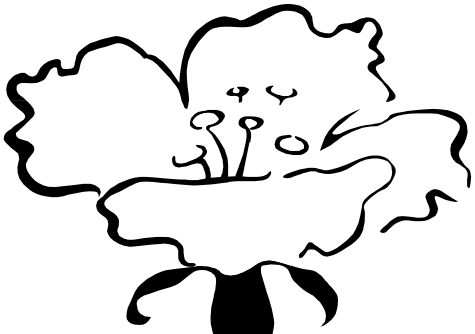


Dedicace

J’ai le grand plaisir de dédier ce travail en témoignage d’affectation et de reconnaissance

A mes parents,

Pour votre amour, votre affection, vos prières et vos conseils Que ce travail

Soit le fruit de toutes vos peines et vos sacrifices.

Acceptez ce travail comme témoignage de l’estime, le respect et le grand

Amour que j’éprouve pour vous.

A mes frères et sœurs,

Symboles de fraternité, de soutien et d’encouragement En témoignage

Mon profond respect et affection. A toutes ma famille

Avec toutes mes affections,

Et mes souhaits de bonheur et de réussite.

A tout (es) mes fidèles ami(e) s,

Que notre amitié puisse durer éternellement. Puisse ce travail vous exprime

Mes souhaits de succès.

A tous ceux qui me soutiennent encore,

A tous mes professeurs, A tous mes amis, A tous le personnel de centre de calcul,

À toute personne qui m’ayant consacré un jour, un moment

De sa vie pour m’aider me conseiller, m’encourager ou simplement me sourire,…

Mounia

Remerciement

nnaissance va tout d'abord à M. Youssef BAGUI qui a bien voulu m'encadrer. Grâce à sa disponibilité et à sa volonté, j'ai pu surmonter certains obstacles.

emerciements vont également aux enseignants du département informatique de la des sciences et techniques de SETTAT pour leurs précieux enseignements. Je tiens à er particulièrement le Coordonnateur du «MASTER RESEAUX ET SYSTEMES» M. DDINE pour leurs précieux conseils et leur dévouement pour le bon déroulement de notre formation.

vail étant le fruit d'un stage de six mois au sein de l'entreprise SIGMATEL je tiens à ner ma profonde gratitude à MR Oualid TAHAOUI directeur de la BU « réseaux et systèmes » pour sa disponibilité et ses conseils permanents.

cie également Mme ZAYDI Hayat chef service du parc informatique de l'ENIM, pour outien financier et moral tout au long de mes études.et pour l'opportunité qui m'a offerte pour réaliser une mission d'audit au sein des locaux de l'école.

cie tous les étudiants de « MASTER RESEAUX ET SYSTEMES » pour leur esprit de fraternité et de partage tout au long de cette formation.

Résumé

et porte sur l'audit de sécurité des systèmes d'information, ce présent rapport est la se d'une mission d'audit que j'ai mené avec l'équipe SIGMATEL pour le compte de l'Ecole Nationale de l'Industrie Minérale(ENIM).

e mission se décompose en plusieurs phases, chacune d'elles comporte plusieurs s. La première étape consiste en l'audit organisationnel et physique, je m'intéressais aspects de gestion et d'organisation de la sécurité, sur les plans organisationnels, ns et physiques, afin d'avoir un aperçu global de niveau de sécurité de l'organisme selon la norme ISO 27002.

uxième étape consiste en l'audit de sécurité technique du système informatique de , pour le mener à bien j'ai commencé par la collecte d'information sur le réseau de é, pour ce faire j'ai fait un audit d'architecture pour tracer la topologie réseau, puis it un scan de ports pour savoir les ports ouverts, également j'ai effectué un scan de abilités pour mettre à nu les failles et les brèches du système informatique, et pour a robustesse de ce système et son degré de résistance à toute éventuelle attaque, j'ai un test d'intrusion dont j'ai exploité toutes les vulnérabilités découvertes durant les précédentes phases.

La dernière étape consiste en la proposition de différentes recommandations anisationnelles et techniques pour prémunir le système d'information de l'école.

Abstract

ject focuses on security auditing information systems, this report is a synthesis of an I conducted with the team SIGMATEL on behalf of the National School of Industry mineral (ENIM).

sion is divided into several phases, each of which includes several activities. The first o is the organizational and physical audit, I was interested here in the aspects of ment and organizational security, both organizational, human and physical, to get an overview of security level the body according to ISO 27002.

nd step in the security audit system technical school computer to complete it I started g information on the network of the audited to do this I made an audit architecture to the network topology, then I did a port scan to find open ports, also I did a scan of ilities to expose the flaws and loopholes in the system, and to know the robustness of em and its degree of resistance to any possible attack, I did a penetration test which I used all the vulnerabilities discovered during previous phases.

The last step consists in the proposal of various organizational and technical recommendations to protect the information system of the school.

e figures :

Introduction générale :

a sécurité des systèmes d'information constitue un domaine qui a toujours été té, encore plus de nos jours vu les mutations et avancées permanentes qui surviennent monde des technologies de l'information. Garantir la sécurité d'un système ation n'est pas une tâche ponctuelle. Elle constitue un processus continue et cyclique ectue autour des points suivants :

tection : Définir nos ressources sensibles à protéger ainsi que les mécanismes de n.

ction : Détecter les failles aux quelles sont exposées nos ressources.

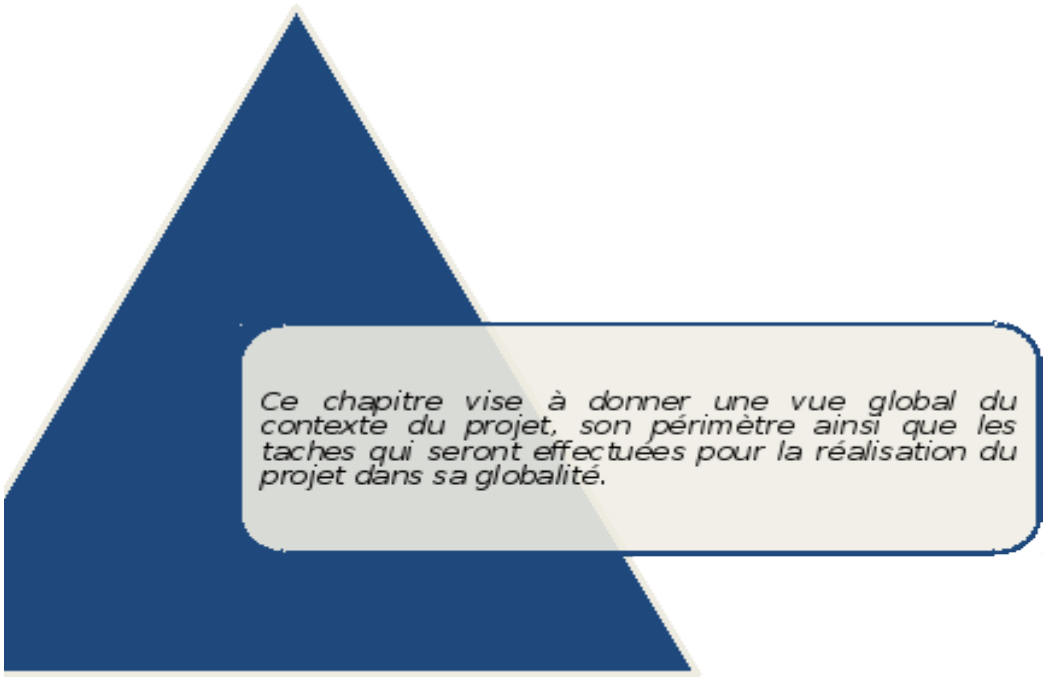
tion : Définir les solutions à mettre en place pour la correction.

ision : S'assurer que nos correctifs ne sont pas en conflit avec les politiques de déjà en place et s'y intègrent parfaitement.

n moyen pour suivre la sécurité d'un système d'information de façon continue est er un audit de sécurité des systèmes d'information de façon périodique. C'est dans ce que s'inscrit ce projet qui vise l'audit du système d'information de l'école nationale ie minérale (ENIM).

our se faire, je présenterai certains concepts clé de l'audit des systèmes ation, ainsi que l'organisme cible (l'audité). Par la suite, j'entamerai ma mission ar l'audit organisationnel et physique, ensuite l'audit technique. Enfin ma mission 'achèvera par un ensemble de recommandations visant à améliorer la sécurité du d'information de l'ENIM et palier aux éventuelles lacunes et insuffisances.

apitre I : Contexte et présentation du projet



Présentation de l'entreprise d'accueil

ɹe Groupe SIGMATEL

ΓEL est l'interlocuteur de référence dans l'intégration d'infrastructures de ication sécurisées au Maroc. Fruit d'une présence affirmée sur le **SIGMATEL** a développé depuis sa création en 1991 une expertise de pointe en le conception, d'intégration et d'exploitation de solutions de communication, et ceci, domaines de la voix, des données, des images, de la vidéo et des applications de et de sécurité.

ıe la tendance dominante à cette époque chez les sociétés télécoms était de se er exclusivement dans un des métiers, à savoir la voix ou les données, **SIGMATEL** a e miser sur les deux technologies en même temps, anticipant l'avenir de la ɨnce Voix et Données. Le résultat de ce choix se justifie par une longue et solide en convergence qui fût couronnée par un partenariat avec AVAYA, l'un des leaders x de la Téléphonie et des Centres d'Appels.

re, **SIGMATEL** se présente aujourd'hui comme l'un des leaders marocains de ɨion Voix et Données. Sa force réside dans son positionnement d'interlocuteur unique ıtégration d'infrastructures de communication sécurisées. Ainsi le groupe contient iétés qui appartiennent au secteur des TIC :

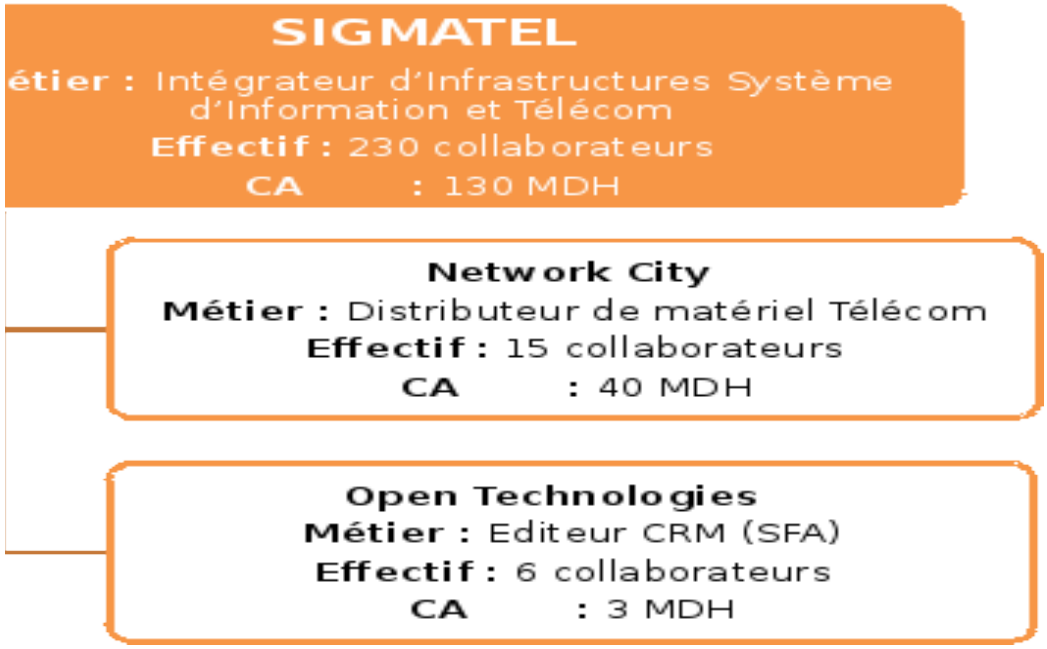


Figure 1 : Organisation du groupe SIGMATEL

)rganisation interne du Groupe SIGMATEL

é de direction du groupe est organisé comme suit :

Figure 1 : Organigramme du comité direction du groupe SIGMATEL

gramme du Groupe **SIGMATEL** est constitué de 2 pôles : pôle commerciale et
e Le pôle commercial est organisé comme suit :

Figure 1 : Organigramme du pôle commercial du groupe SIGMATEL

technique est organisé comme suit :

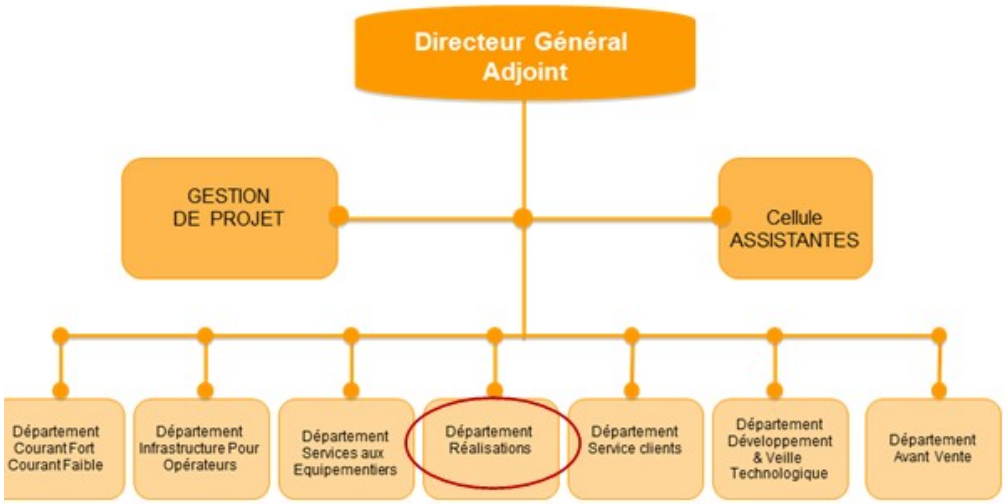


Figure 1 : Organigramme du pôle technique du groupe SIGMATEL

a été effectué au sein du département Réalisations du pôle technique, qui s'occupe de tion des projets chez les clients.

résentation du projet et des tâches réalisées :

d'audit de sécurité du système d'information de l'audité que doit mener SIGMATEL dans une vision global de complémentarité par rapport à un projet précédent : un offre pour la mise à niveau et la refonte du réseau local de l'ENIM.

de ce projet, SIGMATEL s'est engagé à offrir au soumissionnaire un rapport d'audit de gage d'une bonne réalisation de l'AO, ce qui sera aussi une base pour tion d'un contrat de maintenance à moyenne durée avec la même entreprise Cet audit upé en phases cohérentes et chronologiquement logiques, à commencer par un audit ionnel et physique pour avoir une vue global de la sécurité au niveau organisationnel, et humain.

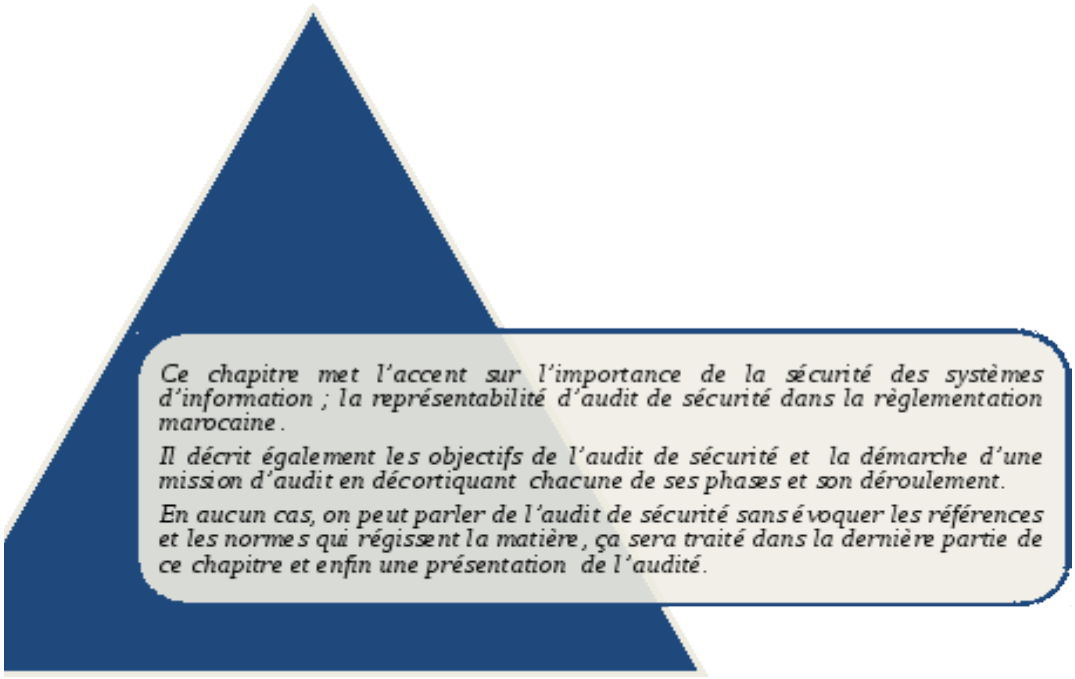
ème activité consiste en l'audit technique du système informatique afin de déceler vulnérabilités et les brèches de la sécurité.

ır doit étudier et proposer une prestation d'audit de sécurité visant à les moyens de protection mis en œuvre sur le plan organisationnel et ue, au regard de la politique de sécurité.

Périmètre de l'audit :

ue je vais effectuer tiendra pour cible le réseau de management de l'école Il sera d'auditer l'architecture réseau, des postes de travail et serveurs et d'effectuer des usifs sur base d'éventuelles vulnérabilités qui seront détectées lors de l'audit en la

hapitre II : Mission d'audit de sécurité des systèmes d'information



uction :

es entreprises ou organismes ne sont plus constitués de nos jours d'une entité, mais en plusieurs entités distantes qui échangent entre elles des informations. La sécurité systèmes d'information en général et de leurs réseaux informatiques en particulier est portance capitale pour assurer le bon fonctionnement de leurs activités. C'est dans ce qu'est introduit l'audit de sécurité des systèmes d'informations. Il est un moyen de a sécurité des systèmes d'information.

e chapitre premier présente le déroulement de l'audit de sécurité des systèmes ation, les normes sur lesquelles il peut se baser, ainsi que mon cadre de travail. Mais er lieu, j'évoquerai ce que représente l'audit de sécurité des systèmes d'informations .

dit de sécurité des systèmes d'information au Maroc :

ıal officiel du 17 octobre 2011, est paru le Décret n° 2.11.508 portant sur la création **mmission Stratégique de la Sécurité des Systèmes d'Information** et le Décret n° portant sur la création d'une **Direction Générale de la Sécurité des Systèmes nation**. Les deux instances seront créées au sein de la direction de défense nationale.

nission stratégique de la sécurité des systèmes d'information :

s :

tablir les orientations stratégiques dans le domaine de la sécurité des Systèmes ormation pour garantir la sécurité et l'intégrité des infrastructures critiques caines ;

'approbation du plan d'action de la Direction Générale de la Sécurité des mes d'Information et l'évaluation de ces résultats ;

délimitation des prérogatives de la Direction Générale de la Sécurité des Systèmes ormation ;

tatuer sur les projets de lois et des normes relatifs à la sécurité des systèmes ormation.

ident :

e ministre délégué chargé de l'administration de la défense nationale.

es et objectifs de l'audit :

sion d'audit vise différents objectifs. En effet je peux 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 l'information.

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

ème, un organisme audité pourra corriger les failles de sécurité.

on: Essentiellement l'audit de sécurité est souvent désignée comme étant l'outil de pour vérifier que les moyens et les procédures mis en œuvre pour la protection de èmes d'information, SI, sont efficaces ou le cas échéant, en relever leurs faiblesses. ens et les procédures de protection du SI étant définis dans la politique de sécurité, e sécurité est aussi appelé audit de la politique de sécurité. Il est utile de relever que le d'audit de sécurité à travers les méthodes d'analyse et de gestion des risques peut nt être utilisé pour aboutir à la politique de sécurité.

tion: Il est très important de rappeler qu'en aucun cas l'audit de sécurité ne doit se à l'une de ses actions la plus simple, la recherche active des failles, à l'aide de de vulnérabilités, qui effectuent les recherches sur la base d'attaques connues et qui tent donc que les failles connues. Cette fonction de l'audit effectue les tests de ilités d'un point donné du réseau contrôlé tandis qu'une autre fonction de l'audit, les trusion, sont pratiqués depuis l'extérieur. Ces derniers ne peuvent mettre en évidence intrusions possibles à travers des vulnérabilités identifiées et il est très fréquent, là e des failles potentielles ne soient pas décelées.

l l'audit purement technique, qui, à l'issue d'une véritable étude inspectera cture du réseau télécommunication et informatique ainsi que le système ation, pourra assurer que le système ne présente pas de failles pouvant être exploitées ntraire, le SI est sujet à des failles qu'il faut combler.

est généralement pratiqué après de l'audit organisationnel qui identifie les risques et out élément critique, métier et informatique, et confronte les pratiques de sécurité s à la réalité du terrain. D'ailleurs l'audit de sécurité se doit d'être organisationnel, nique. C'est cette approche que les puristes de la profession qualifient d'audit de

Elle permet d'apprécier la sécurité d'une manière générale en tenant compte de la physique, organisationnelle, logique, informatique, télécommunication et métier.

ement: Bien que souvent sa nécessité soit méconnue, l'audit est indispensable pour reprise, quel que soit sa taille, dès lors que celle-ci utilise des SI. Sa première mise en doit normalement s'effectuer lors de la conception du SI afin d'aboutir au Choix des techniques y compris les solutions de sécurité et déboucher dans le même temps sur ique de sécurité.

suite l'audit est nécessaire à la mise en place initiale de la PSSI, la politique de des systèmes d'information. Ceci pour contrôler l'efficacité des moyens et procédures euvre et que la PSSI est correctement appliquée, ou, le cas échéant, en relever les s.

e sécurité doit ensuite être effectué assez régulièrement pour s'assurer que les usages onformes à la réglementation édictée par la PSSI, mais surtout pour s'assurer que les de sécurité sont mises à niveau à chaque détection d'une nouvelle vulnérabilité et que à jour des failles et des logiciels sont continuellement réalisées.

le de vie d'un audit de sécurité des systèmes d'information :

ssus d'audit de sécurité est un processus répétitif et perpétuel. Il décrit un cycle de st schématisé à l'aide de la figure suivante :

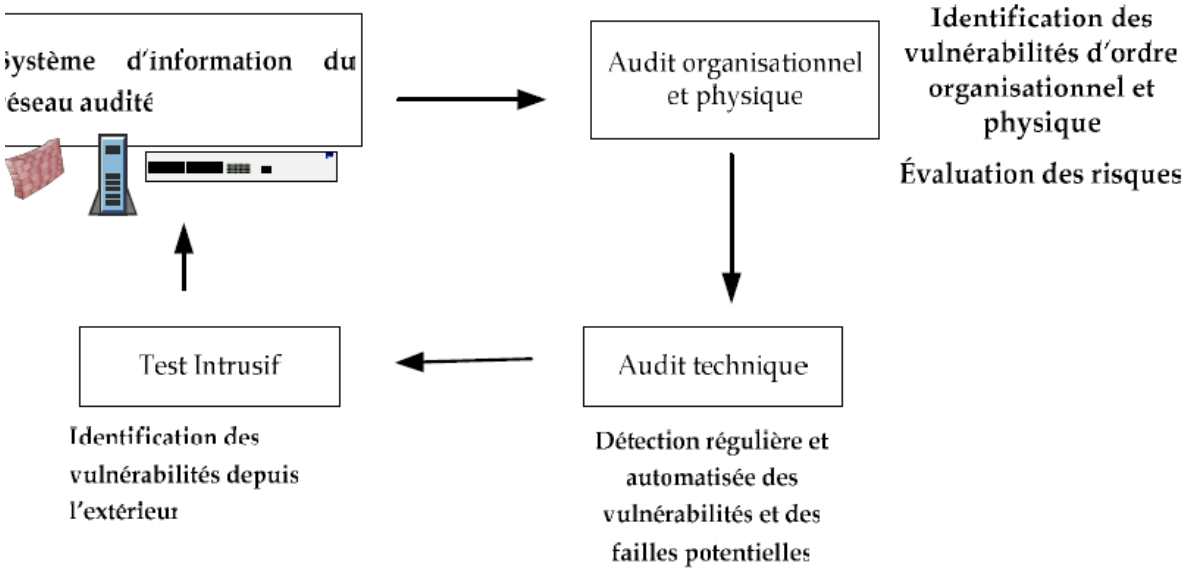


Figure 5- Cycle de vie d'un audit de sécurité

le sécurité informatique se présente essentiellement suivant deux parties comme le le précédent schéma :

L'audit organisationnel et physique.

L'audit technique.

sième partie optionnelle peut être également considérée. Il s'agit de l'audit intrusif. rapport d'audit est établi à l'issue de ces étapes. Ce rapport présente une synthèse de ll présente également les recommandations à mettre en place pour corriger les ces organisationnelles ou techniques constatées.

entation plus détaillée de ces étapes d'audit sera effectuée dans le paragraphe suivant nte le déroulement de l'audit.

émarche de réalisation d'une mission d'audit de sécurité des es d'information :

précédemment évoqué, l'audit de sécurité des systèmes d'information se déroule leux principales étapes. Cependant il existe une phase tout aussi importante qui est e de préparation. Je schématise l'ensemble du processus d'audit à travers la figure :

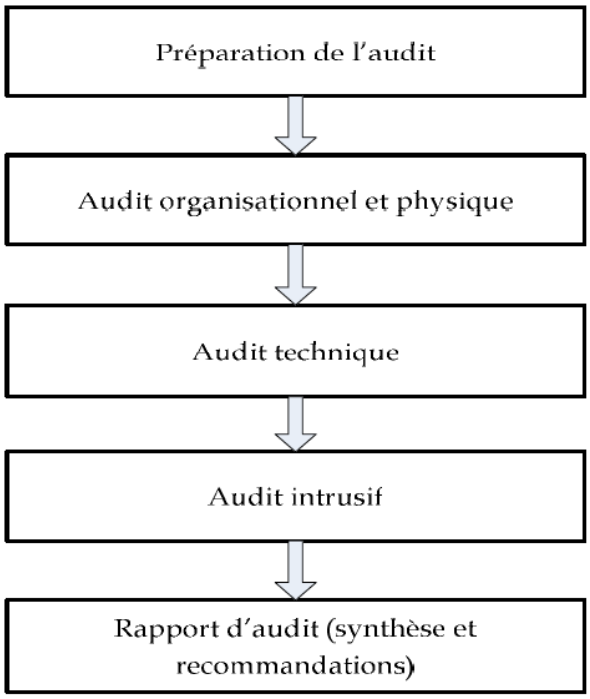


Figure 6- Les phases de l'audit

Préparation de l'audit :

ase est aussi appelée phase de pré audit. Elle constitue une phase importante pour la n de l'audit sur terrain. En effet, c'est au cours de cette phase que se dessinent les xes qui devront être suivis lors de l'audit sur terrain. Elle se manifeste par des s entre auditeurs et responsables de l'organisme à auditer. Au cours de ces entretiens, tre exprimées les espérances des responsables vis-à-vis de l'audit. Aussi,

re fixé l'étendu de l'audit ainsi que les sites à auditer, de même qu'un planning de
n de la mission de l'audit.

sonnes qui seront amenées à répondre au questionnaire concernant l'audit
ionnel doivent être également identifiées. L'auditeur (ou les auditeurs) pourrait
nt) également solliciter les résultats de précédents audits.
que les deux parties (auditeur-audité) ont "harmonisé leur accordéons ", l'audit sur
eut être entamé. Il débute par l'audit organisationnel et physique.

Audit organisationnel et physique :

tifs :

te étape, il s'agit de s'intéresser à l'aspect physique et organisationnel de l'organisme
uditer. Je m'intéresse donc aux aspects de gestion et d'organisation de la sécurité, sur
organisationnels, humains et physiques.
f visé par cette étape est donc d'avoir une vue globale de l´état de sécurité du
d´information et d´identifier les risques potentiels sur le plan organisationnel.

lement :

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

n contexte, suivant les recommandations de l'ANSI et du fait de sa notoriété, cet
endra comme référentiel une norme de l'ISO. Il s'agit de toutes les clauses (ou
ou domaines) de la version 2007 de la norme ISO/IEC 27002.
ionnaire que je propose se compose d'un peu moins d'une centaine de questions.
uestion est affectée d'un coefficient de pondération portant sur l'efficacité de la règle
ntiel sur laquelle porte la question, en matière de réduction de risque.

validation du Questionnaire (QSSI), les réponses choisies seront introduites dans tion que j'ai développée pour permettre l'automatisation du traitement du naire.

ment consiste au calcul d'une moyenne pondérée par les notes obtenues en fonction ses choisies et du coefficient d'efficacité. L'on obtient un résultat chiffré (de 0 à 6 ou en pourcentage) représentant le niveau de sécurité (la maturité) du système ation audité.

cette phase réalisée, il est question de passer à l'étape suivante de l'audit ; il s'agit nt de l'audit technique.

uestionnaire en annexe.

Audit technique :

tifs :

ape de l'audit sur terrain vient en seconde position après celle de l'audit ionnel. L'audit technique est réalisé suivant une approche méthodique allant de la te et la reconnaissance du réseau audité jusqu'au sondage des services réseaux actifs ables.

alyse devra faire apparaître les failles et les risques, les conséquences d'intrusions ou ulations illicites de données.

s de cette phase, l'auditeur pourra également apprécier l'écart avec les réponses lors des entretiens. Il sera à même de tester la robustesse de la sécurité du système ation et sa capacité à préserver les aspects de confidentialité, d'intégrité, de ilité et d'autorisation.

nt, l'auditeur doit veiller à ce que les tests réalisés ne mettent pas en cause la é de service du système audité.

lement :

ojectifs escomptés lors de cette étape, leurs aboutissements ne sont possibles que par on de différents outils. Chaque outil commercial qui devra être utilisé, doit bénéficier ence d'utilisation en bonne et du forme.

nt les outils disponibles dans le monde du logiciel libre sont admis.

ble des outils utilisés doit couvrir entièrement/partiellement la liste non exhaustive gories ci-après :

Outils de sondage et de reconnaissance du réseau.

Outils de test automatique de vulnérabilités du réseau.

Outils spécialisés dans l'audit des équipements réseau (routeurs, switchs).

Outils spécialisés dans l'audit des systèmes d'exploitation.

Outils d'analyse et d'interception de flux réseaux.

Outils de test de la solidité des objets d'authentification (fichiers de mots clés).

Outils de test de la solidité des outils de sécurité réseau (firewalls, IDS, outils l'authentification).

les outils à utiliser devra faire l'objet d'une présentation de leurs caractéristiques et nalités aux responsables de l'organisme audité pour les assurer de l'utilisation de ces

Audit intrusif :

tifs

t permet d'apprécier le comportement du réseau face à des attaques. Egalement, il e sensibiliser les acteurs (management, équipe informatique sur site, les utilisateurs) rapports illustrant les failles décelées, les tests qui ont été effectués (scénarios et nsi que les recommandations pour pallier aux insuffisances identifiées.

lement

de déroulement de cet audit doit être réalisée par une équipe de personnes ignorante ne audité avec une définition précise des limites et horaires des tests. Etant donné risqué (pour la continuité de services du système d'information) que porte ce type 'auditeur doit.

Bénéficier de grandes compétences.

Adhérer á une charte déontologique.

S'engager (par écrit) à un non débordement: implication à ne pas provoquer de perturbation du fonctionnement du système, ni de provocation de dommages

Rapport d'audit :

les précédentes phases d'audit sur terrain, l'auditeur est invité à rédiger un rapport de sur sa mission d'audit.

nthèse doit être révélatrice des défaillances enregistrées. Autant est-il important de un mal, autant il est également important d'y proposer des solutions andations), détaillées, pour pallier aux défauts qu'il aura constatés.

mmandations doivent tenir compte de l'audit organisationnel et physique, ainsi que echnique et intrusif.

éférences pour l'audit :

des systèmes d'information est un moyen de vérifier l'écart d'un système ation par rapport à une référence donnée. Une mission d'audit s'appuie donc vement sur une référence. Dans ce domaine, il existe différentes normes sur s se basent les missions d'audit de sécurité des systèmes d'information.La famille de SO 27000 constitue un véritable espoir pour les RSSI dans la mesure où elle apporte indéniable dans la définition, la construction et la déclinaison d'un SMSI efficace à ne série de normes dédiées à la sécurité de l'information :Comme décrit la figure :

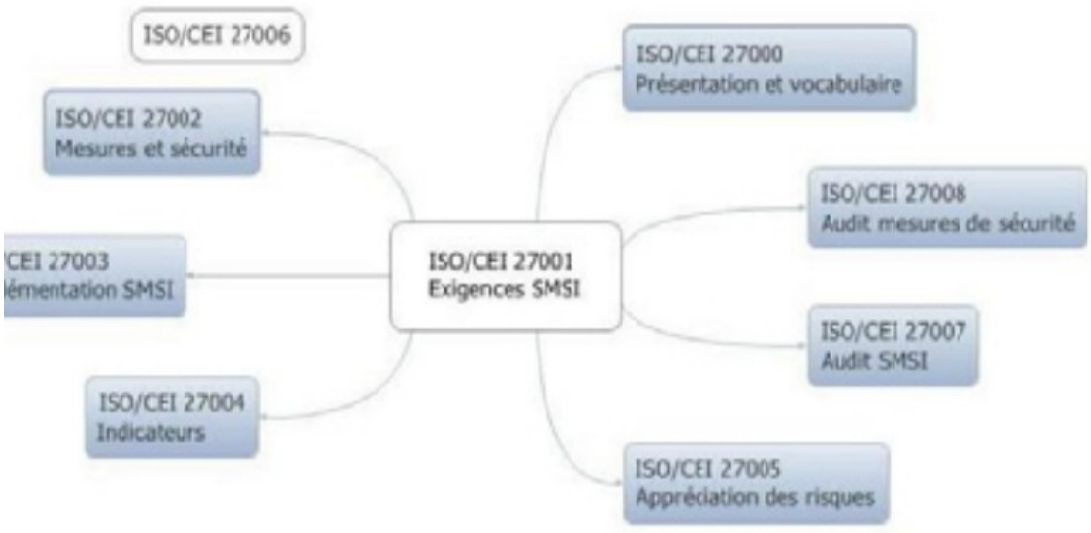


Figure 7 : Normes de la famille ISO/CEI 2700x

ISO/CEI 27001 : système de Gestion de la Sécurité de l'Information (ISMS) Exigences ;

SO/CEI 27002 : code de bonnes pratiques pour la gestion de la sécurité de information (anciennement ISO/CEI 17799) ; En résumé, l'ISO/CEI 27002 est un uide de bonnes pratiques, une série de préconisations concrètes, abordant les aspects nt organisationnels que techniques, qui permettent de mener à bien les différentes ctions dans la mise en place d'un SMSI.

norme a constitué le socle de ma mission d'audit. La norme ISO 27002 est un nble de recommandations pour la gestion de la sécurité de l'information et un entiel en matière de bonnes pratiques de sécurité. Elle émane de la norme britannique 799. La norme ISO 27002 couvre aussi bien les aspects techniques, organisationnels ysiques et peut être utilisée par n'importe quel organisme quel que soit son activité et mension. Les aspects qu'elle recouvre sont structurés suivant onze (11) grandes atiques. Les clauses constitutives de l'ISO/IEC 27002 :2007 sont les suivantes, nnées tel qu'évoqué dans la norme:

- Politique de sécurité
- Organisation de la sécurité
- Classification et contrôle des actifs
- Sécurité des ressources humaines
- Sécurité physique et environnementale
- Gestion des communications et de l'exploitation
- Contrôle d'accès
- Acquisition, développement et maintenance des systèmes d'information
- Gestion des incidents de sécurité
- Gestion de la continuité d'activité
- Conformité

SO/CEI 27003 : système de Gestion de la Sécurité de l'Information (ISMS) - Guide 'implémentation ; Publiée en janvier 2010, ISO 27003 facilite la mise en œuvre du MSI. Elle est utilisée en complément de la norme ISO 27001. L'ISO 27003 propose inq étapes pour implémenter le SMSI.

étapes concernent l'initialisation du projet, sa politique et son périmètre, l'analyse des ences en matière de sécurité de l'information, l'appréciation des risques et enfin boration du SMSI. Chacune de ces étapes est divisée en activités qui font l'objet e clause contenant :

- un résumé de l'activité (explication de l'étape en question),
- les entrées (tous les documents à utiliser au cours de l'étape),
- les recommandations (détail des points à aborder),
- les sorties (liste des livrables à produire).

ISO/CEI 27004 : mesure de la gestion de la sécurité de l'information ; Cette norme oncerne la gestion des indicateurs. L'utilisation d'indicateurs dans le domaine de la écurité est nouvelle. La norme ISO/CEI 27001 impose leur mise en place dans le MSI mais sans préciser comment et lesquels utiliser. En utilisant les mesures des ndicateurs l'objectif est d'identifier les points du SMSI qui nécessitent une mélioration ou une correction.

ISO/CEI 27005 : gestion du risque en sécurité de l'information ; Une des étapes du DCA les plus difficiles à mettre en œuvre est « l'appréciation des risques 7 ». 'ISO/CEI 27001 fixe des objectifs à atteindre pour être en conformité avec la norme, ais ne donne aucune indication sur les moyens d'y parvenir. Nous verrons qu'il xiste un nombre important de méthodes d'appréciation des risques qui offrent une émarche formelle et pragmatique. Néanmoins, l'ISO/CEI a souhaité proposer sa ropre méthode avec la norme ISO/CEI 27005. L'objectif n'est pas de remplacer ou endre obsolètes les méthodes existantes mais d'harmoniser le vocabulaire employé. 'ISO/CEI 27005 est constituée de douze chapitres. Les points les plus importants ont traités dans les chapitres sept à douze.

- Chap. 7, établissement du contexte
- Chap. 8, appréciation du risque
- Chap. 9, traitement du risque
- Chap. 10, acceptation du risque
- Chap. 11, communication du risque
- Chap. 12, surveillance et révision du risque

ISO/CEI 27006 : exigences pour les organismes réalisant l'audit et la certification de ystèmes de Gestion de la Sécurité de l'Information (ISMS) ;

ISO/CEI 27007 : guide pour l'audit de Systèmes de Gestion de la Sécurité de Information (ISMS). Cette norme est à l'état de brouillon « WD ». On peut ependant avancer qu'elle sera le pendant de la norme générique ISO 190119 pour les MSI. L'ISO/CEI 27007 donnera les lignes directrices pour auditer les SMSI.

ISO/CEI 27008 :

'état de WD, l'ISO/CEI 27008 traitera de l'audit des SMSI en proposant un guide qui mettra de contrôler les mesures de sécurité. Elle fournira pour chacune des mesures sécurité de la 27002, des moyens d'analyse des besoins en contrôle, en tenant compte l'importance des risques et des actifs. On pourra ainsi déterminer les mesures à ntrôler. Ces points sont importants car les auditeurs internes ou externes doivent ntrôler des mesures aussi variées que la gestion des mots de passe, la procédure de stion des incidents et le suivi de législation en vigueur.

sentation de l'audité L'Ecole Nationale d'Industrie Minérale(ENIM) :

Nationale de l'Industrie Minérale (ENIM), basée à Rabat, est l'une des plus anciennes arocaines d'ingénieurs d'états.

en 1972, l'ENIM avait, au début, pour mission principale de former des ingénieurs ecteur minier et l'industrie minérale. Ainsi entre 1975 et 1983, plus de 400 ingénieurs ormés dans les domaines des Mines, traitement des Minerais, et plus de 60 ingénieurs domaine de la métallurgie. En 1983, l'ENIM a vu la création de deux nouveaux nents, à savoir l'Électromécanique et le Génie Chimique Énergétique. En 1990, le nent informatique a vu le jour.

aussi, une réforme des études a eu lieu pour s'adapter à la suppression des cycles des préparatoires dans les écoles d'ingénieurs et la création des centres de classes

ɔires aux grandes écoles (CPGE) à l'échelle nationale. Ainsi la formation à l'école est
ɛ six à trois ans, et les programmes de certaines spécialités ont été revus et adaptés à
au système et aux nouveaux besoins : Le département Génie Chimique Energétique a
formé en Génie des Procédés Industriels.

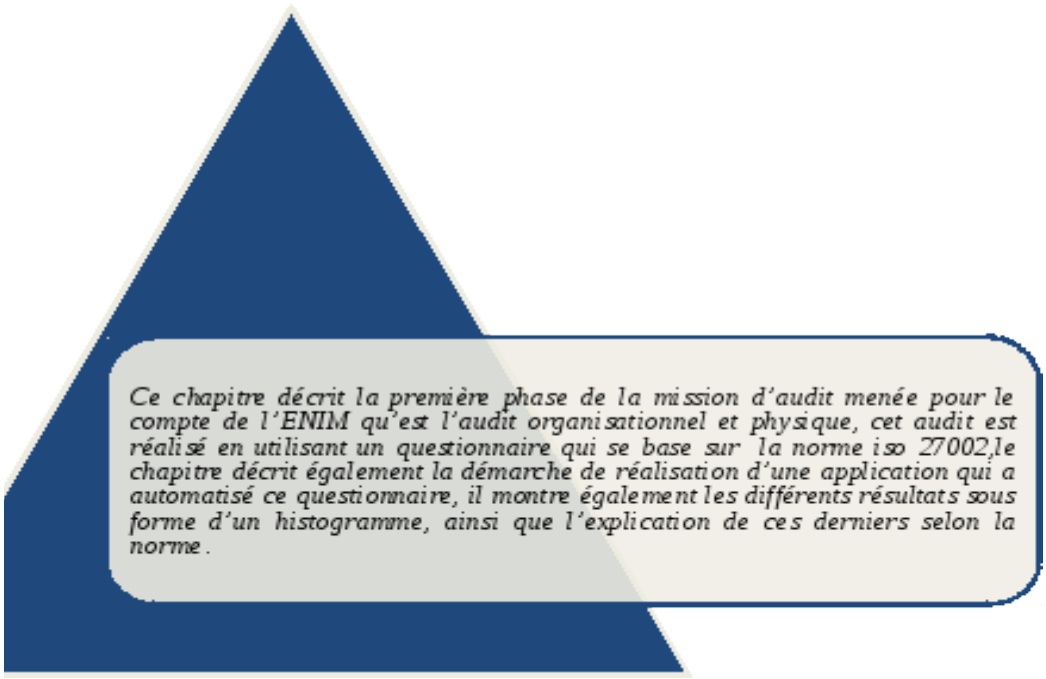
pétences développées par l'école sont donc dès l'origine très diverses, et l'école a su
ıu cours du temps pour devenir aujourd'hui une école dite « généraliste ».

Conclusion

ıs d'exposer, une liste non exhaustive d'un ensemble de normes qui constituent des ıces dans le cadre d'un audit de systèmes d'information ainsi que les procédures de réalisation de celui-ci, et l'enjeu que présente ce dernier au Maroc.

eau de l'organisme présenté constitue mon cadre de travail. La suite de ce document ra à mettre en pratique les précédents aspects de réalisation d'un audit, ça sera débuté par un audit organisationnel.

ɔitre III : Audit organisationnel et physique de M



ıction :

sion d'audit organisationnel et physique s'est déroulée à l'école nationale de le minérale (ENIM) à rabat. Elle s'est réalisée du 02 au 07 juin 2012. J'ai eu pour teur l'ingénieur principal en informatique, et un technicien réseaux, tous deux s au sein de l'ENIM. Soulignons que les objectifs fixés, sont :

Evaluer le niveau de sécurité du système d'information de l'école.

Valider les mesures de sécurité mises en œuvre.

Sensibiliser nos interlocuteurs aux risques et coût du non sécurité.

tre présente les points clés suite à nos entrevues au sujet de la sécurité du réseau de

ner à bien cet aspect de l'audit, je me suis servi d'une application web développée à ava et jsf ce qui m'a facilitée le traitement du questionnaire, puis les résultats de cet anisationnel.

qui suit, je vais présenter les différentes fonctionnalités de la dite application, ainsi
nception et sa mise en pratique.

ıde de l'existant organisationnel et physique :

.1.1 organisation de l'audité :

an organisationnel, l'ENIM est constituée de 3 directions rattachées directement à la
générale ; pour chacune de ces directions on trouve des services et/ou départements
ont directement rattachées comme illustré dans le diagramme suivant :

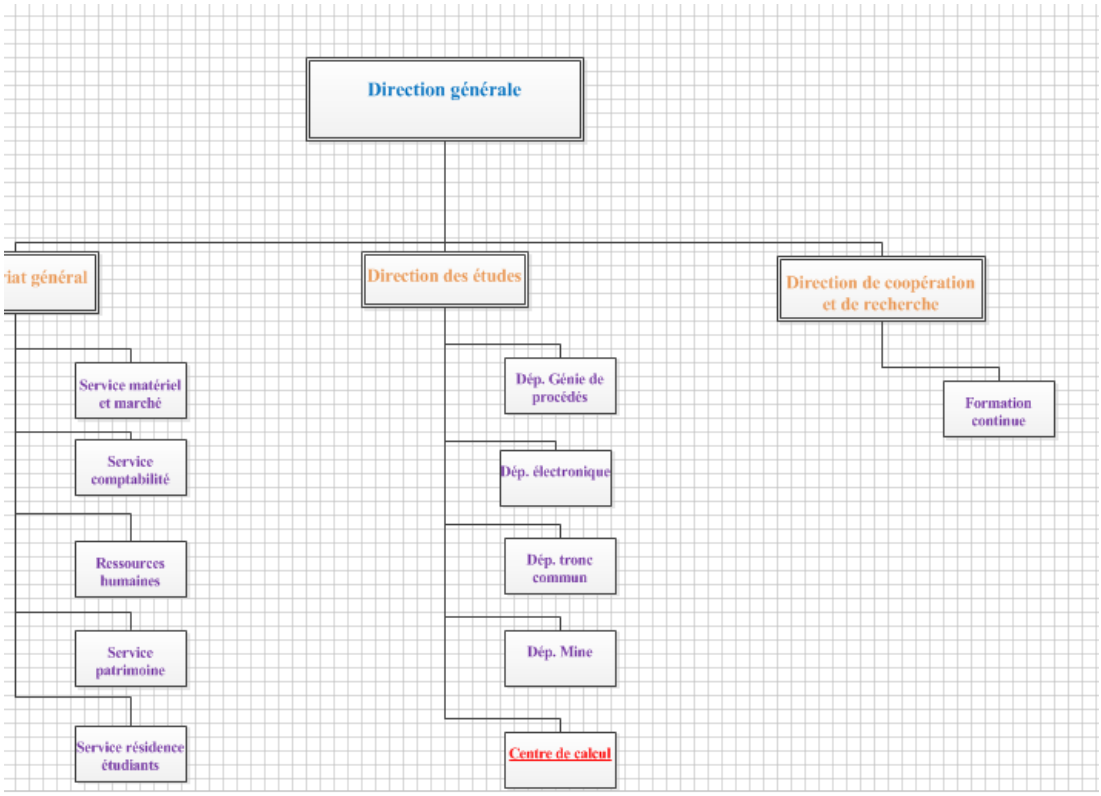


Figure 8 : Organigramme de l'école

.1.2 Réseau et équipements :

ı local de l'audité est présenté par deux topologies : physique et logique.

opologie physique, il s'agit de deux Etoiles optiques reliées par deux FO (une fibre afic échangé, et le deuxième lien sert de backup).

de ces deux étoiles dessert un ensemble de bâtiments (départements, services et cités ants) par ligne fibre optique.

ıa suivant illustre clairement cette topologie :

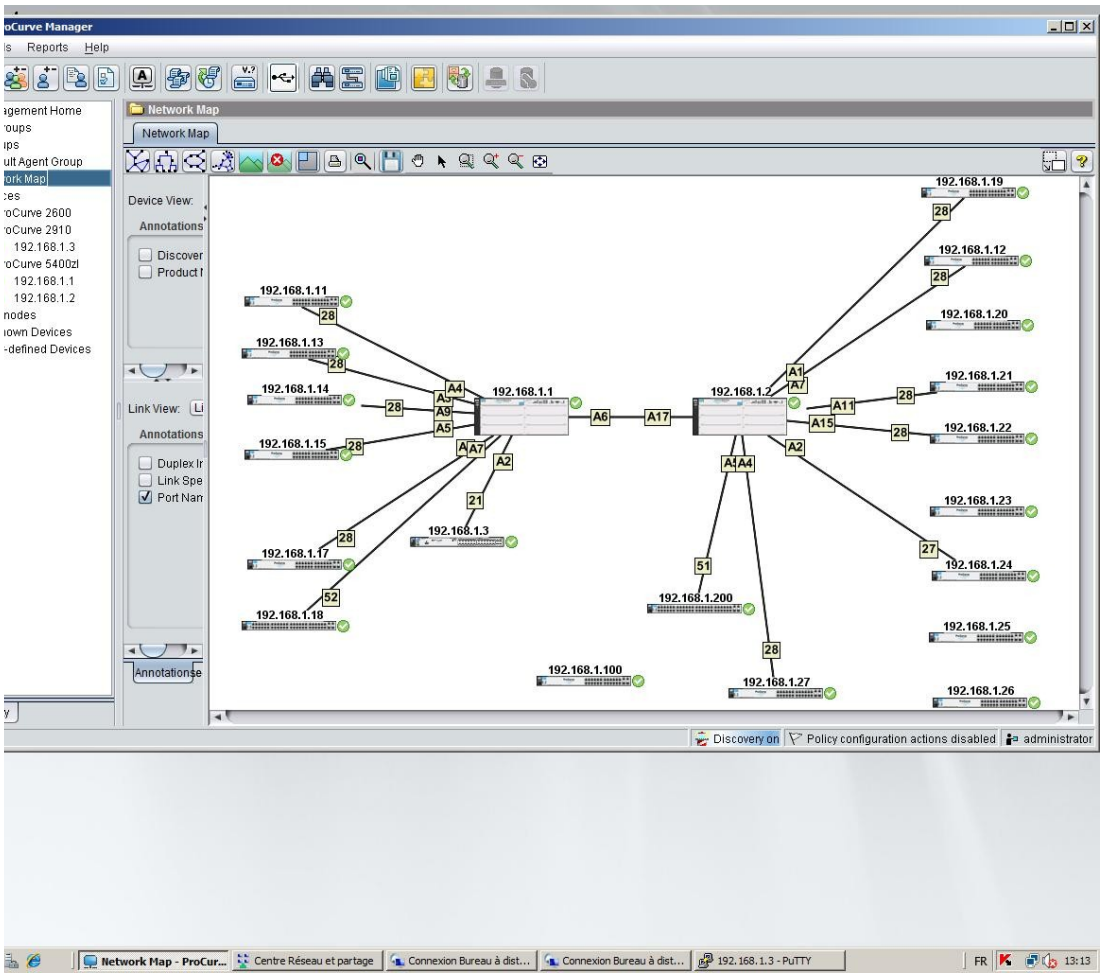


Figure 9: La MAP réseau de l'audité

topologie logique, le LAN de l'audité est constitué en réalité de plusieurs vlan ue qui sont attribués à l'utilisateur lors de sa connexion au domaine grâce à un adius en utilisant l'authentification 802.1x, le nombre de vlan dynamique est de 15. ı est constitué aussi d'un segment DMZ et d'un VLAN dédié au WIFI, et d'un autre dédié au BTS (équipements ALTAI). Le tout se trouve derrière un firewall ATE comme montre le schéma suivant :

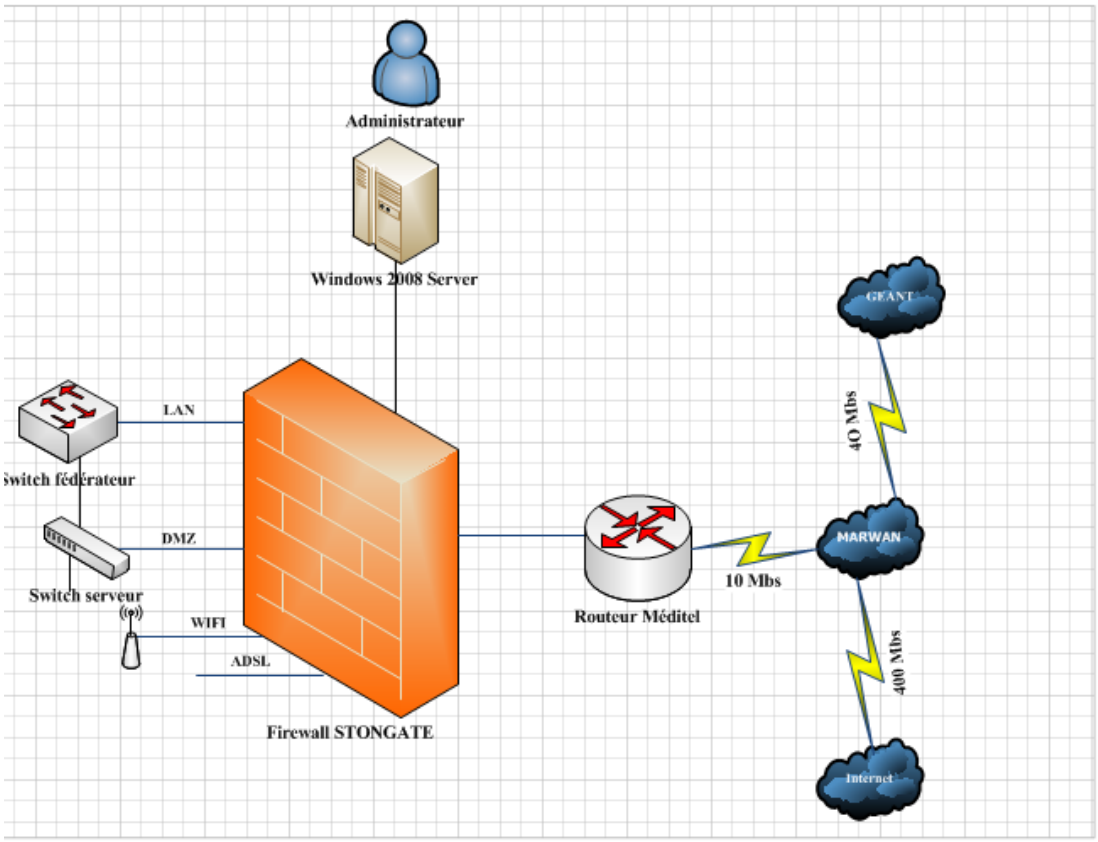


Figure 10 : La topologie logique de l'audité

audit organisationnel de l'ENIM : ISO 27002

e réalisation de l'application :

omatiser le traitement du questionnaire, j'ai réalisé une application qui consiste en on de pages Html, java, JSF et d'un serveur web local. En effet, le questionnaire se sous forme de page Html. Par la suite le traitement sous-jacent, du questionnaire, a ble grâce à un traitement Java. Chacune des réponses est pondérée d'un coefficient

exécution de l'ensemble s'est réalisée par l'utilisation d'un serveur web local Apache.
uite j'obtiens une moyenne pour chaque clause défini par la norme ISO/IEC
007.
ainsi à mesurer la conformité de l'organisme par rapport à chacune des clauses
par la norme ISO/IEC 27002 :2007.
ıa suivant indique les étapes de réalisation de cette application.

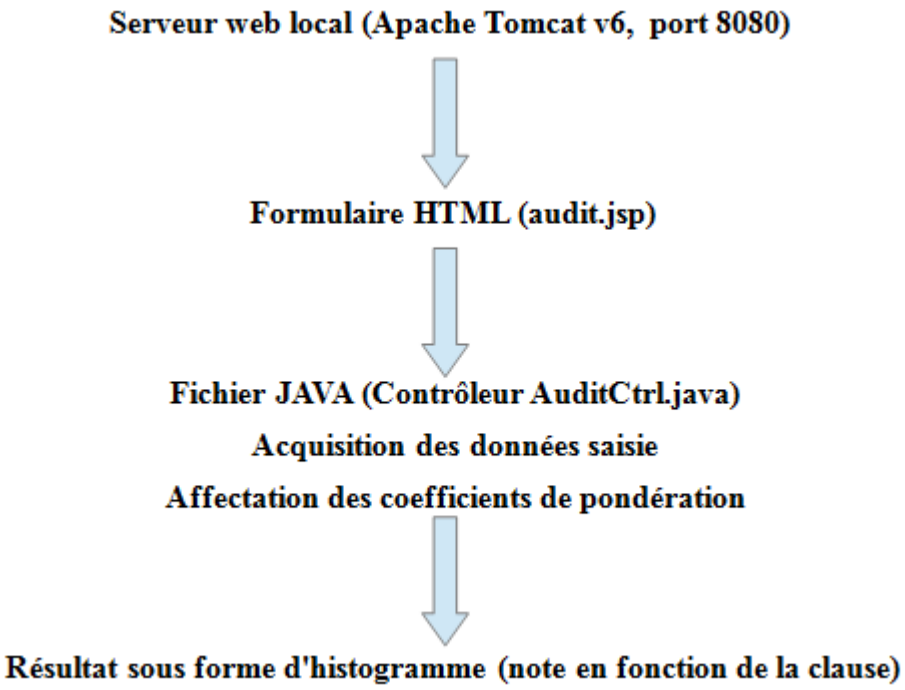


Figure 11: Automatisation du traitement du questionnaire

sultat de graphique de l'audit organisationnel :

ennes (exprimées en pourcentage) sont révélatrices de la maturité (niveau de sécurité)
ınisme au niveau organisationnel. Une note en dessous de 60% dénote d'un manque
ité. Soulignons que le barème pour le questionnaire a été décidé par le responsable

l'audité selon l'importance de chaque volet dans la sécurité de l'organisme, et c'est lement et approximativement c'est les mêmes coefficients utilisés dans les autres

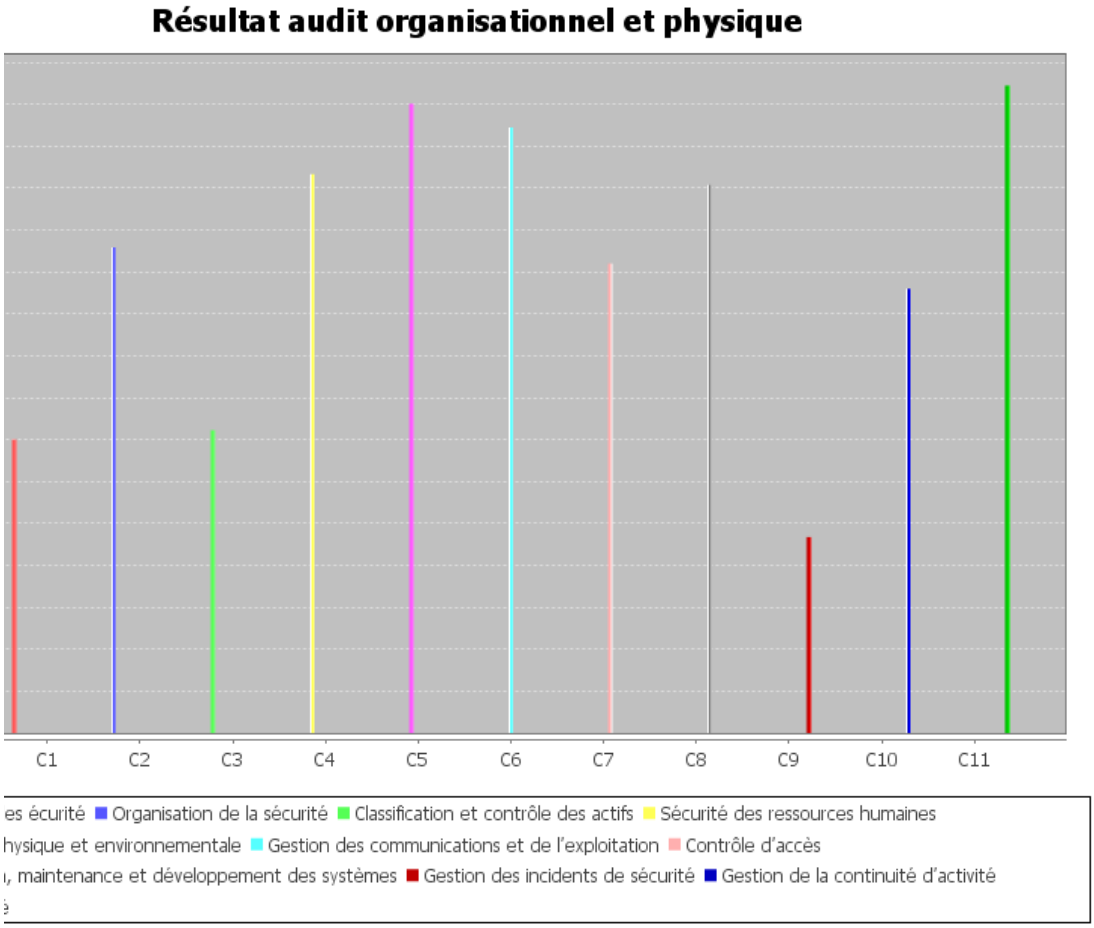


Figure 12 : Histogramme représentatif du niveau de sécurité de l'ENIM

de ces résultats, l'école enregistre une conformité globale de 65%, par rapport à la SO/IEC 27002 ; cette valeur situe l'état de santé de la sécurité de l'audité dans la zone turité. J'aborde à présent l'analyse des résultats obtenus. Les points seront abordés es clauses (ou chapitres) définis dans la norme ISO/IEC 27002 :2007 selon l'ordre uel elles ont été évoquées.

alyse des résultats :

l'analyse de chacune des clauses, nous leurs attribuerons une classification en du degré de gravité de non-conformité par rapport à la norme ISO/IEC 27002 :2007. ssification comprendra trois classes :

Faible: indique une pratique de sécurité qui nécessite une attention (conformité>=80%).

Moyenne: indique une pratique de sécurité importante car les risques sont importants. Ainsi cela nécessite une attention toute particulière à court ou moyen terme (60%<conformité<80%.).

Critique: indique une pratique de sécurité très importante, car les risques encourus sont très importants. (Conformité<60%).

litique de sécurité :

iveau de conformité de cette clause par rapport à la norme ISO 27002 est de 56%. s'explique par la présence d'une forte politique de sécurité.

sécuriser l'accès aux données d'une façon logicielle, l'école exige une ntification centralisée et l'implémente via une architecture à base de RADIUS.

ninistrateur de l'école sécurise également l'accès physique aux données : les serveurs s dans une salle portant des fiches interdisent tout accès non autorisé. Seules les nnes habilitées y ont l'accès.

le dispose aussi d'un firewall STONGATE de la famille stonsoft, qui permet de r le trafic réseau entrant et sortant, rediriger les trafics sur des supports internet ents, prioriser les trafics selon leurs provenances, il permet aussi de faire l « 'deep ction » et le filtrage URL.

ur sécuriser les différentes machines branchées sur le réseau, l'école dispose d'un irus avec une licence de 500 machines d'une durée de 3 ans, avec les mises à jour alisées.

ui manque à cette PSSI, c'est qu'elle n'est pas documentée, cela veut dire que l'école ispose pas d'un document écrit de la PSSI, et elle n'est pas communiquée aux

ɔnnels de l'école afin de les sensibiliser de l'importance de la sécurité. Le niveau de ité accordé à cette clause est moyen

ganisation de la sécurité :

u de conformité de cette clause par rapport à la norme ISO 27002 est de 44,7%. Ce e conformité s'explique par le fait que les services fournis par des personnes tiers ement) sont contrôlés. Egalement, les informations sensibles de l'école sont es et attirent l'attention des responsables quant à leur protection. Cependant, il pas pour l'instant la fonction de Responsable de Sécurité du Système d'Information u sein de l'école. Cette responsabilité reste planifiée, mais n'a pas encore vu le jour. use enregistre un degré de sévérité critique.

ɔntrôle et classification des actifs :

ıuse enregistre une conformité de 36,11% ; cela lui inflige une sévérité critique. ble des principaux actifs de l'organisme est identifié puis répertorié. Il s'agit entre es serveurs métiers, des postes de bureau, des équipements réseau, des applications par l'école, des équipements de lutte contre les incendies, etc. toute personne ant un équipement en devient responsable jusqu'à son retour. Les documents sous format papier sont rangés dans des armoires. Chaque dossier est muni d'une telle que la date d'entrée, la date de sortie etc.

nt, les procédures de classification ne se basent pas sur une documentation précise ıit les critères de classification, de sorte à pouvoir évaluer les conséquences d'une ı de cet actif sur l'école.

il n'existe pas de procédure d'étiquetage pour la classification ; simplement, les considérés sensibles sont astreints à rester dans le bureau du responsable en question.

curité liée aux ressources humaines :

ant le volet ressources humaines et sécurité, la vérification de l'authenticité des ıts (diplômes, documents fournis,…) des employés faite par un service dédié

es humaines. En effet, le recrutement du personnel est effectué par l'organisation de sous la responsabilité de service recrutement. Il revient donc au jury établi par 'examiner minutieusement les pièces fournies par les participants retenues.

ant de prendre effectivement la fonction, les candidats retenus sont informés de leur sponsabilité vis-à-vis de l'organisme. Ces nouveaux employés sont informés (et de leurs droits et devoirs vis-à-vis de la sécurité de l'école également. Le personnel e est ainsi informé de son rôle dans la gestion de cette sécurité. En dehors de ces ions à l'embauche, il n'est pas défini de procédures visant à rappeler à l'ensemble du l son rôle dans la sécurité de l'école. Le personnel du service informatique est soumis éances de formations pour les sensibiliser sur l'importance de la sécurité de ation et leur inculquer les notions de bonnes exploitations des technologies de ation.

u de sévérité appliqué à cette clause est moyen car elle reste conforme à la norme 99 à 62,96%.

curité physique et environnementale

nne de cette clause est de 69,72% par rapport à la norme iso 27002, soit une sévérité . L'environnement de localisation ne présente pas d'exposition à des dangers naturels s. En ce qui concerne la sécurité physique des locaux elle est assurée par une clôture ntoure, ainsi que des postes de gardiennage qui surveillent les principales entrées. Un ne d'enregistrement des visiteurs a été instauré. Il permet de relever les identités des ainsi que les dates et heures d'entrée et sortie.

sensible qu'est la salle serveur bénéficie d'une sécurité toute particulière, et ce à accès qui y est très réservé. En effet pour protéger cette salle de toutes malveillances s, l'accès est protégé par une clé que seulement trois personnes possèdent. Elles sont s habilitées à y pénétrer.

ction des serveurs, routeurs et commutateurs contre les aléas électriques est mise en aque serveur est muni d'un onduleur, et d'autres onduleurs veillent à l'alimentation eurs et commutateurs en cas de coupure d'alimentation électrique. Les câblages es et réseau sont encastrés.

u de la salle serveur le câblage réseau est bien organisé. Egalement ces câbles sont , ce qui rend la tâche d'authentification d'un câble très facile.

ens réglementaires de lutte contre les incendies sont en place tel que des bouches à
s ou des détecteurs de fumées. Cependant aucune procédure de test de ces moyens et
ents de protection n'est réalisée.

aux des employés sont dotés de serrures, offrant la possibilité de les verrouiller en
ence. Egalement l'accès physique aux postes de travail de chacun des utilisateurs,
tain, est protégé par un mot de passe. Pour éviter toutes tentatives de vol des
ents, ceux devant quitter ou entrer dans les locaux doivent bénéficier de bons de
de décharges en non des bénéficiaires. A travers ces bons les équipements sont
és, en entrée comme en sortie.

estion de l'exploitation et des communications :

eurs métiers sont constitués à70 % de serveurs LINUX et à 30 % de serveurs
s 2008 et 2003. Les postes de bureau sont à 100% équipé de système d'exploitation
t Windows XP et windows7. Les systèmes d'exploitation utilisés bénéficient de
d'exploitation. Les mesures de continuité de services sont en parties assurées. Le
AN de l'école est de type Ethernet, et un adressage privé a été mis en place. Bien
ste une politique d'adressage par VLAN qui permet une segmentation à un niveau
é. Egalement le réseau LAN est organisé en domaine ce qui rend difficile de passer
upe à un autre et qui rend la sécurité robuste.

employé (corps administratif ou enseignant) bénéficie d'un ordinateur de bureau, dont
l'entière responsabilité.

ole des serveurs est protégé des intrusions externes par un firewall StoneGate de la
nesoft. Il existe une zone DMZ contient tous les serveurs qui doivent avoir un accès
n de l'intérieur que l'extérieur notamment le serveur de messagerie et le serveur
nt le site web de l'école.

ntrôle d'accès :

enregistre une moyenne de 58%, par rapport à la norme, donc une sévérité critique.
tique de mot de passe est instaurée au sein de l'organisme, pour l'accès à certaines
ons. Cependant ces mots de passe ne sont pas changés suivant une fréquence bien
La permanence de ces mots de passe ne permet pas de réduire les risques d'usurpation
de passe ou de vol. Egalement, l'accès aux locaux sensibles tel que la salle serveur

tégé par une simple clef. Seul le chef de service est habilité à accéder à ce local . nt, la salle ne dispose pas d'une alarme (sonore) indique l'ouverture de la porte de e, et ce, pendant et en dehors des heures de travail.

listant, à partir de l'Internet est protégé on utilisant un VPN d'accès. Etant donné peut garantir qu'un accès illicite ne peut se réaliser à 100%, il est donc important de de système de détection d'éventuelles intrusions. De ce fait l'école se dote d'un de détection d'intrusion (IDS), et une option de prévention d'intrusion (IPS) intégré irewall.

quisition, maintenance et développement des systèmes :

use présente une sévérité critique due à la moyenne de 58% par rapport à la norme 002. L'acquisition de nouveaux systèmes porte l'attention particulière des iciens afin de s'assurer que le système à acquérir correspond aux besoins de l'école et a pas à mal la sécurité. Egalement des tests pour s'assurer qu'un nouvel équipement as source de régression de service sont effectués. Cependant, Les fichiers systèmes ts informatiques ne suivent pas de procédures particulières de préservation de toute ion.

nt les procédures de chiffrement ou de signature électronique ne sont pas intégrées procédures de l'école. De même la sécurité de la documentation des systèmes n'est ualité.

estion des incidents de sécurité :

use enregistre une moyenne de 38,37% par rapport à la norme ISO 27002, donc une critique. Le personnel a été sensibilisé sur la nécessité de déclarer les incidents ou e sécurité rencontrée. Cependant, pour l'instant il n'est planifié l'instauration de es pour la gestion des incidents de sécurité. L'école a planifié l'élaboration d'un ombre de règles pour la reprise d'activité en cas de catastrophe ou d'incident liés à urs humaines. Cependant les rapports détaillés des incidents qui surviennent ne sont s. Il n'est donc pas possible de s'informer des incidents déjà survenus.

Gestion de la continuité d'activité :

use présente une sévérité moyenne liée à sa moyenne de 60% par rapport à la norme
)2.

ne dispose pas de plan clair et précis révélant dans les détails et dans l'ordre les entreprendre en cas de reprise suite à une catastrophe.

mettre une continuité d'activité en cas de coupure de la fourniture électrique, chaque st doté d'un onduleur. Lors de mon enquête, j'ai constaté que la salle serveur se dote oements de la haute gamme pour la climatisation.

de veiller à une température idéale au fonctionnement des serveurs métiers n'est pas lace, de même pour une alarme en cas d'augmentation de la température.

uation est d'autant plus critique si cela arrivait en pleine nuit. Aussi il n'est pas prévu surveillance de la salle serveur.

Conformité :

use a une moyenne de 76%, d'où une sévérité moyenne par rapport à la norme ISO

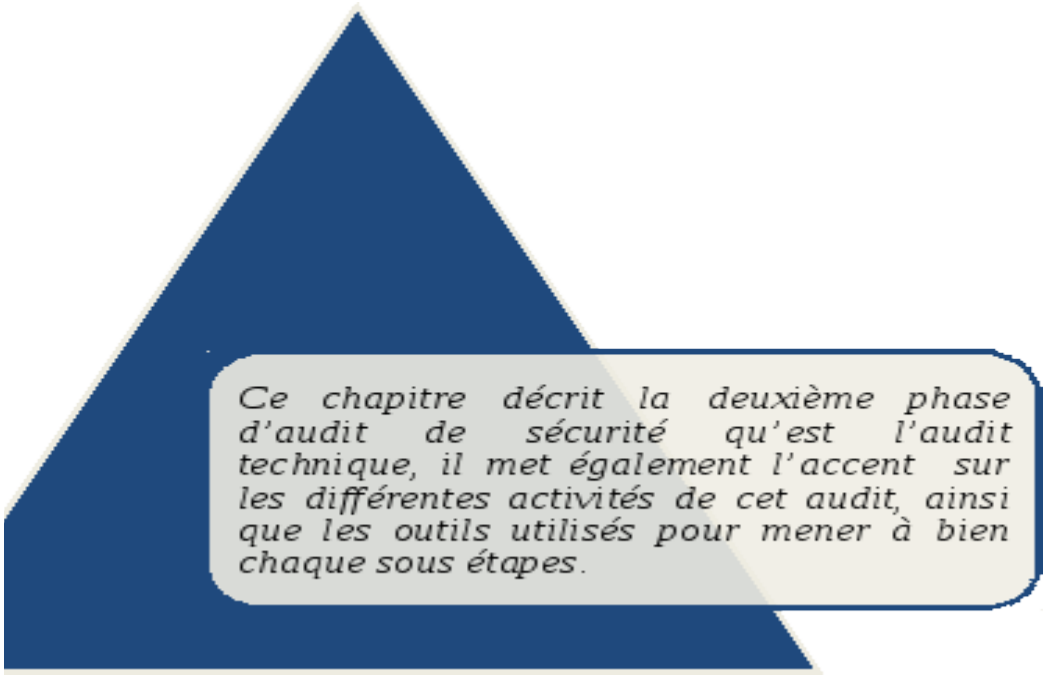
es applications commerciales utilisées au sein de l'école sont dotées de licences ation.

nt, le personnel n'est pas averti sur les bonnes utilisations des technologies de ation au sein de l'école à l'aide d'une charte. Egalement, l'audit périodique n'est pas ncré dans les habitudes de l'école. Il en est de même pour le suivi des règles édictées le elle-même.

Conclusion

de cette étape de l'audit, je constate au vu des réponses obtenues, que la maturité en de sécurité de l'école admet un niveau en général en dessous de 60%. Je vérifie ce u grâce à l'audit technique qui constitue la prochaine étape de ma mission d'audit.

Chapitre IV : Audit technique de l'ENIM



ıction :

à présent la deuxième étape importante de mon audit de l'ENIM. Cette étape ur l'audit technique. Il s'agit dans un premier temps de déterminer la topologie ou cture du réseau de l'audité. Dans un second temps, j'établirai un diagnostic des actifs sur le réseau de l'audité, ainsi que de leurs éventuelles vulnérabilités. Enfin je ai au test de vulnérabilité des équipements, pour estimer leur capacité à résister aux

faire je me suis basée sur la distribution Unix Backtrack5 qui englobe tous les outils
t de sécurité réseau et de pentest (Test d'intrusion).

udit de l'architecture réseau :

pe constitue la première étape dans la phase de l'audit technique. Elle consiste en la
te de différentes architectures (physique et logique) du réseau audité.
ase a été faite au niveau de l'étude de l'existant : voir II.1.2 page 32

acktrack 5 R1 :

ck est une distribution GNU/Linux dont l'objectif est de regrouper un ensemble
nécessaires à des tests de sécurité sur un réseau. C'est un outil complet qui vise à
ous les problèmes de sécurité moderne.
suivante montre l'interface d'accueil de backtrack 5 :

Figure 13 : L'interface backtrack5

ière version de BackTrack est sortie au début 2006, aujourd'hui la version 5 Pre-
2 est disponible.

tribution comprend environ 300 outils d'audit de sécurité, permettant par exemple de
r le réseau (***Genlist***), de sniffer ce réseau (***Wireshark***), de craquer une connexion Wifi
k), d'écouter les ports (***Nmap***) ou de pénétrer une machine distante (**Metasploit**).

que Tenable, qui est le développeur de l'excellent outil d'audit réseau Nessus, n'a pas
son intégration dans BackTrack, donc je vais l'installer et l'utiliser.

ck est à l'heure actuelle la distribution la plus aboutie en matière de sécurité
ique. BackTrack se qualifie tant par le nombre impressionnant d'outils que leur par
econnu par les professionnels. C'est pourquoi, BackTrack a été élu comme étant la
distribution de sécurité.

ondage des services réseau :

: l'ensemble des services actifs par poste de travail au niveau de l'audité a été chose grâce aux outils Nessus et Nmap.

application incontournable dans le cadre des scanners réseau nous a été d'un apport t.

Sondage avec Nessus :

st un outil de test de vulnérabilité. Il fonctionne en mode client/serveur, avec une graphique. Une fois installé, le serveur« Nessusd », éventuellement sur une machine effectue les tests et les envoie au client « Nessus » qui fonctionne sur une interface e.

st un produit commercial diffusé par la société TENABLE Network Security. Il peut être utilisé gratuitement avec une base des vulnérabilités dont la mise à jour est l'une semaine.

f de cette partie est surtout de présenter les résultats des scans de vulnérabilités sur le réseau informatique de l'audité. Dans ce qui suit l'interface d'initialisation de

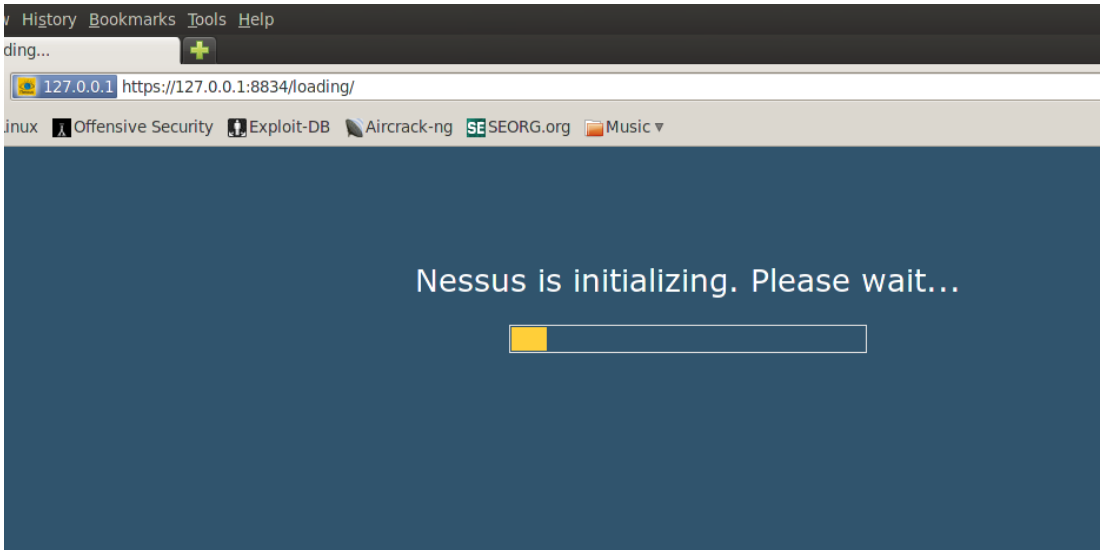


Figure 14 : Initialisation de Nessus

Nessus est démarré, il affiche une interface de connexion comme la figure suivante puis on lance le scan selon les paramètres désirés et qui répondent à notre besoin.

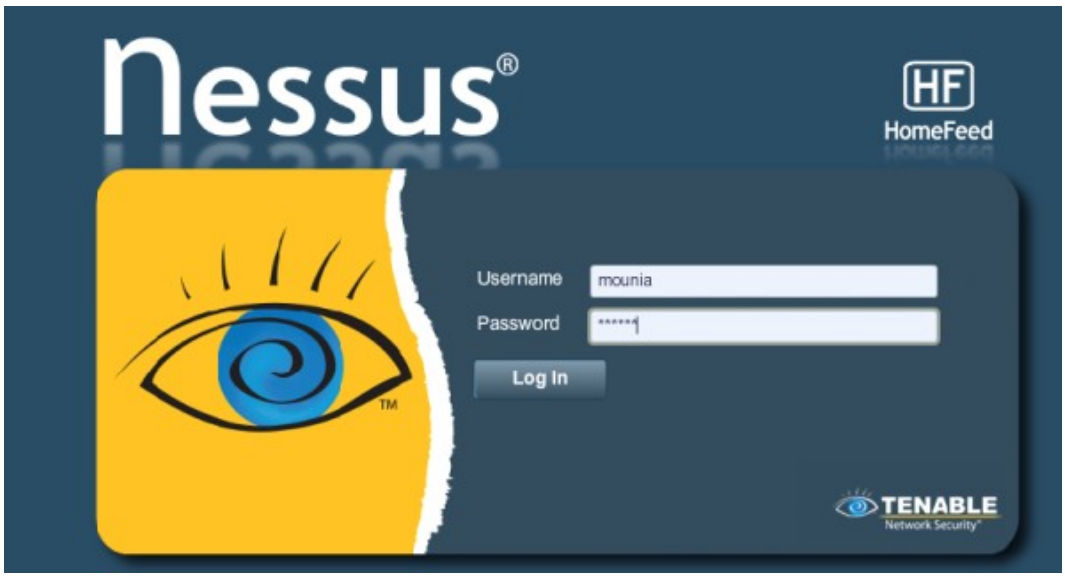


Figure 15 : Connexion au service Nessus

n cas le scan lancé concerne le réseau de management de l'audité et qui contient 29 ent actifs comme montre la capture suivante.

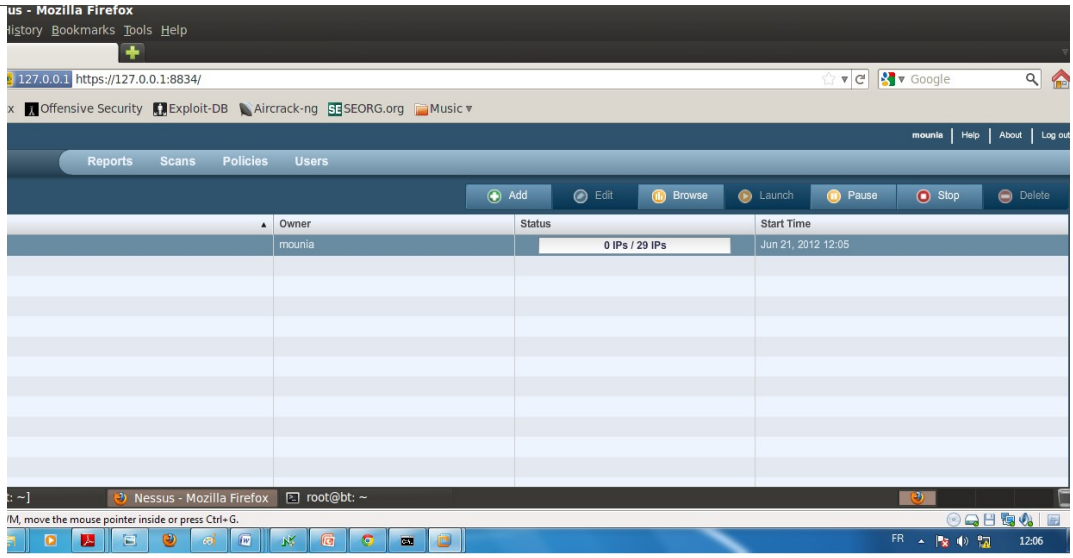


Figure 16 : Lancement de scan de réseau de management

le scan terminé, Nessus génère un rapport de vulnérabilités trouvées, en les classant rs états de criticités, ainsi des solutions possibles pour corriger ces failles.

ple de rapport Nessus est capturé ci-contre :

Figure 17 : Rapport de vulnérabilités de réseau de management

Sondage avec Nmap :

st un outil d'exploration réseau et scanneur de ports/sécurité dont la syntaxe est la : ***nmap [types de scans ...] [options] {spécifications des cibles}.*** Nmap existe aussi en aphique sous le nom « Zenmap GUI ».

ermet d'éviter certaines attaques et aussi de connaître quels services tournent sur une . Une installation faite un peu trop vite peut laisser des services en écoute (donc des verts sans que cela ne soit nécessaire) et donc vulnérables à une attaque. Nmap est un rès complet et très évolutif, et il est une référence dans le domaine du scanning.

ion de Nmap :

été conçu pour rapidement scanner de grands réseaux, mais il fonctionne aussi très une cible unique. Nmap innove en utilisant des paquets IP bruts (raw packets) pour er quels sont les hôtes actifs sur le réseau, quels services (y compris le nom de ion et la version) ces hôtes offrent, quels systèmes d'exploitation (et leurs versions) ent, quels types de dispositifs de filtrage/pare-feux sont utilisés, ainsi que des s d'autres caractéristiques. Nmap est généralement utilisé pour les audits de sécurité nombreux gestionnaires des systèmes et de réseau l'apprécient pour des tâches de comme les inventaires de réseau, la gestion des mises à jour planifiées ou la nce des hôtes et des services actifs.

ort de sortie de Nmap est une liste des cibles scannées ainsi que des informations ientaires en fonction des options utilisées.

e suivante présente une interface d'exécution de Nmap. Les trois fonctionnalités s peuvent être simultanément exécutées.

écouverte du réseau,

étermination des ports ouverts,

étermination du système d'exploitation des machines cibles.

mon approche à travers l'exécution de la commande : **Nmap –v –O 192.168.1.0/24** sultat suivant :

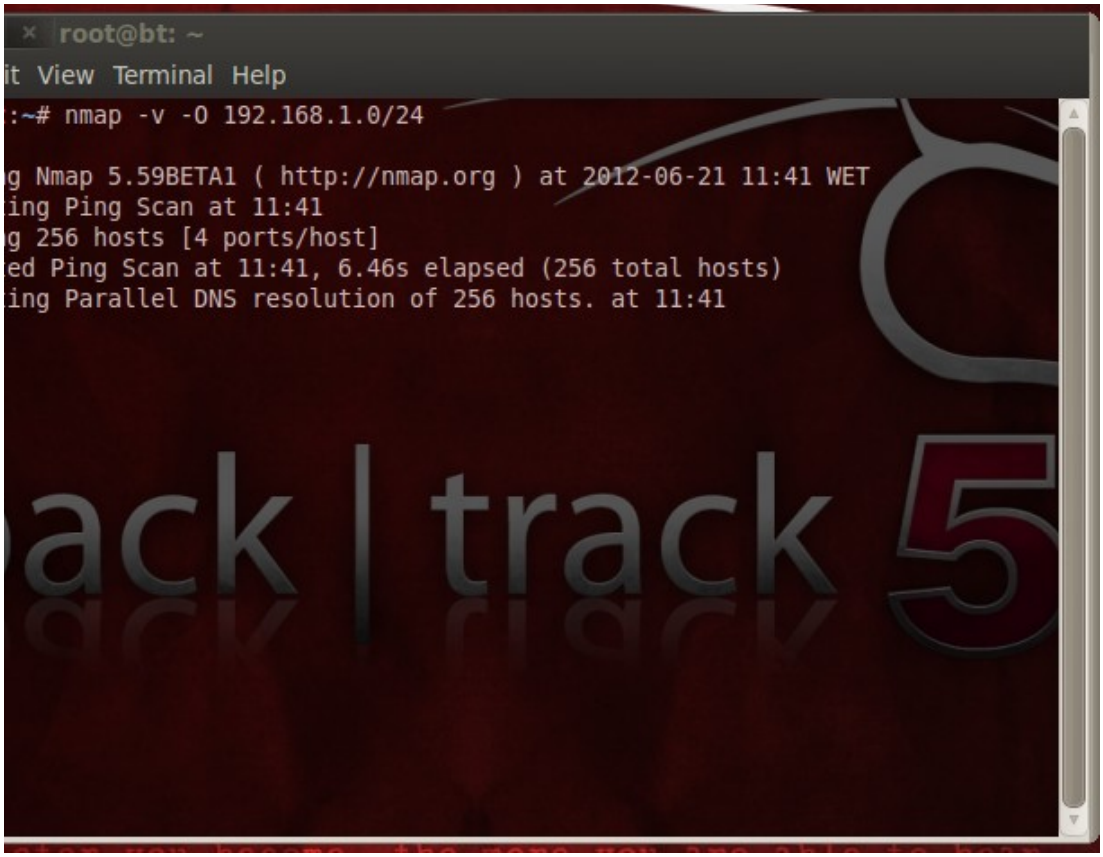


Figure 18 : Scan de réseau 192.168.1.0 avec NMAP

I-5 Analyse des services vulnérables par serveur :

eau de travail, il m'a été autorisé de faire une analyse sur les serveurs suivants :

web, Serveur de messagerie et serveur de nom de domaine DNS.

l'outil Nessus, j'ai pu dégager un ensemble de protocoles et ports ouverts qui ne pas l'être, certains d'entre eux présentent un risque majeur de fait que les ilités qui leurs sont associées sont susceptibles d'être exploitées.

yses ont été effectuées en boite blanche, pour des raisons de confidentialité, il ne s autorisé de les faire figurer dans mon rapport, qui est un rapport public.

s, pour mettre en évidence cet outil en pratique, j'ai attaqué une machine dont ne peut pas mettre en cause le fonctionnement du réseau de l'organisme

I-5 Méthodologie globale d'une attaque :

ers ayant l'intention de s'introduire dans les systèmes informatiques recherchent dans er temps des **failles**, c'est-à-dire des *vulnérabilités* nuisibles à la sécurité du système, protocoles, les systèmes d'exploitation, les applications ou même le personnel d'une ion ! Les termes de **vulnérabilité**, de **brèche** ou en langage plus familier de **trou de** (en anglais *security hole*) sont également utilisés pour désigner les failles de sécurité.

voir mettre en œuvre un exploit (il s'agit du terme technique signifiant *exploiter une ilité*), la première étape du hacker consiste à récupérer le maximum d'informations itecture du réseau et sur les systèmes d'exploitations et applications fonctionnant sur La plupart des attaques sont l'œuvre de *script kiddies* essayant bêtement des exploits ur internet, sans aucune connaissance du système, ni des risques liés à leur acte.

que le hacker a établi une cartographie du système, il est en mesure de mettre en on des exploits relatifs aux versions des applications qu'il a recensées. Un premier ne machine lui permettra d'étendre son action afin de récupérer d'autres informations, ellement d'étendre ses privilèges sur la machine.

n accès administrateur (le terme anglais *root* est généralement utilisé) est obtenu, on rs de compromission de la machine (ou plus exactement en anglais *root compromise*), ichiers systèmes sont susceptibles d'avoir été modifiés. Le hacker possède alors le niveau de droit sur la machine.

d'un pirate, la dernière étape consiste à effacer ses traces, afin d'éviter tout soupçon t de l'administrateur du réseau compromis et de telle manière à pouvoir garder le plus s possible le contrôle des machines compromises.

a suivant récapitule la méthodologie complète :

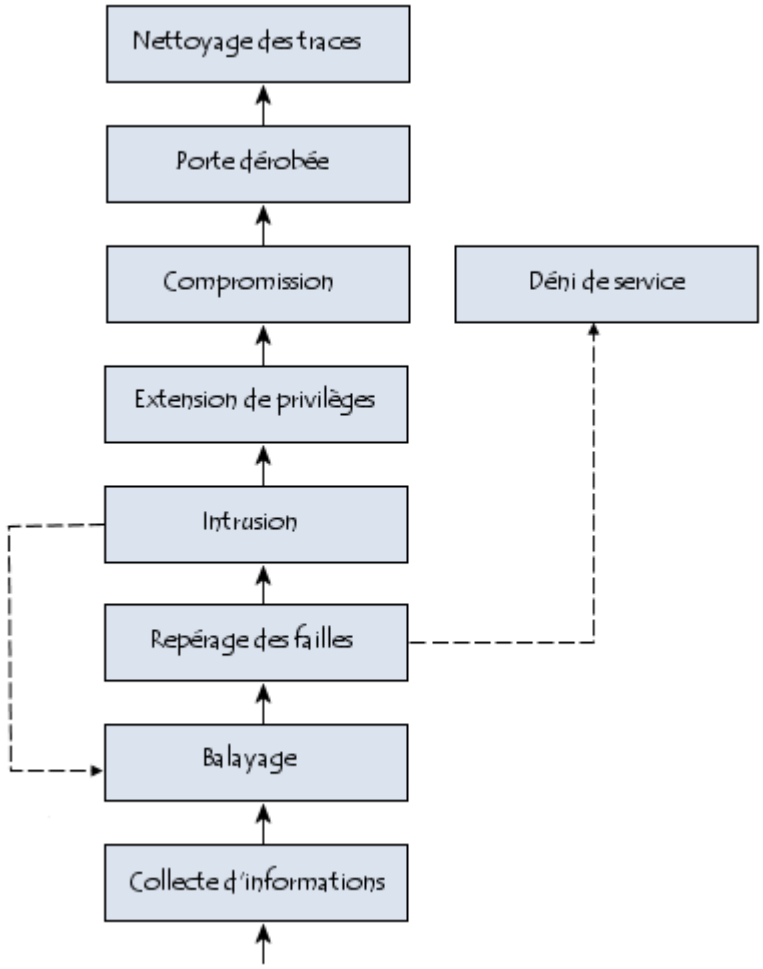


Figure 19 : La méthodologie d'une attaque

I-6 Test intrusif :

d'intrusion (en anglais *penetration tests*, abrégés en *pen tests*) consistent à éprouver ens de protection d'un système d'information en essayant de s'introduire dans le en situation réelle.

ıgue généralement deux méthodes distinctes :

a méthode dite « boîte noire » (en anglais « *black box* ») consistant à essayer trer le réseau sans aucune connaissance du système, afin de réaliser un test en ion réelle ;

a méthode dite « boîte blanche » (en anglais « *white box* ») consistant à tenter de ɔduire dans le système en ayant connaissance de l'ensemble du système, afin ɔuver au maximum la sécurité du réseau.

démarche doit nécessairement être réalisée avec l'accord (par écrit de préférence) du t niveau de la hiérarchie de l'entreprise, dans la mesure où elle peut aboutir à des ventuels et étant donné que les méthodes mises en œuvre sont interdites par la loi en de l'autorisation du propriétaire du système. Un test d'intrusion, lorsqu'il met en une faille, est un bon moyen de sensibiliser les acteurs d'un projet. Cette phase de este très importante. En effet, elle permet de faire prendre conscience aux bles de la gravité de leurs vulnérabilités, face aux attaques d'un esprit malveillant à l'organisme. Elle permet également de donner un aperçu de l'ampleur des ences néfastes qui pourraient advenir dans le cas où un esprit malveillant venait à leurs vulnérabilités.

complissement de cette étape, j'ai joué le rôle de l'attaquant étant à l'intérieur de me. Puis j'ai installé la version backtrack 5 R1 disponible sous format ISO sous une ne virtuelle VMware Workstation 7.

tribution se compose de différentes applications et j'en ai utilisé quelques-unes.

sant sur le Framework Metasploit la plateforme d'attaque, les résultats de Nessus et exploits et des payload afin de mener à bien une attaque.

Jtilisation de Métasploit :

ɔit est une plateforme d'attaque, open source, basée sur l'utilisation d'exploits afin er un code arbitraire sur un hôte distant. Chaque exploit est composé de payload. Ces

sont les codes qui sont exécutés pour permettre le succès de l'exploit. Le lancement
:aque à partir de Métasploit s'effectue en choisissant l'exploit, le payload puis la
l'attaque.

: suivante montre la console de Metasploit.

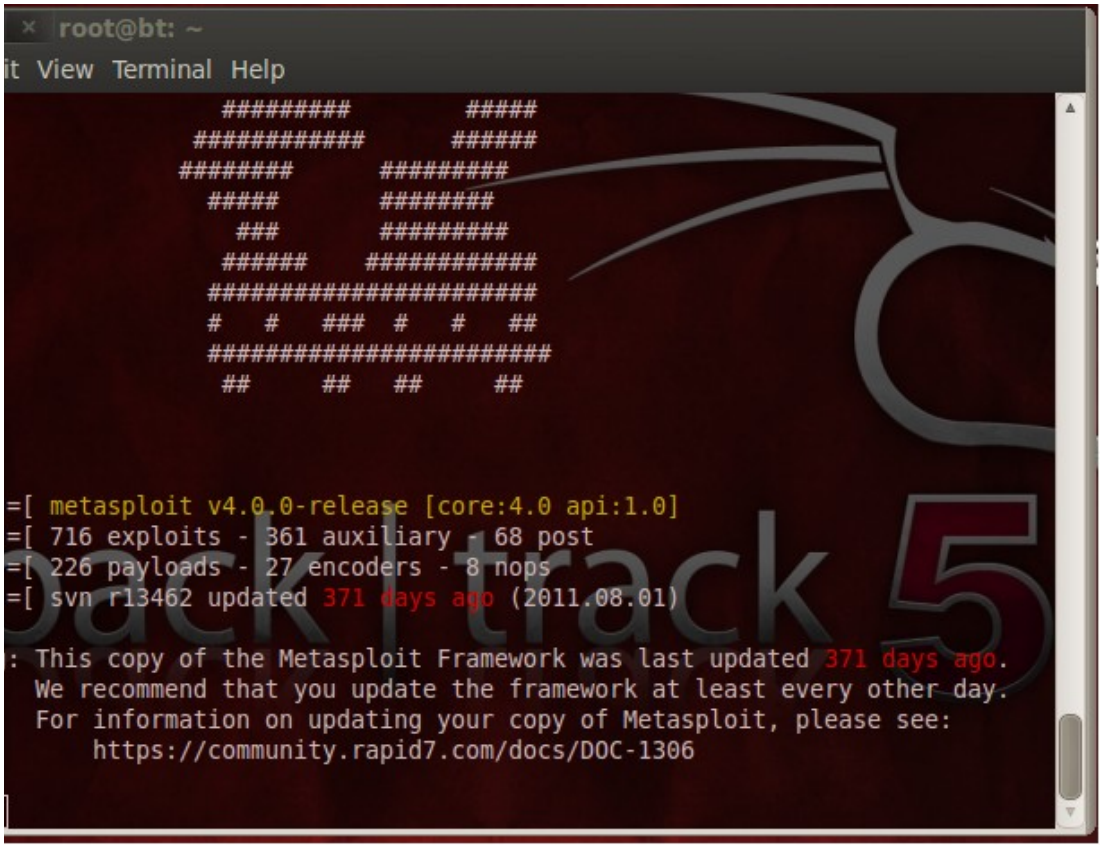


Figure 20 : Console d'accueil de Metasploit

lifférentes investigations, différentes vulnérabilités ont été découvertes. Métasploit,
d'exploits dans sa base, qui peuvent être utilisés pour les vulnérabilités observées.
ıyer mes propos, j'ai trouvé au sein de la base des exploits de Métasploit,
)67_netapi» qui utilise une vulnérabilité de protocole SMB "port 445". Le résultat de

loit résulte sur une connexion entre la machine d'auditeur et la machine cible (La comme montre la figure suivante :

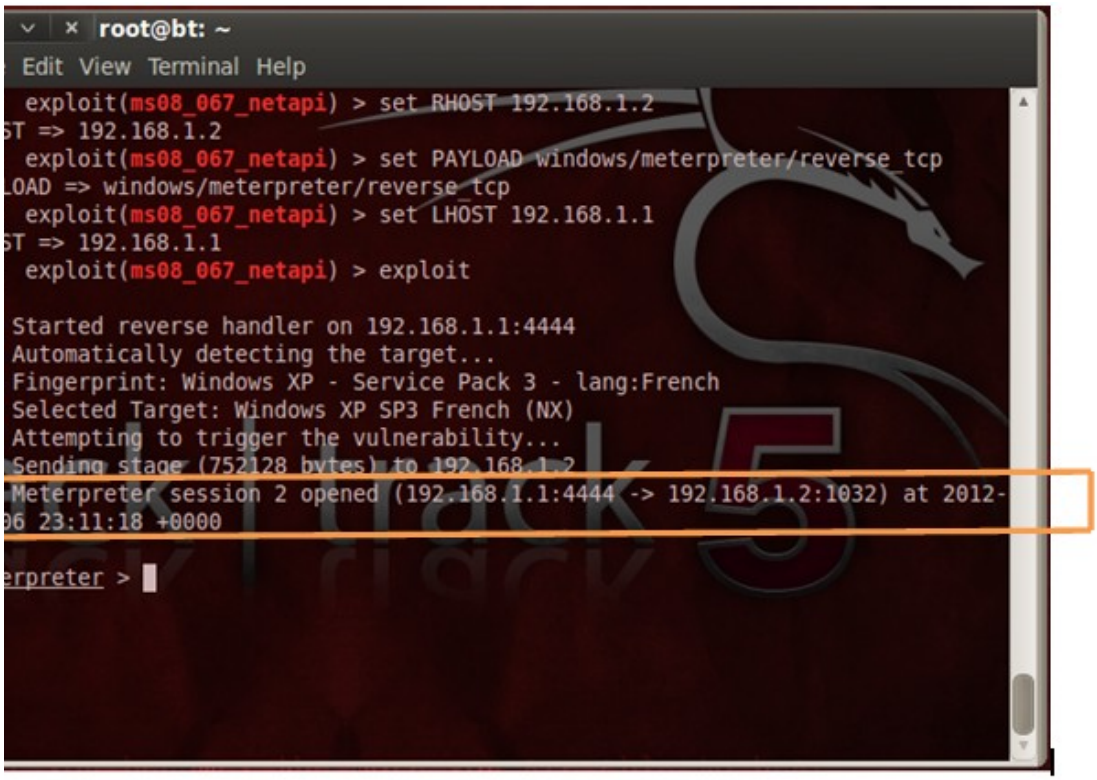


Figure 21: Attaque réussie, connexion établie.

ıple illustre l'exposition dont fait montre les serveurs de l'organisme. Une personne unte peu à dessein mettre à mal le bon fonctionnement des serveurs métiers.

udit des commutateurs :

mutateurs au sein de l'audité proviennent de la firme **HP_Procurve** aussi bien pour mutateurs d'étage que les commutateurs fédérateurs, L'interconnexion des uteurs est effectuée en pile (stack), chaque pile est constituée d'un bloc de

ıteurs, dont un joue le rôle du commander et les autres des salves ; l'accès à chaque fectue via une seule adresse IP et les autres composants de la pile comme des , ce qui facilite le management de l'actif.

dorsale de l'architecture est composée de deux Switch fédérateurs de la même firme urve.

ıst connecté par fibre optique sous forme de deux principales Etoiles, chacune autour érateur comme montre le schéma 9 (La MAP du réseau LAN).

udit des routeurs :

eau d'audit, on n'a pas pu aller plus loin, du fait que le routeur de l'ENIM est sous la otal de Meditel dans le cadre du réseau MARWAN.

st important à signaler, c'est que le contrat en question charge l'operateur de veiller à état de santé du routeur en termes de sécurité respecte les exigences en vigueur.

udit des firewalls :

es de firewaling on va détailler les principales fonctionnalités du firewall dont 'ENIM afin de monter qu'il réponde aux exigences en la matière

estion de la bande passante ;

oursuite des adresses suspectes ;

alcklisting des adresses bavardes ;

eep inspection.

Conclusion

ésent chapitre m'a permis certes de manipuler différents outils, mais il a été surtout portance capitale pour mettre à nu les failles de sécurité de système d'information de té. Suite aux résultats des tests de vulnérabilités et d'intrusion effectués, plusieurs andations à fournir sur le niveau organisationnel et technique. Le chapitre suivant mit l'accent sur ces préconisations.

pitre V: Recommandations organisationnelles et techniques

Ce chapitre porte sur la dernière phase d'audit de sécurité qui est une finalité des différentes étapes précédentes, elle donne lieu aux recommandations à faire à l'audité sous la lumières résultats de l'audit pour être en mesure de corriger la PSSI dans l'optique de palier aux failles et lacunes.

uction :

tre fait office de chapitre visant à proposer des recommandations par rapport aux es clauses de la norme ISO/IEC 27002. Egalement, au vu des vulnérabilités s lors du chapitre précédent, je vais proposer une architecture réseau sécurisé.

commandations au niveau organisationnel et physique :

mmandations suivantes visent à apporter des suggestions pour améliorer l'aspect ionnel et physique de la sécurité du système d'information de l'ENIM.

itique de sécurité :

tion de l'école doit fournir les directives précises et claires pour l'édition d'un t de sécurité qui renfermera la politique de sécurité. Egalement, cette dernière doit son engagement et son appui pour l'établissement de cette politique. Ce document élaboré et approuvé par la direction, pourra être publié au personnel, tout en veillant à ommuniquer des informations sensibles. Aussi une revue régulière de cette politique té doit être planifiée pour tenir compte des possibles changements qui surviendront.

ganisation de la sécurité :

r la sécurité de l'organisme passe par l'établissement et la désignation d'un able de Sécurité des Systèmes d'Information (RSSI). Ce dernier devra documenter s mesures ou règles de sécurité qu'il devra mettre en œuvre. Une définition claire et

les rôles et responsabilités vis-à-vis de la sécurité de l'information est nécessaire. nt, l'école doit se faire aider de spécialistes en sécurité quand le besoin se fait sentir.

ıssification et contrôle des actifs :

aire des actifs ne doit pas seulement tenir compte des équipements, mais également ments. La classification et le contrôle des actifs nécessitent une définition claire et es différentes classes d'actifs possibles. Partant de ce fait, il serait aisée de classer les de les marquer de cette classe (exemple : politique d'étiquetage…), puis de les le niveau de sécurité nécessaire. Aussi l'organisme doit préciser pleinement et nt les procédures liées à la destruction des informations.

:urité des ressources humaines :

ortant de mettre en place une procédure d'information et de formation continuelle du l sur les risques de sécurité, ainsi que leur contribution à l'élaboration de cette L'élaboration de chartes précisant le comportement à avoir vis-à-vis des technologies unication est un moyen pour y parvenir. Aussi l'école doit apporter les changements es en cas de départ d'un membre du personnel (surtout s'il est lié à des informations), pour réduire les risques d'atteinte à la sécurité de l'école de la part de cet employé.

:urité physique et environnementale :

intuitive, la sécurité évoque la sécurité physique et environnementale, et cette vision une réalité au sein de l'école. N'empêche que cette sécurité doit s'appuyer sur un t qui lui est lié et également sur un contrôle des moyens de sécurité mis en place par

s. Aussi l'école doit s'assurer de la mise en œuvre d'une zone sécurisée des ents à réutiliser.

stion des communications et de l'exploitation :

doit définir des procédures d'exploitation du réseau qui spécifie l'exécution du ıt informatique, les sauvegardes ainsi que la gestion des anomalies. Egalement, pour ı bon fonctionnement des équipements qui concourent à la protection de l'intégrité aussi bien du local que de ces équipements. Il s'agit entre autre de veiller au ıement des moyens réglementaires de lutte contre les incendies. Toujours pour veiller rité physique de son matériel informatique (serveurs), il est opportun de se doter ırme qui serait active au cas où la température de la salle serveur serait au-dessus il fixé. Bien évidemment il faudra définir des rondes par les gardiens autour de ces Aussi, elle doit définir des critères rigoureux d'acceptation d'équipements. Afin de les traitements d'information non autorisés, il faut mettre en place une surveillance et afin d'enregistrer les activités sur un système donné. Pour une structure d'une telle e il serait nécessaire de se doter de serveur de Back Up afin d'éviter une interruption e en cas de défaillance de l'un des serveurs.

ntrôle d'accès :

tion des accès utilisateurs est nécessaire pour permettre l'accès aux personnes s et empêcher ceux n'étant pas autorisé d'accéder au système d'information. Aussi, ique efficace et rigoureuse de gestion de mots de passe utilisateurs doit être définie et e au sein de l'école. Egalement, les droits d'accès attribués aux utilisateurs doivent s de façon périodique par la direction concernée.

quisition, maintenance et développement des systèmes :

ation de procédures pour assurer la confidentialité tel que le chiffrement ou la électronique doit faire partie des procédures développées de l'école. Il s'en suit donc estion des clés doit être mise en place pour la meilleure organisation de l'utilisation

niques cryptographiques. Egalement assurer la sécurité des fichiers de projets iques doit être tenu.

stion des incidents de sécurité :

portant de s'assurer que les évènements de sécurité, ainsi que les faiblesses relatives me d'information de l'école sont communiqués aux entités concernées qui se nt d'appliquer les mesures correctives dans les délais les plus brefs.

pose que la définition et la structuration de la remontée des incidents de sécurité se faire afin de pouvoir agir immédiatement dans les cas urgents. Le personnel doit rmé de l'importance à signaler les failles de sécurité détectées. La gestion des de sécurité doit attirer l'attention des responsables de sécurité. En effet une gestion e d'incident survenu serait profitable pour l'organisme. Egalement un rapport détaillé cident permettrait de se prémunir d'une répétition de ce dernier, ou d'y faire face ent en cas d'occurrence du même type d'incident.

estion de la continuité d'activité :

peut être confrontée à un désastre de quelques origines et à n'importe quel moment ; pouvant altérer le système d'information. C'est pourquoi il est important de mettre en s processus de recouvrement pour assurer la continuité d'activité de l'école. Cela r l'élaboration d'un plan de continuité d'activité qui répond aux exigences de Ce plan doit connaître une évaluation de façon régulière. Aussi, assurer la continuité passe par le contrôle continu et permanent des moyens de protection mis en œuvre les sauvegardes qui sont effectuées. D'ailleurs ces dernières peuvent être chiffrées de sécurité.

onformité :

nné que l'école traite des données à caractère confidentiel(les salaires des employés, des étudiants), ces dernières doivent rester secrètes. Définir des procédures d'audit doit être intégré aux procédures de l'école.

commandations au niveau technique :

ommandations de cette partie ne sont qu'une conséquence des scans, des tests ons effectués dans les précédentes sections ainsi que de notre expérience en audit de

neture des ports non utilisés.

s non utilisés peuvent être exploités à tout moment par les attaquants comme porte dans le système.

nt être fermés parce qu'ils présentent un risque pour la sécurité.

re les serveurs furtifs :

igurations par défaut doivent être évitées au niveau des serveurs. Les informations e type et la version du système d'exploitation utilisé, les versions des services qui sur les différents ports doivent être cachées et rendues inaccessibles lors des scans. ons réservées à cet effet se trouvent dans les fichiers de configuration des différents

Les fichiers de configuration des différents serveurs doivent être édités et modifiés
er d'avoir des serveurs dits « bavards ».

serveur Apache par exemple, il faut ajouter les lignes suivantes dans le fichier
:

kens Prod

gnature Off

ise à jour des applications :

on des applications ne concerne pas seulement les commodités d'utilisation au niveau
rface et l'ajout des fonctions supplémentaires mais aussi la sécurité de ces
ons. Ce dernier aspect n'est pas souvent perçu par l'utilisateur non averti qui est de ce
nsible à la mise à jour des applications. Ainsi plusieurs versions d'une même
on offrent souvent les mêmes fonctions ainsi que les mêmes commodités d'utilisation
dernières versions corrigent souvent certains détails de sécurité qui ne sont pas
nt perceptibles.

urité des mots de passe :

s de passe par défaut au niveau des serveurs, des routeurs ainsi que des applications
doivent être supprimés et remplacés par des mots de passe plus sûrs dès la première
n de ces derniers. Bien plus, les mots de passe doivent être choisis de manière à
aux attaques de type dictionnaire (noms, prénoms, date de naissance, mots du
courant) et aux attaques de force brute.

abattre ce type d'attaques il est recommandé de :

ne pas utiliser des mots du langage courant,

choisir des mots de passe longs (souvent au moins 8 caractères), avec une suite de
caractères totalement aléatoires et avec des caractères spéciaux,

lterner les majuscules et les minuscules.

ques sur les protocoles :

roposer dans cette section les parades à prendre pour éviter les attaques sur certains s : ARP, DHCP.

ISONING :

ion la plus immédiate consiste à saisir manuellement sur chaque poste la table de s adresses physiques présentes sur le réseau local. Si elle est immédiate, cette solution ment inapplicable compte tenu du nombre d'hôtes connectés au réseau local.

tion correcte consiste à mettre en place un serveur DHCP avec une liste «fermée» de ndance entre adresses physiques (MAC) et IP. Relativement à la solution précédente, haustive des adresses physiques est centralisée sur le serveur DHCP. On peut ensuite r la journalisation du service pour que toute requête DHCP relative à une adresse connue génère un courrier vers l'administrateur système ou réseau. Pour cela, trateur réseau peut utiliser sous Windows l'outil DHCPCMD pour configurer le lhcp en ligne de commande.

uxième solution convient également pour pallier les attaques sur le serveur DHCP.

e sécurité :

évolution rapide des dangers et des failles de sécurité des systèmes d'information et aux informatiques en particulier, seule la veille stratégique permet de répondre aux de continuité de service, elle permet ainsi d'être à l'écoute permanente des és aussi bien au terme des attaques et intrusions que des solutions.

surer cette veille, les responsables sécurité et veille doivent surveiller l'apparition de s *vulnérabilités* et alerter sur les *menaces* ciblant les systèmes et réseaux iques. Compte tenu du faut que la cellule sécurité et veille (appelé dans d'autres

ues R&D pour recherche et développement), l'audité est dans l'obligation de
: l'équipe pour pouvoir avoir assez de ressources à affecter à cette cellule et veiller à
tion continue.

: sécurité permet aux RSSI et à leurs équipes d'anticiper les incidents de sécurité :
, attaque virale, Dos,

'entreprise peut acquérir la version commerciale du logiciel d'analyse des
ilités connues Nessus pour bénéficier des mises à jour à temps vu la criticité de ce

ts internes de sécurité :

lits internes de sécurité doivent être réalisés de manière permanente et les
ndations qui en découlent doivent intégrer la politique de sécurité.

Conclusion

ue de ce chapitre, on a tracé les grandes lignes des recommandations à adopter pour ux failles détectées, mais aussi des recommandations qui permettront de prévenir les failles.

ctives :

ionnellement, mais pas dans tous les cas, les audits de sécurités donnent suite à tion d'une PSSI adapté à l'organisme audité et selon les résultats de l'audit.

dans ce cas de figure, la finalité était autre que l'aboutissement d'une PSSI, il ne s possible, toutefois de passer à côté de l'importance de la PSSI.

e raison, on en parle en guise de perspectives futures ; il s'agit de pouvoir tirer parti tats de l'audit réalisé pour pouvoir modéliser et rédiger une PSSI convenable .

eau, je recommande vivement l'utilisation du ***MotOrbac*** qui se base sur le modèle de ***OrBac***.

Conclusion générale

le sécurité des systèmes d'information occupe une place de plus en plus importante
es dernières années.

t consiste en l'audit de sécurité du système d'information de l'école nationale
ie minérale. Pour se faire, j'aborde ma mission d'audit à travers l'audit
ionnel et physique. Ce dernier se base sur une série de questions en référence à une
Dans mon cas, il s'agit de la norme ISO/IEC 27002 :2007, constituée d'onze
ux contrôles de sécurité. Cette norme est une référence en matière de bonnes
de sécurité. Grâce au questionnaire réalisé et l'ayant soumis pour réponse à
me audité, ce dernier présente une conformité de 65% par rapport à la norme ISO. Ce

conformité implique une forte maturité en termes de sécurité. Suite à l'audit ionnel, fait place l'audit technique. Cette phase est l'occasion de manipuler certains ns le but de découvrir l'architecture réseau, de détecter les vulnérabilités liées aux et de réaliser des attaques en se basant sur ces vulnérabilités. La découverte du réseau sible en utilisant des outils comme ***Nmap*** et ***Networkview***. Certains outils (Nessus) à scanner les vulnérabilités des services sur l'ensemble du réseau. Je constate que de x services enregistrent des vulnérabilités critiques. Par la suite j'ai exploité ces ilités en utilisant par exemple ***Métasploit*** pour la réalisation d'attaques. Une fois ces nces de sécurité constatées je propose des recommandations sur les aspects ionnels physique et technique.

raphies :

Tableau de bord de la sécurité réseau » de Cédric Llorens , Laurent Levier, Denis

sécurité informatique Ethical hacking « Apprendre l'attaque pour mieux se ».

ALEXANDRE FERNANDEZ-TORO Management de la sécurité de l'information n place d'un SMSI et audit de certification 2e Edition Implémentation ISO 27001 ».

ıtation de référence nmap : http://insecure.org/nmap/man/fr/man-port-scanning-es.html, mai 2007.

ıe Desgeorge. La sécurité des réseaux. Disponible sur http://www.guill.net/, mai

Burgermeister, Jonathan Krier. Les systèmes de détection d'intrusions. Disponible dbprog.developpez.com, mai 2008.

'aphies :

ojet.piratage.free.fr/menaces.html, mai 2007.

ac.org/index.php?page=orbac&lang=fr

w.ansi.tn/fr/audit/modele_cc_audit.htm

w.commune-tunis.gov.tn/fr/mairie_administration.asp#2

w.commune-tunis.gov.tn/fr/prestation_service0.htm

secure.com

w.ssi.gouv.fr/

w.clusif.asso.fr/fr/production/mehari/

w.ansi.tn/fr/audit/norme_iso15408.htm

tilisés :

ack http://www.remote-xploit.org/backtrack.html

loit http://www.metasploit.com/

http://www.nessus.org

http://insecure.org/nmap/

mes :

AO : Appel d'offre

ANSI : Agence Nationale de Système d'Information

BTS : Base Transceiver Station

CPGE : Classes Préparatoires aux Grandes Ecoles

DMZ : Demilitarized Zone

DNS : Domain Name Server

ENIM : Ecole Nationale d'Industrie Minérale

IEC : International Engineering Consortium

IDS : Intrusion Detection System

IPS : Intrusion Prevention System

LAN: Local Area Network

MARWAN:

PSSI : Politique de sécurité des Systèmes d'Information

QSSI : Questionnaire de Sécurité des Systèmes d'Information

RSSI : Responsable de Sécurité des Systèmes d'Information

SI : Système d'Information

SMSI : Système de management de Système d'information

SMB :

URL : Uniform Resource Locator

VPN : Virtual Private Network

VLAN : Virtual Local Area Network

WIFI : Wireless Fidelity

s:

nnaire pour l'audit organisationnel et physique se référant à la ISO/CEI 27002 :

nses sont choisies de 0 à 6 comme suit :

- Oui

- Partiellement oui
- Planifié
- Non
- Non applicable

1- Politique de sécurité :

politique de sécurité de l'information est-elle documentée et spécifient–elle nt les objectifs de sécurité de l'organisme, ainsi que des mesures de révisions de cette ?

que de sécurité de l'organisme définie-t-elle :

structure en charge de la définition de la politique de sécurité des systèmes ation ainsi que de sa mise en place ?

olan de continuité d'exercice, une éducation aux exigences de sécurité et aux risques rité, les conséquences d'une violation des règles de sécurité ainsi que les bilités des incidents de sécurité ?

structure chargée de l'évaluation des risques et de leurs gestions ?

principes de sécurité de l'information tel qu'ils soient conforment à la stratégie et aux objectifs de l'organisme ?

présentation de la stratégie de sécurité de l'information aux employés ainsi qu'aux es de l'organisme?

responsabilités générales et spécifiques liées à la gestion de la sécurité de tion ainsi que les incidents?

olitique de sécurité définie bénéficie-t-elle de l'appui de la direction générale?

2- Organisation de la sécurité :

lirection soutient activement la politique de sécurité au sein de l'organisme au moyen ives claires, d'un engagement démontré, d'attribution de fonctions explicites et d'une ssance des responsabilités liées à la sécurité de l'information ?

s activités relatives à la sécurité de l'information sont coordonnées par des unts ayant des fonctions et des rôles appropriés représentatifs des différentes parties nisme ?

règles de sécurité précisent t-elles une définition claire des tâches, rôles spécifiques on des responsables de sécurité de l'information ?

e-t-il une définition des possibles utilisations des informations confidentielles ?

e-t-il une définition des possibles utilisations des informations confidentielles ?

isques d'accès des tiers sont ils identifiés et contrôlés?

e-il un contrat formel contenant, ou se référant à toutes les exigences de sécurité pour a conformité avec les politiques de sécurité de l'organisation et les normes

xigences de sécurité sont abordées dans le contrat avec le tiers, lorsque l'organisation la gestion et le contrôle de tout ou partie de ses systèmes d'information, réseaux et / onnements de bureau?

informations sensibles sont-elles protégées de l'accès des partenaires de l'organisme ?

3- Classification et contrôle des actifs

ctifs de l'organisme sont ils identifiés et répertoriés ?

aque actif est-il associé un propriétaire qui doit en assurer également la responsabilité

ctifs sont ils classifiés suivant un degré de protection ?

assification bénéficie elle d'une documentation détaillée ?

4- Sécurité des ressources humaines

ôles et responsabilités en matière de sécurité des salariés, contractants et utilisateurs t-ils définis et documentés conformément à la politique de sécurité de l'information nisme?

ganisme s'accorde t-il les moyens de vérifier l'authenticité et la véracité des diplômes ıents fournis par les potentiels futurs employés ?

ersonnel est il informé de ces responsabilités vis-à-vis de la sécurité des actifs :

'embauche,

t la période de son exercice,

emerciement ?

ermes et conditions de l'emploi couvre la responsabilité de l'employé pour la sécurité mations. Le cas échéant, ces responsabilités pourraient continuer pendant une période près la fin de l'emploi?

te-t-il des sessions (de sensibilisation et d'éducation) d'information du personnel sur é des systèmes d'information de l'organisme?

te- il un processus disciplinaire formel élaboré pour les salariés ayant enfreint les sécurité ?

5- Sécurité Physique et Environnementale

zones contenant des informations et des moyens de traitement de l'information sont-tégées par des périmètres de sécurité (obstacles tels que des murs, des portes avec un d'accès par cartes, ou des bureaux de réception avec personnel d'accueil)?

te-t-il une politique de contrôle des entrées et sorties des locaux de l'organisme s, actifs…) ?

ervice de traitement d'information est protégé contre les catastrophes naturelles et ısées par l'homme ?

e t-il une politique de prévention et de gestion des incendies ?

points d'accès tels que les zones de livraison/chargement et les autres points par des personnes non habilitées peuvent pénétrer dans les locaux sont-ils contrôlés?

équipements ont été situés dans un endroit approprié afin de minimiser l'accès inutile zones de travail ?

te-t-il une protection contre les risques de menaces potentielles (le vol, le feu, les , surtension, variation de tension…) ?

ıblage électrique est il conforme aux règles de sécurité ?

équipements acquis suivent-ils une politique de maintenance ?

maintenance est effectuée seulement par les personnels autorisés ?

assure-t-on que les équipements à abandonner sont dépourvues d'informations tes pour la sécurité de l'organisme ?

ste-t-il une documentation liée à la sécurité physique et environnementale?

s vérifications ponctuelles ou des audits réguliers ont été effectués pour détecter le n autorisé de la propriété?

6- Gestion des télécommunications et de l'exploitation

olitique de sécurité identifie toutes les procédures d'exploitations telles que Back-up, nce des équipements, etc ?

changements apportés aux systèmes et moyens de traitement de l'information sont-ils ; ?

ournaux d'audit sont maintenus pour toute modification apportée aux programmes de on?

e-t-il une politique de gestion des incidents de sécurité ?

te-t-il une distinction entre les phases de développement, de test et d'intégration ations ?

lisation des ressources est surveillée et ajustée au plus près, et des projections sont-es sur les dimensionnements futurs pour assurer les performances requises par le ?

e-t-il une protection contre les codes malicieux (malveillants) (virus, vers, cheval de) ainsi qu'une mise à jour périodique et constante de ces derniers ?

copies de sauvegarde des informations et logiciels sont-elles réalisées et soumises ment à essai conformément à la politique de sauvegarde convenue ? Exemple: Mon-remental Backup and Fri: Full Backup.

réseaux sont-ils gérés et contrôlés de manière adéquate pour qu'ils soient protégés des et pour maintenir la sécurité des systèmes et des applications utilisant le réseau, nt les informations en transit ?

ste-t-il des procédures mises en place pour la gestion des supports amovibles (disks, , carte mémoire et reports) ?

s procédures de manipulation et de stockage des informations sont établies pour ces informations d'une divulgation non autorisée ou d'un mauvais usage ?

ste-il des politiques, procédures et mesures d'échange formelles mises en place pour les échanges d'informations liées à tous types d'équipements de télécommunication ?

s informations liées aux transactions en ligne sont protégées pour empêcher la sion incomplète, les erreurs d'acheminement, la modification non autorisée, la on non autorisée, la duplication non autorisée du message ou la réémission ?

informations liées à la messagerie électronique sont protégées de manière adéquate ?

7- Contrôle d'accès

esoins de l'entreprise pour le contrôle d'accès ont été définis et documentés ?

te-t-il une politique de contrôle d'accès qui traite les règles et les droits pour chaque r ou un groupe d'utilisateurs ?

procédure formelle d'inscription et désinscription des utilisateurs destinée à accorder rimer l'accès à tous les systèmes et services d'information est-elle définie ?

tribution et l'utilisation des privilèges sont-ils restreint existe-il un processus des droits d'accès des utilisateurs à intervalles réguliers. Exemple: examen privilège us les 3 mois, les privilèges normaux tous les 6 mois et contrôlées ?

te-t-il une procédure mise en place pour guider les utilisateurs dans le choix et le de mots de passe sécurisés?

tilisateurs et les entrepreneurs soient mis au courant des exigences et procédures de pour la protection de l'équipement sans surveillance, ainsi que leur responsabilité de œuvre une telle protection?

e-t-il une politique d'authentification forte pour l'accès aux services réseaux?

e-t-il un mécanisme d'authentification pour contester les connexions externes.

te-t-il un contrôle de connexion réseau pour les réseaux partagés qui s'étendent au- frontières organisationnelles. Exemple: courrier électronique, l'accès à Internet, s de fichiers, etc ?

identifiant unique est fourni à chaque utilisateur tels que les opérateurs, les rateurs système et tous les autres membres du personnel, y compris technique ?

ste il un système de gestion des mots de passe qui applique des contrôles de mot de férents tels que: mot de passe individuel, de faire appliquer les modifications de mot mots de passe sous forme cryptée, pas afficher les mots de passe sur l'écran, etc ?

ste-t-il une procédure de surveillance de l'utilisation des technologies de 'information rsonnel?

protection de l'informatique nomade est elle assurée ainsi que les séances de télé

8- Acquisition, développement et maintenance des systèmes

sure-t-on que l'équipement à acquérir répondra aux besoins exprimés ?

arantie de la confidentialité, l'authenticité et l'intégrité de l'information s'effectue-t- oyen de signature électronique ou de cryptographie ?

e-t-il une politique de maintenance périodique et assidue des équipements ?

écurité de la documentation du système d'informations elle assurée ?

politique d'utilisation des mesures cryptographiques en vue de protéger l'information rée et mise en œuvre ?

sure-t-on du non régression de service lors du développement ou de l'intégration x services

te-il une procédure de gestion des clés mise en place pour favoriser l'utilisation par me de techniques cryptographiques. ?

procédures sont mises en place pour contrôler l'installation du logiciel sur les en exploitation ?

ès au code source du programme est-il restreint ?

mise en œuvre des modifications est-elle contrôlée par le biais de procédures s ?

sque des modifications sont apportées aux systèmes d'exploitation, les applications métier sont-ils réexaminées et testées afin de vérifier l'absence de tout effet le sur l'activité ou sur la sécurité ?

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

événements liés à la sécurité de l'information sont-ils signalés, dans les meilleurs ar les voies hiérarchiques appropriées ?

e-t-il un report détaillé des incidents qui surviennent ?

l défini une politique de répartition des responsabilités en cas d'incident ?

otentielles faiblesses descellées font elles objet de rapport complet et détaillé ?

responsabilités et des procédures sont-elles établies, permettant de garantir une apide, efficace et pertinente en cas d'incident lié à la sécurité de l'information

mécanismes sont-ils mis en place, permettant de quantifier et surveiller les différents ncidents liés à la sécurité de 'information ainsi que leur volume et les coûts associés ?

qu'une action en justice civile ou pénale est engagée contre une personne physique ganisme, à la suite d'un incident lié à la sécurité de l'information, les éléments de ont-ils recueillis, conservés et présentés conformément aux dispositions légales à la présentation de preuves régissant la ou les juridiction(s) compétente(s) ?

10-Continuité des activités

processus de continuité de l'activité dans l'ensemble de l'organisme est-il élaboré et satisfait aux exigences en matière de sécurité de l'information requises pour la é de l'activité de l'organisme ?

nements pouvant être à l'origine d'interruptions des processus métier sont-ils , tout comme la probabilité et l'impact de telles interruptions et leurs conséquences écurité de l'information ?

unités organisationnelles liées à la sécurité informatique ont-elles été définies?

ste-t-il un plan de reprise en cas de désastre ?

cas de changement d'équipe de travail, la continuité de service est elle assurée ? ste-t-il une politique de sauvegarde d'autres actifs de l'organisme ?

ste t-il une (des) alarme(s) pour l'avertissement lors d'accès aux actifs sensibles en es heures de travail ou en cas d'accès non autorisés?

plan de continuité d'activité est il défini ?

11-Conformité

ıs les législatives pertinentes, les exigences réglementaires et contractuelles ont été ment définis et documentés pour chaque système d'information.

droit à la propriété intellectuelle et la protection des données personnelles sont-ils s ?

ste-t-il des procédures qui sont bien mises en œuvre ?

dossiers importants de l'organisation sont protégés de la destruction et de la perte ?

s utilisateurs sont-ils dissuadés de toute utilisation de moyens de traitement de ation à des fins illégales ?

s mesures cryptographiques sont-elles prises conformément aux accords, lois et ıtations applicables ?

iste-t-il une procédure définissant une bonne utilisation des technologies de ation par le personnel ?

ste-t-il une procédure d'audit interne et régulier de l'organisme ?

ccès aux outils d'audit du système d'information est-il protégé afin d'empêcher tous usage ou compromission éventuels ?