ? 01. Non, cartographie des processus (une représentation graphique) sans pilotage, pilotage non formalisé. 02. Quelques processus, sans hiérarchisation, font l'objet d'une cartographie et sont pilotés. 03. Tous les processus stratégiques et/ou critiques sont pilotés. 04. Tous les processus de l'entreprise, y compris les processus support, sont pilotés. 05. Tous les processus sont pilotés et font l'objet de comparaison avec des processus similaires.	02	Obj01 Obj03 Obj06 Obj11	S S S S	
19	Les évolutions du SI sont-elles planifiées en adéquation avec celles des processus ? 01. Non. 02. Pour quelques processus. 03. Pour tous les processus dans le cadre d'un plan annuel.	02	Obj07 Obj16	S S	Obj01 (S) Obj03 (S) Obj06 (P) Obj07 (S)

N	Questions	R	Objectifs	Degré	Degré Global
20	Les démarches d'automatisation et de monitoring des processus (workflow, règles métiers, BAM ,...) sont-elles mises en oeuvre ? 01. Non. 02. Partiellement de façon expérimentale. 03. Oui, dans le cadre de l'optimisation de chacun des processus.	02	Obj06 Obj10	P S	Obj10 (S) Obj11 (S) Obj15 (S) Obj16 (S)
21	La DSI a-t-elle adoptée une démarche processus pour piloter sa performance (par exemple de type : Itil, Cobit, Cmmi,...) ? 01. Oui, effectivement 02. Non 03. Partiellement ou approche à l'étude	03	Obj15 Obj16	S S	
F03 Gouvernance de l'information et des données Processus métiers					
22	Comment percevez-vous le degré d'importance de la gouvernance informationnelle dans votre organisation ? 01. Pas du tout important 02. Peu important 03. Moyennement important 04. Très important 05. Ne sais pas	03	Obj08 Obj12	S S	Obj05 (P) Obj06 (P) Obj07 (P) Obj08 (S) Obj12 (S)
23	Les objectifs de l'information en matière de la qualité et sécurité sont-ils définis et atteints ? 01. Oui 02. Non	01	Obj05 Obj06 Obj07	P P P	
F04 Les services, l'infrastructure et les applications					
24	Effectuez-vous des contrôles de gestion périodique de services, infrastructure et applications ? 01. Oui 02. Non	01	Obj03 Obj04 Obj06 Obj16	P P P P	Obj03 (P) Obj04 (P) Obj06 (P) Obj15 (P)
F05 Compétences et culture digitale					
25	Selon vous à quel stade de maturité se situe cette stratégie de transformation numérique ? 01. Début de réflexion stratégique 02. Conception du projet ou des projets 03. Mise en œuvre opérationnelle des plans d'actions 04. Évaluation des bénéfices ou des projets de transformation numérique 05. Je ne sais pas	02	Obj01 Obj03 Obj07 Obj12 Obj15	S S S S S	

N	Questions	R	Objectifs	Degré	Degré Global
26	Quel(s) nouveau(x) postes ont été créés au sein de votre entreprise, dans le cadre de sa transformation numérique ? 01. Directeur numérique 02. Gestionnaire de communauté 03. Data scientist 04. Autre(s) 05. Aucun nouveau poste n'a été créé	01 04	Obj01 Obj03 Obj06 Obj14 Obj15	P P P P P	Obj01 (S) Obj03 (S) Obj06 (S) Obj07 (S)
27	Selon vous, quels sont les principaux freins à la transformation numérique de votre entreprise ? 01. Complexité des projets de transformation numérique (impact du numérique sur le business model de l'entreprise) 02. Manque de compétences technologiques 03. Manque de compétences managériales 04. Manque de compétences juridiques 05. Manques de ressources financières 06. Résistances aux changements internes	02 03	Obj03 Obj07 Obj12 Obj14	S S S S	
28	Pensez-vous que votre entreprise soit armée aujourd'hui pour affronter un risque d'attaque numérique ? 01. Oui 02. Non 03. Je ne sais pas	02	Obj01 Obj03 Obj06	S S S	
29	Globalement êtes-vous satisfait(e) des objectifs numériques atteints de votre entreprise ? 01. Pas du tout satisfait(e) 02. Pas satisfait(e) 03. Ni satisfait(e) ni insatisfait(e) 04. Satisfait(e) 05. Très satisfait(e)	03	Obj01 Obj02 Obj07 Obj08 Obj15	S S S S S	Obj12 (S) Obj14 (S) Obj15 (S)
30	Comment évaluez-vous les compétences numériques de vos collaborateurs (personnels sous votre responsabilité) ? 01. Pas bonnes 02. Moyennes 03. Bonnes 04. Excellentes	02	Obj01 Obj12 Obj14	S S S	

BIBLIOGRAPHIE

[1] CLUB DE LA SÉCURITÉ DE L'INFORMATION FRANÇAIS (CLUSIF). *MEHARI, Principes fondamentaux et spécifications fonctionnelles*. Mai 2017.

[2] ISO/IEC 27000. *Information technology — Security techniques — Information security management systems — Overview and vocabulary, 5th edition*. 2018.

[3] A. Deyrieux. *Le systéme d'information nouvel outil de stratégie*. MAXIMA, 2004.

[4] ISACA. *COBIT 5 : A Business Framework for the Governance and Management of Enterprise IT*. 2012.

[5] M. Juergens. *Guide pratique d'audit des technologies de l'information (GTAG)4 : Management de l'audit des systèmes d'information*. IIA (Institute of Internal Auditors, 2006.

[6] Documents interne de l'EPB. *Présentation de l'Entreprise Portuaire de Béjaïa*.

[7] A. Martínez. *Guide essentiel, Qu'est ce-que l'informatique décisionnelle peut-elle faire pour votre entreprise ?* Captio.

[8] C. Morley, M.B. Figueiredo et Y. Gillette. *Processus métiers et systèmes d'information : Gouvernance, management, modélisation*. Dunod, 2011.

[9] BATTAT Nadia. *Cours Système de Sécurité*. Université de Béjaia, 2022.

[10] Alain Fernandez Nodesway. *la gouvernance des Systèmes d'information à l'épreuve du terrainn cas pratique en 10 fiches*. 2014.

[11] P. O'brian. *Positive Management :Assertiveness for Managers*. 1993.

[12] S. Rivard. *Le développement de systèmes d'information : Une méthode intégrée à la transformation des processus, 4e édition*. Presses de l'Université du Québec, 2013.

[13] S. Servigne. *Conception, architecture et urbanisation des systèmes d'informations*. 2010.

[14] ISO (the International Organization for Standardization). *Guidelines for auditing management systems (ISO 19011 :2011)*. 2011.

[15] R. Yende. *Cours d'Audit des systémes d'information*. HAL, 2018.

RÉSUMÉ

Depuis de nombreuses années, les systèmes d'informations sont au cœur du développement des entreprises, ceux-ci sont devenu des facteurs stratégiques de la réalisation des performances et de la pérennité.

Suite à cette évolution exponentielle,Les SI se trouvent confrontés à plusieurs difficultés en matière de sécurité (Les cyber-attaques), il est donc devenu crucial pour les entreprises de protéger leurs systèmes d'informations et de maintenir la confiance avec leurs clients.

L'objectif de notre projet consiste à réaliser un audit de sécurité d'un SI d'une entreprise nationale (EPB), suivant les exigences de la norme ISO/IEC 27000. On a adopté la méthode MEHARI pour l'analyse des risques, et le référentiel COBIT5 pour l'analyse de la gouvernance.

Mots Clés : SI, Audit, Sécurité, cyber-attaques, Référentiel, Norme, ISO, IEC, MEHARI, COBIT5.

ABSTRACT

For many years, information systems have been at the heart of business development and have become strategic factors in achieving performance and sustainability.

As a result of this exponential development, IS is facing several security challenges (cyber-attacks), so it has become crucial for companies to protect their information systems and maintain trust with their customers.

The objective of our project is to carry out a security audit of an IS of a national company (EPB), following the requirements of the ISO/IEC 27000 standard. We adopted the MEHARI method for the risk analysis, and the COBIT5 referential for the governance analysis.

Key words : IS, Audit, Security, cyber-attacks, referential, Standard, ISO, IEC, MEHARI, COBIT5.