Ministère de l'Enseignement Supérieur
et de la Recherche Scientifique
Université Virtuelle de Tunis

UVT
جامعة تونس الافتراضية
UNIVERSITÉ VIRTUELLE DE TUNIS

MEMOIRE

DE STAGE DE FIN D'ETUDES

Pour l'obtention du

«Mastère professionnel en Nouvelles Technologies des Télécommunications et Réseaux (N2TR)»

Présenté par :

BILEL ARFAOUI

Audit de sécurité du système d'information de Le Moteur Diesel

Soutenu le : ……

Devant le jury :

Président : Mr. (Mme.)……

Encadreur : Mme. Ahlem Ben Youness

Rapporteur : Mr. (Mme.)……

Membre : Mr. Wael Boumaiza

Année Universitaire : 2016 / 2017

www.uvt.rnu.tn
14, Rue Yahia Ibn Omar - 1082 Mutuelleville - Tunis
Tél. : +216 71 28 99 81 / +216 71 89 17 31 - Fax : +216 71 89 26 25

Dédicaces

Je dédie ce travail

A mon père qui m'a indiqué la bonne voie en me rappelant que la volonté fait toujours les grands hommes ...

A ma mère qui a attendu avec patience les fruits de sa bonne éducation ...

A ma sœur et à mon frère qui ont été toujours présents avec leur soutien moral et leur amour ...

A tous mes cousins, mes amis et mes professeurs et tous ceux que j'aime.

Je vous dédie ce présent travail qui sans vous n'aurait pas pu être achevé. Avec toute ma gratitude et mon amour ...

Bilel Arfaoui

Remerciement

Le travail présenté dans ce rapport a été effectué dans le cadre de stage de fin d'études pour l'obtention du diplôme de Mastère professionnel en Nouvelles Technologies des Télécommunications et Réseaux à l'Université Virtuelle de Tunis (UVT).

Ce travail réalisé au sein du Le Moteur Diesel (LMD), a pu être mené à terme grâce à la collaboration de certaines personnes qu'il nous plaît de remercier.

Nous remercions Monsieur Wael Boumaiza, responsable informatique au sein de la LMD, de nous avoir accordé la chance d'intégrer son équipe pendant ce stage.

Nous remercions également Mlle Ahlem Ben Youness Notre encadrante pour ses conseils lucides et pertinents.

Nous remercions également tous les enseignants du Mastère N2TR pour la qualité de la formation dispensée.

Nous associons à ces remerciements toute l'équipe de l'unité informatique du LMD avec lesquels nous avons travaillé dans une ambiance forte sympathique.

Nous remercions enfin tous ceux qui, d'une manière ou d'une autre, ont contribué à la réussite de ce travail et qui n'ont pas pu être cités ici.

Table des matières

Liste des Figures

Liste des Tableaux

Introduction Générale

Dans le nouveau contexte économique, le besoin d'informations sécurisées est de plus en plus crucial pour les entreprises de nos jours. Certaines entreprises et institutions, en quête de développement de leurs activités, cherchent continuellement des informations qui leur permettent de mieux cerner les variables de leur environnement et de les maîtriser. Ce phénomène a toujours existé et ne fait qu'évoluer et se moderniser au fil du temps.

De nos jours, si les technologies de l'information et de la communication permettent aux responsables et dirigeants, d'améliorer et de sécuriser leurs données. Malheureusement, ces technologies permettent à d'autres individus assez doués (comme les HACKERS) d'en prendre part et de les utiliser illégalement.

Face à cette situation et pour protéger ces précieuses données, des barrières sont mises en place pour filtrer et bloquer les accès illicites. Toutefois, on se rend compte rapidement que les méthodes et la nature des attaques des Hackers changent et évoluent sans cesse, obligeant les institutions à sécuriser leurs Systèmes d'Informations et de Communications (SIC) mis en place.

Le meilleur moyen de suivre la sécurité d'un SI est d'effectuer un audit de sécurité des SI de façon périodique. L'audit, exercé par un auditeur, est un processus systématique, indépendant et documenté permettant de recueillir des informations objectives pour déterminer dans quelle mesure les éléments du système cible satisfont aux exigences des référentiels du domaine concerné. C'est dans ce contexte que s'inscrit ce projet qui vise l'audit de la sécurité SI du Le MOTEUR DIESEL.

Pour se faire, nous présenterons notre organisme cible ensuite certains concepts clé de l'audit des systèmes d'information. Par la suite, nous entamerons notre mission d'audit par l'audit organisationnel et physique ainsi que l'analyse des risques, ensuite l'audit technique. Enfin notre mission d'audit s'achèvera par un ensemble de recommandations et la proposition d'une solution technique pour améliorer la sécurité du LE MOTEUR DIESEL.

Chapitre I. Contexte du projet et état de l'art

Introduction :

Dans ce premier chapitre, nous allons présenter brièvement la société d'accueil qui est la société LMD, ainsi que et le Service Informatique au sein de la quel a été réalisé le projet et finalement l'étude de l'existant pour la partie contexte du projet. Pour la partie état de l'art nous allons commencer par présenter les normes sur laquelle elle peut se baser une mission d'audit, ensuite nous évoquerons ce que représente l'audit de sécurité des systèmes d'informations et finalement nous allons détailler les étapes nécessaires pour le déroulement de cette mission d'audit.

I- Contexte du projet :

I-1- Organisme d'accueil :

Le Moteur Diesel est l'une des plus anciennes sociétés du secteur elle a été créée en 1945, elle est spécialisée dans la vente de Matériel Roulant, Matériel Agricole et dans le Matériel de Travaux Publics, Forte de ses 67 ans d'existence elle a accumulé une large connaissance du milieu des Affaires en Tunisie.

HISTORIQUE :

- 1945 : Représentant de Camions « UNIC » et matériels agricoles « LANDZ »
- 1952 : représentant de la marque « SOMECA » matériels agricoles
- 1960 : représentant de la marque « OM » camions
- 1964 : représentant de la marque « FIAT TATTORI » matériels agricoles et travaux publiques
- 1970 : représentant de la marque « FIAT ALICE » matériels de travaux publics
- 1978 : représentant de la marque « IVECO » camions
- 2006 représentant de la marque « HELI » matériels de manutentions

- Maintenant : représentant des marques : « IVECO » camions, « NEW HOLLAND AGRICULTURE » matériels agricoles, « NEW HOLLAND CONSTRUCTION » matériels de travaux publiques, « FPT » moteurs marins et groupes électrogènes, « HELI » matériels de manutentions. **[1]**

I-2- Présentation du service Informatique :

Le service informatique du LMD siège social est actuellement composé de deux personnes. Il a pour mission :

- L'évolution et la maintenance du parc informatique,
- L'administration du réseau local et sa sécurité,
- Conception et développement des applications répondant aux besoins des différents services, l'assistance des utilisateurs.

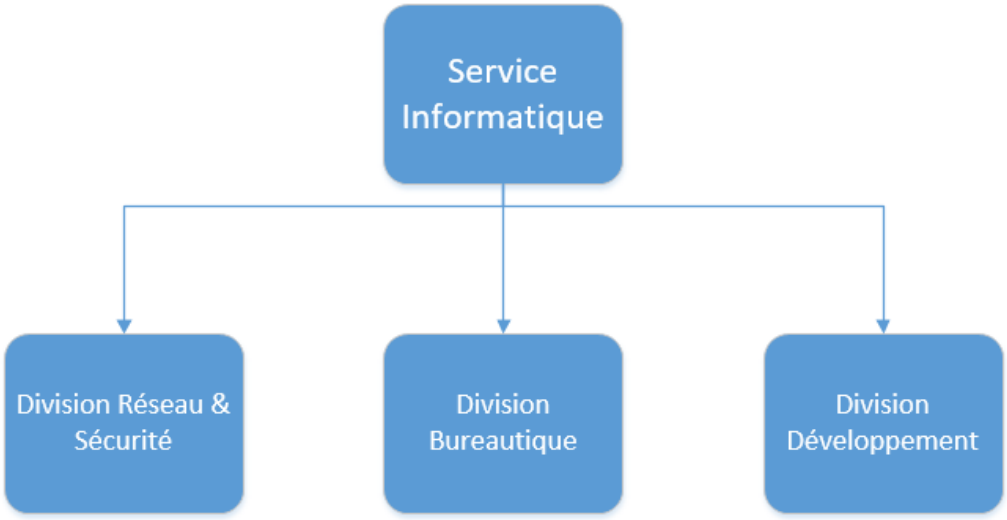

Figure 1. Organigramme du service informatique

I-3- Etude de l'existant :

D'après cette brève présentation, on remarque l'importance de cet organisme et le rôle majeur qu'il joue dans le développement du secteur Matériel Roulant, Matériel Agricole et dans le Matériel de Travaux Publics.

D'où la nécessité de mettre en place une politique de sécurité fiable et capable de faire face aux différentes intrusions ou autre problème de ce genre. IL est vrai que le LMD a intégré

dans son infrastructure des routeurs, firewalls, des antivirus et anti-spam... mais le souci d'adaptation avec les nouvelles techniques et technologiques surtout en matière de sécurité informatique exige plus de vigilance.

Le rôle de cet audit est ainsi de chercher à déceler les failles et les limites des dispositifs sécuritaires mis en place et de proposer les recommandations pour en faire face.

II- Etat de l'art :

II-1- Description des Normes d'audit :

L'organisation international de normalisation (ISO) a réservé la série ISO/IEC 27000 pour une plage de normes dédiée au pilotage de la sécurité de l'information, tout en s'accordant avec les normes de gestion de la qualité et de gestion des questions relatives à l'environnement que sont les normes ISO 9000 et ISO 14000.

Appelée à devenir une référence internationale reconnue, la famille des normes ISO 27000 donne aux responsables de la sécurité des systèmes d'information, l'opportunité de mettre en œuvre un véritable système de management de la sécurité de l'information. **[2]**

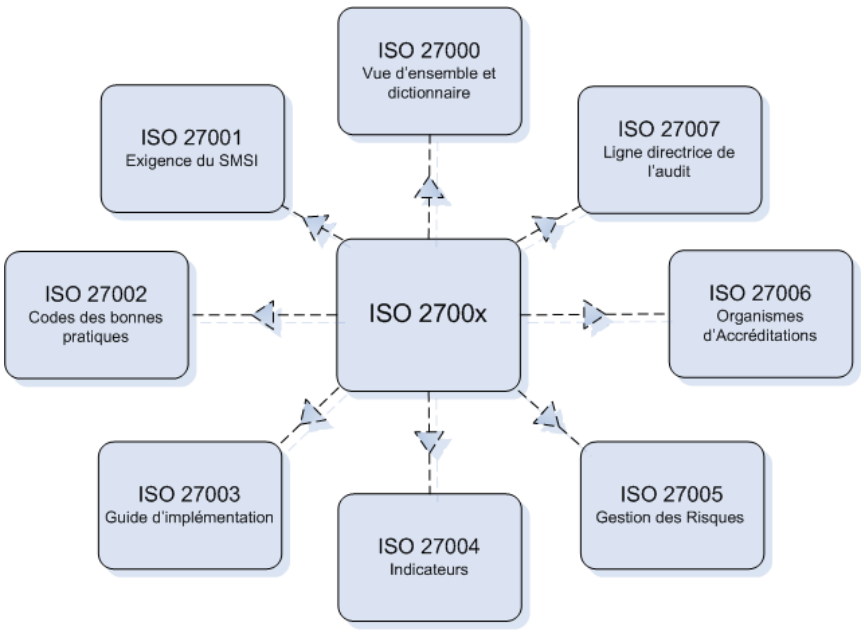

Figure 2. Les normes de la série ISO2700X

Elle porte essentiellement sur les questions de sécurité de l'information, Chaque norme porte sur les aspects précis suivants de la sécurité de l'information :

ISO 27001 : Modèle d'établissement, de mise en œuvre, d'exploitation, de suivi, d'examen, de maintien et d'amélioration de systèmes de gestion de la sécurité de l'information.

ISO 27002 : Liste de centaines de mesures et mécanismes de contrôle susceptibles d'être adoptés suivant les lignes directrices de la norme ISO 27001.

ISO 27003 : Conseils et lignes directrices quant à la mise en œuvre de système de sécurité de l'information, particulièrement en ce qui concerne la boucle d'amélioration continue.

ISO 27004 : Instruments de mesure et indicateurs d'évaluation de la gestion de la sécurité de l'information (publication de la norme à venir).

ISO 27005 : Instrument de définition du processus de gestion des risques du système de gestion de la sécurité de l'information, notamment le relevé des actifs, des menaces et des vulnérabilités (publication de la norme à venir).

ISO 27006 : Lignes directrices à suivre pour accréditer les entités qui offrent le service de certification et d'inscription relativement à un système de gestion de la sécurité de l'information. Les lignes directrices précisent les éléments à observer en plus des exigences stipulées dans la norme ISO 17021.

ISO 27007 : Rentrée très récemment en période d'étude, cette norme va être un guide spécifique pour les audits d'ISMS, notamment en support à l'ISO 27006.

L'ensemble de ces normes constitue des standards internationaux. Elles sont donc destinées à tout type de société, quelle que soit sa taille, son secteur d'activité ou son pays d'origine. Elles ont donc pour but de décrire un objectif à atteindre et non la manière concrète d'y arriver, cette dernière étant généralement dépendante du contexte de l'organisation.

II-2- Audit de sécurité de système d'information :

II-2-1- Audit de sécurité de système d'information en Tunisie :

L'ANSI est l'organe accrédité pour les missions d'audit en Tunisie conformément au décret N° 2004-5 du 3 février 2004 relatif à la sécurité informatique. Cet organisme définit l'audit de sécurité tel une « intervention de spécialistes, utilisant des techniques et des méthodes adéquates, pour évaluer la situation de la sécurité d'un système d'information et les risques potentiels. En Tunisie, la réalisation d'un audit de sécurité informatique possède un caractère obligatoire. En effet depuis le décret N°2004-1250, du 25 Mai 2004, l'audit de sécurité informatique est imposé aux organismes suivants :

- Les opérateurs de réseaux publics de télécommunications et fournisseur des services de télécommunication et d'Internet,
- Les entreprises dont les réseaux informatiques sont interconnectées à travers des réseaux externes de télécommunication,
- Les entreprises qui procèdent au traitement automatisé des données personnelles de leurs clients dans le cadre de la fourniture de leurs services à travers les réseaux de télécommunications.

De ce point de vu, l'audit de sécurité se présente comme une nécessité, pour répondre à une obligation règlementaire.

Cependant, l'audit de sécurité peu présenter un aspect préventif. C'est-à-dire qu'il est effectué de façons périodiques afin que l'organisme puisse prévenir les failles de sécurité. **[3]**

II-2-2- Objectifs de l'audit de sécurité :

Une mission d'audit vise différents objectifs. En effet nous pouvons énumérer à ce titre :

- La détermination des déviations par rapport aux bonnes pratiques de sécurité.
- La proposition d'actions visant l'amélioration du niveau de sécurité du système d'information.

Egalement, une mission d'audit de sécurité d'un système d'information se présente comme un moyen d'évaluation de la conformité par rapport à une politique de sécurité ou à défaut par rapport à un ensemble de règles de sécurité.

II-2-3- Cycle de vie d'un audit de sécurité des systèmes d'information :

La mission d'audit de sécurité informatique est effectuée selon un processus cyclique. Il décrit un cycle de vie qui est schématisé à l'aide de la figure suivante :

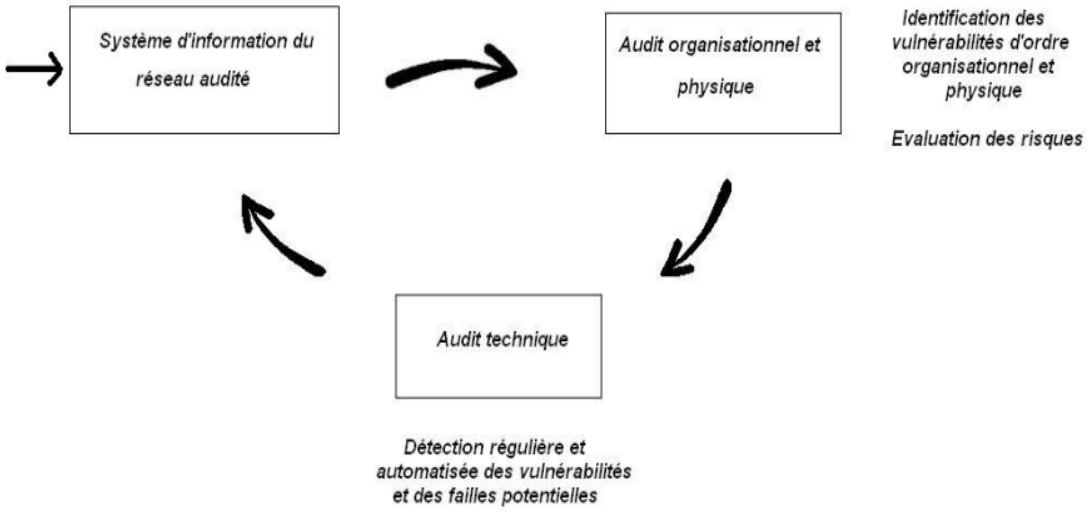

Figure 3. Cycle de vie d'un audit de sécurité

Ce processus permet d'étudie le niveau de sécurité du système d'information d'un point de vue :

- Organisationnel (étude des procédures de définition, de mise en place et de suivi de la politique de sécurité, etc...).
- Technique (les points d'entrées sur le réseau, les équipements de sécurité, les protocoles mis en œuvre, etc…).

Enfin un rapport d'audit est établi à l'issue de ces étapes. Ce rapport présente une synthèse de l'audit. Il présente également les recommandations à mettre en place pour corriger les défaillances organisationnelles ou techniques constatées. **[4]**

II-3- Démarche de réalisation d'une mission d'audit :

Tel que précédemment évoqué, l'audit de sécurité des systèmes d'information se déroule suivant deux principales étapes. Cependant il existe une phase tout aussi importante qui est une

phase de préparation. Nous schématisons l'ensemble du processus d'audit à travers la figure suivante :

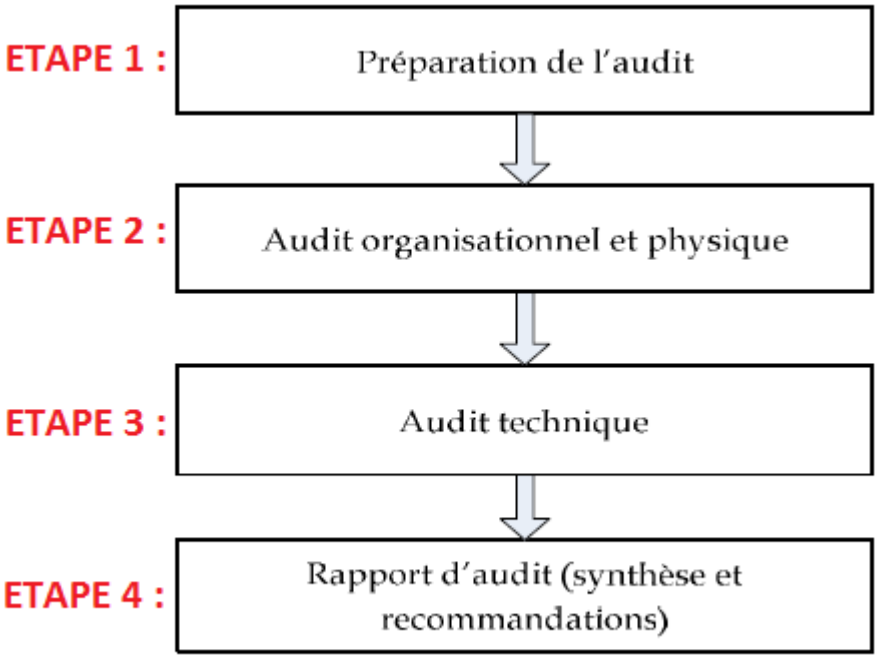

Figure 4. Les phases d'audit

II-3-1- Préparation de l'audit :

Cette phase est aussi appelée phase de pré audit. Elle constitue une phase importante pour la réalisation de l'audit sur terrain. En effet, c'est au cours de cette phase que se dessinent les grands axes qui devront être suivis lors de l'audit. Elle se manifeste par des rencontres entre auditeurs et responsables de l'organisme à auditer. Au cours de ces entretiens, devront être exprimées les espérances des responsables vis-à-vis de l'audit. Aussi, il doit être fixé l'étendu de l'audit ainsi que les sites à auditer, de même qu'un planning de réalisation de la mission de l'audit.

Les personnes qui seront amenées à répondre au questionnaire concernant l'audit organisationnel doivent être également identifiées. L'auditeur pourrait également solliciter les résultats de précédents audits.

Une fois que les deux parties (auditeur-audité) ont "harmonisé leur accordéons ", l'audit sur terrain peut être entamé. Il débute par l'audit organisationnel et physique.

II.3.1.1 Périmètre de l'audit :

Lors des réunions de préparation avec les responsables, nous avons fixé les objectifs de la mission et nous avons élaboré un planning des tâches à exécuter ainsi que la liste des personnes impliquées. Nous avons aussi délimité le périmètre de l'audit. Notre mission s'intéresse au SI du LMD (site central de Tunis), pour l'audit niveau 1, nous allons s'intéresser aux composants de ce SI. L'audit technique que nous allons effectuer tiendra pour cible le réseau informatique de la société. Le périmètre physique est celui des locaux du siège du LMD.

II.3.1.2 Planning de la mission :

Désignation des phases	Durée approximative	
Phase 1 : Préparation de la mission	Deux semaines	**Rédaction du rapport**
Phase 2 : Audit Organisationnel et Physique	Quatre semaines	
Phase 3 : Analyse des risques	Deux semaines	
Phase 4 : Audit technique	Quatre semaines	
Phase 5 : Recommandations	Trois semaines	
Total	**100 jours**	

Tableau 1. Planning de la mission

II-3-2- Audit organisationnel et physique :

Dans cette étape, il s'agit de s'intéresser à l'aspect physique et organisationnel de l'organisme cible, à auditer. Nous nous intéressons donc aux aspects de gestion et d'organisation de la sécurité, sur les plans organisationnels, humains et physiques.

Cette première phase de l'audit sécurité permet :

- D'avoir une vision qualitative et quantitative des différents facteurs de la sécurité informatique du site audité.
- D'identifier les points critiques du système d´information.

Afin de réaliser cette étape de l'audit, ce volet doit suivre une approche méthodologique qui s'appuie sur « une batterie de questions ». Ce questionnaire préétabli devra tenir compte et s'adapter aux réalités de l'organisme à auditer. A l'issu de ce questionnaire, et suivant une métrique, l'auditeur est en mesure d'évaluer les failles et d'apprécier le niveau de maturité en termes de sécurité de l'organisme, ainsi que la conformité de cet organisme par rapport à la norme référentielle de l'audit.

Dans notre contexte, suivant les recommandations de l'ANSI et du fait de sa notoriété, cet audit prendra comme référentiel une norme de l'ISO .Il s'agit de toutes les clauses (ou chapitres ou domaines) de la version 2005 de la norme ISO/IEC 27002.

II-3-3- Audit technique :

Cette étape de l'audit vient en seconde position après celle de l'audit organisationnel. L'audit technique est une analyse technique de la sécurité de toutes les composantes du système informatique et la réalisation de tests de leur résistance face aux attaques avec une analyse et une évaluation des dangers qui pourraient résulter de l'exploitation des failles découvertes suite à l'opération d'audit. Cet audit s'applique aux environnements suivants :

- Réseau d'accès Internet, réseau d'interconnexion intersites (Frame Relay, X25, Faisceau Hertzien, etc...).
- Serveurs internes du site audité et les postes sensibles du LAN.
- Systèmes critiques spécifiques.
- Composants et équipements actifs de l'infrastructure réseau du site audité (firewalls, routeurs filtrants, commutateurs niveau 3, etc…).

Cette technique s'effectue principalement en quatre phases :

- **Phase 1 : Audit de l'architecture du système :**

Lors de cette phase on va recenser les caractéristiques d'un système d'information à travers :

- La reconnaissance du réseau et du plan d'adressage
- Le sondage des systèmes

- Le sondage des services réseau
- Le sondage des applications (A ne pas confondre avec un audit des applications)

- **Phase 2 : Analyse des Vulnérabilités (intrusif interne) :**

Cette phase consiste à scanner le réseau, par le biais de plusieurs outils automatisés d'identification et de test de vulnérabilités, afin de déterminer les failles existantes et d'identifier les composants vulnérables du système.

- **Phase 3 : Analyse des Vulnérabilités (intrusif externe) :**

Au cours de cette phase on va vérifier les possibilités offertes à un attaquant de récupérer, depuis l'extérieur les caractéristiques du système d'information. Lors de cette phase l'auditeur procède à :

- L'énumération des services et protocoles internes du réseau.
- L'édification de scénarios d'éventuelles attaques expertes.

- **Phase 4 : Audit de l'architecture de sécurité existante :**

Cette phase a pour but l'inspection de la qualité de l'architecture de sécurité du système audité, l'identification des périmètres de sécurité mis en place, la sécurité de circulation des flux sensibles et la qualité d'administration des outils de sécurité. Parmi les points essentiels à inspecter:

- La politique d'usage de mots de passe.
- La solidité du système, face aux essais d'interception des flux.
- La résistance aux attaques de déni de Service.
- Les firewalls & des ACLs (Liste de Contrôle d'Accès).

II-3-4- Rapport d'audit :

La phase finale du processus d'Audit Sécurité est consacrée à la rédaction des rapports de synthèse :

- Recueil des principales vulnérabilités et insuffisances décelées.
- Synthèse des solutions et outils de sécurité proposés,
- Synthèse des recommandations de mise en œuvre (organisationnelles, physiques et techniques),
- Esquisse d'un plan d'action sécurité (Estimation des budgets à allouer pour la mise en œuvre des mesures recommandées).

Conclusion :

Ce chapitre nous a permis de présenter le cadre général du projet. Nous venons aussi d'exposer, une liste non exhaustive d'un ensemble de normes qui constituent des références dans le cadre d'un audit de systèmes d'information ainsi que les procédures de réalisation d'un audit de systèmes d'information, et la place de l'audit des systèmes d'informations en Tunisie. La suite de ce document consistera à mettre en pratique les précédents aspects de réalisation d'un audit, par l'entame de l'audit organisationnel.

Chapitre II. Audit organisationnel et physique

Introduction :

Dans ce chapitre, nous allons aborder la première étape de la mission : la reconnaissance du système d'information à étudier en se focalisant sur le réseau informatique, ensuite nous allons entamer l'audit physique des différents composants du SI, pour s'intéresser après à l'audit organisationnel basé sur la norme ISO 27002.

I- Description de l'existante :

Avant d'entamer la phase d'audit organisationnelle et physique il est nécessaire de collecter des informations concernant l'infrastructure, les composants informatiques et réseaux du site à auditer.

I-1- Description de l'infrastructure de site :

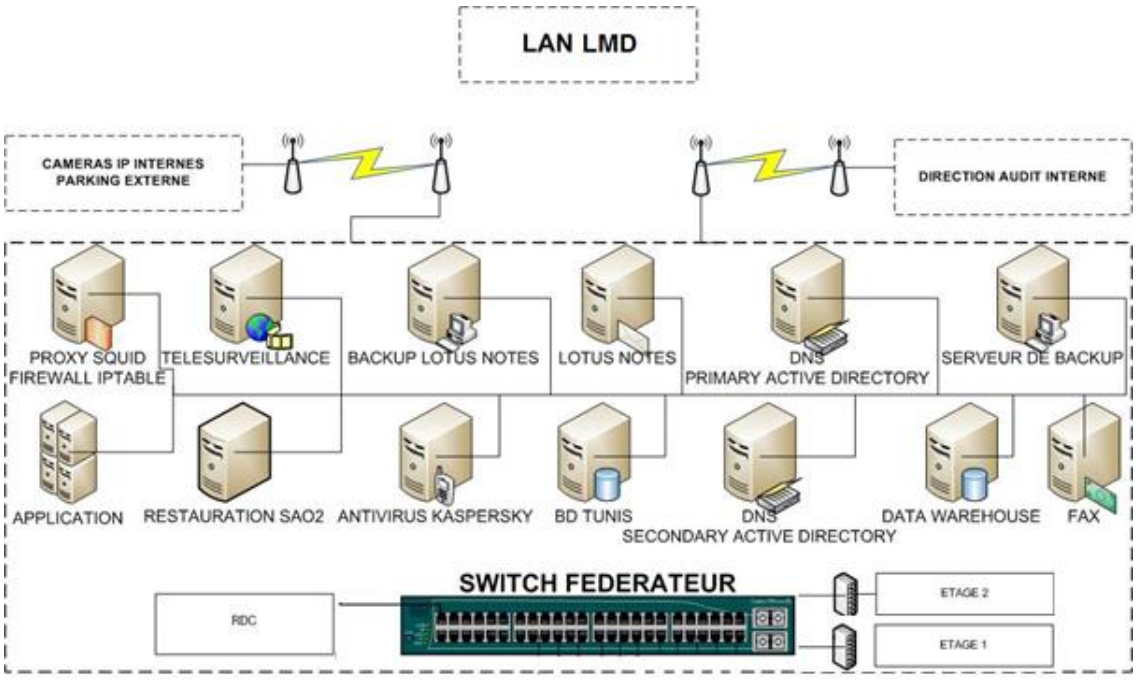

Figure 5. Architecture actuelle du réseau du LMD

La topologie du site est une topologie en étoile, le réseau est segmenté physiquement en des 5 niveaux en utilisant un répartiteur dans chaque niveau.

I-1-1- Les Serveurs :

Nous allons détailler dans le tableau ci-dessous la liste des serveurs du LMD :

Serveur	Application	Plateforme
Serveur de domaine « Active Directory »	Fournir des services centralisés d'identification et d'authentification au réseau de LMD utilisant le système Windows.	Windows server 2003
Serveur proxy– Firewall « Squid-IPtables »	Intermédiaire entre le réseau local et internet.	Red Hat Advanced server 3
Serveur antivirus	Solution antivirale : Kaspersky Administration Kit 6.0	Windows server 2003
Serveur DATA WAREHOUSE		Windows server 2003
Serveur Lotus Notes	Solution IBM : Lotus Notes	Windows server 2003
Serveur de Backup		Windows server 2003
Serveur Application		Windows server 2003
Serveur BD		Windows server 2003

Tableau 2. Liste des serveurs

I-1-2- Les composants réseau :

Nous allons détailler dans le tableau ci-dessous la liste des composants réseau du LMD :

Modèle	Nombre
Routeur Cisco 1721	1
Switch D-Link 3828	1
Switch 3Com 4500	1
Switch D-Link 3100	1
Switch Cisco Catalyst 2900	1

Tableau 3. Liste des composants réseau

I-2- Les mesures de sécurité existantes :

I-2-1- Sécurité réseaux :

L'architecture est protégée en entrée de réseau par un firewall IP tables destiné à filtrer les flux de données entrant depuis l'extérieur. Le firewall a pour le rôle de bloquer les accès non autorisées.

Aucune solution de sécurité contre les intrusions n'est mise en place (IDS/IPS), notamment pour le suivi des journaux du Firewall.

I-2-2- Sécurité physique :

Elle est basée principalement sur les aspects suivants :

- Des agents d'accueil qui contrôlent l'accès au périmètre du site et enregistrent des informations relatives à chaque visiteur.
- Salle serveur fermée à clef et seuls les personnes autorisées et qui en possèdent peuvent y accéder,
- Les serveurs ne sont pas tous organisés dans une armoire (quelques un sont mis par terre).
- La climatisation est assurée au niveau de la salle des serveurs,
- Seuls les serveurs et les composants réseaux à importance élevée sont protégés par des onduleurs pour éliminer les problèmes d'alimentation électrique de courte durée,
- Absence d'un groupe électrogène pour coupure de courant à long terme.
- Les extincteurs d'incendies sont disponibles dans chaque étage.
- Absence des caméras de surveillance pour les zones sensibles.

I-2-3- Sécurité logique :

Pour la sécurité logique, les principaux points cités sont :

- l'architecture réseau segmenté
- Existence d'un contrôleur de domaine pour gérer l'accès aux postes de travail des utilisateurs.

- Les filtrages des accès depuis et vers le réseau Internet et assuré par un proxy.
- Existence d'un Firewall pour configurer des Access liste.

I-2-4- Sécurité des machines :

- **Gestion des mises à jour et distribution de correctifs :**

  - Pas des mises à jour correctives en termes de sécurité pour les systèmes Windows.
  - Tous les systèmes d'exploitation ne bénéficient pas de licence.
  - Pas de mise à jour pour les systèmes d'exploitation des switchs et des routeurs

- **Le système Antiviral :**

Un système antiviral centralisé est mis en place (solution Kaspersky) pour détecter et éliminer les menaces et les codes malicieux mais la stratégie de scan présente une défaillance car le choix de l'action dépend du client.

- **Gestion des mots de passe :**

  - Il y a une politique d'affectation des mots de passes.
  - Les mots de passe des serveurs ne change pas.
  - L'utilisateur a le droit de changer son mot de passe.

II- Analyse des résultats de l'Audit organisationnel et physique :

Dans la phase d'audit organisationnel et physique de la sécurité réseau du LMD nous nous sommes appuyés sur les questionnaires de la méthode MEHARI pour modeler un questionnaire découpé en cinq domaines qui sont :

- Domaine d'Organisation,
- Domaine des Locaux,
- Domaine du Réseau Local (LAN),
- Domaine du Réseau Étendu Intersites (WAN),
- Domaine de l'Exploitation des Réseaux.

Pour chaque question, le responsable devait répondre par « oui » ou par « non ».Ce questionnaire va nous permettre d'évaluer le niveau de conformité de chaque clause par rapport aux différents chapitres définis dans la norme.

Une synthèse claire des résultats obtenus sur la maturité par chapitre est représentée dans le tableau au niveau de l'**[Annexe B]**.

Niveau de maturité	Description
Plus que 75%	Niveau de maturité optimal
50%->75%	Niveau de maturité moyen
Moins de 50%	Niveau de maturité faible

Tableau 4. Les niveaux de maturité

A l'issu de notre questionnaire, l'organisme enregistre une conformité globale de 66,03%, par rapport à la norme ISO/IEC 72002 preuve que des efforts sont à faire pour ce qui est de la sécurité. Nous abordons à présent l'analyse des résultats obtenus. Les points seront abordés suivant les clauses (ou chapitres) définis dans la norme ISO/IEC 17799 :2005 selon l'ordre dans lequel elles ont été évoquées.

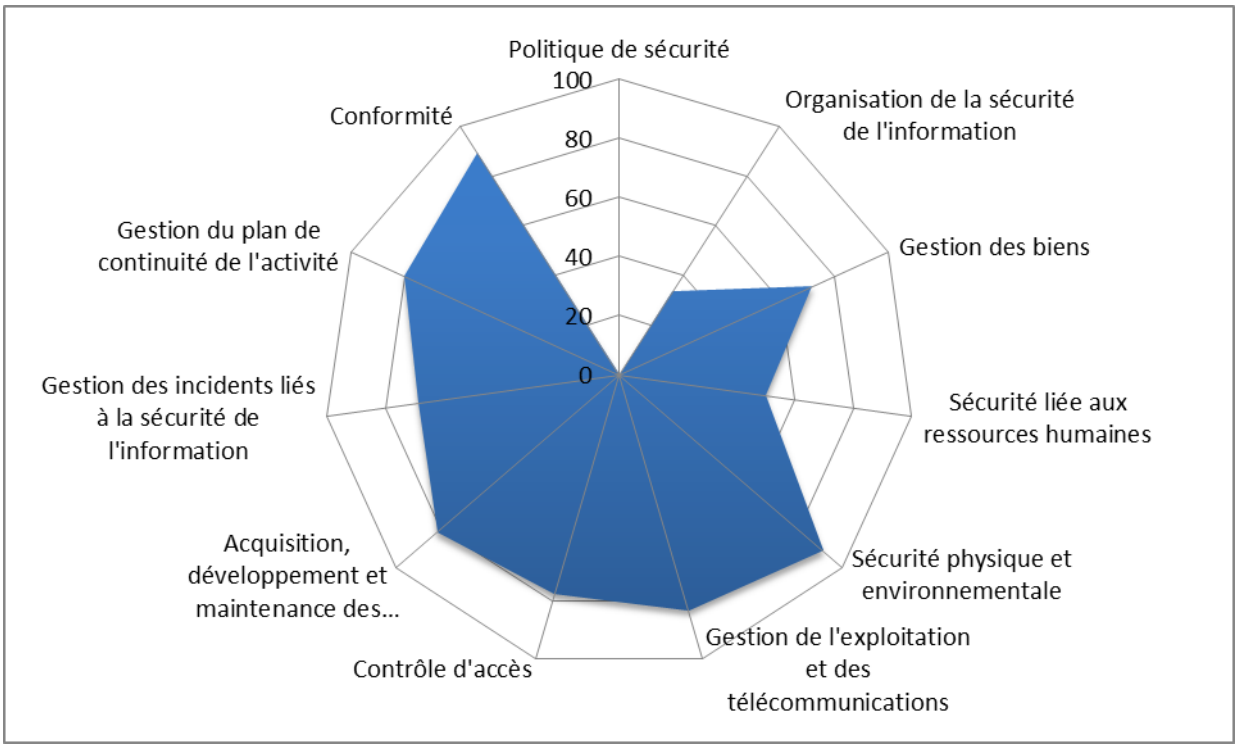

Figure 6. Rosace de niveau de maturité par chapitre

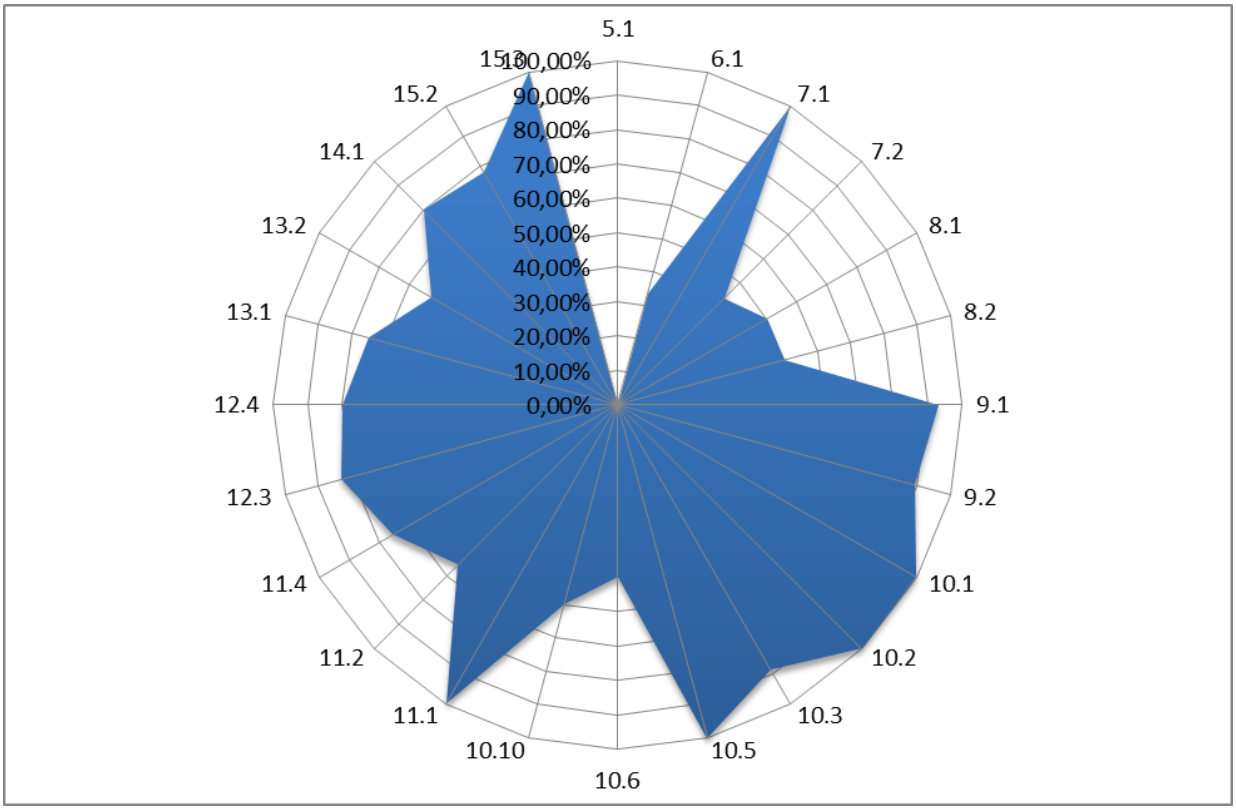

Figure 7. Rosace de niveau de maturité par sous-chapitre

- **Politique de sécurité :**

Le niveau de conformité de cette clause par rapport à la norme ISO/IEC 27002 est de **0%**. Cela s'explique par l'absence de documents de synthèse représentant le document de la politique de sécurité. Il n'existe ainsi aucun document de sécurité. Ainsi en plus de mettre en place une politique de sécurité, il faut prévoir également des mesures pour permettre à cette dernière d'être revue périodiquement. Le niveau de maturité accordé à cette clause est donc **faible**.

- **Organisation de la sécurité :**

Le niveau de conformité de cette clause par rapport à la norme ISO/IEC 27002 est de **33,3%.** Ce niveau de conformité est le résultat des travaux du comité chargé de la sécurité au sein de l'organisme. Cependant les fonctions des responsables de sécurité ne sont pas formellement définies. Le département informatique n'a pas élaboré un plan directeur informatique permettant une visibilité et prévision de l'évolution du système dans les années à venir. Le niveau de maturité accordé à cette clause est donc **faible**.

- **Gestion des actifs :**

Le niveau de conformité de cette clause par rapport à la norme ISO/IEC 27002 est de **71.87%.**L'ensemble des principaux actifs est identifié et inventorié, cet inventaire est tenu à jour. Pour chaque actif les règles d'utilisation sont définies et documentées. Ceci implique, en particulier, de définir l'usage privé qu'un collaborateur peut faire d'un actif de l'entreprise. Cependant, les procédures de classification ne se basent pas sur une documentation précise qui définit les critères de classification, de sorte à pouvoir évaluer les conséquences d'une altération de cet actif sur l'organisme. De plus il n'existe pas de procédure d'étiquetage pour la classification ; simplement, les dossiers considérés sensibles sont astreints à rester dans le bureau du responsable en question. Le niveau de maturité accordé à cette clause est donc **moyen**.

- **Sécurité liée aux ressources humaines :**

Le niveau de conformité de cette clause par rapport à la norme ISO/IEC 27002 est de **50%**. Les nouveaux employés sont informés de leurs droits et devoirs vis-à-vis de la sécurité de l'organisme également, mais cet engagement n'est pas formalisé avec la signature d'un document ou d'une charte, et il n'est pas indiqué dans les contrats de recrutement. Ainsi il n'est pas défini de procédure visant à rappeler à l'ensemble du personnel son rôle dans la sécurité de l'organisme. Le niveau de maturité accordé à cette clause est donc **moyen**.

- **Sécurité physique et environnementale :**

La moyenne de cette clause est de **91,2%** par rapport à la norme ISO/IEC 27002. L'environnement de localisation ne présente pas d'exposition à des dangers naturels apparents En ce qui concerne la sécurité physique des locaux elle est assurée par une clôture qui les entoure, ainsi que des postes de gardiennage qui surveillent les principales entrées. Un mécanisme d'enregistrement des visiteurs a été instauré. Il permet de relever les identités des visiteurs ainsi que les dates et heures d'entrée et sortie. La zone sensible qu'est la salle serveur bénéficie d'une sécurité toute particulière, et ce à travers l'accès qui y est très réservé. En effet pour protéger cette salle de toute malveillance physique l'accès est limité aux personnes concernées possédant les clefs. La salle des serveurs est climatisée est ceci pour compenser les effets de la dissipation thermique et de l'échauffement qui peuvent nuire au bon fonctionnement des équipements et des

serveurs sensibles. Concernant les actifs critiques (Firewall, switch…), certains d'eux utilisent la technologie de clustering, afin d'assurer la répartition de charge et la disponibilité et éviter l'arrêt des services. Les bureaux des employés sont dotés de serrures, offrant la possibilité de les verrouiller pendant leur absence. Egalement l'accès physique aux postes de travail de chacun des utilisateurs, pour certain, est protégé par un mot de passe. Le niveau de maturité accordé à cette clause est donc **optimal.**

- **Exploitation et gestion des communications :**

La moyenne de cette clause est de **83,14%** par rapport à la norme ISO/IEC 27002.Les mesures de continuité de services sont en parties assurées. Il s'agit des sauvegardes des bases de données des serveurs, effectuées une seule fois par jour. Ces sauvegardes sont conservées dans un coffre. Nous notons également qu'il existe de redondances des serveurs pour permettre une reprise presque instantanée en cas de panne de l'un des serveurs. L'ensemble des serveurs est protégé d'intrusions externes (provenant de l'Internet) malveillantes par un firewall open source « IPtables ». Il n'existe donc pas de DMZ pour l'instant au sein de cet organisme. Le réseau LAN de l'organisation est de type Ethernet, et un adressage privé a été mis en place. Bien qu'il existe une politique d'adressage par sous réseau, il n'existe cependant pas de réalisation de LAN virtuel pour permettre une segmentation, à un niveau plus élevé, du réseau de l'organisme. Le système ne dispose pas d'une fonction automatique de surveillance en temps réel en cas d'accumulation d'événements anormaux, pour le moment il n'existe pas un système de détection d'intrusion et d'anomalies sur le réseau mais ça sera mis en place prochainement. Le niveau de maturité accordé à cette clause est donc **optimal.**

- **Contrôle d'accès :**

La clause enregistre une moyenne de **77 ,44%** par rapport à la norme ISO/IEC 27002. Une politique de mot de passe est instaurée au sein de l'organisme, pour l'accès à certaines applications. Cependant les bonnes pratiques en matière de choix et de l'utilisation de mot de passe ne sont pas centralisées pour les postes de travail des utilisateurs. La permanence de ces mots de passe ne permet pas de réduire les risques d'usurpation de mots de passe ou de vol. De même on remarque l'absence d'un dispositif de revue des droits d'accès à des intervalles réguliers. Cependant, il y a un certain contrôle partiel ciblant les téléchargements pour en limiter

les effets négatifs, de même pour empêcher tout abus tel que les outils de téléchargement Peer to Peer, par exemple, qui exposent le réseau aux risques d'infiltration et d'infection par les spywares et les virus. Egalement, l'accès aux locaux sensibles tel que la salle serveur reste protégé par des clefs. Seules les personnes qui en possèdent, sont habilitées à y accéder à. En plus la climatisation est assurée au sein de cette salle. L'accès distant, à partir de l'Internet est protégé par les règles d'accès gérées par le Firewall. Etant donné qu'on ne peut garantir qu'un accès illicite et qui ne peut se réaliser qu'à 100%, il n'ya pas de système IDS/IPS pour contrer et réagir contre les actions malveillantes qui peuvent être des intrus interne/externe, scannage, des accès non autorisés. Le niveau de maturité accordé à cette clause est donc **optimal.**

- **Acquisition, développement et maintenance des Systèmes d'information :**

La clause enregistre une moyenne de **81,62%** par rapport à la norme ISO/IEC 27002. L'acquisition de nouveaux systèmes porte l'attention particulière des dirigeants afin de s'assurer que le système à acquérir correspond aux besoins de l'organisme, ne mettra pas à mal la sécurité. Egalement des tests pour s'assurer qu'un nouvel équipement ne sera pas source de régression de service sont effectués. Egalement les procédures de chiffrement ou de signature électronique ne sont intégrées dans les procédures de l'organisme. Le niveau de maturité accordé à cette clause est donc **optimal.**

- **Gestion des incidents liés à la sécurité de l'information :**

La clause enregistre une moyenne de **68,75%** par rapport à la norme ISO/IEC 27002. Le personnel a été sensibilisé sur la nécessité de déclarer les incidents ou failles de sécurité rencontrée. Cependant, pour l'instant il n'est planifié l'instauration de procédures pour la gestion des incidents de sécurité ainsi que les rapports détaillés de ces derniers qui surviennent ne sont pas édités. Il n'est donc pas possible de s'informer des incidents déjà survenus. Le niveau de maturité accordé à cette clause est donc **moyen**.

- **Gestion du plan de continuité de l'activité :**

Le niveau de conformité de cette clause par rapport à la norme ISO/IEC 27002 est de **80%.** Le plan de continuité d'activité ou de reprise d'activité se base essentiellement sur les

sauvegardes de bases de données. Ainsi l'organisme dispose d'un plan révélant dans les détails et dans l'ordre les actions à entreprendre en cas de reprise suite à une catastrophe. Ce plan est testé d'une manière opérationnelle au moins une fois par an. Concernant la protection électrique, seuls les serveurs et les composants réseaux sont protégés par des onduleurs pour éliminer les problèmes d'alimentation électrique de courte durée, les prises de courant électriques sont non-ondulés. Le niveau de maturité accordé à cette clause est donc **optimal.**

- **Conformité :**

Le niveau de conformité de cette clause par rapport à la norme ISO/IEC 27002 est de **89 ,06%.** Les responsables s'assurent de l'exécution correcte de l'ensemble de procédures de sécurité placées sous leur responsabilité en vue de garantir leur conformité avec les normes de sécurité. Des tests de pénétration du réseau et des audits techniques spécialisés sont procédés une fois par an. Les résultats d'audit sont protégés contre toute modification ou divulgation. Le niveau de maturité accordé à cette clause est donc **optimal.**

Conclusion :

L'audit fonctionnel a mis l'accent sur les vulnérabilités d'ordre organisationnel et physique existantes au niveau du système de l'information du LMD. L'étape suivante consiste à quantifier les risques présents en estimant leurs impacts, leurs potentialités et leurs gravités.

Chapitre III. Analyse des risques

Introduction :

Après avoir mesurer la maturité de l'entreprise en termes de sécurité du système d'information aux bonnes pratique de la norme ISO 27002, nous allons à présent nous intéresser à l'analyse des risques en identifiant les risques et en estimant leurs impacts, leurs potentialités et leurs gravités.

I- Etude comparative des méthodologies d'audit :

Plusieurs normes, méthodes et référentiels de bonnes pratiques en matière de sécurité des systèmes d'information sont disponibles. Elles constituent des guides méthodologiques ainsi que le moyen de fournir l'assurance d'une démarche de sécurité cohérente.

I-1- COBIT :

Méthode publiée par l'ISACA (Information Systems Audit and Control Association) en 1996.Actuellement dans sa 4ème édition (4.1 depuis Mai 2007), COBIT se veut accessible à tous, dans un langage simple. Les outils fournis permettent la mesure des performances une liste de facteurs clés de succès et de bonnes pratiques pour les non techniciens. Les outils fournis permettent la mesure des performances mais la méthode est aujourd'hui davantage assimilée à une méthode de gouvernance des SI. CobiT décompose tout système informatique en 34 processus regroupés en 4 domaines. Les processus établis se divisent en 220 activités. CobiT est aussi une approche multicritères, qui permet à chaque utilisateur de ce référentiel d'obtenir pour chaque processus les informations qui l'intéressent. **[5]**

I-2- CRAMM :

CRAMM est une méthode d'analyse de risque, conforme aux normes BS7799 et ISO 17799. Créée en 1987, la méthode est reprise par Insight Consulting pour devenir une boite à

outils en sécurité de l'information. Elle comprend des outils d'aide pour soutenir des responsables de la sécurité de l'information pour créer rapidement, entre autres, les politiques de sécurité de l'information adéquates.

CRAMM est une méthode de gestion du risque lourde et exhaustive : plus de 3000 commandes de sécurité référencées aux risques appropriés et rangées par les outils essentiels d'efficacité et de coût pour aider à réaliser la certification ou la conformité à BS7799. Cette méthode est donc, plus adaptée aux grands organismes. **[6]**

I-3- EBIOS :

Elle a été créée par la DCSSI (Direction Centrale de la Sécurité des Systèmes d'Information) en 1996. EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) permet d'identifier les risques d'un SI et de proposer une politique de sécurité adaptée aux besoins de l'entreprise (ou d'une administration).

La méthode EBIOS se compose de 5 guides (Introduction, Démarche, Techniques Outillages) et d'un logiciel permettant de simplifier l'application de la méthodologie explicitée dans ces guides. Ce logiciel, libre et gratuit, (les sources sont disponibles) permet de simplifier l'application de la méthode et d'automatiser la création des documents de synthèse. **[7]**

I-4- MEHARI :

La méthode MEHARI (Méthode Harmonisée d'Analyse de Risques) est proposée par le CLUSIF (Club de la Sécurité des Systèmes d'Information Français). Elle est destinée à permettre l'évaluation des risques mais également le contrôle et la gestion de la sécurité de l'Entreprise sur court, moyen et long terme, quelle que soit la répartition géographique du système d'information. **[8]**

II- Choix de la méthodologie d'audit Mehari 2013 :

Pour pouvoir choisir la méthode la plus convenable il s'avère nécessaire de faire une synthèse comparative des différentes méthodes.

Le tableau suivant résume quelques aspects des méthodes observées sur lesquels le choix peut s'appuyer :

	Cobit v4	CRAMM v5	Ebios v3	Mehari
Caractéristiques				
Analyse des risques	Non	Oui	Oui	Oui
Analyse des vulnérabilités	Non	Oui	Oui	Oui
Plan de sécurité	Non	Oui	Oui	Oui
Contrôle et vérification	Oui	Non	Non	Oui
Bilan de sécurité	Non	Non	Non	Oui
Périmètre				
Adapté à toutes les tailles d'entreprises	Oui	Oui	Oui	Oui
Conçu pour des environnements	Technologiques divers	Oui	Oui	Oui
Outils				
Questionnaires	Oui	Oui	Oui	Oui
Modèles (formulaires, grilles...)	Oui	Oui	Oui	Oui
Logiciel disponible	Non	Oui	Non	Oui
Divers				
Licence gratuite (concernant le logiciel)	Non	Oui	Oui	Non
Subit encore des mises à jour	Oui	Oui	Oui	Oui

Tableau 5. Comparaison entre les méthodologies

Après cette comparaison entre ces différentes méthodes d'analyse de risque, nous nous sommes basés sur ces critères pour choisir une méthode adéquate à notre mission :

- la compatibilité avec une ou plusieurs normes nationales ou internationales
- la facilité d'utilisation et le pragmatisme de la méthode
- les domaines de sécurité que la méthode peut couvrir
- la quantité de moyens humains qu'elle implique et la durée de mobilisation
- la taille de l'entreprise à laquelle elle est adaptée
- le support de la méthode par son auteur, une méthode abandonnée n'offre plus la possibilité de conseil et de support de la part de son éditeur
- la langue de la méthode, il est essentiel de maîtriser le vocabulaire employé la qualité de la documentation.

Le choix de Mehari découle de plusieurs facteurs :

La méthode est conforme aux exigences techniques, environnementales et légales auxquels se réfère notre travail. De même elle offre une très bonne couverture par rapport aux autres, et une focalisation plus importante sur le risque en général pas seulement informatique, mais aussi les autres aspects qui touchent à la sécurité.

Si on y ajoute le fait d'être gratuite, bien documentée et récemment mise à jour (2010), le choix de Mehari sera bien justifié. Le seul inconvénient est que son logiciel (Risicare) est payant, ce qui va nous laisser opérer « manuellement » lors des différentes étapes d'analyse et de calcul.

III-Paramètre d'analyse de risque :

L'analyse des risques est l'utilisation systématique d'informations pour estimer le risque. Elle fournit une base à l'évaluation, au traitement et à l'acceptation du risque.

L'objectif de cette analyse est d'évaluer deux paramètres caractéristiques du risque encouru par l'entreprise ou l'organisme dans l'hypothèse d'occurrence d'un tel scenario. Ces paramètres sont :

- **La potentialité** : la potentialité du risque qui représente, en quelque sorte, sa probabilité d'occurrence, cette potentialité est en fonction du contexte et des mesures de sécurité en place.
- **L'impact :** l'impact du risque sur l'entreprise, qui présente la gravité des conséquences directes et indirectes qui découleraient de l'occurrence du risque. Il est éventuellement réduit par la mise en œuvre de mesures de sécurité adaptées.
- **La gravité :** la gravité du scénario ou de la situation de risque résulte à la fois de sa potentialité et de son impact.

Afin de quantifier le risque correspondant au scénario analysé, les évaluations de la potentialité et de l'impact seront faites sur une échelle ayant 4 niveaux, ainsi que nous le préciserons d'après les paragraphes suivants :

- L'impact total devrait être considéré comme un nombre entre 1 et 4.

  1 : L'impact est négligeable,

  2 : L'effet important : l'impact est notable, mais reste supportable.

  3 : L'effet est désastreux, mais l'Entreprise peut survivre à un coût considérable

  4 : L'effet est vital, l'Entreprise ne peut pas suivre

- la potentialité de la survenance d'un scénario de risque, devrait être considérée comme un nombre entre 0 et 4.

  0 : Le risque est non envisagé

  1 : Le risque est très improbable

  2 : Le risque est improbable, mais sa survenance demeure possible

  3 : Il est probable que le risque se produise à plus ou moins court terme

  4 : Il est très probable que le risque se produise très certainement et à court terme

III-1- Analyse des risques :

Notre méthode consiste à calculer la gravité de chaque menace en calculant son impact et sa potentialité et nous nous basons pour le faire sur la démarche d'analyse de risque de MEHARI expliquée dans la figure ci-dessous. **[8]**

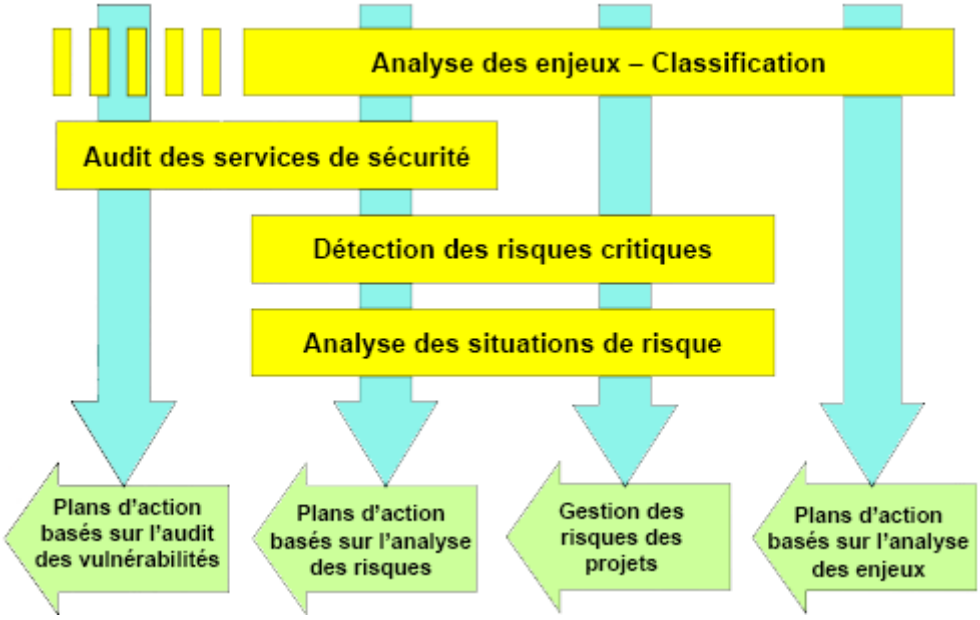

Figure 8. Démarche d'analyse d'une situation de risque

L'estimation de risque que nous proposons de réaliser aura pour objectif de déterminer les risques les plus graves sur le réseau du LMD. Le risque peut être défini comme la conséquence de l'exploitation d'une faille en tenant compte de son impact et de sa potentialité.

Dans notre audit de sécurité réseau, nous avons recensé d'après la base de connaissance de MEHARI, la liste des scénarios, des causes et des origines du risque.

Un scénario comprend un nombre de causes et chaque cause comprend un nombre d'origine de risque. **[Annexe C]**

III-2- Evaluation de la potentialité et de l'impact :

Pour analyser les risques, MEHARI s'appuie sur un modèle de risque qui distingue :

- Deux facteurs structurels, indépendants de toutes mesures de sécurité qui sont l'exposition naturelle et l'impact intrinsèque.
- Deux facteurs de réduction de la potentialité : Dissuasion et prévention.
- Trois facteurs de réduction de l'impact : confinement (ou protection), mesures palliatives et transfert du risque**.**

La figure ci-dessous explique mieux le concept de mesure de la potentialité et de l'impact par la méthode MEHARI.

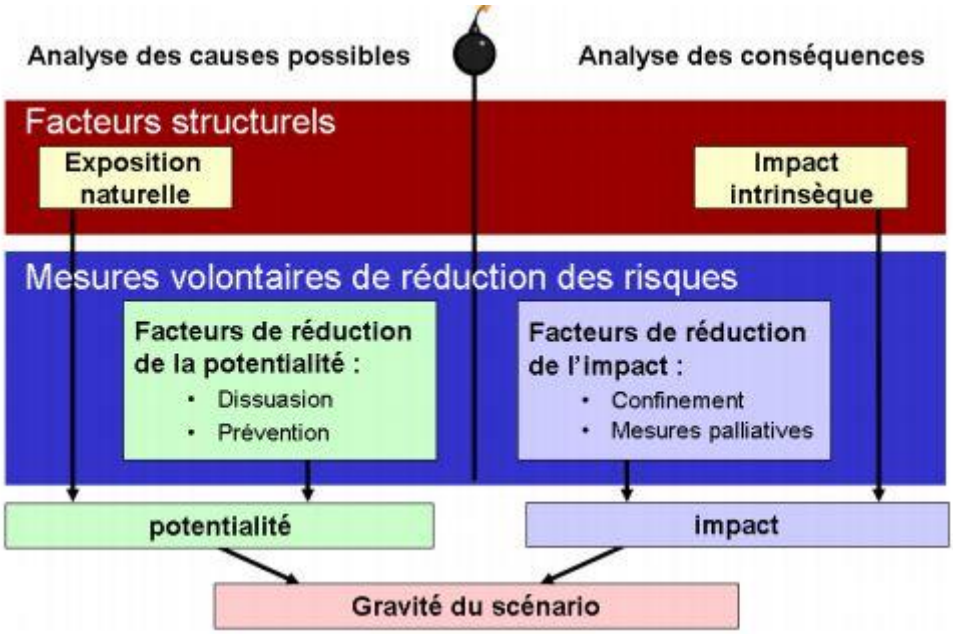

Figure 9. Concept et mesure de la potentialité et de l'impact

III-2-1- Evaluation de potentialité :

MEHARI propose une évaluation de la potentialité en partant de l'évaluation de l'exposition naturelle et du niveau de mesure de dissuasives et préventif.

- L'exposition naturelle à un risque donné peut dépendre de :
  - Sa localisation et de son environnement, pour les risques naturels.
  - L'enjeu potentiel d'un acte volontaire, pour son auteur (vol, détournement, satisfaction intellectuelle, etc.).
  - La probabilité d'une action volontaire vise l'entreprise (inversement proportionnel au nombre de cibles potentiels : notion de ciblage).
- Les mesures dissuasives qui permettent d'éviter la mise en œuvre des menaces potentielles.
- Les mesures préventives qui empêchent qu'une menace se réalise.

III-2-2- Evaluation de l'impact :

L'évaluation de l'impact se fait par l'analyse préalable de plusieurs facteurs :

- L'impact intrinsèque : L'impact intrinsèque d'un scénario est l'évaluation des conséquences de l'occurrence du risque, indépendamment de toute mesure de sécurité.
- Les mesures de protection qui limitent l'impact d'une menace, qui souvent des menaces de détection/réaction. Ces mesures de protection sont :
  - Mesures d'isolement et de compartimentage physique.
  - Mesures de détection (intrusion, accidents, erreurs, etc.).
  - Contrôle a posteriori incorporés aux processus et applications informatique.
  - Capacité d'investigation sur détection d'anomalies.
  - Capacité d'intervention rapide.

- Les mesures palliatives qui permettent de limiter les conséquences de la mise en œuvre d'une menace. Ces mesures concernent :
  - L'étude préalable des modes dégradés acceptable, des fonctions minimales à remplir et des services indispensables.
  - L'anticipation et de la préparation des solutions palliatives adéquates.
  - La préparation et de la formation des hommes et des structures en préavisant des situations de crise (gestion de la crise, communication de crise, etc.).

- Les mesures de récupération qui visent à récupérer une partie du préjudice par transfert du risque se basent sur :

- Analyse spécifique des risques à couvrir par l'assurance.
- Couverture des risques insoutenables par l'assurance.
- Préparation spécifiques des actions en justice.

III-3- Evaluation de la gravité de risque :

La mesure globale du risque, sa gravité, résulte d'une décision stratégique de l'organisation fondée sur les valeurs d'impact et de potentialité. La gravité du scénario ou de la situation de risque résulte à la fois de sa potentialité et de son impact.

La grille d'acceptabilité des risques suivante définie, en fonction de l'impact et de la potentialité estimés si le risque est acceptable ou non. **[Annexe A]**

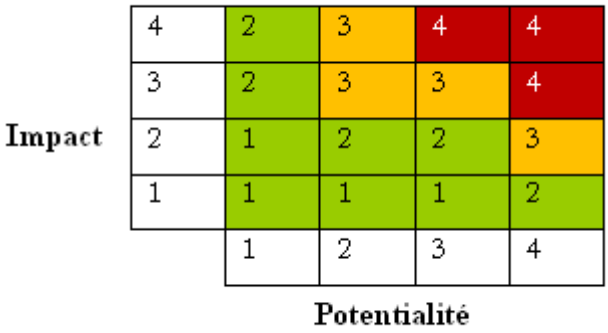

Tableau 6. Grille d'acceptabilité des risques

Gravité du risque	Description
3.1 → 4	Risques insupportable
2.1 → 3	Risques inadmissibles
0.0 → 2	Risques tolérés

Tableau 7. Les niveaux de risque

IV-Application de Mehari :

IV-1- La phase préparatoire :

Pour notre cas, notre estimation des risques majeurs à un périmètre bien défini qui sera celui du réseau informatique du LMD, tout ce qu'il contient de point de vue matériel et logiciel.

Nous allons dans la suite essayer de dégager les ressources les plus critiques en se basant sur une discussion approfondie avec les responsables du service informatique du LMD et par la suite dégager une base de scénarios spécifique qui servira comme point de départ dans l'estimation et la classification des risques majeurs.

IV-2- Identification et classification des ressources :

Nous avons essayé de rassembler toutes les personnes en relation avec le sujet et de collecter leur vision sur la classification. Les personnes concernées feront partie du service informatique, le fait d'être liés au SI et conscients des risques qu'ils affrontent nous a permis de mener cette classification avec rigueur.

Ressources logiques		
Nom	**Type**	**Domaine**
Solution antivirale Kaspersky	Logiciel	Réseau
Lotus Notes	Logiciel	Réseau
IPtables	Logiciel	Réseau

Tableau 8. Ressources logiques

Ressources Matérielles et Humaines		
Nom	**Type**	**Domaine**
Serveur BD	Serveur	Réseau
Serveur DATA WAREHOUSE	Serveur	Réseau
Serveur fax	Serveur	Réseau
Serveur Proxy / Firewall	Serveur	Réseau
Serveur Télésurveillance	Serveur	Réseau
Serveur Antivirus Kaspersky	Serveur	Réseau
Serveur de Backup	Serveur	Réseau
Serveur Lotus Notes	Serveur	Réseau
Serveur Application	Serveur	Réseau

Serveur Active Directory	Serveur	Réseau
Onduleur	Equipement électricité	Réseau
Modem/routeur	Equipement réseau	Réseau
Routeur pour la liaison Internet	Equipement réseau	Réseau
Personnel informatique	Ressource humaine	Réseau
Réseau local	Réseau	Réseau

Tableau 9. Ressources Matérielles et Humaines

Après avoir identifié les ressources globales liées au périmètre, nous avons eu une discussion avec les responsables au service informatique pour choisir quels sont les ressources les plus critiques que lesquels l'estimation doit être focalisée. Enfin nous avons décidé d'étudier les risques liés aux :

- **Serveur Proxy / Firewall**
- **Serveur Active Directory**

IV-3- Création d'une base spécifique de scénarios :

La recherche des situations à analyser est une étape préliminaire qui consiste, à partir de la base de scénarios types proposés par la méthode, de s'en inspirer et bâtir une base de scénarios adaptée au domaine étudié. Le choix des scénarios sera basé sur la discussion avec les responsables correspondants, cette étude est focalisée sur les ressources critiques précédemment identifiées.

Dans ce tableau nous résumons les scénarios choisis en précisant les références dans la base de connaissance MEHARI, en évoquant les possibles causes et en les classifiant selon le niveau d'impact qu'ils ont sur le réseau du LMD.

Ressource	N	Scenario	Impact
Serveur Proxy / Firewall	1	Indisponibilité passagère de ressources	3
	2	Destruction d'équipements	2
	3	Performances dégradées	3
	4	Destruction de software	2
	5	Altération de logiciel	3
	6	Manipulation de données	3
	7	Divulgation de données ou d'informations	4
	8	Détournement de fichiers de données	4
	9	Perte de fichiers de données ou de documents	4

Tableau 10. Base spécifique des scénarios pour serveur Proxy

Ressource	N	Scenario	Impact
Serveur Active Directory	1	Indisponibilité passagère de ressources	4
	2	Destruction d'équipements	4
	3	Performances dégradées	3
	4	Perte de fichiers de données ou de documents	3
	5	Altération de logiciel	3
	6	Manipulation de données	3
	7	Divulgation de données ou d'informations	4
	8	Sinistre immatériel total	4

.

Tableau 11. Base spécifique des scénarios pour Serveur Active Directory.

IV-4- Evaluation quantitative des scénarios

La gravité du scénario ou de la situation de risque résulte à la fois de sa potentialité et de son impact en se basant sur la grille d'aversion du risque.

Partant de la base spécifique de scénarios et de l'évaluation automatique de leur gravité, il devient aisé de calculer le niveau de gravité de chaque scénario comme le montrent les tableaux ci-après.

Pour Serveur Proxy / Firewall :

Scénario	Potentialité	Impact	Gravité
Indisponibilité passagère de ressources	2	3	**3**
Destruction d'équipements	2	2	**2**
Performances dégradées	1	3	**2**
Destruction de software	1	2	**1**
Altération de logiciel	2	3	**3**
Manipulation de données	1	3	**2**
Divulgation de données ou d'informations	2	4	**3**
Détournement de fichiers de données	2	4	**3**
Perte de fichiers de données ou de documents	1	4	**2**

Tableau 12. Evaluation quantitative des risques pour Serveur Proxy / Firewall

Pour serveur Switch Fédérateur :

Scénario	Potentialité	Impact	Gravité
Indisponibilité passagère de ressources	2	4	**3**
Destruction d'équipements	2	4	**3**
Performances dégradées	1	3	**2**
Perte de fichiers de données ou de documents	1	3	**2**
Altération de logiciel	2	3	**3**
Manipulation de données	1	3	**2**
Détournement de fichiers de données	1	4	**2**
Sinistre immatériel total	1	4	**2**

Tableau 13. Evaluation quantitative des risques pour Switch Fédérateur

On remarque la présence des risques intolérables et très graves pour cela nous allons essayer de détailler les actions à prendre concernant cette analyse dans le dernier chapitre afin d'aider les responsables à améliorer le niveau de sécurité correspondant.

Conclusion :

Dans ce chapitre nous avons essayé de faire une estimation de risques focalisée sur deux actifs critiques afin de déterminer la gravité des différents scénarios de risque possibles, pour les prendre en considération lors de la proposition d'un plan d'action à fin de neutraliser ces risques ou réduire leurs impacts.

Les résultats de cette étape de la mission seront utiles lors de l'élaboration des recommandations finales détaillées dans le dernier chapitre.

Chapitre IV. Audit Technique

Introduction :

L'audit technique suit une étude organisationnelle et physique permettant d'avoir une vue globale de l'état de sécurité du système d'information et d'identifier les risques potentiels. A cette étape nous passons à la recherche des vulnérabilités afin d'analyser le niveau de protection de l'infrastructure face aux attaques notamment celles qui exploitent ces vulnérabilités.

Nous utilisons tout au long de l'audit technique un ensemble des outils permettant d'obtenir les informations nécessaires et de déceler les différentes vulnérabilités.

I- Audit de l'architecture du système :

I-1- Reconnaissance du réseau et du plan d'adressage :

Il s'agit de déterminer le plan d'adressage IP du LMD, la cartographie du réseau et les principaux serveurs et équipements réseaux. L'outil utilisé pour l'identification de la topologie réseau est NetworkView à sa version 3.62 qui permet de fournir une représentation graphique des composantes actives sur le réseau et leurs attributs. **[9]**

Concernant le plan d'adressage, le LMD utilise un adressage statique et dynamique ; statique pour les serveurs (128.**X.X.X**) et les imprimantes (128.**X.X.X** et 10.**X.X.X**) et dynamique pour les poste de travails à travers le DHCP (10.**X.X.X**).

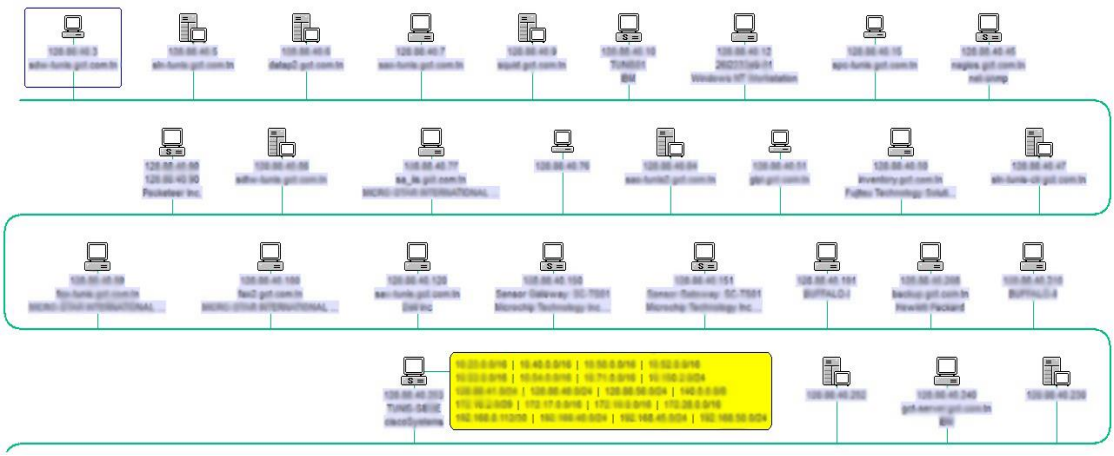

Figure 10. Réseau local LMD

Au terme de l'exécution de cet outil, nous recensons 162 machines actives (postes de travail + serveurs). Parmi ces machines nous avons recensé 13 serveurs.

Nous signalons à cet égard, que la configuration réseau au niveau des postes n'est pas protégée contre les modifications. En effet, chaque utilisateur peut changer son adresse ce qui peut générer des conflits d'adresses. Des attaques de type IP Spoofing (usurpation d'identité) peuvent être facilement menées et générer un déni du service ; il suffit de remplacer l'adresse IP du poste par celle d'un équipement critique (routeur, serveur, etc.). Cette attaque permet la dégradation des performances de l'équipement concerné voir même son arrêt complet.

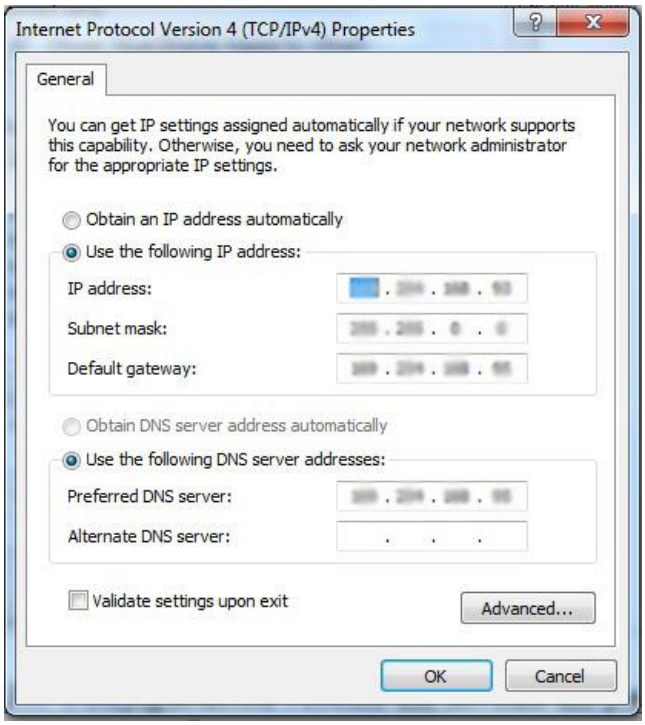

Figure 11. Configuration réseau au niveau du poste

On remarque que la majorité des noms des machines (PC) sont significatifs ; ils portent le nom de la personne qui l'utilise, et cela mène à une probabilité d'un *danger* de sécurité.

Le NetworkView permet de générer un graphique du LAN scanné mais il n'inspecte qu'une liste très limitée des ports usuels et ne permet pas de bien reconnaître certaines entités scannées alors on va utiliser d'autres outils pour avoir une description plus détaillée ciblant les services réseaux mis en jeu.

I-2- Sondage des services réseaux :

Le sondage des services réseau est une étape qui permet de déterminer les services réseau et la stratégie de déploiement ces services identifier les partages réseau et les mesures de sécurité mises en œuvre de savoir quelles sont les ports ouverts sur les machines du réseau audité (ouverts, fermés ou filtrés).

Cette étape est faite à l'aide de ces outils : NetCrunch 5, NMAP , Wireshark et Look@Lan .

I-2-1- Les ports ouverts :

Nmap est un outil open source. Il présente une multitude de fonctionnalités comme la découverte du réseau, La détermination des ports ouverts et la détermination du système d'exploitation des machines cibles. **[10]**

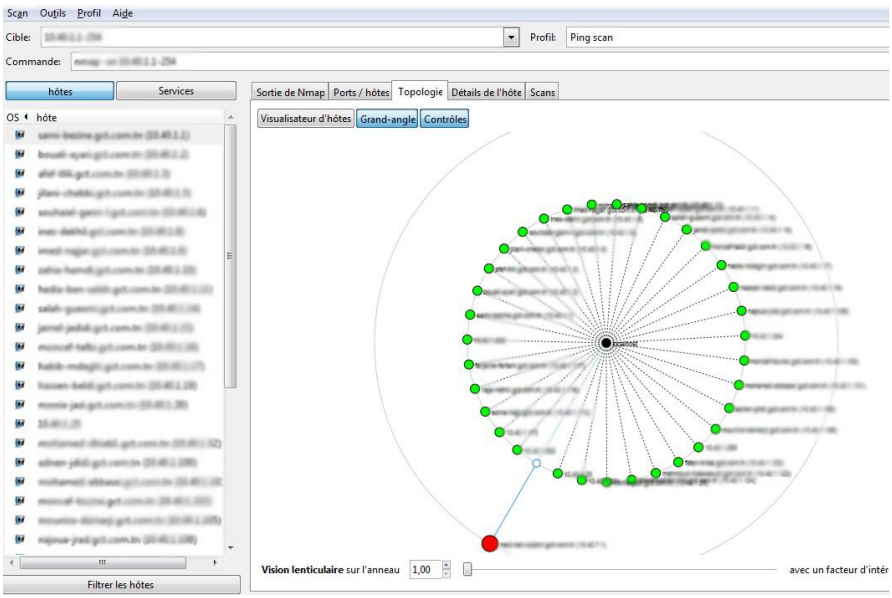

Figure 12. Découverte du réseau du LMD avec Nmap

Nous avons appliquer NMAP sur les serveurs et les équipements critiques et nous avons constaté qu'il existe des ports qui sont ouverts et non utilisés.

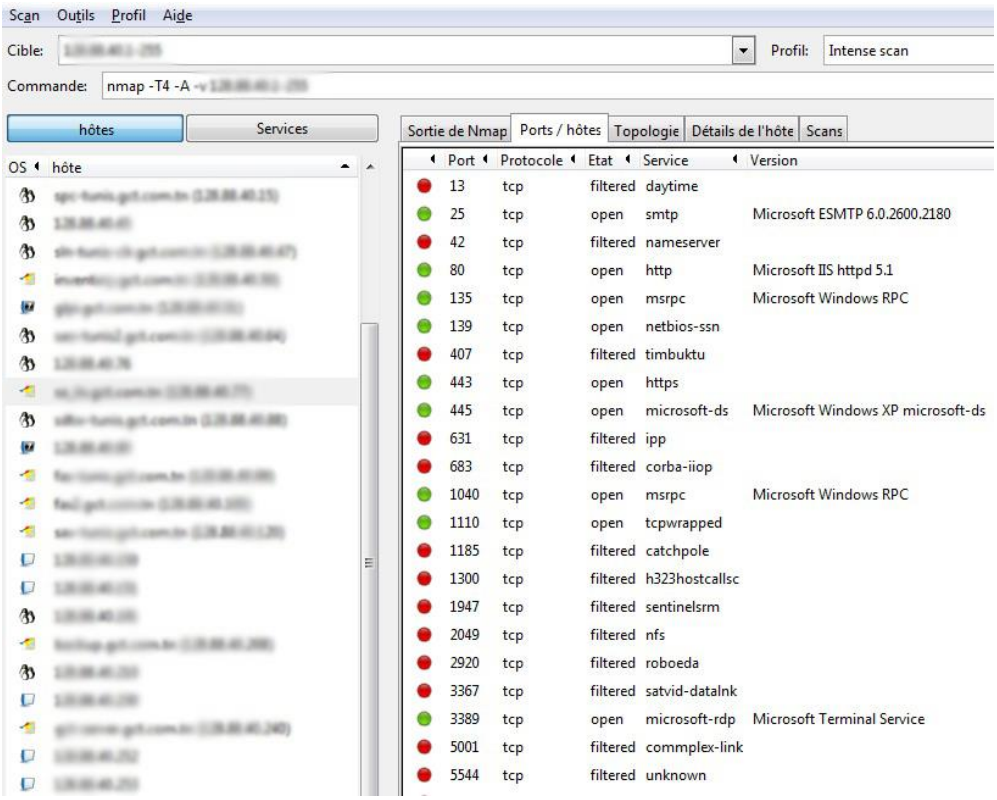

Figure 13. Capture des ports avec NMAP

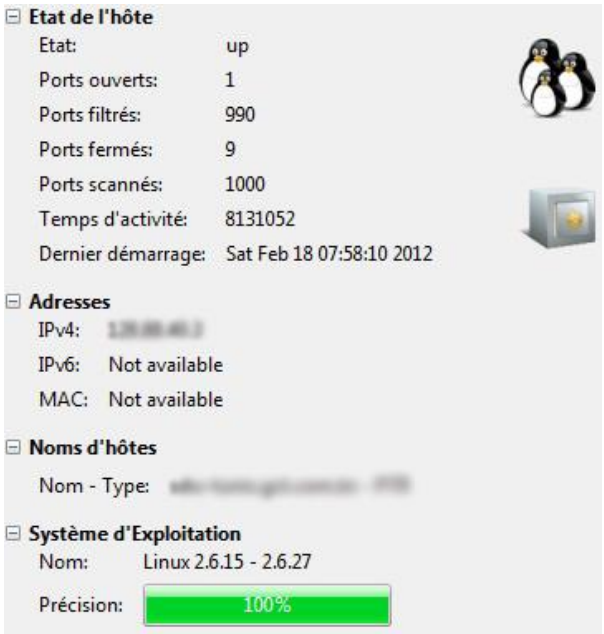

Figure 14. Détermination du système d'exploitation

I-2-2- Les services réseau :

Il s'agit de déterminer les services offerts par les serveurs et les postes de travail qui peuvent être une source de vulnérabilité. **[11]**

Le schéma suivant est donné par NetCrunch présentant les différents services réseau :

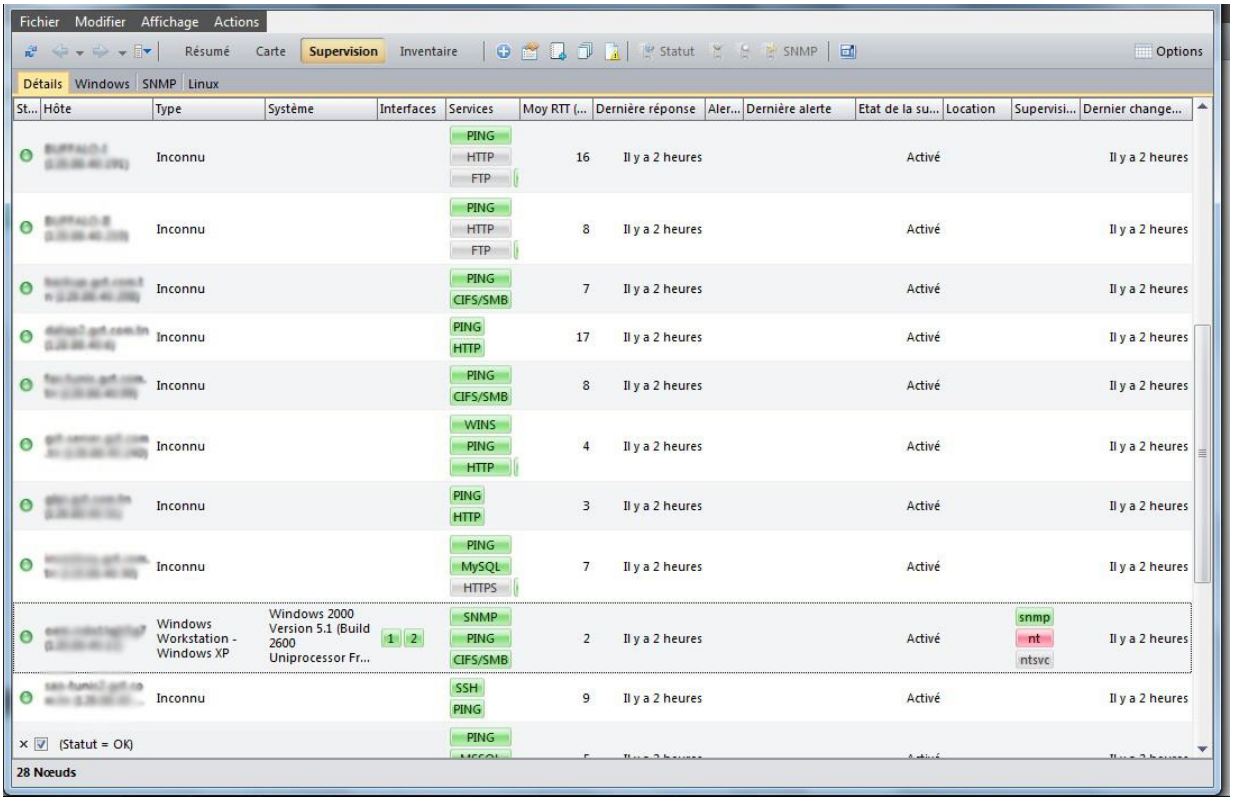

Figure 15. Capture des services avec NetCrunch

Nous avons identifié des services les plus occurrents sur le réseau et qui présentent des failles de sécurité :

HTTP (80/TDP), SSH (22/TCP), CIFS/SMB, DNS (53/TCP), MSSQL, SNMP (161/TCP), FTP (21/TCP), SMTP (25/TCP) ,Netbios-ssn (139/TCP), rpcbind (111/TCP), Microsoft-ds (445/TCP), tcpwrapped (514/TCP), msrpc (135/TCP), telnet (23/TCP).

Il existe également d'autres services, moins fréquents à savoir : X11 (6000/TCP), microsoft-rdp (3389/TCP), rusersd (32772/TCP), snmpXdmid (32778/TCP), finger (79/TCP), login (513/TCP), etc.

I-2-3- Sondage des flux réseaux :

Cette étape concerne l'analyse du trafic, l'identification des principaux flux, protocoles et applications, le taux d'utilisation ainsi que les flux inter-stations et les protocoles superflu.

Nous avons utilisé pour cela Wireshark **[12]** qui est un logiciel libre d'analyse de protocole, ou « packet sniffer », permet d'effectuer de capture sur le réseau ainsi qu'une analyse du trafic. La capture écran suivante représente l'interface d'interception des paquets de Wireshark :

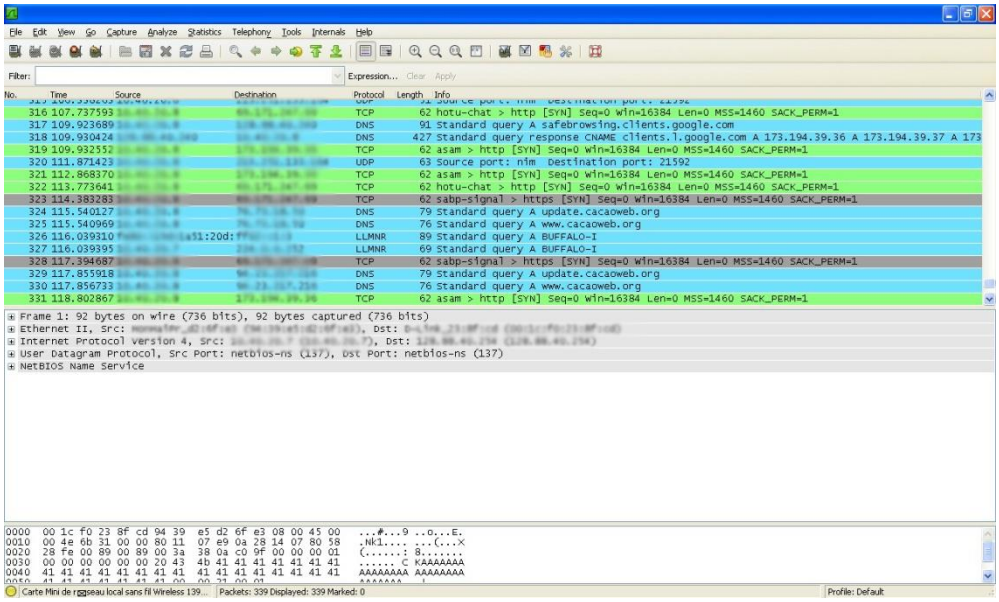

Figure 16. Capture des flux avec Wireshark

La figure suivante montre la hiérarchie des différents protocoles utilisés et leurs pourcentages :

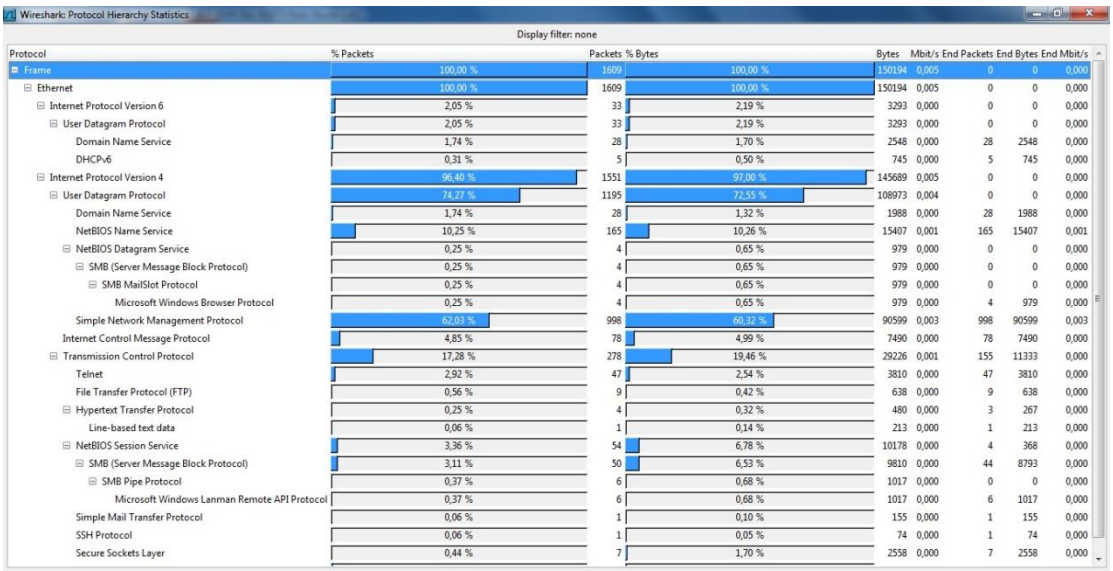

Figure 17. Pourcentage des paquets par protocole

Une première analyse du trafic permet d'identifier l'existence de plusieurs protocoles actifs superflus qui génèrent des informations gratuites et qui pourraient être exploitées par des personnes malintentionnées pour mener des attaques. Les protocoles identifiés sont les suivants :

- Cisco Discovery Protocol (CDP) : Il est utilisé pour obtenir des adresses des périphériques voisins et découvrir leur plate-forme, il utilise le protocole SNMP. CDP peut aussi être utilisé pour voir des informations sur les interfaces qu'un routeur utilise. Ces données peuvent être exploitées dans la recherche des vulnérabilités du routeur et mener des attaques.
- Internetwork Packet eXchange (IPX) : il est employé pour transférer l'information sur des réseaux qui fonctionnent avec le système d'exploitation NetWare.
- Spanning Tree Protocol (STP) : il permet d'apporter une solution à la suppression des boucles dans les réseaux pontés et par extension dans les VLANs.

I-2-4- Le sondage des systèmes :

A cette étape, nous avons utilisé le logiciel Look@Lan **[13]** qui est un logiciel scanneur et moniteur de réseau. Pour chaque adresse qui répond, le logiciel affiche le statut, le système d'exploitation (Windows/nonWindows), le hostname et le nom NETBIOS.

Les systèmes d'exploitation installés sont de majorité Windows (69%) comprenant :

- Windows XP Professionnel SP2 ou SP3, windows 2000, 2000 SP4.
- Windows Server 2003 SP1 ou SP2.

Les 31% restants sont Linux comprenant :

- Linux Kernel 2.6
- Solaris 10
- Free BSD 5.1 ou 5.2

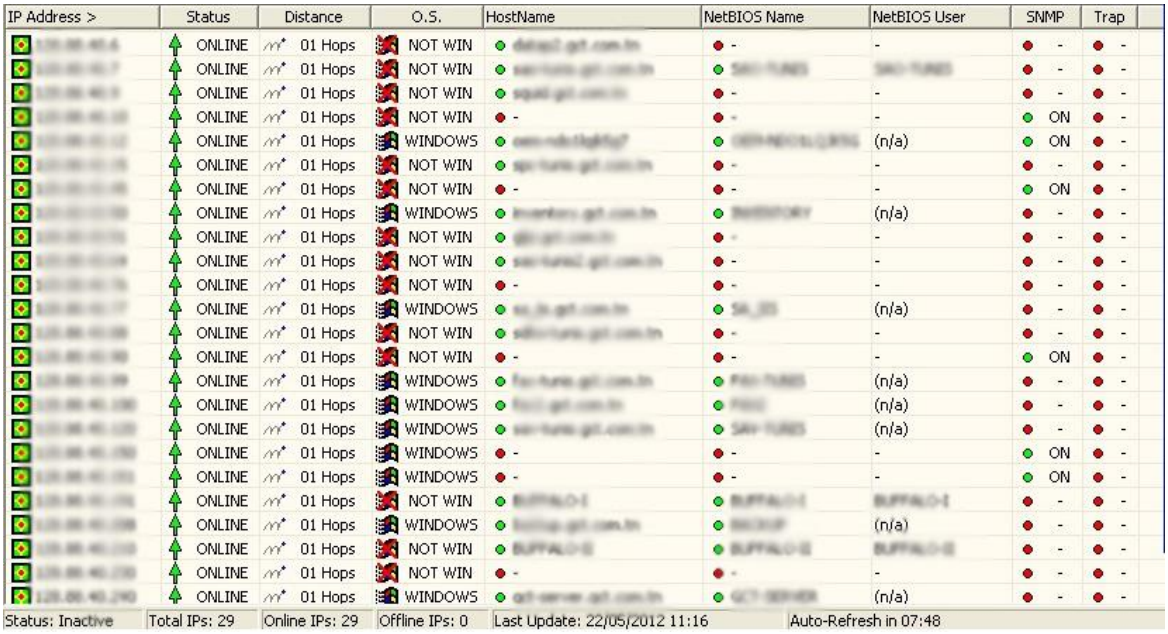

Figure 18. Exploration du réseau local du LMD

Comme indique la figure au-dessous :

- L'utilisation du NETBIOS est de l'ordre de 62% du flux réseau.
- L'utilisation du protocole SNMP est de l'ordre de 28% du flux réseau.

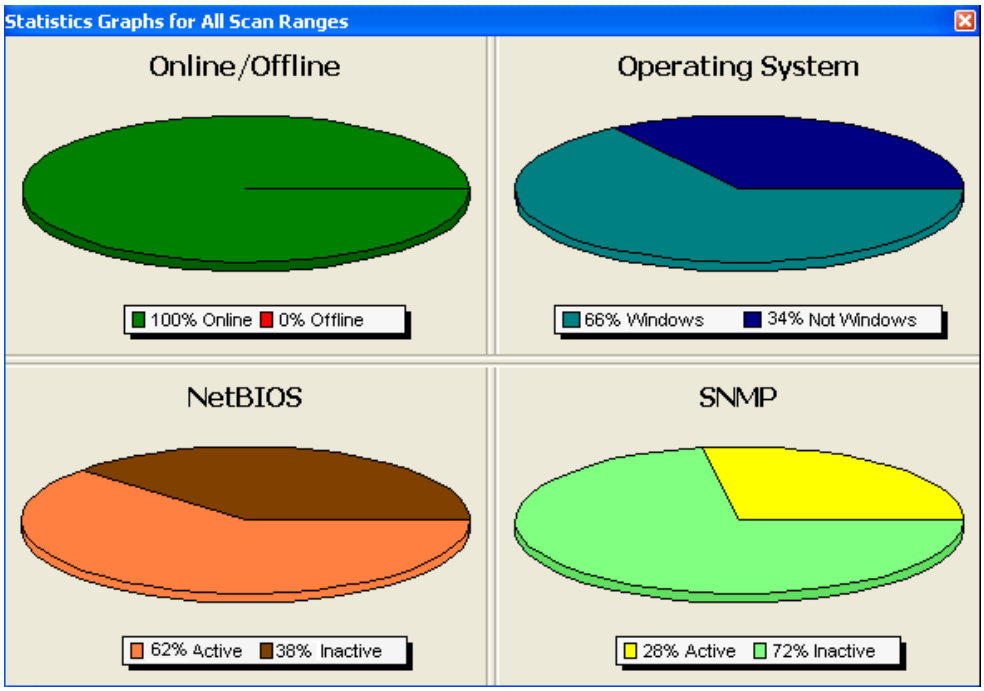

Figure 19. Statistique du scan avec Look@lan

II- Analyse des vulnérabilités :

Cette analyse permet de mesurer les vulnérabilités des parties les plus sensibles du réseau local, permettant de dégager rapidement les failles réellement dangereuses et de dégager à partir des outils, des rapports efficaces et exploitables pour une sécurisation rapide et efficaces du système.

II-1- Analyse des vulnérabilités des serveurs en exploitation :

L'outil Nessus fonctionne suivant l'architecture client-serveur. Ainsi le client paramètre le scanne et c'est le serveur qui se charge de la tache de scanne. Avant chaque opération de scanne, l'outil Nmap est exécuté par Nessus pour déterminer les ports en écoute et service en exécution. Par la suite, grâce à un ensemble de plugins, il passe à l'identification des applications en exécution sur chaque machine cible. Les informations récupérées de la machine cible sont comparées avec la base de vulnérabilité que possède Nessus, pour ensuite données ses conclusions. Le résultat de ce scanne est présenté sous forme de rapport (en page Html) qui contient une description des vulnérabilités déceler de façon à les corriger. **[14]**

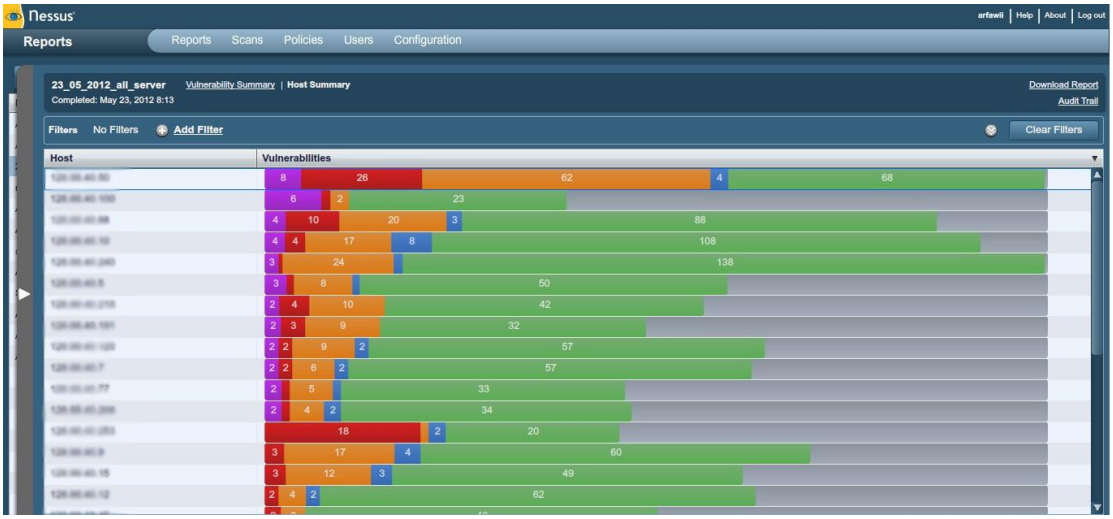

Figure 20. Vulnérabilités (Nessus)

II-1-1- Serveur Squid/IPtable :

Services (port)	Vulnérabilités		
	Gravité élevée	Gravité moyenne	Gravité faible
HTTPS (443/ TCP)		**Description de Synopsis** : Le certificat SSL pour ce service ne peut pas faire confiance. **Description :** Le certificat X.509 de l'hôte n'est pas signé par une autorité de certification publique. Cela est cible d'une attaque man in the middle. **Solution** : Acheter ou générer un certificat approprié pour ce service	
SSH (21/TCP)		**Description :** Le démon SSH supporte les connexions établies avec la version 1.33 et / ou 1.5 du protocole SSH. Ces protocoles ne sont pas complètement cryptographiquement sûrs, pour cela ils ne doivent pas être utilisés **Solution** : Désactiver la compatibilité avec la version 1 du protocole.	
Ndmp (10000/TCP)		**Description de Synopsis** : Il est possible de déterminer quels sont les ports TCP ouverts. **Description :** Ce plugin est un scanner de port SYN "demi-ouvert". Il doit être assez rapide, même contre une cible pare-feu. Notez que les scanners SYN sont moins intrusifs que TCP (pleine de connexion) scanners contre les services cassés, mais ils pourraient tuer pare-feu mal configurés. Ils pourraient également laisser les connexions non fermées sur la cible à distance, si le réseau est chargé. **Solution :** Protégez votre cible avec un filtre IP.	

Tableau 14 . Vulnérabilités du Serveur Squid/IPtable

II-1-2- Serveur Active Directory :

Services (port)	Vulnérabilités	
	Gravité élevée	**Gravité moyenne**
Microsoft-ds (445/TCP)		**Description de Synopsis** : Il est possible d'obtenir l'hôte SID de l'hôte distant, sans informations d'identification. **Description :** En émulant l'appel à LsaQueryInformationPolicy (), il était possible d'obtenir de l'hôte (Security Identifier) SID, sans informations d'identification. L'hôte SID peut ensuite être utilisé pour obtenir la liste des utilisateurs locaux. **Solution :** Vous pouvez empêcher les recherches anonymes de l'hôte SID en définissant le paramètre "RestrictAnonymous" à une valeur appropriée.
LDAPS (636/TCP)		**Description de Synopsis :** certificat SSL du serveur distant a déjà expiré. **Description :** Ce script vérifie les dates d'expiration des certificats associés à des services SSL sur la cible et des rapports si un est déjà expiré. **Solution :** Acheter ou de générer un nouveau certificat SSL pour remplacer celui existant.

FTP (21/CP)		**Description de Synopsis :** Les connexions anonymes sont autorisées sur le serveur FTP distant. **Description :** Ce service FTP permet les connexions anonymes. N'importe quel utilisateur distant peut se connecter et s'authentifier sans fournir un mot de passe ou des informations d'identification uniques. Cela permet à un utilisateur d'accéder à tous les fichiers mis à disposition sur le serveur FTP. **Solution :** Désactiver FTP anonyme si elle n'est pas nécessaire. Vérifiez régulièrement le serveur FTP afin d'assurer le contenu sensible n'est pas disponible
Domain (53/UDP)		**Description de Synopsis :** Le serveur DNS distant est vulnérable aux attaques snooping cache. **Description :** Le serveur distant DNS répond aux requêtes pour les domaines tiers qui n'ont pas le bit de récursivité. Cela peut permettre à un attaquant distant afin de déterminer quels domaines ont été récemment résolus par ce serveur de noms, et donc les hôtes qui ont été récemment visités. encore. **Remarque :** S'il s'agit d'un serveur DNS interne pas accessible à des réseaux extérieurs, les attaques seraient limitées au réseau interne. Cela peut inclure des employés, des consultants et, éventuellement, les utilisateurs sur un réseau invité ou connexion WiFi si pris en charge. **Solution :** Contactez le vendeur du logiciel DNS pour un correctif.

Tableau 15. Vulnérabilités du Serveur Active Directory

III-Audit de l'architecture de sécurité existante :

L'objectif est ici d'expertiser l'architecture technique déployée et de mesurer la conformité des configurations équipements réseaux, pare-feu, commutateur, etc. avec la politique de sécurité définie et les règles de l'art en la matière.

III-1- Audit de Firewall et des règles de filtrages :

Cette étape consiste à déterminer si le firewall fonctionne correctement. Le rôle du firewall consiste à contrôler l'accès selon une politique spécifique adapté.

La démarche adoptée consiste à auditer le firewall, les règles de filtrage et des mécanismes de log. Le firewall utilisé est IPtables.

Lors d'une réunion avec le responsable réseau, nous avons pu déterminer les vulnérabilités suivantes du firewall :

- Le firewall n'a pas la capacité d'avoir des logs sécurisés et d'être envoyé/ enregistré sur un système à distance automatiquement (périphérique enregistrant),
- Absence d'un serveur de log dédié au traitement et à l'archivage des logs du Firewall,
- Absence des statistiques sur l'usage du Firewall,
- Le firewall ne contient pas des outils pour l'analyse des fichiers de log et la production des rapports,
- Absence d'une vérification des derniers patchs et mises à jour,
- Absence d'une procédure de test périodique des vulnérabilités du Firewall ainsi que des essais de test de pénétration pour vérifier la résistance du système contre les attaques,
- Absence d'un rapport d'audit à long terme présentant l'historique des incidents survenus au niveau du firewall (violation des ACLS, crash par débordement du tampon),
- Absence d'un document ou une spécification des règles de filtrage (ACLs) précisant la politique de sécurité implantée (description de l'utilité de chaque filtre/règle),
- Le contrôle d'intégrité du FW n'est pas entièrement automatisé,
- Absence d'un document précisant la configuration du Firewall et le suivi des modifications de cette configuration,
- Absence d'un secours automatique pour le firewall.

III-2- Audit de serveur de mise à jour antivirus :

La politique antivirale est mise en place par un serveur antivirus pour le réseau local, l'installation et la mise à jour se fait automatique via ce serveur. L'antivirus utilisé est Kaspersky.

- L'antivirus possède une console Web protégée par un nom utilisateur et mot de passe.
- La mise à jour de tous les postes est centralisée au niveau du serveur.
- La console d'administration permet de réaliser des rapports et des statistiques et fournit des alertes concernant les infections virales chez les utilisateurs fournissant ainsi des informations telles que le nom de l'hôte, la date et l'heure de l'infection, le fichier suspect, le nom du virus ainsi que le comportement face à cette menace (suppression, mise en quarantaine)

Suite à une réunion avec le responsable de serveur antivirus nous avons constaté :

- Absence d'une charte d'utilisation et d'un plan de sensibilisation des utilisateurs,
- Absence d'une procédure antivirale,
- Absence d'une politique de lutte antivirale,
- Absence d'outils de filtrage amont pour prévenir les infections virales,
- Les utilisateurs ne sont pas responsabilisés et éduqués vis-à-vis de l'usage de la messagerie,
- Absence de sensibilisation des utilisateurs concernant l'utilisation des médias amovibles (Clé USB, disque dur externe,…).

III-3- Audit de la politique d'usage de mots de passe :

Les méthodes d'authentification utilisées sont les mots de passe au niveau postes de travail et serveurs.

Nous remarquons concernant la politique d'usage de mot de passe :

- Pour les serveurs et tous les autres équipements réseau les mots de passe sont robustes de point de vue nombre de caractère et la combinaison de minuscules et majuscules, de chiffres, de lettres et de caractères spéciaux,

- Au niveau poste de travail, chaque utilisateur est responsable de la définition de son mot de passe,
- Certains mots de passe (aux niveaux des postes, des serveurs et des équipements réseaux et sécurité) ressemblent aux noms des utilisateurs ou sont trop courts (inférieur à 10 caractères), ce ne sont pas de bonnes pratiques de sécurité,
- L'absence d'une sensibilisation des utilisateurs et de la mise en place d'une procédure de contrôle a priori,
- Absence d'une charte d'utilisation qui spécifie aux utilisateurs leurs obligations de protection de leurs postes,
- Absence d'une politique qui définit notamment quelle est la typologie de mots de passe autorisés, la longueur des mots de passe, les délais d'expiration, la technique de génération, l'occurrence d'utilisation des mots de passe, etc.

Conclusion :

Au cours de cette étape, nous avons essayé de déceler certaines vulnérabilités au niveau réseau et applications en analysant les différents flux et les politiques de sécurité adoptés par les équipements réseau.

Il s'agit maintenant de proposer des recommandations et des actions à suivre pour remédier à ces faiblesses.

Chapitre V. Recommandations

Introduction :

Ce chapitre a pour but de proposer des recommandations par rapport aux différentes clauses des normes de sécurité, ces recommandations seront divisées en deux grandes parties : les recommandations organisationnelles et physiques, ensuite les recommandations techniques. Egalement, au vu des vulnérabilités constatées lors du chapitre précédent, nous allons proposer une nouvelle architecture réseau.

I- Recommandations d'ordre organisationnel et physique :

Les recommandations suivantes visent à apporter des suggestions pour améliorer l'aspect organisationnel et physique de la sécurité du réseau du LMD.

I-1- Définir et documenter une politique de sécurité :

Le côté formel d'une politique de sécurité devient de plus en plus exigé pour tout organisme intéressé à la sécurité de son SI, c'est pourquoi il est nécessaire que cette politique soit documentée et à la portée de tout le monde en question. Ces étapes permettent d'atteindre cet objectif. Il s'agit de :

- Rédiger une politique de sécurité qui définit clairement les objectifs en termes de sécurité du site,
- Définir des procédures documentées de : mise à jour automatique, gestion des incidents de sécurité, sauvegarde automatique, gestion de la continuité, gestion de l'authentification des utilisateurs du réseau, gestion des supports …

I-2- Classifier les ressources :

Pour faciliter la gestion des ressources et des dangers qui menacent leur utilisation, il est fortement recommandé de :

- Rédiger pour chaque équipement réseau une charte d'utilisation qui décrit comment exploiter cet équipement d'une manière sécurisée, que faut-il faire en cas de panne, et à qui faut-il s'adresser en cas de problème.
- Définir une classification des informations sensibles de l'organisation. Cette classification doit être basée sur les 3 axes correspondant aux besoins en termes de Disponibilité, Intégrité et Confidentialité pour pouvoir lui attribuer le niveau de protection nécessaire.

I-3- Définir une charte de confidentialité :

L'utilisation des ressources du SI peut engendrer des effets négatifs sur sa robustesse envers les failles de sécurité pour palier à ce problème, nous recommandons de :

- Diffuser à l'ensemble du personnel ayant accès au SI une charte de sécurité d'utilisation de la messagerie et de l'Internet et contrôler le respect de cette charte,
- Fournir des documents à signer concernant les bonnes pratiques et les responsabilités,
- Inclure l'accord de confidentialité dans le contrat de chaque utilisateur, contractuel et stagiaire. Les nouveaux utilisateurs du SI doivent être informés de la politique de sécurité de l'organisme dès leurs arrivées.

I-4- Spécifier et documenter les exigences réglementaires et légales :

Le respect des règlements définis à l'échelle nationale et internationale permet au SI d'atteindre un niveau de maturité. Il est indispensable de contrôler régulièrement l'application des lois internes par les utilisateurs et vérifier que les facilités offertes par le réseau local ne sont utilisées que pour le bien de l'organisme.

De même il faut revoir la conformité du SI aux différentes lois et normes qui définissent les critères de sécurité et prendre les mesures nécessaires pour la garantir.

I-5- Désigner et réorganiser les responsabilités :

Le LMD ne possède pas un comité de sécurité groupant des directeurs de différents services.

Organiser les responsabilités vis-à-vis de la sécurité permet d'assurer une implémentation appropriée des mesures de sécurité en rapport avec les objectifs de la société, et de pouvoir prévenir et anticiper les risques éventuels sur les systèmes de la société avec rapidité et efficacité, parmi les étapes à prendre pour garantir ceci :

- Désigner un comité qui aura pour mission le suivi de l'état de sécurité et de prendre les décisions nécessaires,
- Définir une organisation informatique formelle dotée de manuels, de guides de procédures, de politiques et des chartes d'utilisation,
- Définir les responsabilités (en termes de sécurité) de chaque utilisateur du SI et diffuser le document correspondant.

I-6- Faire de l'audit une pratique de base :

Les missions d'audit internes et externes permettent de savoir à quel niveau le SI est-il conforme aux exigences de la sécurité et quelles sont les mesures à prendre pour le sécuriser d'une façon efficace. Nous recommandons de planifier des audits internes et externes d'une manière régulière (au moins une fois par an), et ce-ci pour évaluer le niveau de sécurité de l'organisme et des procédures efficaces de traitement des risques.

En s'appuyant éventuellement sur l'avis d'un expert externe en sécurité dans les décisions importantes.

I-7- Sensibiliser et former périodiquement le personnel :

Les mesures prises pour sécuriser le SI ne peuvent être efficaces que si l'ensemble du personnel soit conscient de l'importance de la sujette et capable de distinguer les bonnes pratique qui met le SI à l'abri de tout danger :

- Planifier des cycles de formation spécifiques et approfondis en sécurité pour tout le service informatique. Une fois formés, les informaticiens seront capables d'organiser des journées de sensibilisation pour le reste des utilisateurs du SI,
- Encourager les responsables du service informatique à consolider leurs connaissances et favoriser les programmes de formation et les cycles de certification,
- Sensibiliser et former le personnel aux menaces dues aux éventuelles intrusions au système d'information et à l'importance de la sécurité,

- Sensibiliser le personnel aux éventuelles manipulations qui menacent la sécurité du système d'information.

I-8- Protéger les ressources et les actifs :

La protection physique des ressources est un des principaux enjeux de la sécurité nous recommandons :

- S'assurer que les actifs les plus critiques sont à l'abri de tout danger : fuite d'eau humidité, chocs électriques…,
- Les supports contenant les sauvegardes de secours doivent être fortement protégées dans des armoires anti-feu par exemple et ne doivent pas être dans le même endroit qui abrite la version originale.

I-9- Contrôler l'abandon et la destruction des supports :

L'abandon des supports physiques et logiques ne subit aucun contrôle. Il est fortement recommandé de définir une politique de destruction des équipements les plus sensibles et d'abondons des supports contenant des informations sensibles.

Pour s'assurer que les informations critiques ne seront pas divulguées, on recommande d'acquérir un équipement de démagnétisation pour détruire définitivement des anciens disques durs.

I-10- Garantir la disponibilité de l'énergie :

Parmi les points faibles dégagés pendant notre mission on doit citer l'absence de mesures spécifiques pour garantir la disponibilité de l'énergie et particulièrement l'électricité hors la salle serveur. Ceci nous invite à recommander :

- La sécurisation de tous les équipements réseaux et les postes de travails des utilisateurs avec des onduleurs afin d'éviter l'endommagement du matériel informatique ou électrique, la perte de données non sauvegardées, la destruction de supports logiques surtout les disques durs,
- L'achat d'un groupe électrogène pour éviter les effets des coupures de courant qui dépassent 30 minutes.

II- Recommandations d'ordre technique :

Après avoir étudié les différentes vulnérabilités affectant le réseau et les systèmes, nous proposons au niveau de ce chapitre des recommandations à suivre à fin de faire face ou minimiser le risque.

II-1- Renforcer l'architecture du réseau LAN :

Une architecture fiable est la première clé de réussite pour un organisme et la garantie de la sécurité de son SI.

Pour améliorer l'architecture actuelle, nous recommandons ces mesures :

- Créer une zone DMZ pour protéger les actifs critiques,
- Sécuriser les accès distants entre les serveurs : authentification par certificat et utilisation d'un canal sécurisé de communication (SSH, IPsec),
- Créer une zone d'administration permettant aux responsables de contrôler le réseau facilement et en toute sécurité,
- Changer le Proxy/firewall existant par un autre qui intègre la fonctionnalité du Load-balancing.

II-2- Limiter les services réseaux disponibles :

Nous avons constaté que beaucoup de services inutiles ou peu sûrs sont activés sur les serveurs ou /et les postes des utilisateurs. Ceci expose le réseau à plusieurs types de dangers et il est indispensable de :

- Fermer les ports inutilisables sur tout équipement réseau,
- Désactiver le protocole SNMP au niveau des équipements réseaux afin d'empêcher les pirates de cartographier rapidement la topologie du réseau.

II-3- Définir des procédures de configuration des équipements réseaux :

Il est recommandé de développer des procédures de configuration sécurisée des différents équipements informatiques du **LMD**. Dans l'élaboration de ces procédures, le responsable

sécurité peut se référer aux règles de bonne pratique définie par les organismes internationaux spécialisés (ANSI, SANS Institute, CERT/CC, …). Ils devraient inclure nécessairement :

- Les règles de bonnes pratiques de configuration des systèmes (Windows2000, XP, 2000 Server et 2003 Server),
- Les règles de bonnes pratiques de configuration d'un Firewall,
- Les règles de bonnes pratiques de configuration des applications.

II-4- Renforcer de la solution antivirale :

La lutte antivirale est indispensable pour le bon fonctionnement et la robustesse du réseau et du SI. Parmi les mesures proposées :

- Définir et mettre en place une passerelle antivirale pour les accès web, cette passerelle peut être en hardware ou en software,
- Accélérer les mécanismes de déploiement de la procédure de lutte antivirale. Prévoir une procédure de sauvegarde sur un support externe pour le serveur antivirus,
- Installer une solution antivirale qui permet de supprimer automatiquement un virus lors de sa détection contrairement à celle qui existe, elle laisse le choix de l'action au client (supprimer, mettre en quarantaine, ignorer).

II-5- Sécuriser les équipements réseaux critiques :

Nous recommandons de revoir les configurations des équipements dorsaux de l'architecture réseau :

- Mettre à jour des versions des Firmware (tel que les IOS) des firewalls et Switch niveau 3,
- Définir des ACL et les mettre à jour sur ces équipements.
- Mettre en place une solution de duplication pour ces équipements.

II-6- Consolider la protection contre les attaques internes :

Les attaques auxquels le réseau peut être exposé ne viennent pas seulement de l'extérieur mais aussi des entités ou des utilisateurs internes. Nous recommandons ces mesures concernant ces équipements :

- Mettre en place une solution de protection logique qui inclut un Pare-feu applicatif
- Prévenir des intrusions et le renforcement des politiques de sécurité : revoir les ACL des différents composants et les définir en cas de besoin (comme c'est le cas pour le Switch N3).

II-7- Recommandations système :

Nous avons constaté que les vulnérabilités recensées étaient liées au fait que des mises à jour software n'étaient pas constamment tenues. C'est pourquoi nous invitons les administrateurs réseau du LMD à visiter le site web de Microsoft, qui propose des mises à jour pour les corrections des failles découvertes. Il s'agit de l'adresse : http://www.microsoft.com/tecnet/security/bulletin/.

II-8- Améliorer la méthodologie d'administration :

Durant notre mission, nous avons constaté que la méthodologie d'administration n'est pas assez souple et que les tâches sont parfois assez lourdes à gérer. De même la communication avec les utilisateurs est aussi à revoir en procédant ainsi :

- Pour les ressources critiques (serveurs par exemple) utiliser la stratégie « restreindre tout » puis donner l'accès seulement qu'à celui qui le mérite,
- Normaliser et standardiser les postes de travail,
- Lutter contre l'abus de droits : installation des clients P2P, streaming …,
- Intégrer des solutions de contrôle des applications installées sur les postes utilisateurs.

II-9- Mettre en place une procédure formalisée pour la gestion des utilisateurs :

Il est clair que la gestion des utilisateurs au sein du LMD n'est pas encore formalisée, il est nécessaire de définir une méthodologie pour la standardiser. Nous recommandons de

synthétiser un document décrivant les droits d'accès et qui soit installé pour les différents systèmes de la société. Par conséquent, il faudrait formaliser au minimum les procédures suivantes :

- La création d'un nouvel utilisateur sur les systèmes d'exploitation et les applications,
- La modification d'un profil utilisateur (suite à un changement d'affectation).
- La gestion de l'identification de l'utilisateur,
- Le départ d'un utilisateur (démission, départ en congé ou à la retraite),
- La revue ou l'audit de la sécurité logique (systèmes et applications).

La réussite d'une telle étape permettra de s'assurer que le paramétrage de la sécurité logique tel qu'il a été défini est conforme aux droits que devraient avoir les utilisateurs.

II-10- Renforcer les mesures d'authentification :

Il faut déterminer une stratégie d'authentification plus efficace et plus évoluée. Ceci nécessite une révision qui passe par les points suivants :

- Contrôler la gestion des mots de passe (ce qui n'est pas encore le cas),
- Définition d'une politique stricte d'expiration automatique des mots de passe non renouvelés,
- Contrôler la qualité des mots de passe,
- Définir des mots de passe pour le bios en cas de besoin,
- Les applications sensibles doivent être protégées par un fort mécanisme d'authentification.

II-11- Mettre en place une plateforme de support technique :

Mettre en place une plateforme de support technique permettant de gérer les requêtes des utilisateurs de façon plus efficace : support technique, dépannage, améliorations …

Une telle solution assurera :

- Le classement des requêtes.
- L'adhésion à une démarche et à un processus clair lors de leur traitement.
- Le suivi de toutes les actions en cours.
- Avoir des statistiques concernant les différents problèmes, leurs sources et les solutions possibles.

III-Solution proposée:

Dans le but d'avoir une architecture réseau plus robuste, nous proposons une solution qui permet de garantir la continuité de service, le partage de charge ainsi que la sécurité du trafic réseau.

III-1- Zone DMZ :

Lorsque certaines machines du réseau interne ont besoin d'être accessibles de l'extérieur, il est souvent nécessaire de créer une nouvelle interface vers un réseau à part, accessible aussi bien du réseau interne que de l'extérieur.

Une séparation du réseau interne, à protéger, des services non sensibles, public, accessible de l'extérieur et susceptibles d'être attaqués (Serveur Messagerie, Serveur Public,...).

III-2- Détection et prévention d'intrusion :

La mise en place d'un contrôle d'accès (FW, Proxy) ne permet pas de répondre à toutes actions frauduleuses. En effet les systèmes d'exploitations ainsi que les applications publiques ou internes, peuvent faire l'objet d'attaques (interne ou externe), ces attaques peuvent être sous forme de :

- Tentatives d'accès non autorisés,
- D'un envoi des requêtes erronées par le réseau,
- D'un débordement de pile d'une application, etc.

Ces problèmes de sécurité peuvent être minimisés en utilisant un système de détection et de prévention d'attaques et d'intrusions en temps réel (IPS). Son fonctionnement est basé sur la reconnaissance de signatures d'attaques, via les techniques suivantes :

- Comparaisons d'expression ou de code,
- Fréquence et seuil d'apparition d'un événement,
- Corrélations de différents événements,
- Anomalie statistique.

La mise en place de l'IPS sera entre le FW et la DMZ serveurs.

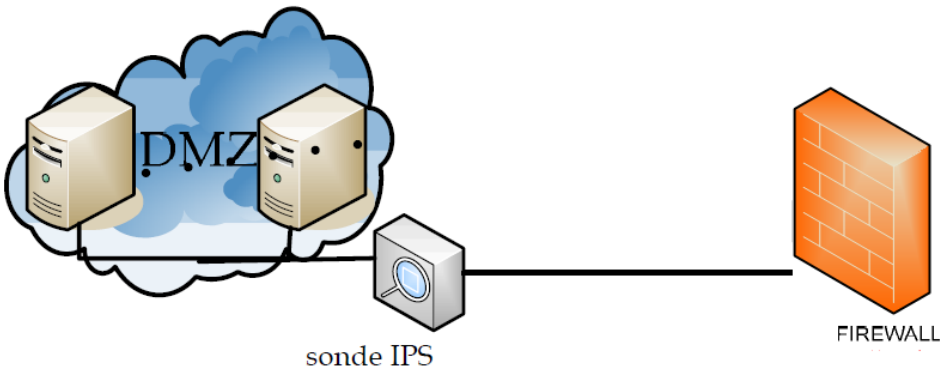

Figure 21. Intégration de la sonde IPS

III-3- Architecture réseau proposée:

Le schéma suivant présente la solution finale de l'architecture que nous proposons.

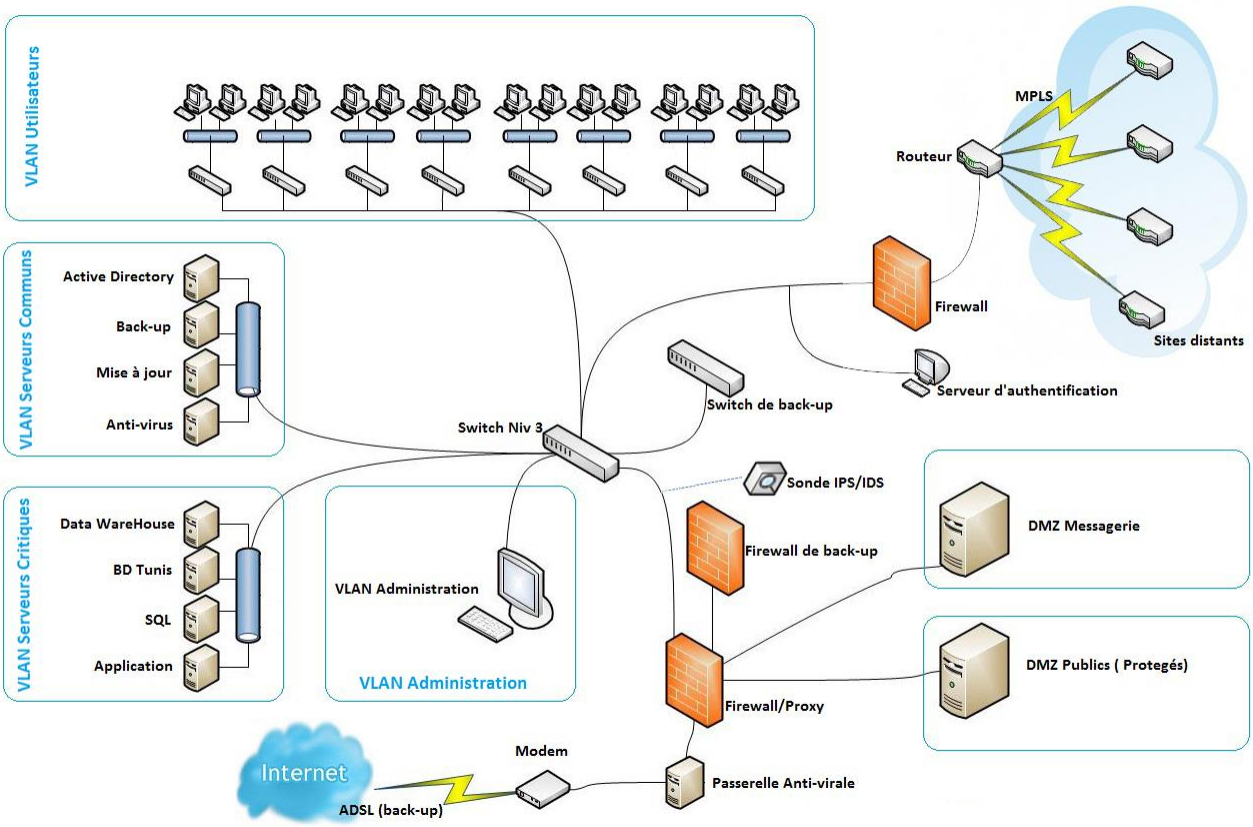

Figure 22. Solution proposée de l'architecture

La mise en place de notre solution se base sur les préalables suivants :

- **Séparer les lignes de connexion à internet et de connexion des sites distants :** Dédier la ligne MPLS à la connexion des sites distants et la ligne ADSL à la connexion à l'internet.
- **Mise en place de deux DMZs :** la première inclut les serveurs de messageries, la deuxième inclut les serveurs publics projetés
- **Création d'une zone d'administration :** l'évolution de la méthodologie d'administration nécessite l'existence d'une telle zone permettant aux administrateurs d'avoir une vue sur la totalité du réseau tout en étant isolé.
- **Passerelle antivirus :** le volume de trafic entrant et sortant du réseau via la connexion Internet mérite plus de prudence pour éviter les différents types d'attaques et la propagation des virus et des spywares. Une passerelle antivirus sera la première interface de lutte contre ces dangers. Cette passerelle peut être de type hardware ou software.
- **Ajout d'un serveur de mise à jour** : ce serveur va assurer la mise à jour des patchs systèmes.
- **Ajout d'un serveur d'authentification** : Assurer l'authentification des sites distants.
- **Segmenter le réseau en des sous-réseaux par des VLAN :**
  - VLAN1 : réservé aux serveurs communs.
  - VLAN2 : réservé aux serveurs critiques et stratégiques
  - VLAN3 : réservé aux postes d'administration des serveurs et d'autres équipements réseau ou de sécurité.
  - Les postes des travails doivent être aussi segmentés suivant les départements.

Conclusion :

Dans cette partie, en premier lieu, nous avons proposé des recommandations que nous jugeons nécessaires à mettre en œuvre pour améliorer la sécurité du réseau du LMD en se basant sur la norme 27002 : 2005.

En deuxième lieu nous avons proposé des recommandations sur le plan technique à fin de minimiser le risque d'exposition aux attaques et d'exploitation des vulnérabilités du réseau et de protéger les différents équipements pour assurer la continuité et la disponibilité du réseau. Enfin nous avons proposé des améliorations de l'architecture réseau.

Conclusion Générale

L'audit de sécurité des systèmes d'information occupe une place de plus en plus importante depuis la promulgation de décret N°1249 et 1250 de mai 2004. C'est dans ce contexte que s'inscrit notre projet qui vise l'audit de la sécurité du système d'information du Le Moteur Diesel (LMD).

Notre mission s'articule sur la norme ISO 27002 qui est notre référentiel d'audit. Elle s'est réalisée sur deux parties, la première partie est l'audit organisationnel et physique qui est achevée par l'estimation du risque inspirée de la méthodologie MEHARI. La deuxième partie est l'audit technique qui représente un diagnostic des vulnérabilités de l'architecture réseau et de ses composants.

Nous avons par la suite proposé des recommandations nécessaires à mettre en œuvre pour améliorer la sécurité du réseau du LMD ainsi qu'une architecture réseau plus robuste.

A travers ce projet, nous avons pu travailler avec des outils du monde libre qui sont destinés au recensement des failles et des vulnérabilités et leurs exploits sur système audité, qu'il soit en Unix ou Microsoft.

La mission que nous avons effectuée durant ce projet nous a été très enrichissante du fait qu'elle nous a permis d'acquérir de nouvelles connaissances aussi bien théoriques que pratiques et qui nous seront bien précieuses et d'un grand apport pour de futures activités professionnelles. Elles viennent s'ajouter à notre formation acquise au sein de l'Université Virtuelle de Tunis (UVT).

Bibliographie et Webographie

BIBLIOGRAPHIE

- Sécurité informatique Principes et méthode à l'usage des DSI, RSSI et administrateurs (2édition), Laurent Bloch Christophe Wolfhugel.
- INFORMATION TECHNOLOGY AUDITING and ASSURANCE (third edition), James A. Hall, Lehigh University.
- Menaces sur le réseau (sécurité informatique : guide pratique des attaques passives et indirects), Michal Zalewski.

WEBOGRAPHIE

[1] Site officiel du GCT : http://www.gct.com.tn

[2] Les normes ISO 27000 : www.iso27001security.com

[3] Portail de l'ANSI : http://www.ansi.tn

[4] Portail de l'ANSSI : www.ssi.gouv.fr/fr/bonnes-pratiques/

[5] Portail web de la méthode COBIT : http://pages.infinit.net/labo/corbit.htm

[6] Portail web de la méthode CRAMM : http://www.cramm.com/

[7]Ressources de la méthode Ebios : http://www.ssi.gouv.fr/fr/confiance/ebiospresentation.html

[8] Méthode MEHARI sur le site de CLUSIF : https://www.clusif.asso.fr/fr/production/mehari/

[9] Site de l'outil Networkview : www.networkview.com/

[10] Site de l'outil Nmap : http://nmap.org/

[11] site de l'outil NetCrunch : http://www.adremsoft.com/netcrunch/

[12] site de l'outil wireshark *http://www.wireshark.org/*

[13] site de l'outil LOOK@LAN *http:/ www.lookatlan.com/*

[14] Site de l'outil Nessus : www.nessus.org/

Liste des acronymes

ACL	:	**Access control list**
ADSL	:	**Asynchronus Digital Subscriber Line**
ANSI	:	**Agence nationale de la sécurité informatique**
BD	:	**Base de Données**
CCTA	:	**Central Computer and Telecommunications Agency**
CDP	:	**Cisco Discovery Protocol**
CIFS	:	**Common Internet File System**
CLUSIF	:	**Club de la Sécurité des Systèmes d'Information Français**
COBIT	:	**Control Objectives for Information and related Technology**
CRAMM	:	**Risk Analysis and Management Method**
DAP	:	**Di Ammonium Phosphate**
DCP	:	**Di Calcium Phosphaté**
DCSSI	:	**Direction Centrale de la Sécurité des Systèmes d'Information**
DMZ	:	**DeMilitarized Zone**
DNS	:	**Domain Name System**
EBIOS	:	**Expression des Besoins et Identification des Objectifs de Sécurité**
FTP	:	**File Transfer Protocol**
HTTP	:	**HyperText Transfer Protocol**
HTTPS	:	**HyperText Transfer Protocol Secure**
IDS	:	**Intrusion Detection System**
IPS	:	**Intrusion Prevention System**
IEC	:	**International Electrotechnical Commission**
ISO	:	**International Standard Organisation**
ISMS	:	**Information Security Management System**
LAN	:	**Local Area Network**
LMD	:	**Le Moteur Diesel**
LS	:	**Ligne Spécialisée**
MEHARI	:	**Méthode Harmonisée d'Analyse de Risques**
RSSI	:	**Responsable de la Sécurité des Systèmes d'Information**
SACA	:	**Information Systems Audit and Control Association**
SI	:	**Système d'Information**
SIC	:	**Systèmes d'Informations et de Communications**

SMB	**:**	**Server Message Block**
SMTP	**:**	**Simple Mail Transfer Protocol**
SNMP	**:**	**Simple Network Management Protocol**
STP	**:**	**Spanning Tree Protocol**
TCP	**:**	**Transmission Control Protocol**
TSP	**:**	**Triple SuperPhosphate**
VLAN	**:**	**Virtual Local Area Network**
WAN	**:**	**Wide Area Network**

ANNEXE

Annexe A

Domaine : Sécurité applicative (09)			
Service A : Contrôle d'accès applicatif **Sous service A01 : Gestion des profils d'accès aux données applicatives**			
Question N°	**Question**	**Rép.**	**P**
09A01-01	A-t-on établi une politique de gestion des droits d'accès aux données et à l'information s'appuyant sur une analyse préalable des exigences de sécurité, basées sur les enjeux business?	1	2
09A01-02	Les droits d'accès aux différentes applications et données applicatives sont-elles définies par rapport à des "profils" métiers regroupant des "rôles" ou des "fonctions" dans l'organisation (un profil définissant les droits dont disposent les titulaires de ce profil) ? Nota : La notion de profil peut, dans certaines circonstances, être remplacée par une notion de "groupe".	1	4
09A01-03	Est-il possible d'introduire, dans les règles de définition des droits (qui déterminent les droits attribués à un profil), des paramètres variables en fonction du contexte tels que la localisation du demandeur ou les réseaux utilisés, ou fonction des moyens employés (protocoles, chiffrement, etc.) ou de la classification des ressources accédées ?	0	4
09A01-04	Les profils permettent-ils également de définir des créneaux horaires et calendaires de travail (heures début et fin de journée, week-end, vacances, etc.) ?	1	2
09A01-05	Ces profils et l'attribution de droits aux différents profils ont-ils reçu l'approbation des propriétaires d'information et/ou du RSSI ?	1	4

$$\textit{Qualité du service} = 4 * \sum Ri\ Pi / \sum Pi$$

Et par suite, on obtient comme résultat une valeur de qualité de service = **4* 12/16 = 3**

Annexe B

Score ISO 27002 : 2013						
5	**Politique de sécurité**					**0%**
	5.1	**Politique de sécurité de l'information**			0%	
		5.1.1	Document de politique de sécurité de l'information	0,0		
		5.1.2	Réexamen de la politique de sécurité de l'information	0,0		
6	**Organisation de la sécurité de l'information**					**33.3%**
	6.1	**Organisation interne**			33.3%	
		6.1.1	Engagement de la direction vis-à-vis de la sécurité de l'information	0,0		
		6.1.2	Coordination de la sécurité de l'information	4,0		
		6.1.3	Attribution des responsabilités en matière de sécurité de l'information	0,0		
		6.1.4	Système d'autorisation concernant les moyens de traitement de l'information	2.66		
		6.1.5	Engagement de confidentialité	0,0		
7	**Gestion des biens**					**71.87%**
	7.1	**Responsabilités relatives aux biens**			100%	
		7.1.1	Inventaire des biens	4,0		
		7.1.2	Propriété des biens	4,0		
		7.1.3	Utilisation correcte des biens	4,0		
	7.2	**Classification des informations**			43.75	
		7.2.1	Lignes directrices pour la classification	1,0		
		7.2.2	Marquage et manipulation de l'information	2.5		
8	**Sécurité liée aux ressources humaines**					**50%**
	8.1	**Avant le recrutement**			50%	
		8.1.1	Rôles et responsabilités	4,0		
		8.1.3	Conditions d'embauche	0,0		
	8.2	**Pendant la durée du contrat**			50%	
		8.2.1	Responsabilités de la direction	0,0		
		8.2.2	Sensibilisation, qualification et formations en matière de sécurité de l'information	4,0		

9	**Sécurité physique et environnementale**					**91.2%**
	9.1	**Zones sécurisées**			93.12%	
		9.1.1	Périmètre de sécurité physique	3.75		
		9.1.2	Contrôle physique des accès	4,0		
		9.1.3	Sécurisation des bureaux, des salles et des équipements	3.2		
		9.1.4	Protection contre les menaces extérieures et environnementales	4,0		
		9.1.5	Travail dans les zones sécurisées	4,0		
		9.1.6	Zones d'accès public, de livraison et de chargement	3.4		
	9.2	**Sécurité du matériel**			89.28%	
		9.2.1	Choix de l'emplacement et protection du matériel	3.33		
		9.2.2	Services généraux	3.67		
		9.2.3	Sécurité du câblage	3.50		
		9.2.4	Maintenance du matériel	4,0		
		9.2.5	Sécurité du matériel hors des locaux	2.5		
		9.2.6	Mise au rebut ou recyclage sécurisé(e) du matériel	4,0		
		9.2.7	Sortie d'un bien	4,0		
10	**Gestion de l'exploitation et des télécommunications**					**83.14%**
	10.1	**Procédures et responsabilités liées à l'exploitation**			100%	
		10.1.1	Procédures d'exploitation documentées	4,0		
		10.1.2	Gestion des modifications	4,0		
		10.1.3	Séparation des tâches	4,0		
		10.1.4	Séparation des équipements de développement, de test et d'exploitation	4,0		
	10.2	**Gestion de la prestation de service par un tiers**			100%	
		10.2.1	Prestation de service	4,0		
		10.2.2	Surveillance et réexamen des services tiers	4,0		
		10.2.3	Gestion des modifications dans les services tiers	4,0		
	10.3	**Planification et acceptation du système**			88.87	
		10.3.1	Dimensionnement	4,0		
		10.3.2	Acceptation du système	3.11		
	10.5	**Sauvegarde**			100%	

		10.5.1	Sauvegarde des informations	4,0		
	10.6	**Gestion de la sécurité des réseaux**				
		10.6.1	Mesures sur les réseaux	4,0	50%	
		10.6.2	Sécurité des services réseaux	0,0		
	10.10	**Surveillance**				
		10.10.1	Rapport d'audit	4,0		
		10.10.2	Surveillance de l'exploitation du système	2,0	60%	
		10.10.3	Protection des informations journalisées	4,0		
		10.10.4	Journal administrateur et journal des opérations	4,0		
		10.10.5	Rapports de défaut	0,0		
11	**Contrôle d'accès**					
	11.1	**Exigences métier relatives au contrôle d'accès**				
		11.1.1	Politique de contrôle d'accès	4,0	100%	
	11.2	**Gestion de l'accès utilisateur**				
		11.2.2	Gestion des privilèges	2.54	65.75%	
		11.2.3	Gestion du mot de passe utilisateur	0,0		
		11.2.4	Réexamen des droits d'accès utilisateurs	4,0		**77.44%**
	11.4	**Contrôle d'accès au réseau**				
		11.4.1	Politique relative à l'utilisation des services en réseau	1,0		
		11.4.2	Authentification de l'utilisateur pour les connexions externes	2.31		
		11.4.3	Identification des matériels en réseau	4,0		
		11.4.4	Protection des ports de diagnostic et de configuration à distance	4,0	75.57%	
		11.4.5	Cloisonnement des réseaux	3,0		
		11.4.6	Mesure relative à la connexion réseau	2.85		
		11.4.7	Contrôle du routage réseau	4,0		

12	**Acquisition, développement et maintenance des systèmes d'information**					**81.62%**
	12.3	**Mesures cryptographiques**			83.25	
		12.3.1	Politique d'utilisation des mesures cryptographiques	2.66		
		12.3.2	Gestion des clés	4,0		
	12.4	**Sécurité des fichiers système**			80%	
		12.4.1	Mesures relatives aux logiciels en exploitation	3.2		
13	**Gestion des incidents liés à la sécurité de l'information**					**68.75%**
	13.1	**Signalement des événements et des failles liés à la sécurité de l'information**			75%	
		13.1.1	Signalement des événements liés à la sécurité de l'information	3,0		
		13.1.2	Signalement des failles de sécurité	3,0		
	13.2	**Gestion des améliorations et incidents liés à la sécurité de l'information**			62.5%	
		13.2.1	Responsabilités et procédures	4,0		
		13.2.2	Exploitation des incidents liés à la sécurité de l'information déjà survenus	1,0		
14	**Gestion du plan de continuité de l'activité**					**80%**
	14.1	**Aspects de la sécurité de l'information en matière de gestion de la continuité de l'activité**			80%	
		14.1.1	Intégration de la sécurité de l'information dans le processus de gestion du plan de continuité de l'activité	3,0		
		14.1.2	Continuité de l'activité et appréciation du risque	4,0		
		14.1.3	Elaboration et mise en oeuvre des plans de continuité intégrant la sécurité de l'information	4,0		
		14.1.4	Cadre de la planification de la continuité de l'activité	1,0		
		14.1.5	Mise à l'essai, gestion et appréciation constante des plans de continuité de l'activité	4,0		
15	**Conformité**					**89.06%**
	15.2	**Conformité avec les politiques et normes de sécurité et conformité technique**			78.12%	
		15.2.1	Conformité avec les politiques et les normes de sécurité	3,0		
		15.2.2	Vérification de la conformité technique	3.25		
	15.3	**Prises en compte de l'audit du système d'information**			100%	
		15.3.1	Contrôles de l'audit du système d'information	4,0		
		15.3.2	Protection des outils d'audit du système d'information	4,0		

Annexe C

Scénario			Impact	Potentialité	Gravité	Remarques
1	**Indisponibilité passagère de ressources**					
	01.10	**Absence de personnel**				
		Départ de personnel stratégique				
	01.20	**Accident ou panne mettant hors service une ou plusieurs ressources matérielles**				
		Accident de nature électrique (court-circuit), mettant hors service un équipement informatique critique				
		Accidents dus à l'eau ou à des liquides (fuite d'une canalisation, liquides renversés accidentellement, etc.), mettant hors service un équipement du réseau étendu informatique critique				
		Panne rendant indisponible un équipement informatique critique				
		Panne rendant indisponible un système terminal mis à la disposition des utilisateurs (PC, imprimante, périphérique spécifique, etc.)				
		Servitude indispensable HS : arrêt de la climatisation entraînant l'arrêt des équipements informatiques (panne grave ou rupture de canalisation d'eau)				
		Accident de nature électrique externe à l'entreprise (court-circuit extérieur, coupure d'un câble, défaillance extérieure, etc.) empêchant de fonctionner les systèmes centraux.				
	01.30	**Bug logiciel**				
		Arrêt d'une application critique dû à un bug système ou à un bug de progiciel				
		Arrêt d'une application critique dû à un bug d'un logiciel interne				
	01.40	**Impossibilité de maintenance**				
		Défaillance matérielle d'un équipement critique impossible à résoudre par la maintenance, ou indisponibilité du prestataire				
	01.50	**Vandalisme depuis l'extérieur**				
		Tir d'armes légères ou lancement de projectiles depuis la rue, rendant indisponible des équipements du réseau local, étendu, systèmes informatiques centraux				
	01.60	**Vandalisme intérieur**				

		Petit vandalisme sur les équipements informatiques critiques, par des personnes autorisées à pénétrer dans l'établissement (personnel, sous-traitants, etc.).				
	01.70	**Indisponibilité totale des locaux**				
		Interdiction totale d'accès décrétée par les autorités entraînant un arrêt du système informatique				
		Interdiction totale d'accès décrétée par les autorités empêchant les utilisateurs d'accéder à leurs bureaux				
2	**Destruction d'équipements**					
	02.10	**Chute de foudre**				
		Chute de la foudre endommageant gravement des équipements informatique critiques				
	02.20	**Incendie**				
		Incendie : accident interne (corbeille à papier, cendrier, etc.) endommageant gravement des équipements informatiques critiques				
	02.30	**Inondation**				
		Inondation due à une canalisation percée ou crevée et rendant indisponibles des équipements informatiques critiques				
		Catastrophe naturelle telle que crue d'une rivière, remontée de la nappe phréatique, débordement du réseau d'égouts, tornade avec destruction de la couverture, etc. mettant hors service des équipements critiques				
		Inondation due à l'extinction d'un incendie voisin, mettant hors service des équipements critiques				
	02.40	**Terrorisme ou sabotage depuis l'extérieur**				
		Terrorisme sabotage par des agents extérieurs : explosifs déposés à proximité des locaux sensibles, mettant hors service des équipements critiques				
3	**Performances dégradées**					
	03.10	**Modification du logiciel**				
		Dégradation involontaire des performances applicatives, à l'occasion d'une opération de maintenance corrective ou évolutive de logiciel ou de progiciel				
	03.20	**Modification du matériel**				
		Dégradation involontaire de performances, à l'occasion d'une opération de maintenance matérielle évolutive d'un équipement du réseau local (hors télémaintenance)				
		Dégradation involontaire de performances, à l'occasion d'une opération de maintenance matérielle à la suite d'une panne d'un système central				

	03.30	**Surutilisation accidentelle de ressources informatiques ou réseau**				
		Dégradation des performances du réseau local due à une saturation accidentelle de ressources résultant d'un incident ou d'une panne sur un équipement du réseau				
		Dégradation des performances applicatives due à une saturation accidentelle de ressources résultant d'un incident système				
	03.40	**Sur-utilisation malveillante de ressources informatiques ou réseau**				
		Dégradation des performances applicatives due à la saturation répétitive malveillante de moyens informatiques par un groupe d'utilisateurs				
		Dégradation de performances du réseau local due à la saturation du réseau par un ver				
4	**Destruction de software**					
	04.10	**Effacement de code exécutable ou de configurations**				
		Effacement direct de code exécutable par une personne autorisée (exploitation, support informatique, maintenance, etc.)				
	04.20	**Ecrasement accidentel d'un disque fixe**				
		Ecrasement accidentel d'un disque fixe contenant des programmes exécutables dû à une panne de matériel				
	04.30	**Effacement accidentel de logiciel**				
		Effacement accidentel de logiciel exécutable par erreur humaine				
	04.40	**Vol ou effacement d'un support amovible**				
		Vol ou effacement d'un support amovible contenant le code source d'un logiciel dans les locaux informatiques, par une personne autorisée				
		Vol répété de bandes archives de programmes dans les locaux de stockage des media, par une personne non autorisée				
	04.50	**Effacement ou destruction de configurations logicielles utilisateurs**				
		Effacement de configurations utilisateurs par un virus				
		Effacement de logiciels spécifiques utilisateurs par un virus				
5	**Altération de logiciel**					
	05.10	**Altération malveillante des fonctionnalités prévues d'une application via une bombe logique ou une porte dérobée,...**				

		Altération malveillante des fonctionnalités prévues d'une application via une bombe logique ou une porte dérobée				
	05.20	**Modification volontaire des fonctionnalités prévues d'une application informatique**				
		Modification volontaire des fonctionnalités prévues d'une application par les équipes de développement, par la maintenance ou par le personnel d'exploitation				
	05.30	**Modification volontaire ou accidentelle des fonctionnalités prévues d'une fonction bureautique**				
		Modification malveillante des fonctions ou macro-instructions d'un fichier bureautique (Excel, Access, etc.) par une personne ayant accès à l'espace de travail partagé où est archivé le fichier, où au poste de travail des utilisateurs				
		Modification accidentelle ou malencontreuse des fonctions ou macro-instructions d'un fichier bureautique (Excel, Access, etc.) par un utilisateur d'un fichier partagé.				
6	**Altération de données**					
	06.10	**Accident de traitement**				
		Altération accidentelle des données pendant la maintenance				
		Altération accidentelle des données pendant une opération de maintenance à chaud				
	06.20	**Erreur de saisie**				
		Erreur pendant le processus de saisie				
7	**Manipulation de données**					
	07.10	**Données applicatives faussées pendant la transmission**				
		Données applicatives faussées pendant la transmission par un membre du personnel manipulant un équipement de réseau local				
		Données applicatives faussées pendant la transmission par un membre du personnel branchant un équipement parasite en coupure sur le réseau local (man in the middle)				
		Données applicatives faussées pendant la transmission entre un utilisateur nomade et le réseau interne				
	07.20	**Rejeu de transaction**				
		Rejeu de transaction.				
	07.30	**Saisie faussée de données**				
		Saisie de fausses données par un agent autorisé, mais déloyal				
		Saisie de fausses données par un membre du personnel usurpant l'identité d'un utilisateur autorisé				

	07.40	**Substitution volontaire de supports**				
		Substitution volontaire de supports de données par un tiers non autorisé				
		Substitution volontaire de supports de données par une personne autorisée (légitimement)				
	07.50	**Manipulation de fichiers**				
		Manipulation de fichiers de données par un tiers non autorisé usurpant l'autorité d'un utilisateur autorisé				
		Manipulation de fichiers de données par un membre du personnel autorisé illégitime				
	07.60	**Falsification de message**				
		Faux message émis par un membre du personnel usurpant l'identité d'une personne accréditée avec falsification de signature				
		Message faussé pendant la transmission entre un utilisateur nomade et le réseau interne				
8	**Divulgation de données ou d'informations**					
	08.10	**Accès au système et consultation**				
		Accès au système et consultation en ligne, par un pirate se connectant depuis l'extérieur sur un port ouvert du réseau étendu				
		Accès au système et consultation en ligne, par un tiers autorisé à pénétrer dans les locaux et ayant accès (physique) au réseau local interne (prise LAN dans une salle de réunion)				
		Accès au système et consultation en ligne, par un membre du personnel autorisé illégitime				
	08.20	**Captation d'informations fugitives**				
		Captation d'informations fugitives : branchement d'un équipement parasite sur le réseau local (gaines techniques), dans les locaux de l'entreprise, par une personne autorisée à y pénétrer				
		Captation d'informations fugitives : modification distante d'un équipement de réseau, pour piéger les messages échangés, par un utilisateur autorisé à se connecter sur le réseau interne				
		Captation d'informations fugitives : écoute de la connexion d'un utilisateur nomade se connectant depuis l'extérieur au réseau interne				
		Captation d'informations fugitives : compromission électromagnétique				
		Transfert de données sensibles détourné par un pirate ayant connecté un équipement usurpant l'identité d'une entité connectée au réseau étendu				
	08.30	**Vol de documents écrits ou imprimés**				
		Vol de listings ou d'impressions pendant la phase de diffusion (à l'extérieur des locaux sensibles)				

		Vol de listings ou d'impressions par un membre du personnel autorisé illégitimement à pénétrer dans les locaux de la production				
		Vol répétitif de documents dans des bureaux, par un membre du personnel (n'appartenant pas au service)				
		Vol répétitif de documents dans des bureaux, par un ancien membre du personnel ayant conservé ses droits				
		Vol de documents dans des bureaux, par un visiteur				
		Vol de documents dans des bureaux, par une personne autorisée à y pénétrer en dehors des heures ouvrables (femmes de ménage, services de surveillance, etc.)				
		Vol de courrier sensible, dans le local du courrier, en dehors des heures ouvrables				
9	**Détournement de fichiers de données**					
	09.10	**Accès au système et copie de fichiers de données applicatives**				
		Copie répétée de fichiers de données applicatives par un pirate se connectant depuis l'extérieur sur un port ouvert du réseau étendu				
		Copie répétée de fichiers de données applicatives par une personne non membre du personnel ayant accès aux locaux et la possibilité de se connecter sur le LAN				
		Accès au système et copie de fichiers de données applicatives par un agent autorisé illégitime				
		Accès au système et copie de fichiers de données applicatives par un membre du personnel exploitant une faille de sécurité laissée ouverte après une opération de maintenance				
		Accès au système et copie de fichiers de données applicatives par une personne du développement via une porte dérobée placée dans une application				
		Accès aux disques système et copie de fichiers de données applicatives par du personnel de maintenance à l'occasion d'une opération de maintenance				
		Accès aux réseaux de stockage et lecture de fichiers de données applicatives par un serveur non autorisé				
	09.20	**Vol de supports de données applicatives**				
		Vol de supports de données applicatives pendant l'exploitation, par une personne autorisée à manipuler les supports				
		Vol de fichiers de données applicatives dans les locaux de stockage des media sur site, par une personne non autorisée				
		Vol de fichiers de données applicatives dans les locaux de stockage des media hors site, par une personne non autorisée				
	09.30	**Accès aux serveurs et copie de fichiers bureautiques**				

		Copie répétée de fichiers bureautiques partagés (serveur de données partagées) par un pirate se connectant depuis l'extérieur sur un port ouvert du réseau étendu				
		Copie répétée de fichiers bureautiques partagés (serveur de données partagées) par une personne non membre du personnel ayant accès aux locaux et la possibilité de se connecter sur le LAN				
		Copie ponctuelle de fichiers bureautiques partagés (serveur de données partagées) par un pirate se connectant via une liaison modem ouverte sur Internet sur un poste utilisateur lui-même connecté au réseau interne avec des sessions ouvertes sur des serveurs autorisés				
		Copie répétée de fichiers bureautiques partagés (serveur de données partagées) par une personne membre du personnel usurpant l'identité d'une personne autorisée				
		Copie répétée de fichiers bureautiques partagés (serveur de données partagées) par une personne membre du personnel utilisant des outils de hackers				
		Copie répétée de fichiers bureautiques par une personne membre du personnel non autorisée sur le poste de travail				
		Divulgation de fichiers bureautiques par un agent de maintenance intervenant sur un poste de travail				
	09.40	**Détournement de code source**				
		Détournement du code source d'une application stratégique par un membre de l'équipe de développement				
10	**Perte de fichiers de données ou de documents**					
	10.10	**Effacement par bombe logique**				
		Effacement de fichiers de données applicatives par bombe logique introduite par un administrateur ou un ingénieur système				
	10.20	**Effacement de supports par virus**				
		Effacement des fichiers bureautiques personnels, par un virus				
		Effacement des fichiers bureautiques partagés, par un virus				
	10.30	**Effacement malveillant direct de supports**				
		Effacement massif de fichiers d’archives de données par le personnel d’exploitation				
	10.40	**Perte accidentelle de fichiers**				
		Perte accidentelle de fichiers de données applicatives par un automate ou une application				
	10.50	**Vol de supports**				
		Vol de supports d’archives personnelles dans un bureau				

	10.60	**Perte accidentelle de documents**				
		Perte d'archives patrimoniales ou de documents ayant valeur de preuve suite à un incendie				
11	**Sinistre immatériel total**					
	11.10	**Effacement de fichiers par bombe logique**				
		Destruction ou pollution massive de fichiers de données applicatives et de leurs sauvegardes, par voie logique par un ingénieur système de l'équipe d'exploitation				
		Destruction ou pollution massive de fichiers programmes (codes sources) et de leurs sauvegardes, par voie logique par un ingénieur système de l'équipe d'exploitation				
	11.20	**Effacement malveillant des supports**				
		Effacement malveillant de l'ensemble des supports de données sensibles : supports opérationnels, sauvegardes et archives par le personnel d'exploitation				
12	**Non-conformité à la législation et à la réglementation**					
	12.10	**Attaque d'une tierce société**				
		Attaque d'une tierce société ayant des connexions autorisées avec l'entreprise, par du personnel interne				
		Attaque d'une tierce société n'ayant pas de connexion autorisée avec l'entreprise, par du personnel interne				
		Attaque d'une tierce société par un pirate ayant pénétré le système d'information (rebond)				
	12.20	**Violation des droits de propriété industrielle**				
		Utilisation de logiciels sans licences				
	12.30	**Conformité à la législation locale**				
		Risque de non-conformité à la législation tunisienne relative à la sécurité des systèmes d'information				

Résumé

Ce travail s'inscrit dans le cadre du stage de fin d'études pour l'obtention le diplôme du mastère professionnel en Nouvelles Technologies des Télécommunications et Réseaux effectué chez Le Moteur Diesel. L'objectif de ce projet est d'établir un audit de sécurité, cet audit consiste à valider les moyennes de protection mise en œuvre sur les plans organisationnels, procéduraux et techniques pour améliorer son système d'informations.

L'audit de sécurité conduit au-delà du constat, à analyser les risques opérationnels pour le domaine étudié, et par la suite proposer des recommandation et un plan d'action quantifiées et hiérarchisées pour corriger les vulnérabilités et réduire l'exposition aux risques.

Mots clés : Audit – Sécurité – ISO27002 – MEHARI.

Abstract

This work, carried out within the company LMD is a part of our traineeship of graduation to obtain the professional master in new technologies and telecommunications networks. The objective of this project is to establish one audit of safety suitable of LMD, this audit of security consists in validating the means of protection implemented on the organizational, procedural levels and techniques to improve the information system of LMD.

The audit of security led beyond the report, to analyze the operational risks for the studied field, and to thereafter propose recommendations and an action plan quantified and hierarchical to correct the vulnerabilities and reduce the exposure to the risks.

Keywords : Audit – Security – ISO27002 – MEHARI.

تلخيص

يندرج هذا المشروع في مؤسسة المحرك ديزل في إطار الحصول على شهادة الماجستير المهني في التقنيات الحديثة للاتصالات والشبكات. الهدف من هذا المشروع هو إنشاء مراجعة وتدقيق لنظام الحماية للمؤسسة وإضفاء صبغة شرعية على وسائل الحماية المنفذة وتحسين نظام المعلومات المتواجد في المؤسسة.

نتيجة هذا العمل تقرير يبرز مظاهر الضعف في نظام المعلومات واقتراح حلول لمعالجتها .

الكلمات المفاتيح: تدقيق ـــ سلامة ـــ إيزو 27002 ـــ ميهاري