

Université Saad Dahleb Blida

Faculté de science

Département d'Informatique



Mémoire de fin d'études

Pour l'obtention du diplôme de Master en informatique

Option : Sécurité des Systèmes d'information

**Mise en œuvre d'un Système de Gestion des
Vulnérabilités dans les Réseaux Locaux LAN**

Réalisé par :

EZZEROUG EZZRAIMI Oulfa

OUAHRANI Chahinez

Devant le jury composé de :

Mme. CHERFA Imene :	Présidente
M.DOUGA Yacine :	Examinateur
Mme. BACHA Sihem :	Promotrice
M. KESRAOUI Abdelkader :	Encadreur
M. BENYAHY Djamel :	Encadreur

Dédicace

À toi mamita,

Quelle chance j'ai d'avoir la plus merveilleuse des mamans... unique à mes yeux, cette personne représente pour moi l'amour inconditionnel, cette héroïne... c'est toi maman.

Et ce jour-là, je veux te dire encore combien je suis tellement reconnaissante pour tous tes efforts. Merci de me donner ce que personne ne pourra jamais m'offrir.

À toi chère papa,

Merci d'avoir toujours cru en moi, je sais que tu tiens à moi comme à la prunelle de tes yeux et que tu ferais tout pour me protéger et me rendre heureuse.

Papaaaa, ta petite fille chahnou t'aime beaucoup.

À mes chers membres de famille,

À vous mes chers grand parents,

À vous mes chers oncles,

Ils n'ont pas eu tort quand ils ont dit ' Le bonheur familial est un cadeau de dieu '.
Merci alors de m'avoir donné l'amour, le repère, pour les bons moments, les souvenirs...

À toute personne que j'ai rencontré durant mes 5 ans de fac,

À mes amis du club ITC, à mes camarades,

Merci pour les merveilleux moments qu'on a eu ensemble.

Merci pour les choses qu'on a appris ensemble.

Merci pour tout ce que vous m'avez donné.

Très contente de vous connaître.

- *Chahinez*

À mes chers parents,

Quoi que je dise ou que je fasse, je n'arrivai jamais à vous remercier comme il se doit. C'est grâce à vos encouragements, vos bienveillances et votre présence à mes côtés, que j'ai réussi ce respectueux parcours.

Mama, depuis mes premiers pas dans l'apprentissage jusqu'à la réalisation de ce mémoire, vous avez été présente à chaque étape, m'encourager et me poussant à donner le meilleur de moi-même. Mama, je ne pourrai jamais exprimer suffisamment ma gratitude pour tout ce que vous avez fait pour moi.

Papa, tu es le meilleur père qu'une fille puisse avoir, je te remercie de m'avoir donné tant d'amour, d'avoir été gentil et attentionné envers moi, de m'avoir inspiré. Ce modeste travail est le fruit de tous les sacrifices que tu as déployés pour mon éducation et ma formation.

À mes chers soeurs Widad et Nour,

Merci d'être les sœurs qui s'occupe toujours de moi. Votre présences dans ma vie est précieuse.

À mon frère mohamed,

Quelle chance d'avoir un petit frère aussi sympathique que toi.

À mes chers grands-parents disparus,

Sidou, le bonheur de mon enfance. Mima, la femme la plus forte que j'ai vue. Vous vivrez toujours dans mon cœurs.

À mes chers membres de famille,

Je suis infiniment reconnaissante pour votre soutien.

À mes chers amis

- Mes amis d'enfance Achour Sara, Zahef Sara, tout le monde a un ami à chaque étape de leur vie, mais seulement quelques personnes ont le même ami à toutes les étapes de leur vie.

- Mon amie Soumia, très peu de personnes peuvent se vanter d'avoir une amie aussi que toi.

- Sonia, Fella, Amira et Sirine, les moments que nous partageons ensemble sont pleins de rires, de conversations enrichissantes et de moments de complicité.

- Mes amis du club ITC, grâce à vous, j'ai appris beaucoup de choses nouvelles et enrichi mes connaissances, ce qui a contribué à mon développement.

Pour conclure, je tiens à remercier du fond du cœur mon binôme **Chahinez**. Notre expérience a été enrichissante à tous points de vue et je suis honoré d'avoir eu l'occasion de travailler avec vous.

- *Oulfa*

Remerciements

Tout d'abord, On remercions **ALLAH** le tout puissant qui nous a pavés dans le sens de la réalisation de ce modeste travail.

Nous tenons à exprimer notre profonde gratitude à notre promotrice **Mme. BACHA Siham** pour son accompagnement et son soutien tout au long de la réalisation de ce projet, **M. Sahnoune Zakaria** pour sa précieuse contribution au long de notre projet, Sa capacité à communiquer des connaissances de manière claire et accessible nous a permis de mieux comprendre les concepts et les enjeux liés à notre domaine d'étude.

Nous tenons aussi à adresser nos sincères remerciements à nos encadreurs **M. Kesraoui Abdelkader** et **M. Benyahi Djamel** pour nous avoir donné l'occasion de travailler sur un projet aussi excitant et nous avoir fait découvrir le monde du travail.

Nos remerciements vont aussi aux membres du jury qui ont pris de leur temps pour juger ce modeste travail, qu'ils trouvent ici l'expression de notre gratitude et tout notre respect.

Ainsi nos amis du club scientifique IT Community **Bouras Tarek** et **Hadjammar Hamza** pour ses précieux conseils.

On remercie également toutes personnes qui ont contribué de façon explicite ou implicite à la réalisation de ce travail.

Résumé

La sécurité des réseaux LAN est un enjeu majeur pour les entreprises, qui doivent mettre en place des mesures de sécurité solides pour éviter les intrusions, les fuites d'informations, les attaques et d'autres menaces potentielles. Le département de sécurité d'information de la DG d'Algérie Télécom nous a proposé la réalisation d'un outil automatisé qui fait l'inventaire des actifs informatiques et l'évaluation des vulnérabilités dans un réseau LAN conforme à la norme RNSI-2020. Pour y atteindre, nous avons réalisé une maquette virtuelle à l'aide d'un outil de simulation EVE-NG qui permet de simuler un réseau local (LAN) avec ses différents composants comme un environnement de test.

La démarche de notre travail commence par établir un inventaire, ensuite détecter les vulnérabilités afin de générer deux rapports automatiques (d'inventaire et d'évaluation des vulnérabilités). L'établissement d'inventaire se fait sur trois étapes : l'identification, la cartographie et la classification des actifs informatiques. De même pour la détection des vulnérabilités : l'identification, la classification et la recommandation des solutions pour chaque vulnérabilité trouvée. Notre outil dispose d'une interface conviviale qui permet à l'entreprise d'accéder facilement aux informations des actifs informatiques d'un réseau, aux rapports générés, ainsi qu'à d'autres fonctionnalités supplémentaires.

Mots clés : Outil automatisé, Inventaire des actifs informatiques, Gestion des vulnérabilités, Référentiel National de Sécurité de l'Information (RNSI), EVE-NG.

Abstract

Local Area Networks (LAN) security is a major issue for companies, which requires robust security measures to prevent intrusions, information leaks, attacks and other potential threats. The Information Security Department of DG Algérie Télécom has proposed a realization of an automated tool that inventory assets and evaluates LAN network vulnerabilities that conform to the RNSI-2020 standard. To achieve this, we created a virtual mock-up using the EVE-NG simulation tool, which simulates a local area network (LAN) with its various components as a test environment.

Our work approach starts by establishing an inventory, then detecting vulnerabilities to generate two automatic reports (inventory report, and vulnerability assessment report). The inventory process comprises 3 steps : identification, mapping and classification of IT assets. The same applies to vulnerability detection : identification, classification and recommendation of solutions for each vulnerability found. Our tool has a simple interface that gives companies easy access to information about a network's IT assets, the reports generated and other additional functions.

Keywords : Inventory management, Automated vulnerability management, Vulnerability detection, RNSI-2020, EVE-NG.

ملخص

يمثل أمان الشبكة المحلية تحديا كبيرا للشركات ، التي يجب أن تنفذ تدابير أمنية قوية لمنع عمليات الاختحام وتسرب المعلومات والهجمات والتهديدات المحتملة الأخرى. اقترح علينا قسم أمن المعلومات في المديرية العامة للاتصالات الجزائرية تحقيق أداة تقوم بجرد أصول تكنولوجيا المعلومات وتقييم نقاط الضعف في شبكة LAN متوافقة مع معيار RNSI-2020 لتحقيق ذلك ، قمنا بعمل نموذج افتراضي باستخدام EVE-NG يسمح بمحاكاة شبكة محلية (LAN) مع أجهزة شبكة مختلفة كبيئة اختبار.

تبدأ عملية عملنا بإنشاء قائمة جرد ، ثم اكتشاف نقاط الضعف من أجل إنشاء تقرير جرد وتقرير تقييم نقاط الضعف. يتم الجرد في ثلاث خطوات: تحديد أصول تكنولوجيا المعلومات ورسم خرائطها وتصنيفها. وينطبق الشيء نفسه على اكتشاف الضعف: تحديد الحلول وتصنيفها وتوصيات الحلول لكل ثغرة أمنية تم العثور عليها. تحتوي أداتنا على واجهة سهلة الاستخدام تتيح للشركة الوصول بسهولة إلى المعلومات من أصول تكنولوجيا المعلومات الخاصة بالشبكة والتقارير التي تم إنشاؤها والميزات الإضافية الأخرى.

كلمات مفتاحية : أداة آلية,الجرد, EVE-NG, RNSI-2020,الكشف عن الثغرات الأمنية

Liste des sigles et acronymes

LAN	<i>Local Area Network</i>
DSI	<i>Département de sécurité de l'information</i>
DG	<i>Direction Générale</i>
EVE-NG	<i>Emulated Virtual Environment - Next Generation</i>
RNSI	<i>Référentiel National de Sécurité de l'Information</i>
ISO	<i>International Standards Organisation</i>
IEC	<i>International Electrotechnical Commission</i>
WEB	<i>World Wide Web</i>
CID	<i>Confidentialité, Intégrité, Disponibilité</i>
AD	<i>Active Directory</i>
LDAP	<i>Lightweight Directory Access Protocol</i>
DDOS	<i>Distributed Denial-of-Service</i>
RPC	<i>Remote Procedure Call</i>
NIST	<i>National Institute of Standards and Technology</i>
CVE	<i>Common Vulnerabilities and Exposures</i>
CVSS	<i>Common Vulnerability Scoring System</i>
UML	<i>Unified Modeling Language</i>
DMZ	<i>Demilitarized Zone</i>

IP	<i>Internet Protocol</i>
DNS	<i>Domain Name Service</i>
SQL	<i>Structured Query Language</i>
RAM	<i>Random Access Memory</i>
NAT	<i>Network Address Translation</i>

Table des matières

Dédicace	I
Remerciements	III
Résumé	IV
Abstract	V
VI	ملخص
Introduction générale	1
1 Fondements théoriques de la sécurité des systèmes d'information . . .	3
1.1 Introduction	4
1.2 Système d'information et ses composants	4
1.3 Les principes de la base de la sécurité des systèmes d'information	5
1.3.1 Confidentialité, intégrité et disponibilité (CID)	5
1.3.2 Menaces, vulnérabilités et risques	6
1.4 Les types d'attaques	6
1.4.1 Les attaques d'accès	6
1.4.2 Les attaques de modification	6
1.4.3 Les attaques par saturation (dénier de service)	6
1.4.4 Les attaques de répudiation	7
1.5 Normes et référentiels en sécurité des systèmes d'information	7
1.5.1 Présentation du référentiel RNSI2020	7
1.5.2 Principaux critères d'inventaire et de l'évaluation des vulnérabilités selon RNSI2020	8
1.6 Évaluation des risques en matière de sécurité de l'information	8
1.6.1 Description générale de l'évaluation des risques	8
1.6.2 Approche de l'évaluation des risques en matière de sécurité de l'information	9
1.7 Outils d'analyse des vulnérabilités	10
1.8 Synthèse des travaux existants et limites	10
1.9 Conclusion	11
2 Conception de l'outil ATORY	12
2.1 Introduction	13
2.2 La démarche d'établissement d'inventaire et de l'évaluation des vulnérabilités	13
2.2.1 Etablir un inventaire	14
2.2.2 Le rapport d'inventaire	14

2.2.3	La détection des vulnérabilités	15
2.2.4	Le rapport des vulnérabilités	16
2.2.5	La gestion	16
2.2.6	Enregistrement des traces d'utilisateurs	16
2.2.7	Rapport des logs des actions des utilisateurs	17
2.3	Les fonctionnalités du système	17
2.3.1	Le diagramme de cas d'utilisation	17
2.3.2	Le diagramme de séquence	18
2.3.3	Le schéma de la base de données	21
2.4	Conclusion	22
3	Implementation	23
3.1	Introduction	24
3.2	La maquette du réseau	24
3.2.1	EVE NG	24
3.2.2	Présentation de l'architecture réseau	25
3.2.3	Configuration des équipements	25
3.3	Les outils de développement	29
3.3.1	Langage de programmation	29
3.3.2	Bibliothèques et mécanisme	30
3.3.3	Environnement matériel	32
3.3.4	Environnement logiciel	33
3.4	Présentation de l'application	33
3.5	Présentation des points les plus importants des rapports générés	44
3.6	Conclusion	49
	Conclusion et perspectives	50

Table des figures

1.1	Les composants d'un système d'information[3]	4
1.2	Triangle CID	5
1.3	Les étapes d'évaluation des risques [4]	9
2.1	Processus globale	13
2.2	Diagramme de cas d'utilisation	17
2.3	Diagramme de séquence	18
2.4	Diagramme de séquence	19
2.5	Diagramme de séquence	19
2.6	Diagramme de séquence	20
2.7	Diagramme de séquence	20
2.8	Diagramme de séquence	21
2.9	Le schéma de la base de données	22
3.1	L'architecture réseau d'une entreprise	25
3.2	L'interface de l'émulateur Putty	26
3.3	La configuration des ports du pare-feu	26
3.4	Les règles de sécurité	27
3.5	la route statique dans le par-feu	27
3.6	La configuration du commutateur niveau 3	27
3.7	La configuration du commutateur niveau 3	28
3.8	Interface de l'annuaire active directory	29
3.9	Interface d'authentification	34
3.10	La page d'accueil	34
3.11	Les statistiques	35
3.12	Le tableau des services	36
3.13	Le Tableau des ports identifiés	36
3.14	Le tableau des actifs informatiques identifiés	37
3.15	Les changements récents	37
3.16	Les informations du dernier inventaire effectué	38
3.17	Le choix de l'actif informatique à scanner	38
3.18	Résultat obtenu après scan d'un actif informatique selon le choix.	39
3.19	Scanner tout le réseau	39
3.20	Le résultat du Scan total	40
3.21	La liste des rapports générés	40
3.22	L'interface de la gestion	41
3.23	La gestion des groupes	41
3.24	La gestion des utilisateurs	42

3.25	La gestion des actifs informatiques	42
3.26	L'enregistrement des changements	43
3.27	À propos de Atory	43
3.28	Le rapport des logs des actions des utilisateurs	44
3.29	Une page du document de rapport d'inventaire qui représente la cartographie	45
3.30	La cartographie d'un actif informatique WINSERVER du rapport d'inventaire	46
3.31	Des statistiques sur l'ensemble des vulnérabilités détectées lors du scan . .	47
3.32	Une description détaillée d'une vulnérabilité identifiée d'un actif informatique WINSERVER	48

Liste des tableaux

1.2	Outils d'analyse des vulnérabilités	10
2.2	Description de diagramme de cas d'utilisation	18

Introduction générale

La sécurité des systèmes d'information a toujours été au centre des préoccupations des organisations à travers le globe. Cette inquiétude trouve plus d'ampleur grâce à la dépendance croissante aux infrastructures technologiques dans le quotidien des activités. Au cœur de ces systèmes, un élément clé se démarque : le réseau local (LAN). Servant en tant que moyen de connexion des différents dispositifs, serveurs et d'applications critiques, sa sécurité est devenue un enjeu majeur. Il peut également comporter un certain nombre de vulnérabilités intrinsèques.

Ces vulnérabilités peuvent provenir de divers facteurs, tels que la configuration du réseau, les protocoles de sécurité utilisés, les paramètres de pare-feu et les politiques de gestion de réseau. Par exemple, si les paramètres de sécurité ne sont pas correctement configurés, cela peut entraîner des failles de sécurité et faciliter les attaques malveillantes.

Il est crucial de reconnaître et de traiter les vulnérabilités intrinsèques associées. En adoptant une approche proactive en matière de sécurité, on peut renforcer la résilience du réseau et prévenir les potentielles attaques et les pertes de données.

Les ordinateurs, les serveurs, les périphériques, les logiciels et autres équipements liés aux technologies de l'information sont des exemples d'actifs informatiques. Les informations sur chaque actif doivent être saisies, mises à jour et suivies manuellement.

Lorsqu'on effectue un suivi des actifs informatiques manuellement, ce qui peut être un processus fastidieux et long. De plus, il existe un risque accru d'erreurs humaines, telles que des erreurs ou des informations incorrectes, ce qui peut entraîner des lacunes dans le suivi et la gestion des actifs.

Dans le cadre de notre master en Sécurité des Systèmes d'Information, nous avons eu l'opportunité d'effectuer un stage au sein de la division DSI de la DG Algérie Télécom, spécialisée en Sécurité des Systèmes d'Information. Cette dernière possède un réseau LAN complexe et étendu qui relie plusieurs sites et héberge un grand nombre d'utilisateurs.

Algérie Télécom est leader sur le marché algérien des télécommunications en forte croissance, offrant une gamme complète de services de téléphonie fixe et d'internet aux particuliers et aux entreprises. Cette position s'appuie sur une forte politique d'innovation adaptée aux attentes des clients et tournée vers les nouveaux usages.

Son objectif est d'avoir des performances techniques, économiques et sociales élevées afin de se maintenir durablement leader dans son domaine dans un environnement devenu concurrentiel. Il est également préoccupé par la préservation et le développement de sa

dimension internationale ainsi que par la promotion de la société de l'information en Algérie.[1]

C'est dans ce contexte que nous avons été chargés de programmer un outil qui aide l'entreprise à faire l'inventaire automatique de ses systèmes et de ses actifs, ainsi qu'à évaluer les risques et les vulnérabilités associés. L'objectif de cet outil est de fournir à l'entreprise une évaluation complète de sa posture de sécurité et des recommandations pour améliorer sa sécurité globale selon le Référentiel National de Sécurité des Systèmes d'Information (RNSI 2020) [2].

Le présent mémoire vise à fournir une analyse détaillée de la sécurité du réseau LAN de l'entreprise, en mettant l'accent sur l'inventaire des composants et l'évaluation des vulnérabilités. Pour atteindre cet objectif, nous avons suivi une méthodologie rigoureuse, comprenant les étapes suivantes :

- Revue de la littérature : Cette section du mémoire se concentre sur les concepts fondamentaux de la sécurité dans les systèmes d'informaton , les meilleures pratiques et les normes de l'industrie. Synthèse des travaux existants et limites.
- Méthodologie de l'inventaire et d'évaluation des vulnérabilités : Nous détaillerons les étapes et les outils utilisés pour réaliser l'inventaire complet et l'évaluation des vulnérabilités des composants du réseau LAN de l'entreprise. Nous aborderons également les défis et les considérations spécifiques liés à ce travail.
- Implémentation : Nous décrivons les détails pratiques de la mise en œuvre en mettant l'accent sur la maquette du réseau de test , les outils développement . Ensuite, nous expliquerons la méthode de notre développement et nous finirons par des captures d'écran sur les différentes fonctionnalités de notre application.

Chapitre 1

Fondements théoriques de la sécurité des systèmes d'information

1.1 Introduction

Dans ce chapitre, nous présenterons les principes de base de la sécurité des systèmes d'information et leur importance dans la gestion des vulnérabilités au sein d'un réseau LAN.

1.2 Système d'information et ses composants

Un système d'information peut être défini comme un ensemble organisationnel de ressources (matériel, logiciel, personnes, organisations) qui collecte, traite, stocke et distribue des informations pour soutenir les opérations, la prise de décision et la gestion au sein d'une organisation [3].

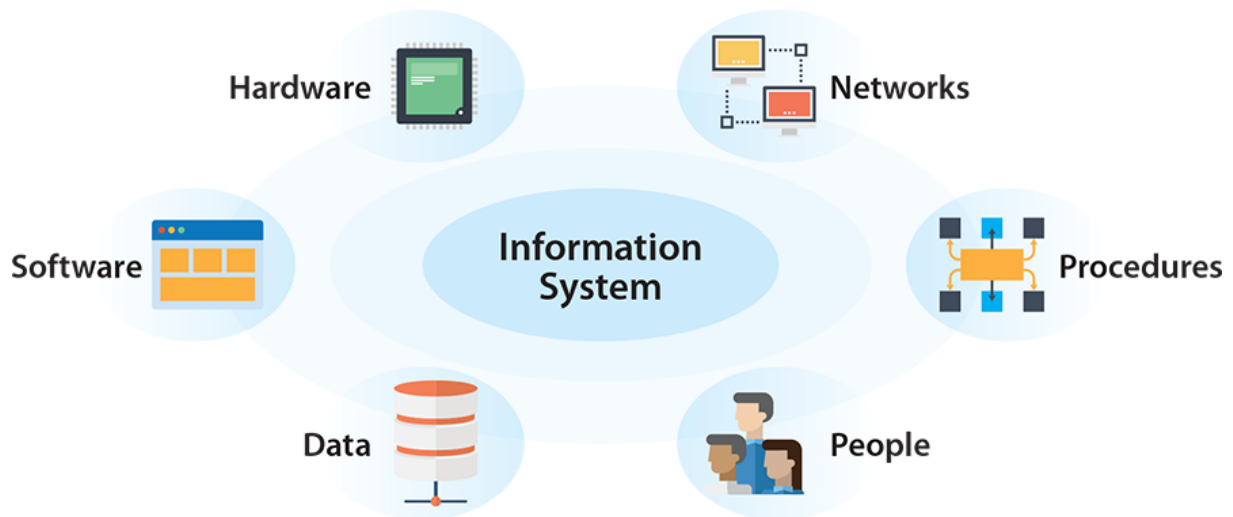


FIG. 1.1 : Les composants d'un système d'information[3]

Les composants principaux d'un système d'information comprennent généralement :

- Matériels informatiques : Les équipements physiques tels que les ordinateurs, les serveurs, les périphériques de stockage et les réseaux qui sont utilisés pour traiter, stocker et transmettre les données.
- Logiciels : Les programmes informatiques qui permettent de réaliser différentes tâches, telles que les systèmes d'exploitation, les logiciels de base de données, les applications métiers et les outils de productivité.
- Données : Les informations brutes collectées, stockées et utilisées par le système d'information. Cela peut inclure des données structurées (telles que les bases de données) et des données non structurées (telles que les documents texte, les images).
- Réseaux : Les infrastructures de communication qui permettent la transmission des données entre les différents composants du système d'information, que ce soit à l'échelle locale ou étendue.

- Personnes : Les utilisateurs, les administrateurs et les personnes impliquées dans l'utilisation, la gestion et le développement du système d'information.
- Procédures : Les règles, les politiques et les processus définis pour l'utilisation, la gestion, la sécurité et la maintenance du système d'information.
- Sécurité : Les mesures et les mécanismes sont mis en place pour protéger les données, les ressources et les infrastructures du système d'information contre les menaces et les attaques potentielles[3] .

1.3 Les principes de la base de la sécurité des systèmes d'information

La sécurité des systèmes d'information repose sur plusieurs principes fondamentaux visent à assurer la protection des données et des infrastructures informatiques contre les menaces, les vulnérabilités et les attaques potentielles.

1.3.1 Confidentialité, intégrité et disponibilité (CID)

La confidentialité concerne la protection des informations sensibles contre les accès non autorisés.

L'intégrité assure l'exactitude et la fiabilité des données, en évitant les modifications non autorisées ou les altérations accidentelles.

La disponibilité garantit l'accès aux ressources et aux services informatiques lorsque cela est nécessaire [3].

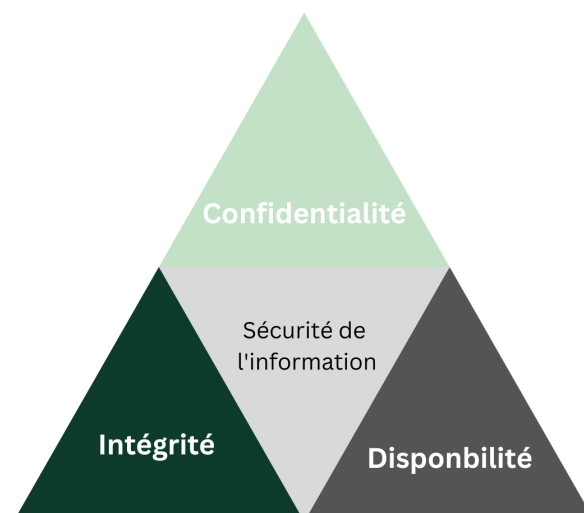


FIG. 1.2 : Triangle CID

1.3.2 Menaces, vulnérabilités et risques

Les menaces représentent les acteurs, les événements ou les circonstances susceptibles de causer des dommages aux systèmes d'information.

Les vulnérabilités sont les faiblesses ou les défauts qui peuvent être exploités par des menaces pour compromettre la sécurité.

Les risques sont l'estimation de la probabilité d'occurrence d'une menace exploitant une vulnérabilité et de son impact potentiel [4].

1.4 Les types d'attaques

Une attaque est un acte qui tire parti d'une vulnérabilité pour compromettre un système contrôlé. Elle est accomplie par un agent de menace qui endommage ou vole les informations ou les biens physiques d'une organisation [3]. Il existe 4 catégories principales d'attaque (d'accès, de modification, déni de service, de répudiation) [5].

1.4.1 Les attaques d'accès

Les attaques d'accès visent à accéder illégalement à un système ou à une ressource informatique sans avoir besoin d'autorisation. Elles peuvent prendre diverses formes, notamment l'hameçonnage (phishing), qui consiste à tromper une personne pour qu'elle révèle des informations sensibles, et le piratage de mot de passe, qui consiste à deviner ou à craquer les mots de passe pour accéder à un compte. Un autre exemple est l'escalade de privilèges, où un attaquant gagne des droits d'accès plus élevés que ceux qui lui ont été attribués.

1.4.2 Les attaques de modification

Ces attaques visent à modifier les données ou les ressources d'un système sans autorisation. Elles comprennent l'utilisation du code malveillant (malware) qui modifie les données ou le fonctionnement d'un système, l'injection de code, où un attaquant insère du code malveillant dans un programme ou une page Web, et l'usurpation, où un attaquant se fait passer pour une autre entité pour modifier les données ou le comportement d'un système.

1.4.3 Les attaques par saturation (déni de service)

Une attaque de déni de service a pour but de rendre un service informatique indisponible pour les utilisateurs légitimes. Il s'agit généralement de surcharger le système avec des requêtes inutiles, de sorte qu'il ne peut pas répondre aux requêtes légitimes. Dans une attaque par déni de service distribué (DDoS), plusieurs systèmes sont utilisés pour lancer l'attaque, rendant la défense plus difficile.

1.4.4 Les attaques de répudiation

Dans ce type d'attaques, l'attaquant profite de l'absence d'un mécanisme de répudiation. Cela implique qu'un utilisateur nie avoir effectué une action, malgré l'existence de preuves de son implication. Par exemple, une personne pourrait nier avoir effectué une transaction en ligne. Les mécanismes de sécurité comme la journalisation des événements et les signatures numériques sont conçus pour prévenir ce type d'attaques.

1.5 Normes et référentiels en sécurité des systèmes d'information

Les normes et les référentiels en sécurité des systèmes d'information fournissent des lignes directrices et de bonnes pratiques pour la gestion de la sécurité. Dans cette section, nous présenterons le référentiel RNSI2020, qui constitue notre cadre d'évaluation des vulnérabilités dans le réseau LAN de l'entreprise étudiée.

1.5.1 Présentation du référentiel RNSI2020

Le Référentiel National de la Sécurité de l'Information (RNSI2020) est une norme développée visant à fournir un cadre et un ensemble de conditions préalables qui permettront le développement et la mise en œuvre de Sécurité au sein des organisations. Nous présenterons les principaux objectifs, critères et recommandations de ce référentiel en lien avec notre étude sur l'évaluation des vulnérabilités.

Les objectifs d'un référentiel perceptible à travers ses différents domaines sont :

- Augmenter le niveau de sécurité des systèmes d'information et la protection des informations organisationnelles en mettant en place des contrôles de sécurité appropriés.
- Adopter une approche basée sur les risques lors de la mise en œuvre des contrôles de sécurité.
- Définir les rôles et responsabilités appropriés pour la protection des informations.

Le RNSI2020 intègre plusieurs normes et référentiels reconnus dans le domaine de la sécurité des systèmes d'information. Ces normes jouent un rôle crucial dans l'établissement des bonnes pratiques et des exigences de sécurité. Voici quelques normes les plus importantes incluses dans le référentiel RNSI 2020 :

- **ISO/IEC 27001:2013** : Systèmes de management de la sécurité de l'information
- **ISO/IEC 27002:2013**:Code de bonnes pratiques pour la sécurité de l'information
- **ISO/IEC 27005:2018**:Management des risques de sécurité de l'information[1]

1.5.2 Principaux critères d'inventaire et de l'évaluation des vulnérabilités selon RNSI2020

Nous détaillerons les critères spécifiques définis par le référentiel RNSI2020 pour l'inventaire des actifs informatiques et l'évaluation des vulnérabilités.

Selon le premier domaine de sécurité "gestion des actifs" qui parle sur les responsabilités relatives aux actifs (inventaire des actifs, propriétaire de l'actif) , la classification de l'information (classification, étiquetage des actifs informatique) .

Selon le cinquième domaine de sécurité "sécurité des réseaux" qui parle sur la gestion du réseau et sa conception.

Cela inclut l'inventaire et la surveillance des actifs informatiques, la classification des vulnérabilités, l'évaluation de leur criticité, ainsi que la prise en compte des aspects techniques et organisationnels pour déterminer le niveau de risque associé à chaque vulnérabilité.[2]

1.6 Évaluation des risques en matière de sécurité de l'information

L'ISO 27005 fournit un cadre solide pour réaliser l'évaluation des risques en matière de sécurité de l'information, qui est un élément essentiel de la gestion de la sécurité de l'information. Bien que cette norme ne précise pas une méthode d'évaluation des risques particulière, elle fournit des instructions pour sélectionner et mettre en œuvre les méthodes d'évaluation qui conviennent à l'organisation.[4]

1.6.1 Description générale de l'évaluation des risques

L'évaluation des risques détermine la valeur des actifs informationnels, identifie les menaces et les vulnérabilités qui existent (ou peuvent exister), identifie les contrôles existants et leur impact sur le risque identifié, détermine les conséquences potentielles et hiérarchise les risques dérivés et les classe en fonction des critères d'évaluation des risques définis dans l'établissement du contexte.[4]

L'évaluation des risques comprend les activités suivantes :

- L'identification des risques.
- L'analyse des risques.
- L'évaluation des risques.

1.6.2 Approche de l'évaluation des risques en matière de sécurité de l'information

Selon l'ISO 27005, l'approche d'évaluation des risques est un processus itératif composé de cinq étapes principales :

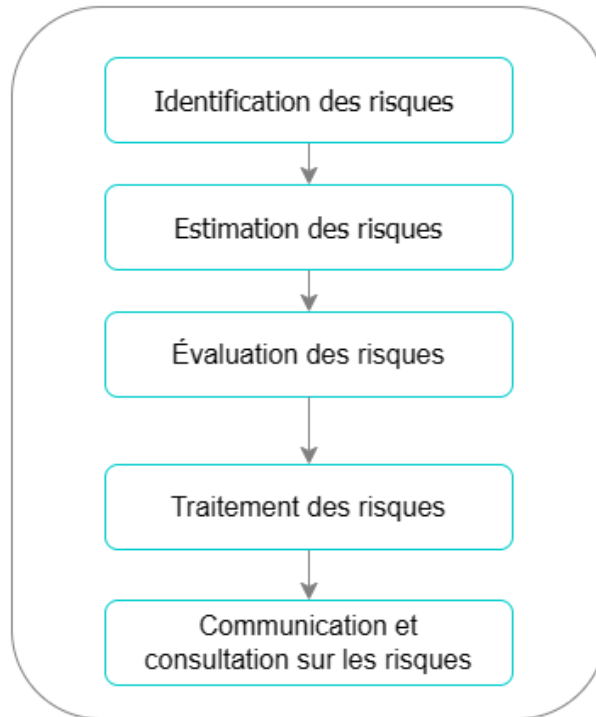


FIG. 1.3 : Les étapes d'évaluation des risques [4]

- **Identification des risques** : La première étape consiste à identifier les actifs qui nécessitent une protection, ainsi que les menaces, vulnérabilités et impacts associés à ces actifs.
- **Estimation des risques** : Une fois les risques identifiés, ils doivent être évalués en termes de probabilité et d'impact. La probabilité est la possibilité qu'une menace exploite une vulnérabilité, et l'impact représente l'effet négatif.
- **Évaluation des risques** : Cette étape consiste à déterminer quels risques l'organisation accepte et lesquels nécessitent un traitement. Cela dépend fréquemment de la tolérance au risque de l'organisation.
- **Traitement des risques** : Il existe plusieurs méthodes pour gérer les risques, notamment l'acceptation, la réduction, le transfert ou l'évitement. L'équilibre entre le coût du traitement du risque et le bénéfice obtenu en réduisant l'impact et/ou la probabilité du risque est le point central de la décision.
- **Communication et consultation sur les risques** : Il est crucial que toutes les parties prenantes concernées soient informées des risques et de la façon dont ils sont gérés. La direction de l'entreprise, les employés, les clients, les fournisseurs et les régulateurs peuvent y être inclus. [4]

1.7 Outils d'analyse des vulnérabilités

Les outils d'analyse des vulnérabilités sont des logiciels essentiels pour protéger les systèmes, les réseaux et les applications des cyberattaques. Les entreprises et les professionnels de la sécurité peuvent prendre des mesures préventives pour renforcer leur posture de sécurité en identifiant et en évaluant ces outils. On mentionne quelques outils :

Outils	Description
Nessus	un scanner de vulnérabilités intégré qui offre la couverture la plus complète pour la gestion des vulnérabilités et la vérification de la configuration, les plugins CVE et les mises à jour, les vérifications SCADA avec une gamme de systèmes UNIX et Linux, et la conformité réglementaire, le tout sous la même licence [6].
Nexpose	un scanner de vulnérabilités disponible en quatre versions différentes, chacune avec ses propres fonctionnalités et avantages qui s'étendent à mesure que l'on obtient plus de licences. NeXpose détecte les services actifs sur la machine, priorise les menaces les plus graves en fonction de l'intelligence des menaces qui est mise en correspondance avec les priorités de l'entreprise [6].
Nmap	un scanner de sécurité gratuit et open-source utilisé par les entreprises pour la découverte de réseau, l'inventaire, la gestion de la planification de mise à niveau de service et la surveillance de la disponibilité de l'hôte ou du service. Nmap est populaire en raison de sa polyvalence, de sa capacité, de sa portabilité et de sa facilité d'utilisation [6].
OpenVAS	un scanner de vulnérabilités open-source maintenu par Greenbone Networks. Le scanner dispose également d'un flux communautaire avec plus de 50 000 tests de vulnérabilités qui sont mis à jour régulièrement [6].

TAB. 1.2 : Outils d'analyse des vulnérabilités

1.8 Synthèse des travaux existants et limites

Avant de passer à la méthodologie de notre étude, il est essentiel de résumer les recherches actuelles sur l'évaluation des vulnérabilités des réseaux locaux. Cela nous permet de situer notre recherche par rapport aux contributions précédentes et d'identifier les lacunes et les limites actuelles.

Nous ne sommes pas les premiers à nous intéresser à la conformité des systèmes d'information. Les principes et les méthodes recommandés par l'ISO 27005 ont été adoptés par de nombreuses recherches dans le domaine de l'évaluation des risques en matière de sécurité des données. Ces travaux ont généralement basé sur les étapes clés du processus d'évaluation des risques. Plusieurs études ont utilisé diverses méthodes pour évaluer les vulnérabilités des réseaux LAN en examinant la littérature académique, les articles scientifiques et les normes de sécurité (iso 27001, iso 27005). D'autres solutions existent, mais

elles sont souvent très coûteuses, soit en rentrant les infos à la main, soit ils nécessitent l'installation d'un client SNMP sur le poste pour l'analyser [7]. Alors que certaines études se sont concentrées sur l'utilisation d'outils de scan de vulnérabilités comme Nessus, rapid7 ou openvas [6], tandis que d'autres ont adopté une approche plus globale en intégrant des questions techniques et organisationnelles [8].

Malgré ces contributions, il existe des limites littéraires. Les critères d'évaluation des vulnérabilités ne font pas l'objet d'un consensus, ce qui rend la comparaison des résultats des différentes études difficile.

Dans notre étude, nous visons à combler ces lacunes en utilisant une approche basée sur le modèle de référence RNSI2020 q. Nous mettons l'accent sur la pertinence et la viabilité des recommandations de sécurité en proposant une méthodologie complète pour l'inventaire et l'évaluation des vulnérabilités du réseau LAN de l'entreprise.

1.9 Conclusion

Ce premier chapitre a posé les bases théoriques nécessaires à la compréhension de la sécurité des systèmes d'information et de l'évaluation des vulnérabilités. Nous avons abordé les principes de confidentialité, d'intégrité et de disponibilité, ainsi que les notions de menaces, de vulnérabilités et de risques. De plus, nous avons présenté le référentiel RNSI2020, qui nous servira de guide pour évaluer les vulnérabilités du réseau LAN de l'entreprise. Enfin, nous avons réalisé un aperçu des travaux existants dans le domaine, en mettant en évidence les limites et les lacunes actuelles. Dans le chapitre suivant, nous présenterons la méthode d'inventaire des vulnérabilités dans un réseau LAN.

Chapitre 2

Conception d'un outil de gestion des vulnérabilités dans un réseau LAN

2.1 Introduction

L’évaluation des menaces et des risques se fait sur deux fronts majeurs, organisationnel et technique. Le premier couvre tous les aspects du système d’information de l’entreprise, de ses employés à ses processus, de nombreuses méthodes et normes ont été développées pour mener des évaluations organisationnelles, notamment Mehari[9], Ebios[10], Octave[11], ISO 27001 et ISO 27005 [8]. Le deuxième étudie en profondeur une architecture particulière (traverse, interconnexion, utilisation). Il utilise principalement des outils cartographiques et des scanners de vulnérabilité.

Dans ce chapitre, on se base sur le côté technique visant à identifier les actifs et évaluer les vulnérabilités dans un réseau LAN d’une entreprise selon la norme RNSI2020. On commence par expliquer la démarche de notre processus puis les fonctionnalités de notre système présenté par des diagrammes UML .

2.2 La démarche d’établissement d’inventaire et de l’évaluation des vulnérabilités

Rappelons que l’objectif de notre étude est de mettre en place une solution automatique (outil) d’inventaire et de scan des actifs informatique. La démarche d’établir un inventaire d’évaluation des vulnérabilités que nous avons proposé est la suivante :

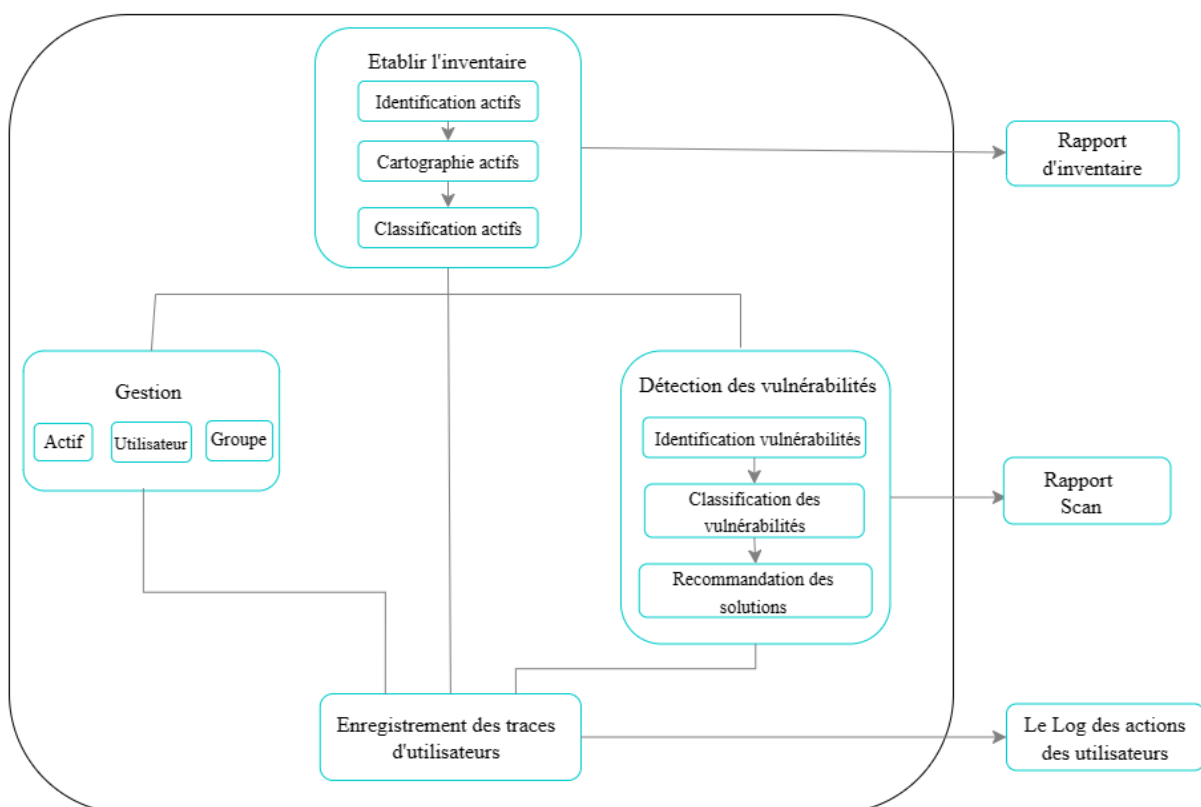


FIG. 2.1 : Processus globale

2.2.1 Etablir un inventaire

Cette étape commence par l’identification des actifs informatiques, ensuite leur classification [3], en ajoutant des détails au fur et à mesure que l’on approfondit l’analyse.

Un actif est tout composant du réseau qui possède une valeur pour l’organisation. Il peut s’agir des ressources matérielles, logicielles ou des données qui sont nécessaires au fonctionnement et à la continuité des opérations de l’entreprise [12]. Dans notre cas on considère l’actif informatique comme ressources matérielles.

L’identification des actifs

Selon la mesure de sécurité 8.1.1 de l’Annexe de la norme ISO 27001, l’inventaire doit contenir : le nom de l’actif, une description, le propriétaire, le type d’actif (nœud final, nœud intermédiaire), l’adresse IP, l’adresse MAC, le système d’exploitation et sa version, l’administrateur de l’actif informatique et son groupe, classification, les dates des derniers audits. Pour la traçabilité du document, une date de dernière revue, la date de dernière modification et un commentaire pour tracer les changements réalisés.

Il est essentiel de dresser une liste aussi complète que possible des actifs par association avec les bases de données internes, les outils de gestion, le monitoring ou un scan d’équipement [13].

La classification des actifs informatiques

Afin d’analyser les performances, gérer les ressources et assurer la sécurité de ces derniers, il est crucial de classer les actifs informatiques de manière organisée et structurée. Il s’agit donc d’identifier, de catégoriser ces actifs informatiques.

2.2.2 Le rapport d’inventaire

Le rapport permet de communiquer sur l’état de la sécurité informatique d’une organisation, il vise à fournir des outils de communication entre les parties prenantes du processus. Dans notre étude, il est plus compatibles d’utiliser un rapport technique et opérationnel [13].

Le rapport d’inventaire est un document essentiel dans la gestion des actifs informatiques d’une entreprise. Il fournit une vue détaillée de l’ensemble et à jour de tous les actifs déployés sur le réseau de l’entreprise. Ce rapport contient la cartographie de chaque actif, des informations clés telles que les adresses IP, adresses Mac, les noms d’hôtes, les systèmes d’exploitation, les versions logicielles et matérielles, ainsi que d’autres détails pertinents.

2.2.3 La détection des vulnérabilités

L'objectif ici est d'identifier et classier les vulnérabilités sur les actifs informatiques identifiés qui sont stockés dans une base de données locale.

Afin de ne pas être dépassé par l'ampleur de la tâche, il convient de hiérarchiser les actifs en fonction des éléments les plus menacés et leur criticité pour l'entreprise, en privilégiant :

- Le cœur de réseau avant ses éléments périphériques.
- Les serveurs avant les postes de travail.

L'identification des vulnérabilités

Pour identifier les vulnérabilités, il consiste à réaliser deux types différents d'audits complémentaires : automatisés et manuels.

- L'automatisation des tests (avec l'utilisation de logiciels contenant des bases de données contenant des milliers de tests) permet une grande couverture fonctionnelle, mais elle est sévèrement limitée par l'analyse logique que seuls les humains sont capables de fournir, typiquement dans le cas des tests d'application [10].
- **Le test manuel** est réalisé par un professionnel complétera donc l'approche systématique et automatique par une analyse logique ciblée. Cette analyse peut avoir pour but de tester l'intrusion dans le système (on parle alors de test de pénétration), ou d'examiner le code source d'une application pour conclure la qualité de ce dernier.[13]

Il est donc logique de combiner les deux approches - manuelle pour une analyse plus approfondie et plus qualifiée, et automatique pour une couverture fonctionnelle plus complète et plus cohérente.

Classification des vulnérabilités

L'impact potentiel d'une vulnérabilité fait référence aux conséquences possibles et aux dommages qu'une vulnérabilité peut causer une fois exploitée par un attaquant.

En fonction de la nature de la vulnérabilité, du contexte dans lequel elle est exploitée et de la sensibilité des actifs concernés, l'impact potentiel peut varier en se basant sur les aspects de sécurité.

La recommandation des solutions

Les recommandations de solutions peuvent prendre différentes formes, en fonction de la nature spécifique de la vulnérabilité. Il peut s'agir de l'application de correctifs

logiciels, de la mise à jour des versions, de la configuration de paramètres de sécurité, de l'ajout de mesures de protection supplémentaires ou même de la révision des procédures opérationnelles.

2.2.4 Le rapport des vulnérabilités

Le rapport d'évaluation des vulnérabilités fournit une analyse approfondie des vulnérabilités présentes sur les actifs informatiques.

Le rapport identifie les vulnérabilités les plus importantes suivie d'une description, classées par ordre de priorité en fonction de leur potentiel d'impact sur la sécurité. De plus, il propose des suggestions claires et concrètes pour réduire leur danger et renforcer la sécurité globale du réseau.

2.2.5 La gestion

Le processus offre 3 fonctionnalités de gestion distinctes. Ces fonctionnalités visent à offrir aux utilisateurs des outils et à effectuer des tâches administratives essentielles de manière efficace et centralisée. Voici un aperçu de ces trois fonctionnalités :

La gestion des groupes

Cette fonctionnalité permet au administrateur d'ajouter un nouveau groupe dans le domaine local du réseau.

La gestion des utilisateurs

Notons que les utilisateurs sont reliev au domaine local. Cette fonctionnalité permet au administrateur d'ajouter ou supprimer un utilisateur. De plus, l'ajouter dans un autre groupe.

La gestion des actifs informatiques

Cette fonctionnalité permet de changer la valeur de classification d'un actif, changer son administrateur ou bien l'ajouter à un autre groupe du domaine local.

2.2.6 Enregistrement des traces d'utilisateurs

Pour bien garder la traçabilité de chaque utilisateurs, on enregistre chaque action qu'un utilisateur fait.

2.2.7 Rapport des logs des actions des utilisateurs

la généralisation d'un rapport log permet de regrouper et d'analyser les informations contenues dans les fichiers logs, facilitant ainsi la prise de décision éclairée, l'optimisation des performances et la sécurité des systèmes.

2.3 Les fonctionnalités du système

Lors de la conception d'un système, il est crucial de le bien comprendre et de le présenter clairement. Les diagrammes UML offrent un moyen utile de visualiser et de présenter ces fonctionnalités de manière structurée et compréhensible.

2.3.1 Le diagramme de cas d'utilisation

Le diagramme de cas d'utilisation est l'un des diagrammes UML les plus courants utilisés pour illustrer les fonctionnalités d'un système. Ce diagramme met en évidence les différentes fonctionnalités offertes par le système du point de vue des utilisateurs en identifiant les acteurs qui interagissent avec le système et les cas d'utilisation qui représentent les actions particulières effectuées par les utilisateurs.

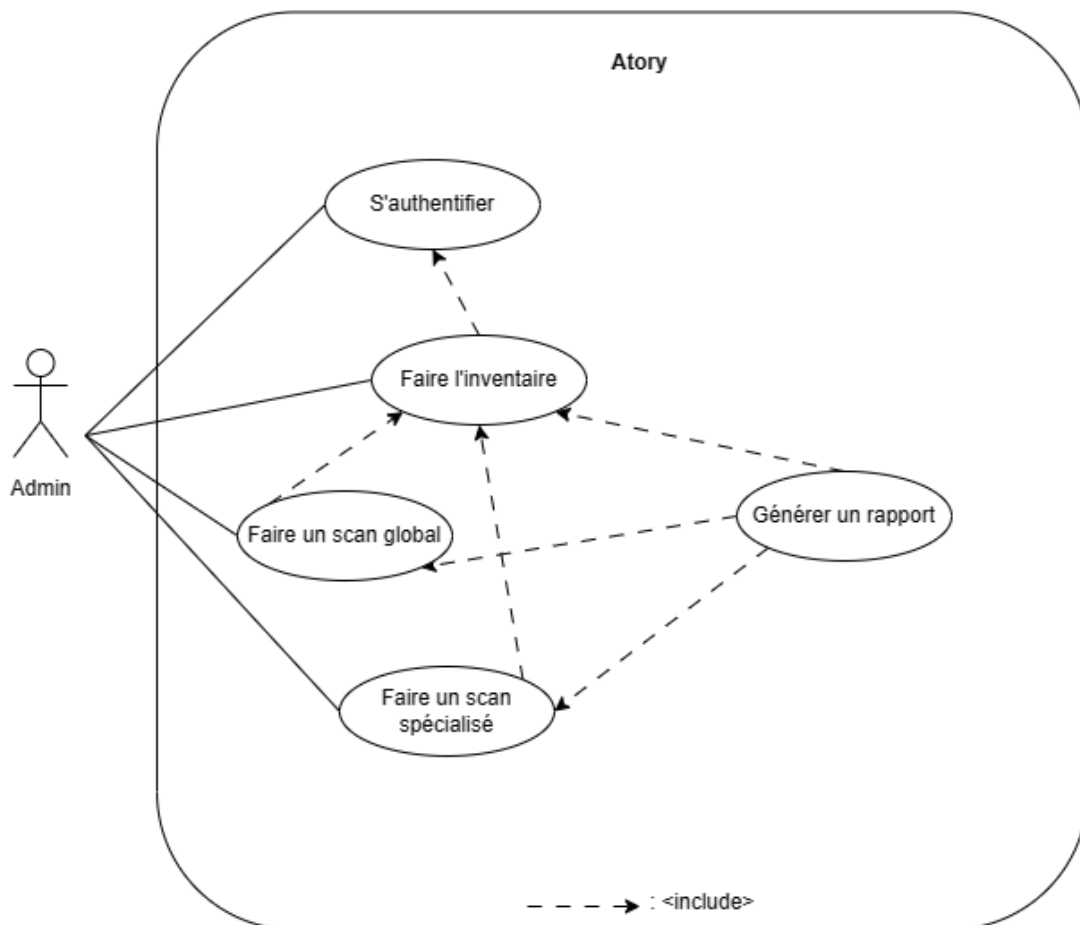


FIG. 2.2 : Diagramme de cas d'utilisation

Acteur	Administrateur
Pre-condition	S'authentifier pour accéder aux différentes fonctionnalités
Post-condition	générer un rapport d'inventaire, générer un rapport de scan
Objectif	<ul style="list-style-type: none">• S'authentifier• Etablir l'inventaire• Etablir un scan spécialisé• Etablir un scan globale• Générer un rapport

TAB. 2.2 : Description de diagramme de cas d'utilisation

2.3.2 Le diagramme de séquence

Notre diagramme de séquence modélisant les interactions du cas d'utilisation du « Processus Atory », il montre la chronologie des événements et des messages passés entre éléments (lignes de vie) au sein d'une interaction. La progression temporelle est verticale et les éléments sont représentés horizontalement.

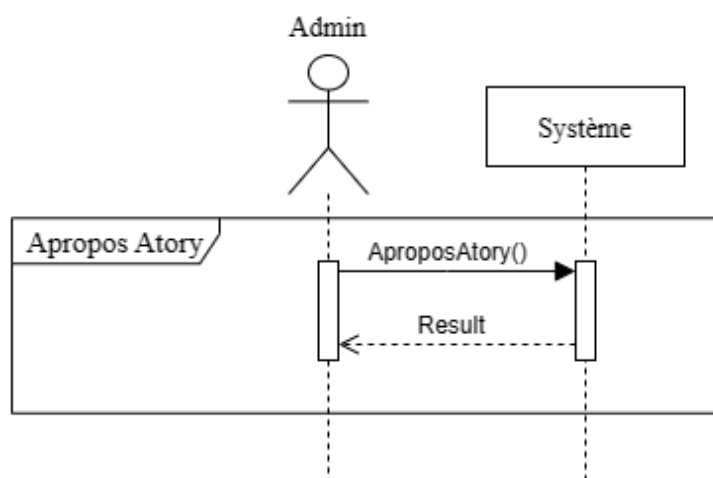


FIG. 2.3 : Diagramme de séquence

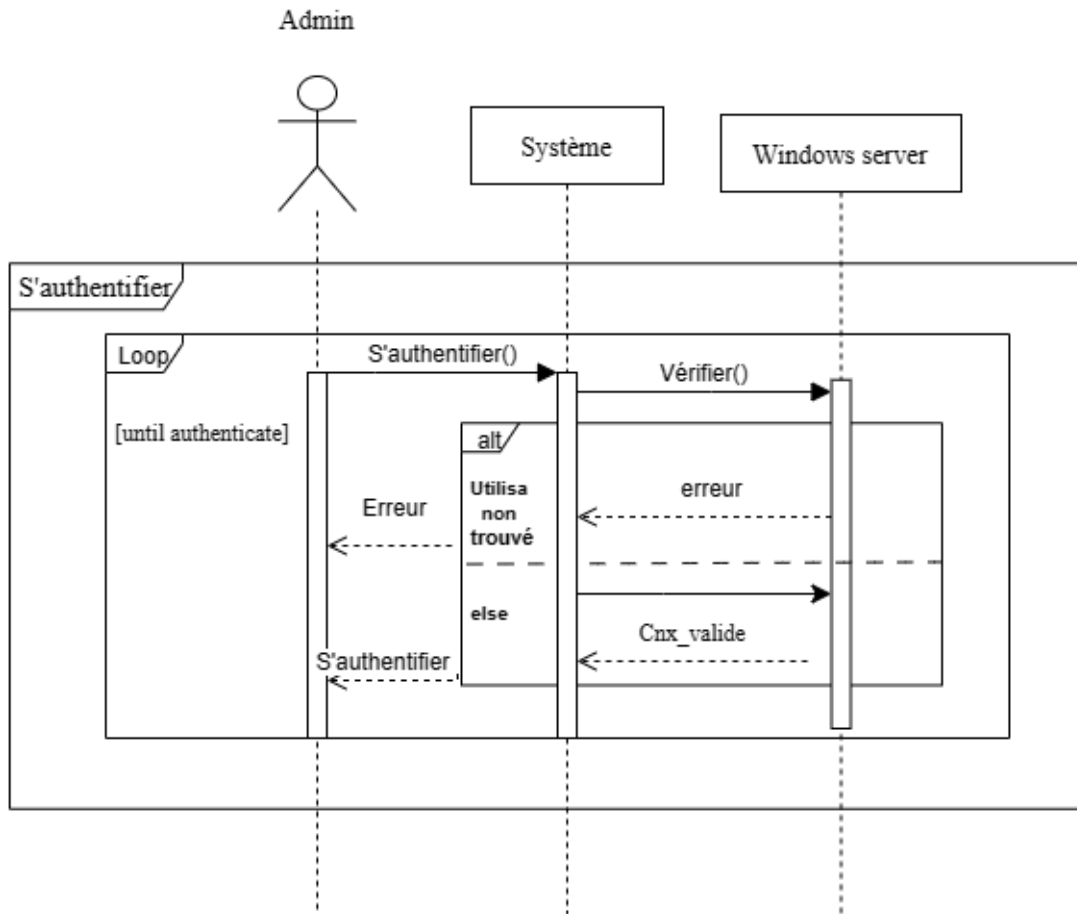


FIG. 2.4 : Diagramme de séquence

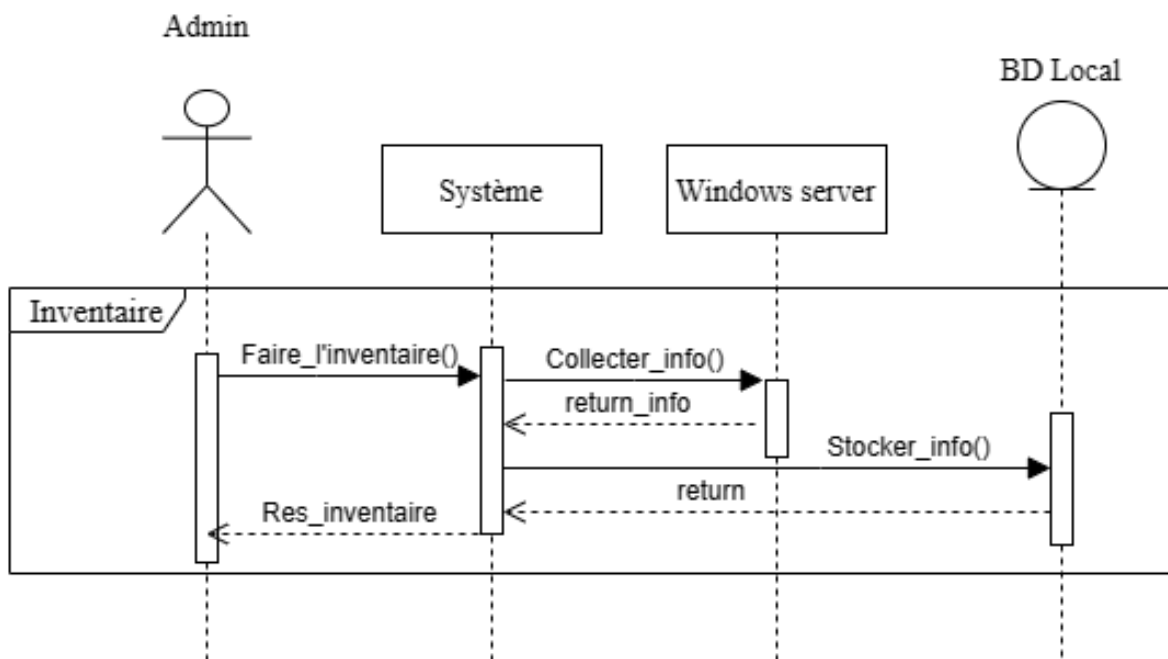


FIG. 2.5 : Diagramme de séquence

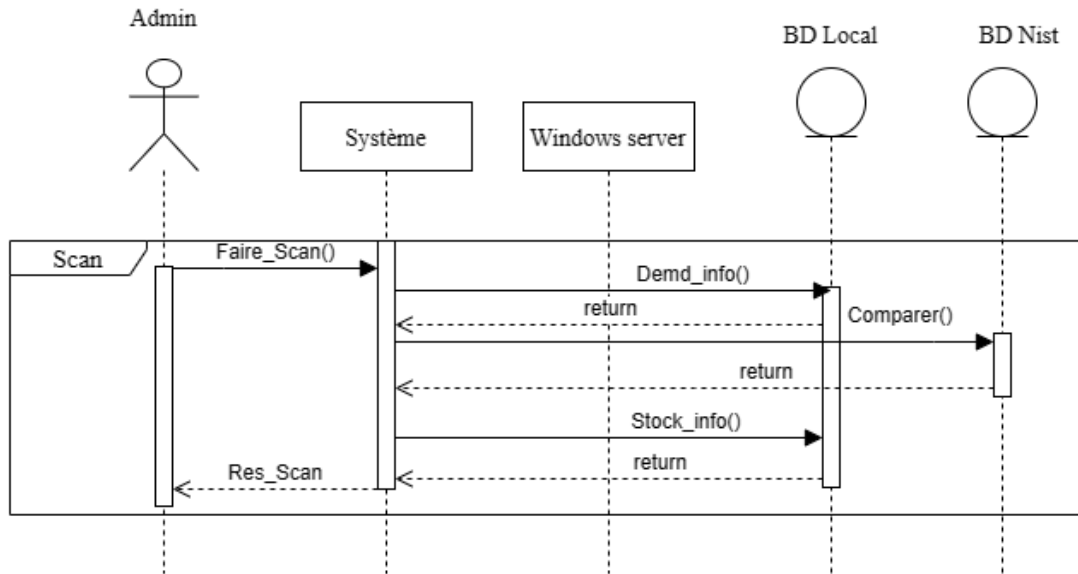


FIG. 2.6 : Diagramme de séquence

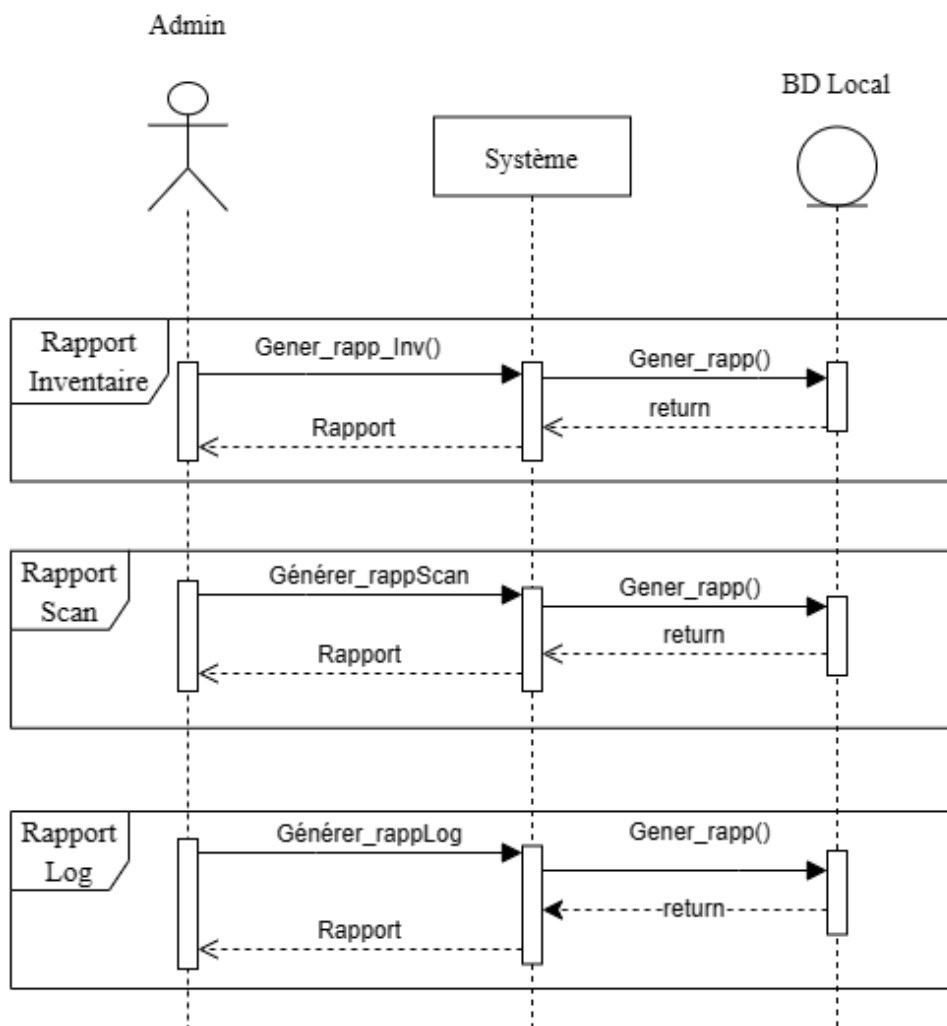


FIG. 2.7 : Diagramme de séquence

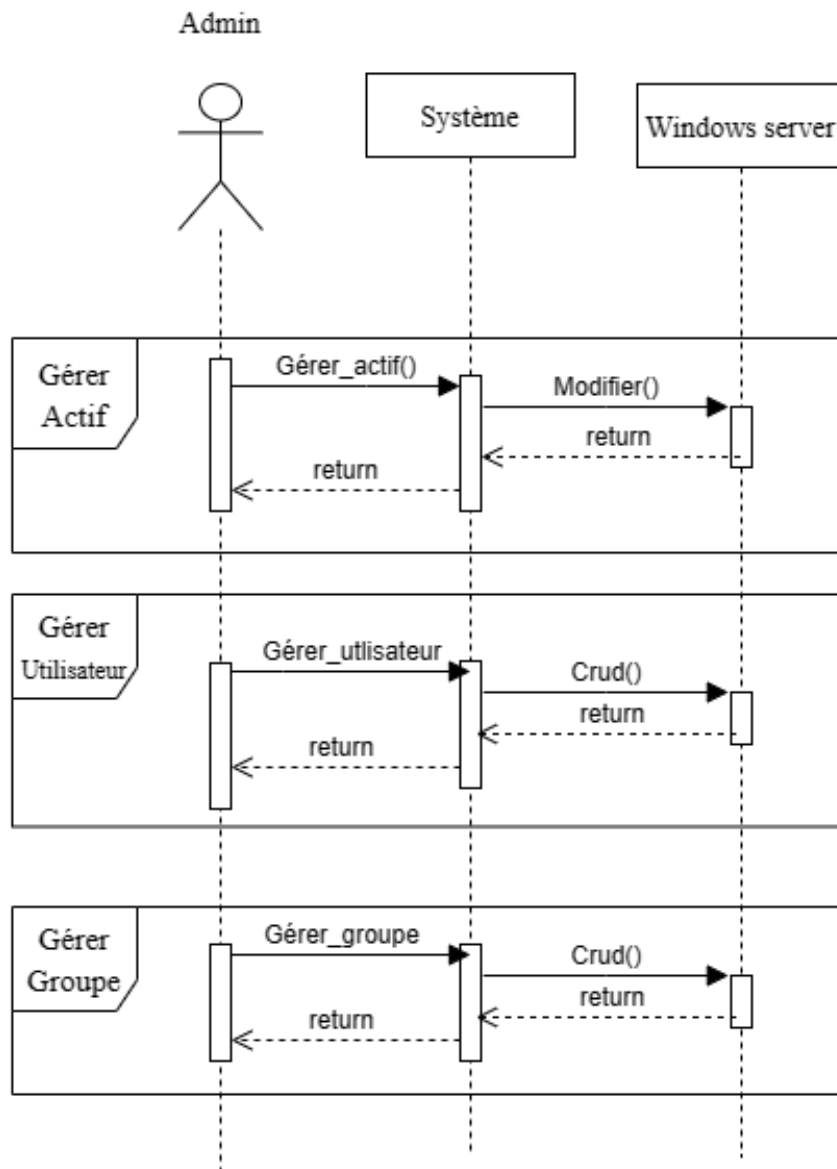


FIG. 2.8 : Diagramme de séquence

2.3.3 Le schéma de la base de données

Le schéma suivant s'agit d'une représentation des relations entre les différentes tables et données. Il permet de bien comprendre l'organisation des données, la maintenance et la manipulation de la base de données. Une fois cette partie est bien conçue, il est possible de gérer les informations de manière structurée, de garantir l'intégrité, et même d'optimiser les requêtes.

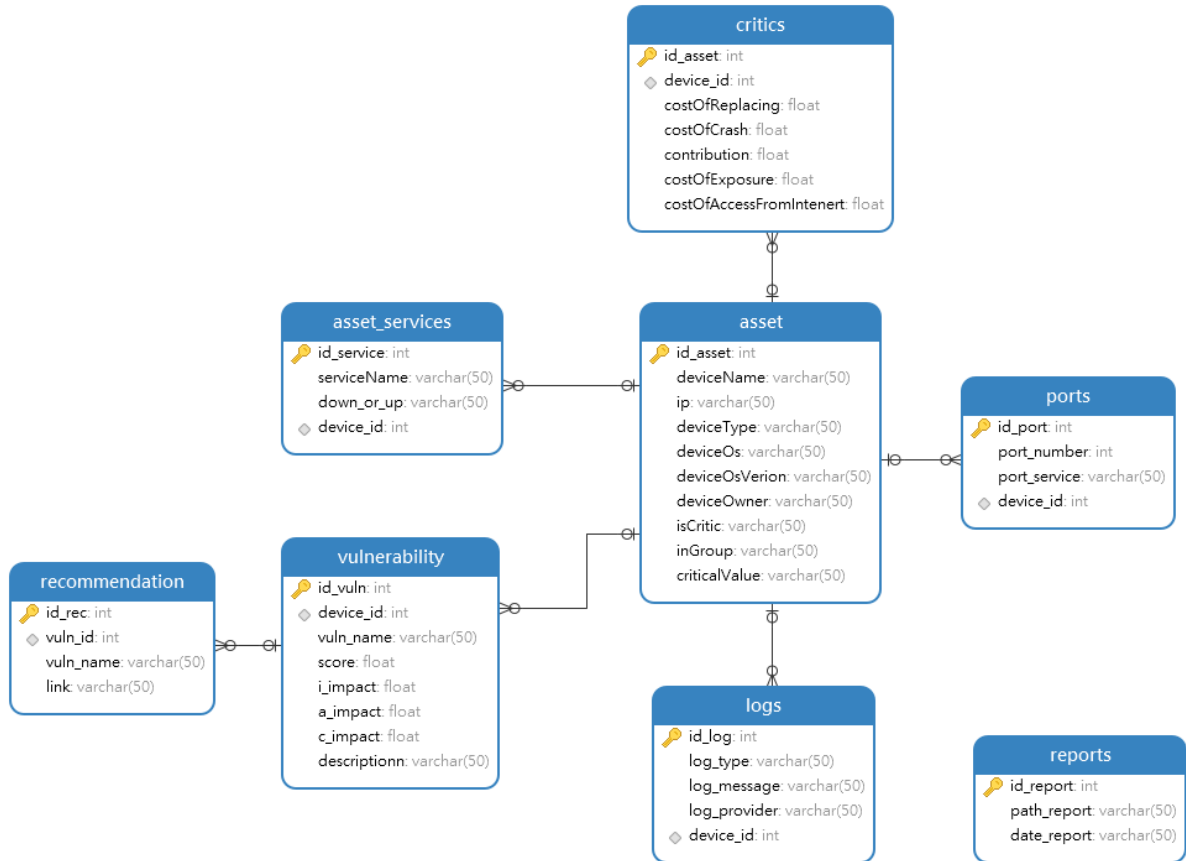


FIG. 2.9 : Le schéma de la base de données

2.4 Conclusion

Dans ce chapitre, nous avons présenter la démarche de notre solution ainsi les fonctionnalités de notre système. Ceci est fait à travers les différents diagrammes permettant de le bien spécifier. Le chapitre suivant va concrétiser cette étude pour aboutir à l'implémentation de notre système.

Chapitre 3

Implementation

3.1 Introduction

Nous rappelons tout d'abord que notre travail vise à identifier les actifs informatiques et évaluer les vulnérabilités dans un réseau LAN d'une entreprise selon la norme RNSI2020.

Ce chapitre se concentre sur les détails pratiques de la mise en œuvre en mettant l'accent sur la maquette du réseau de test, les outils de développement logiciel et matériel utilisés, le langage de programmation et du système de base de données utilisé. Ensuite, nous expliquerons la méthode de notre développement et nous finirons par des captures d'écran sur les différentes fonctionnalités de notre application (Atory) et les rapports générés.

3.2 La maquette du réseau

Le périmètre de stage consiste à créer une maquette virtuelle avec EVE-NG contenant un système d'information doté de ressources variées (Actifs informatiques). Plutôt que de travailler avec des équipements réels, cette méthode nous a permis de simuler un environnement réseau complet avec des équipements virtuels pour estimer le coût, plus de flexibilité, plus sécurisé.

3.2.1 EVE NG

EVE-NG (Emulated Virtual Environment - Next Generation) est une plateforme de virtualisation réseau puissante qui permet de créer des maquettes réseau. Les professionnels des réseaux et les étudiants en informatique utilisent principalement cet outil pour concevoir, configurer, tester et dépanner des architectures réseau. Plus généralement, EVE-NG s'adresse à tous ceux qui travaillent dans le secteur des technologies de l'information.

Il peut être utilisé pour tester des logiciels dans des réseaux simulés, tester des vulnérabilités de sécurité de toutes sortes, et l'ingénierie de systèmes [14].

Après l'installation de la machine virtuelle EVE-NG sur VMware Workstation Player, une plateforme de virtualisation largement utilisée. Nous avons créé un environnement de test fonctionnel et réaliste en configurant une mémoire RAM suffisante (8G), un espace de stockage de (100G) et une connectivité réseau via le mode NAT. Avec cette configuration, nous avons pu tester notre application dans des conditions réalistes et évaluer ses performances avec précision.

Il convient de noter que l'application (Atory) ne dépend pas exclusivement de la maquette créée. La maquette virtuelle que nous avons utilisée est simplement un environnement de test conçu pour évaluer et valider notre application dans des conditions réelles.

3.2.2 Présentation de l'architecture réseau

Pour assurer le bon fonctionnement du réseau et la sécurité des systèmes, nous mettons en place une architecture d'entreprise basique qui se compose généralement d'un réseau LAN (divisé sur zones : zone utilisateurs et zone serveur), DMZ et pare-feu.

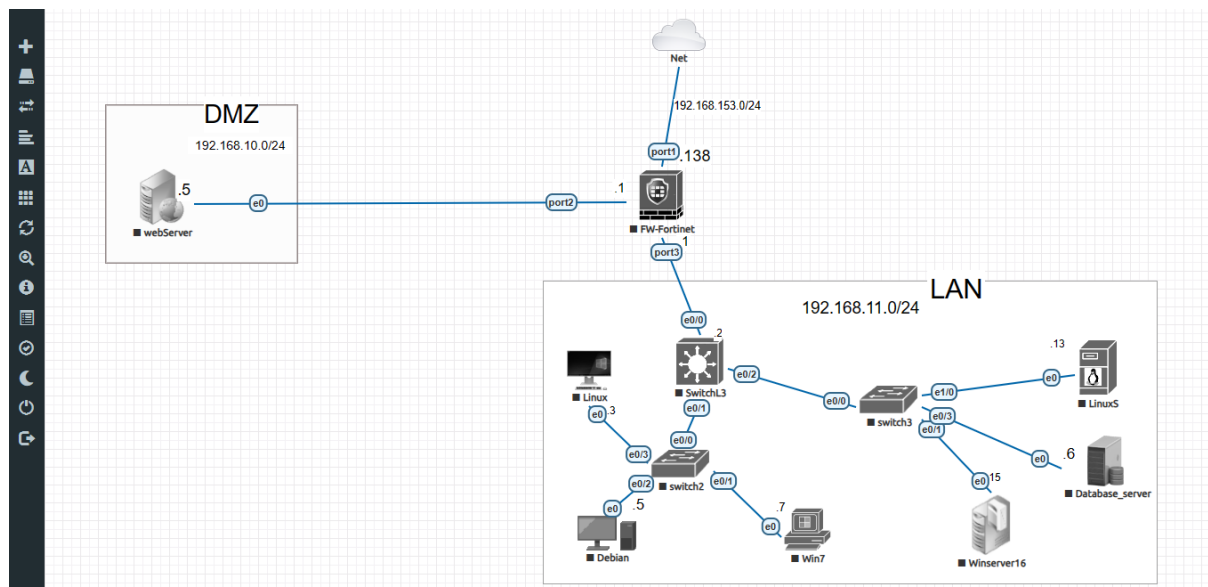


FIG. 3.1 : L'architecture réseau d'une entreprise

- **Le réseau LAN** : est un réseau informatique local qui connecte les appareils internes, comme les ordinateurs de bureau, les serveurs et d'autres appareils locaux. Pour rendre la communication, le partage de ressources et l'accès aux services plus faciles.
- **Pare-feu** : pare-feu filtre le trafic entre deux réseaux en permettant aux utilisateurs d'entrer ou de sortir du réseau local ou en l'interdisant. Comme il y a des succursales et que les utilisateurs externes peuvent accéder au réseau local (LAN).
- **DMZ** : héberge des serveurs tels que des serveurs Web, des serveurs DNS, etc. qui peuvent être accédés à la fois à l'intérieur et à l'extérieur du réseau. Les utilisateurs venant de l'extérieur peuvent se connecter directement aux serveurs de cette DMZ au même pied que les utilisateurs du réseau local.

3.2.3 Configuration des équipements

Pour configurer les équipements, nous avons utilisé l'application Putty

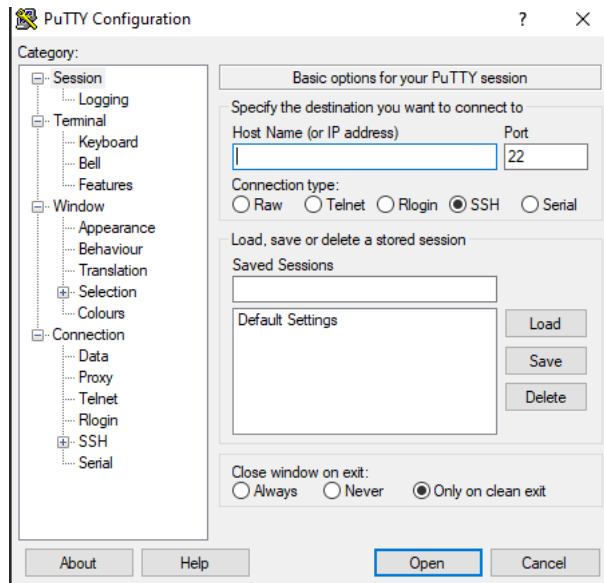


FIG. 3.2 : L'interface de l'émulateur Putty

Configuration du pare-feu

Pour renforcer la sécurité de notre réseau, nous avons utilisé un pare-feu Fortinet qui offre une convergence idéale adaptable à n'importe quel endroit. Nous avons mis en place des règles de sécurité, configuré les ports et mis en place une route statique.

- La configuration des ports :

Nom	Type	Membres	IP/Masque	Accès administratif	Clients DHCP
WAN (port1)	Interface physique		192.168.153.138/255.255.255.0	PING HTTPS SSH HTTP Accès FMG	
DMZ (port2)	Interface physique		192.168.10.1/255.255.255.0	PING HTTPS SSH HTTP TELNET	
NAT interface (naf.root)	Interface de tunnel		0.0.0.0/0.0.0.0		
LAN (port3)	Interface physique		192.168.11.1/255.255.255.0	PING HTTPS	1

FIG. 3.3 : La configuration des ports du pare-feu

- Les règles de sécurité :

- Configuration des ports pour l'établissement de la connexion entre l'application et le Windows Server.
- Ajout d'utilisateurs et de groupes.

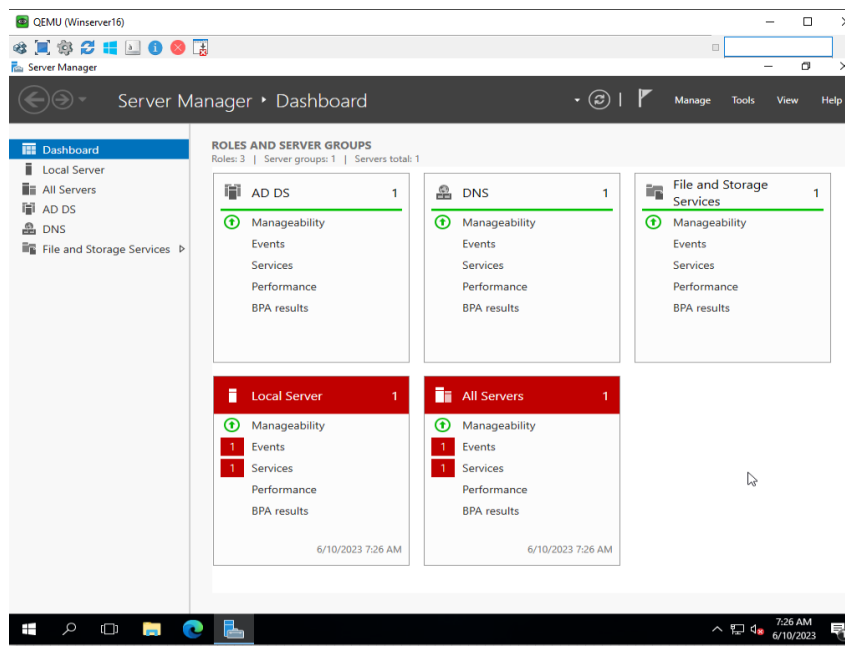


FIG. 3.8 : Interface de l'annuaire active directory

3.3 Les outils de développement

3.3.1 Langage de programmation

Python est un langage de programmation créé en 1991. Contrairement à d'autres langages comme Java ou C++ (qui sont compilés), Python est lui un langage interprété, ce qui signifie que les instructions tapées sont transcrites en binaire au fur et à mesure de leur lecture. Il a l'avantage d'être assez facile à comprendre et à apprendre, tout en restant puissant et adapté pour des projets importants, ce qui fait donc de lui le langage de programmation idéal pour les débutants.

Python est également apprécié pour sa vaste bibliothèque standard, qui comprend un large éventail de modules et d'outils pour effectuer une variété de tâches, allant de la manipulation de chaînes de caractères à la gestion de fichiers, en passant par le développement Web et l'analyse de données. De plus, la communauté Python est très active et offre de nombreuses bibliothèques tierces spécialisées dans divers domaines, ce qui facilite l'extension des fonctionnalités de base du langage [15].

Bibliothèque Python

- **CustomTkinter** est une bibliothèque d'interface utilisateur python basée sur Tkinter qui propose de nouveaux widgets entièrement personnalisables et modernes. Ils

ont été développés et utilisés comme des widgets Tkinter standard. Ils peuvent également être utilisés en conjonction avec d'autres éléments Tkinter. Tous les widgets et fenêtres CustomTkinter prennent en charge la mise à l'échelle HighDPI (Windows, macOS), et les couleurs des widgets et des fenêtres s'adaptent à l'apparence du système ou au mode sélectionné manuellement. Avec CustomTkinter[16].

- **Tkinter** est une bibliothèque Python standard qui permet la création d'interfaces graphiques. Un ensemble d'outils pour la création d'interfaces utilisateur graphiques, de là son nom "Tk interface" [17].

3.3.2 Bibliothèques et mécanisme

Dans notre processus on a utilisé une base de données interne (Active directory) et d'autres services liés à elle. Par exemple, au lieu d'utiliser le monitoring ou un scanner d'équipement, on a opté des bibliothèques Python qui fournissent le même travail comme "python-nmap", ainsi que d'autres bibliothèques tels que :

- **Active Directory (AD)** : un service de gestion des annuaires développé par Microsoft, à partir de Windows 2000. Il permet aux administrateurs de gérer efficacement les informations à l'échelle de l'entreprise à partir d'un répertoire central qui peut être distribué dans le monde entier. Une fois que les informations relatives aux utilisateurs et aux groupes, aux ordinateurs et aux imprimantes, ainsi qu'aux applications et aux services ont été ajoutées à Active Directory, elles peuvent être mises à la disposition du plus grand ou plus petit nombre de personnes possible dans l'ensemble de l'entreprise [18].
- **LDAP (Lightweight Directory Access Protocol)** : C'est un protocole utilisé par Active Directory pour accéder et gérer des services d'annuaire. Il offre également des fonctionnalités d'authentification, de recherche et de modification des objets d'annuaire [19].
- **RPC (Remote Procedure Call)** est un mécanisme de communication qu'un programme peut utiliser pour demander un service à un programme situé sur un autre ordinateur sur un réseau sans comprendre les détails du réseau [20].
- **Nmap** : ("Network Mapper") est un utilitaire libre et gratuit pour la découverte de réseaux et l'audit de sécurité. De nombreux administrateurs des systèmes et réseaux le trouvent également utile pour des tâches telles que l'inventaire du réseau, la gestion des calendriers de mise à jour des services et la surveillance de l'état de fonctionnement des hôtes ou des services[nmap].
- **Python-nmap** : Bibliothèque python qui aide à l'utilisation du scanner de ports nmap. Les administrateurs de systèmes qui souhaitent automatiser les tâches et les rapports de scans trouveront cet outil idéal car il leur permet de manipuler facilement les résultats des scans nmap. De plus, elle prend en charge les sorties de scripts nmap.[21]
- **Netmiko** : Bibliothèque de fournisseurs multiples pour faciliter l'automatisation et la gestion des équipements réseau via SSH ou Telnet.[22]

Cartographie

Il existe plusieurs outils de cartographie des réseaux disponibles pour créer des visualisations graphiques. Dans notre travail on a utilisé les deux bibliothèques suivantes :

- **NetworkX** : un paquetage python pour la création, la manipulation et l'étude de la structure, de la dynamique et des fonctions des réseaux complexes [**networkx**].
- **Matplotlib** : bibliothèque complète permettant de créer des visualisations statiques, animées et interactives en Python. [23]

Classification des actifs informatiques

Les principes de confidentialité, d'intégrité et de disponibilité (CID) sont souvent utilisés pour classer les actifs dans un réseau.

- Confidentialité : Le niveau de confidentialité des actifs est déterminé par des informations sensibles qui possèdent.
- Intégrité : Les actifs nécessitant une protection des données dans tous ces états existants.
- Disponibilité : En fonction de leur importance pour les opérations de l'organisation, les actifs doivent être toujours accessibles et disponibles.[3]

Le rapport d'inventaire

La bibliothèque matplotlib de Python est utilisée pour créer des graphiques, des diagrammes ou des tableaux visuellement attrayants qui présentent les informations d'inventaire [23].

Une fois que les graphiques ont été créés avec matplotlib, il est possible d'utiliser la bibliothèque reportlab pour générer un rapport PDF complet. Cette dernière permet de mettre en page et de créer des documents PDF personnalisés. Dans le rapport, on peut insérer les graphiques créés et ajouter des en-têtes, des pieds de page, des descriptions et d'autres informations pertinentes sur les actifs qui ont été inventoriés [24].

L'identification des vulnérabilités

Parmi les standard base de données on a utilisé NIST CVE.

- **CVE (Common Vulnerabilities and Exposures)** sert de dictionnaire ou de glossaire des vulnérabilités. Les parties intéressées peuvent consulter cette liste pour obtenir des informations sur les vulnérabilités en utilisant un identifiant unique appelé CVE ID. Depuis quelques années, le programme CVE est devenu de plus en

plus connu, il est donc crucial que les participants et les utilisateurs comprennent les fondamentaux du programme[25].

Il permet une coordination et une communication efficaces dans le domaine de la sécurité informatique en fournissant des identifiants uniques et des informations détaillées sur chaque vulnérabilité.

- Chaque vulnérabilité du NIST CVE est accompagnée d'une description détaillée qui explique les aspects techniques de la vulnérabilité ainsi que des recommandations des solutions et des métriques.

Classification des vulnérabilités

Le NIST CVE intègre fréquemment les identifiants CVE au système de classification CVSS. Chaque vulnérabilité est évaluée par le CVSS en fonction de critères tels que son impact sur la confidentialité, l'intégrité et la disponibilité. Les scores de ces vulnérabilités aident à évaluer et à comparer leur gravité [25].

La recommandation des solutions

Après l'identification, la description et la classification des vulnérabilités, le NIST CVE suggère des méthodes pour les atténuer. Bien que le NIST CVE soit un dictionnaire de vulnérabilités, il est lié à d'autres ressources qui offrent des informations supplémentaires et des suggestions pour la gestion des vulnérabilités telles que le NVD, les SP et le CSRC [25].

Le rapport des vulnérabilités

Il est généré comme mentionné dans le rapport d'inventaire en combinant les bibliothèques matplotlib et reportlab.

3.3.3 Environnement matériel

Pour la réalisation de notre projet, nous avons utilisé un ordinateur Acer caractérisé par :

- Système d'exploitation : Linux Mint.
- Processeur : Intel R Core TM i5 CPU 1,6 GHz.
- Ram : 12GO.
- Disque dur : 1T hdd.

3.3.4 Environnement logiciel

- **Visual Studio Code** : c'est un éditeur de code source léger, mais puissant qui s'exécute et qui est disponible sur Windows, macOS et Linux. Il est livré avec une prise en charge intégrée de JavaScript, Typescript et Node.js. Il dispose d'un écosystème d'extensions riche pour d'autres langages (tels que C++, Java, Python, PHP, Go) et des environnements d'exécution (tels que .NET et Unity) [26].
- **MySQL** : est un système de gestion de base de données relationnelle (SGBDR) largement utilisé par les développeurs et est disponible sous licence open source. Il fournit une solution fiable, efficace et évolutive pour le stockage, la gestion et la récupération de données. MySQL utilise le langage de requête structuré[27].
- **Draw.io** : est une plateforme technologique open source a pour mission de "fournir un logiciel de création de diagrammes gratuits et de haute qualité pour tout le monde". La polyvalence de Draw.io est l'une de ses principales caractéristiques. Il propose une large gamme de formes, de symboles et d'icônes préconçus pour représenter divers éléments visuels tels que des boîtes, des flèches, des connecteurs, des organigrammes, des diagrammes de flux, des réseaux, des organes et des cartes. Les utilisateurs peuvent créer des diagrammes complexes en quelques clics, car ces éléments visuels peuvent être facilement glissés-déposés sur la toile de travail [28].

3.4 Présentation de l'application

Notre application ne dépend pas à un environnement de test spécifique. Et afin de garantir sa portabilité et sa compatibilité avec divers environnements de déploiement, elle a été créée en prenant en compte les bonnes pratiques et les normes de programmation. Comme on peut l'exporter pour Windows sous le format.exe, pour macOS sous le format.dmg et pour Linux sous le format.deb ou.rpm. Chaque édition serait adaptée aux caractéristiques de son propre système d'exploitation.

Une fois l'application "Atory" est lancée, la première fenêtre qui apparaît contient un champ de connexion "Login". L'utilisateur doit connecter pour profiter de toutes les fonctionnalités de l'application. Le processus de connexion est simple et sécurisé qui permet d'accéder rapidement à l'espace spécifique. Le bouton "À propos" se trouve juste en dessous pour plus de documentation sur l'interface.

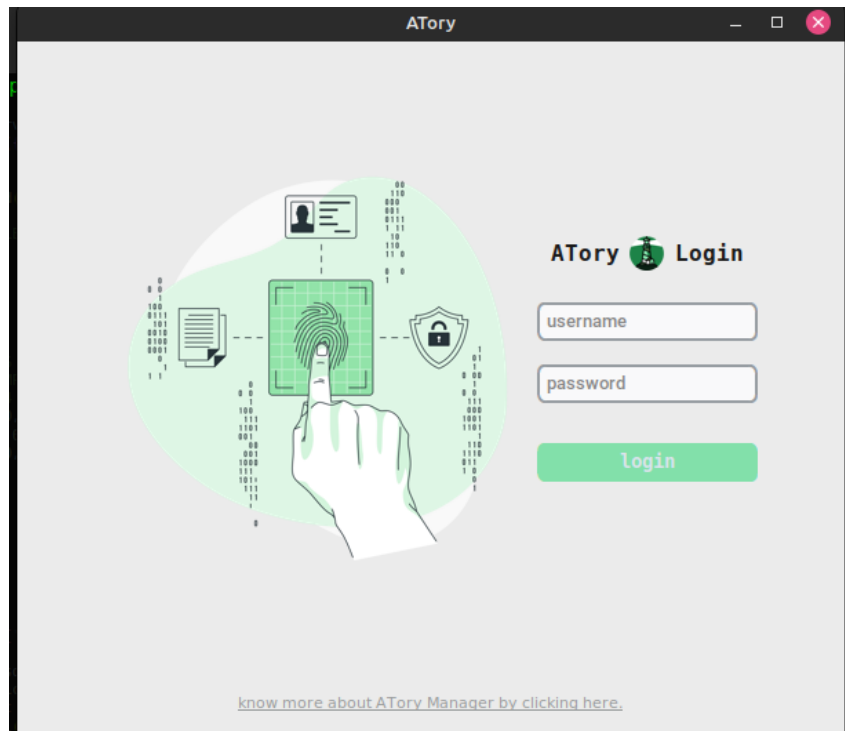


FIG. 3.9 : Interface d'authentification

Une fois l'authentification est validée, l'utilisateur accède à une page d'accueil avec plusieurs boutons situés en haut de l'interface, qui propose des options importantes telles que 'New Inventory', 'Scan', 'Reports', 'Management' et 'About Atory'. Sans oublier l'option "Exit" en haut à droite de l'interface. L'utilisateur peut déconnecter facilement de son compte en cliquant sur ce bouton, ce qui garantit que ses données sont sécurisées et confidentielles.

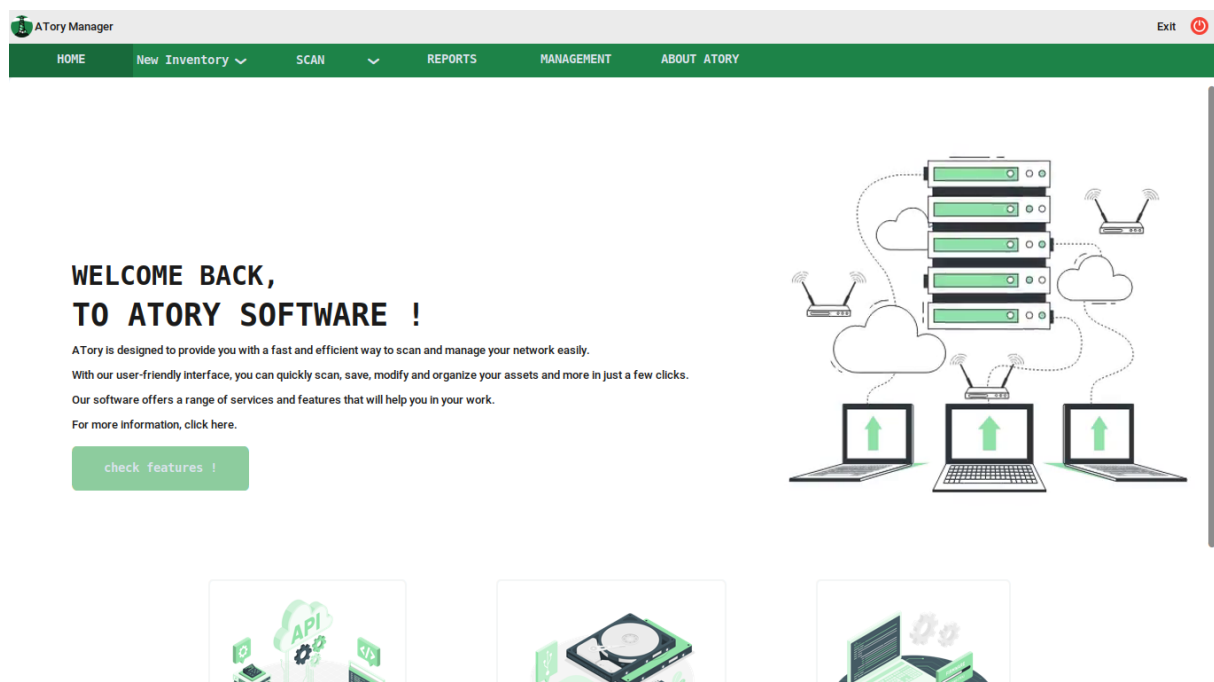


FIG. 3.10 : La page d'accueil

Chapitre 3. Implementation

Lorsque l'utilisateur clique sur le bouton "New Inventory", Le processus d'identification des différents actifs informatiques dans le réseau commence. Par conséquent, une interface sera affichée avec toutes les informations classées dans 3 champs 'Statistics', 'Devices détails' et 'Recent changes'.

Le premier bouton, "Statistics", donne un aperçu complet sur les informations importantes des actifs informatiques, y compris leur configuration, leurs ports ouverts, leurs services.

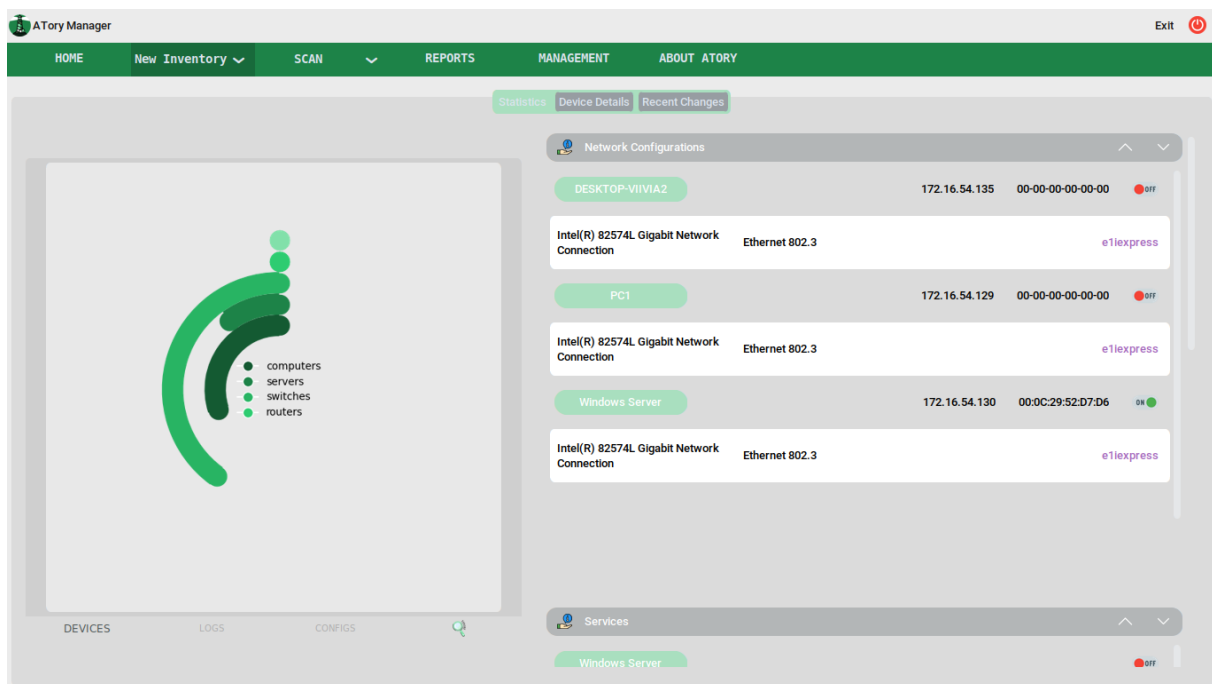


FIG. 3.11 : Les statistiques

Lorsque l'utilisateur fait défiler l'écran, il trouve les services de chaque actif.

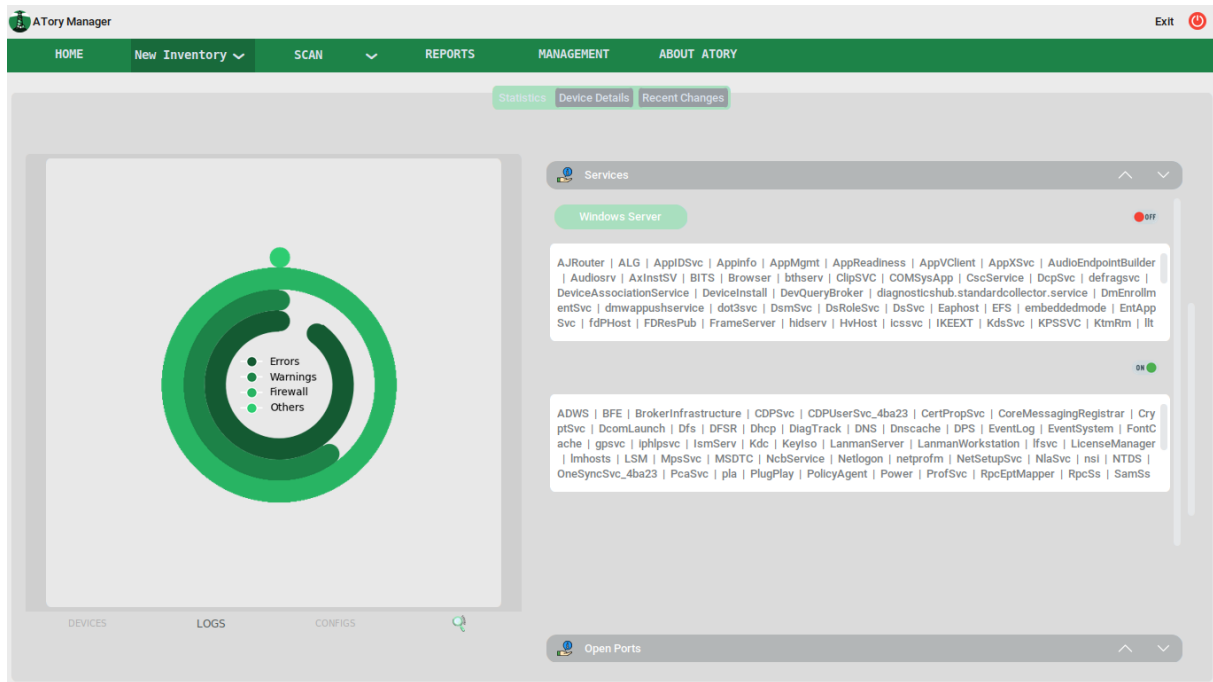


FIG. 3.12 : Le tableau des services

De même pour les ports identifiés.

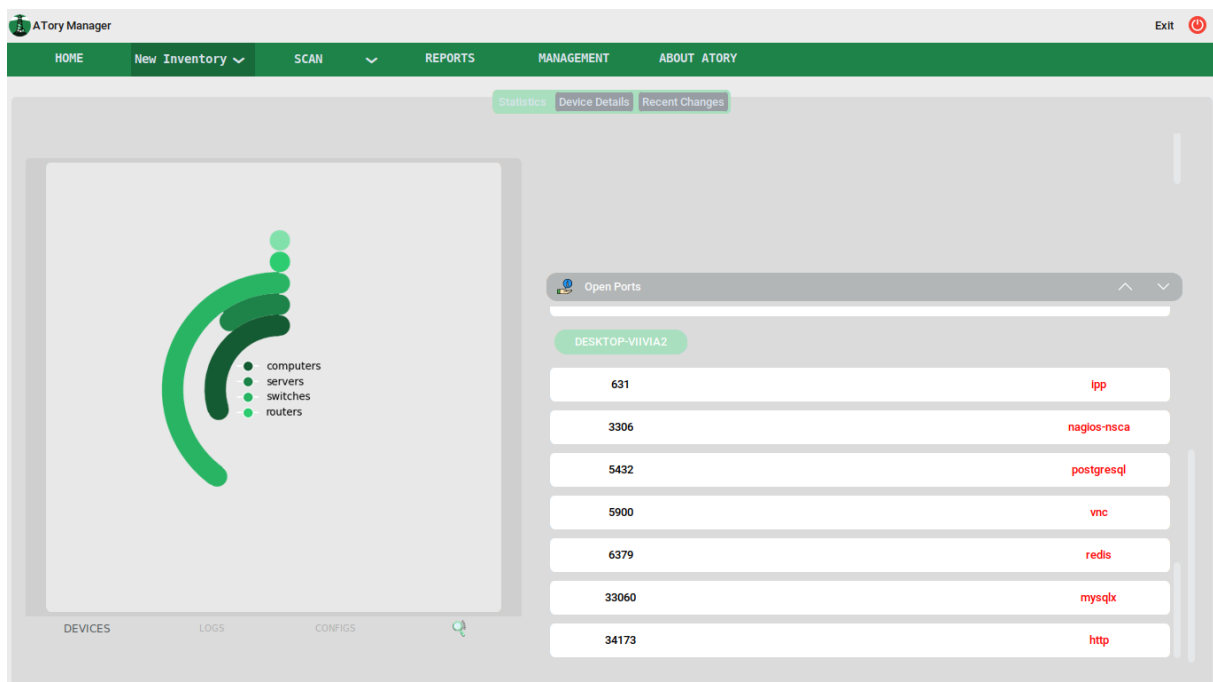
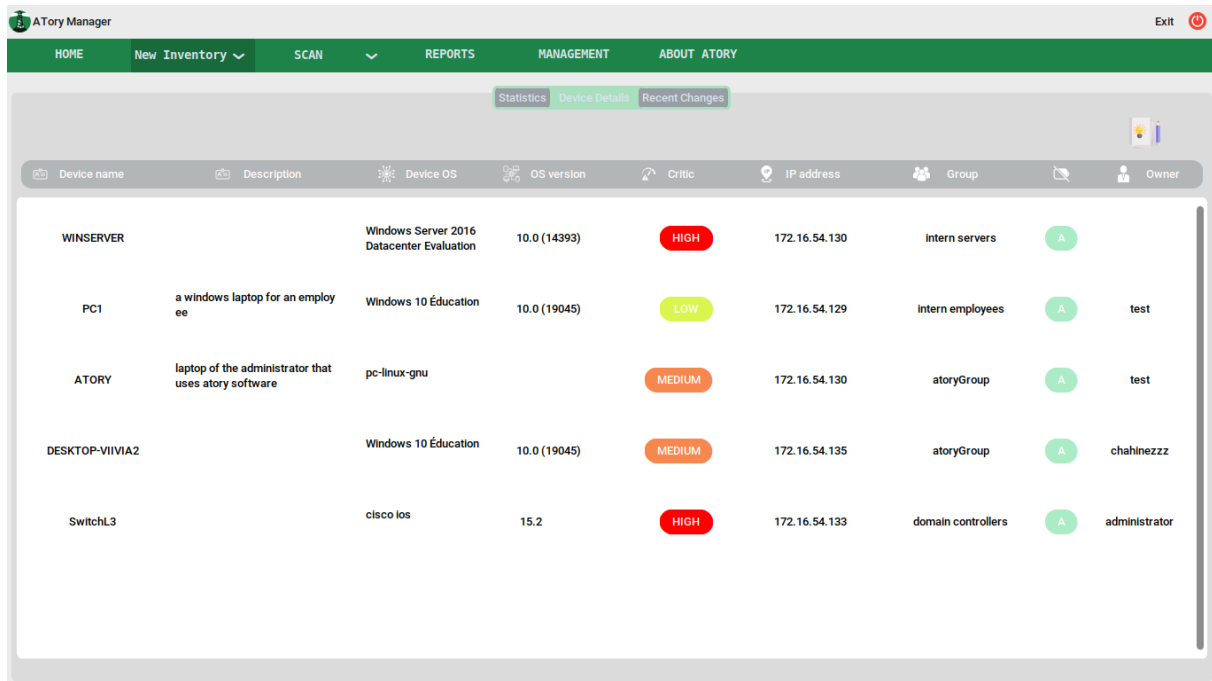


FIG. 3.13 : Le Tableau des ports identifiés

Le deuxième bouton 'Devices détails' est spécialement conçu pour aperçu les détails sur les actifs informatiques. Chaque actif est accompagné par des détails essentiels tels que son nom, sa description, son système d'exploitation, sa version, sa classification, son adresse IP et son groupe, ainsi que son administrateur.

Chapitre 3. Implementation

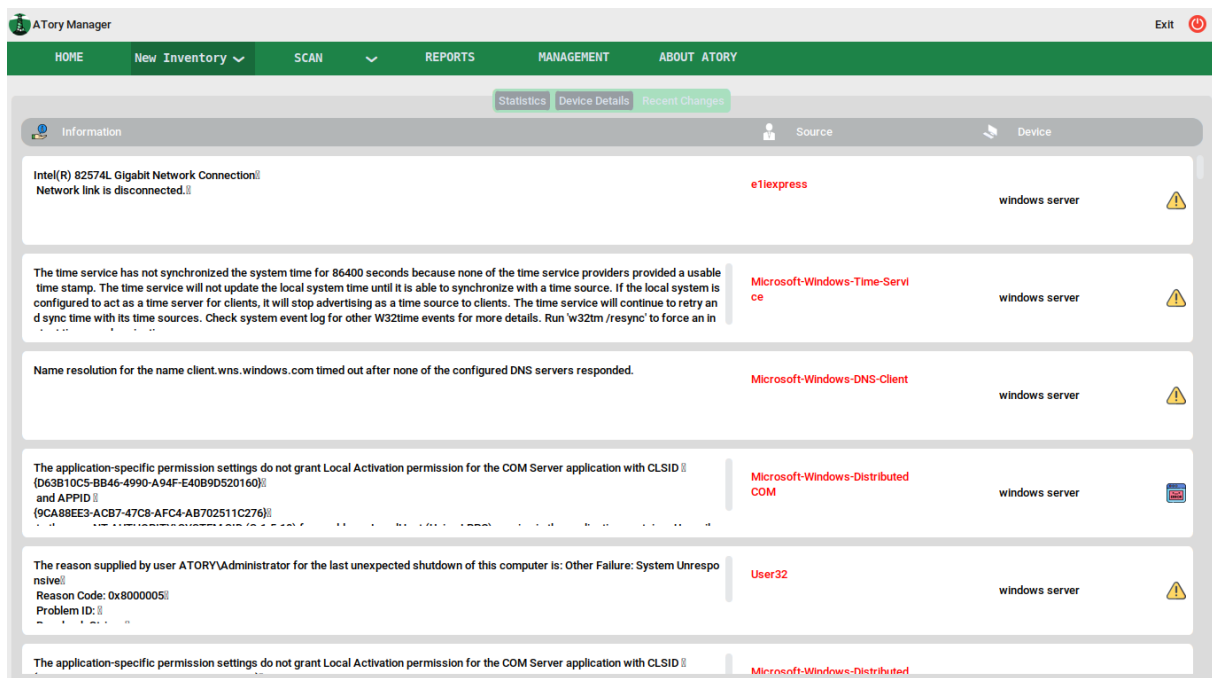


The screenshot shows the ATory Manager interface with a table of identified active devices. The table has columns for Device name, Description, Device OS, OS version, Critic, IP address, Group, and Owner. The data is as follows:

Device name	Description	Device OS	OS version	Critic	IP address	Group	Owner
WINSERVER		Windows Server 2016 Datacenter Evaluation	10.0 (14393)	HIGH	172.16.54.130	intern servers	A
PC1	a windows laptop for an employ ee	Windows 10 Éducation	10.0 (19045)	LOW	172.16.54.129	intern employees	A test
ATORY	laptop of the administrator that uses atory software	pc-linux-gnu		MEDIUM	172.16.54.130	atoryGroup	A test
DESKTOP-VIIVIA2		Windows 10 Éducation	10.0 (19045)	MEDIUM	172.16.54.135	atoryGroup	A chahinezzz
SwitchL3		cisco ios	15.2	HIGH	172.16.54.133	domain controllers	A administrator

FIG. 3.14 : Le tableau des actifs informatiques identifiés

Le troisième ‘Récents Changes’ bouton permet d’accéder à divers changements récents sur Windows Server.



The screenshot shows the ATory Manager interface with the 'Recent Changes' tab selected. The table displays the following information:

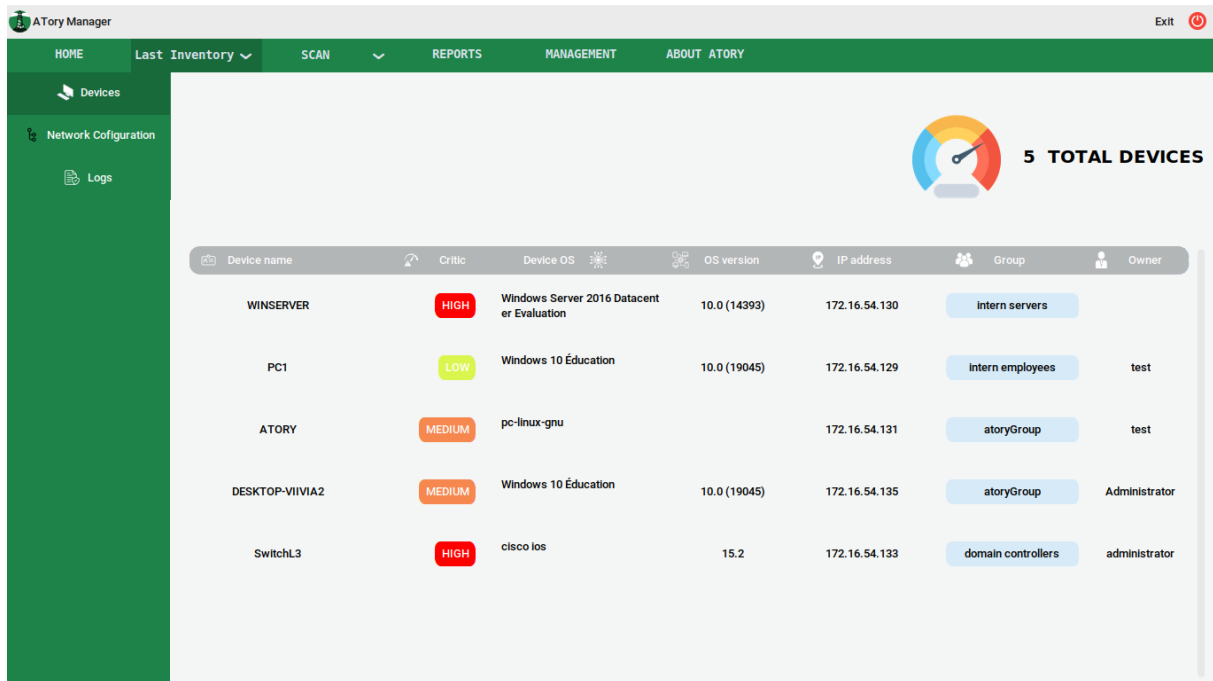
Information	Source	Device
Intel(R) 82574L Gigabit Network Connection: Network link is disconnected.ⓘ	e1express	windows server ⚠
The time service has not synchronized the system time for 86400 seconds because none of the time service providers provided a usable time stamp. The time service will not update the local system time until it is able to synchronize with a time source. If the local system is configured to act as a time server for clients, it will stop advertising as a time source to clients. The time service will continue to retry and sync time with its time sources. Check system event log for other W32time events for more details. Run 'w32tm /resync' to force an in...	Microsoft-Windows-Time-Serv ice	windows server ⚠
Name resolution for the name client.wns.windows.com timed out after none of the configured DNS servers responded.	Microsoft-Windows-DNS-Client	windows server ⚠
The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID ⓘ (D63B10C5-BB46-4990-A94F-E40B9D520160) ⓘ and APPID ⓘ (9CAB8EE3-ACB7-47C8-AFC4-AB702511C276) ⓘ	Microsoft-Windows-Distributed COM	windows server 📄
The reason supplied by user ATORY\Administrator for the last unexpected shutdown of this computer is: Other Failure: System Unrespo nsive ⓘ Reason Code: 0x8000005 ⓘ Problem ID: ⓘ	User32	windows server ⚠
The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID ⓘ	Microsoft-Windows-Distributed	

FIG. 3.15 : Les changements récents

Une le processus d’inventaire est terminé, les données seront stockées dans une base de données automatiquement.

Chapitre 3. Implementation

Le bouton "See last Inventory" permet d'accéder rapidement aux informations de configurations, actifs informatiques du dernier l'inventaire effectué.



Device name	Critic	Device OS	OS version	IP address	Group	Owner
WINSERVER	HIGH	Windows Server 2016 Datacenter Evaluation	10.0 (14393)	172.16.54.130	intern servers	
PC1	LOW	Windows 10 Éducation	10.0 (19045)	172.16.54.129	intern employees	test
ATORY	MEDIUM	pc-linux-gnu		172.16.54.131	atoryGroup	test
DESKTOP-VIIVIA2	MEDIUM	Windows 10 Éducation	10.0 (19045)	172.16.54.135	atoryGroup	Administrator
SwitchL3	HIGH	cisco ios	15.2	172.16.54.133	domain controllers	administrator

FIG. 3.16 : Les informations du dernier inventaire effectué

Après avoir effectué l'inventaire, on trouve le bouton "Asset Scan". Ce bouton permet d'effectuer un scan spécifique d'un actif selon le choix de l'utilisateur. Ce scan utilise la base de données Nist CVE pour interroger et comparer les données de l'inventaire effectué. Chaque vulnérabilité a une description, un impact potentiel et des recommandations.

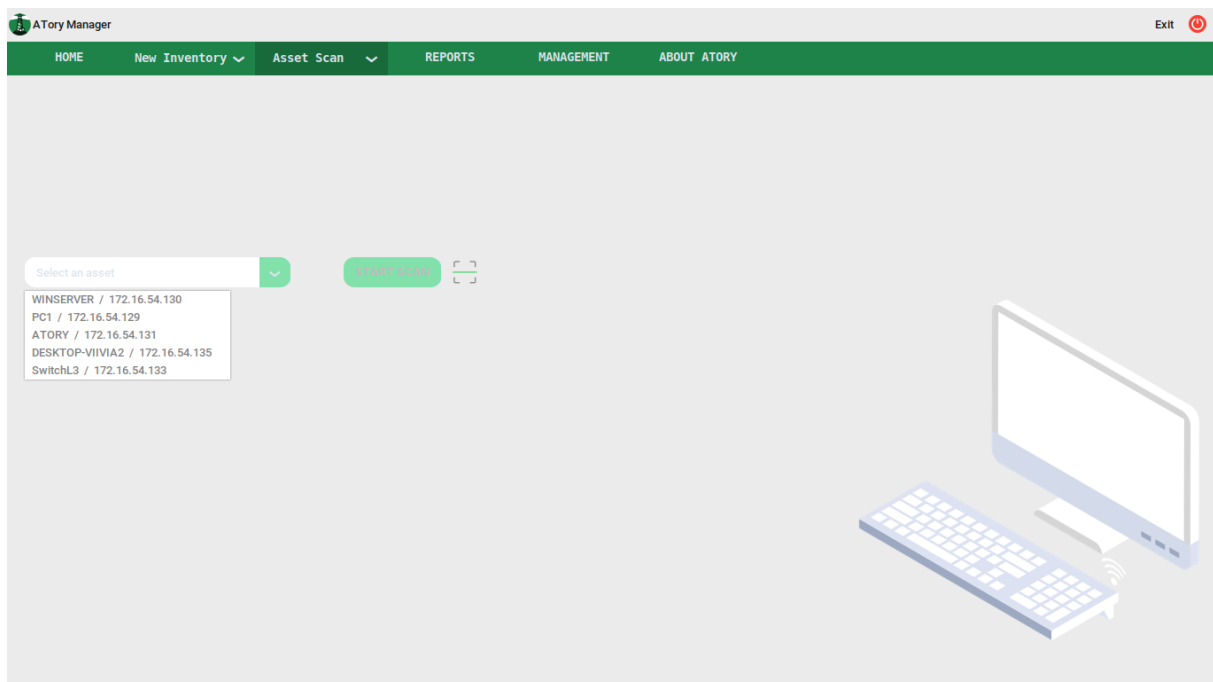


FIG. 3.17 : Le choix de l'actif informatique à scanner

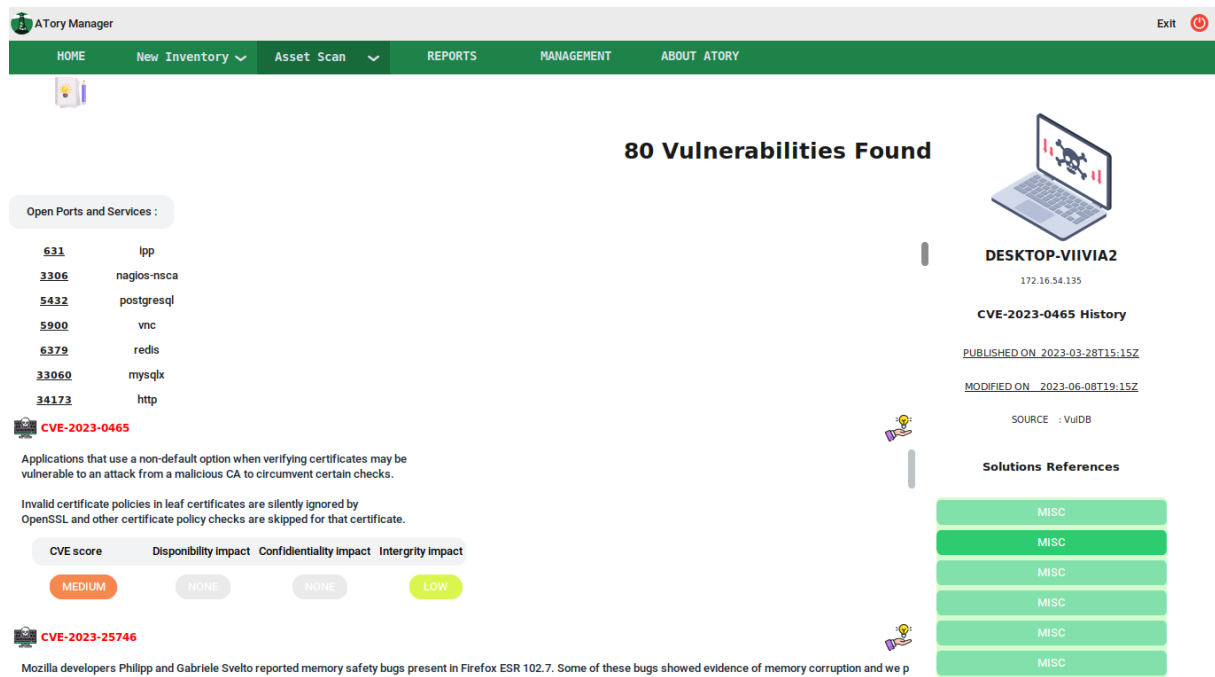


FIG. 3.18 : Résultat obtenu après scan d'un actif informatique selon le choix.

Idem pour le scan total, qui consiste à traiter tous les actifs informatiques existants.

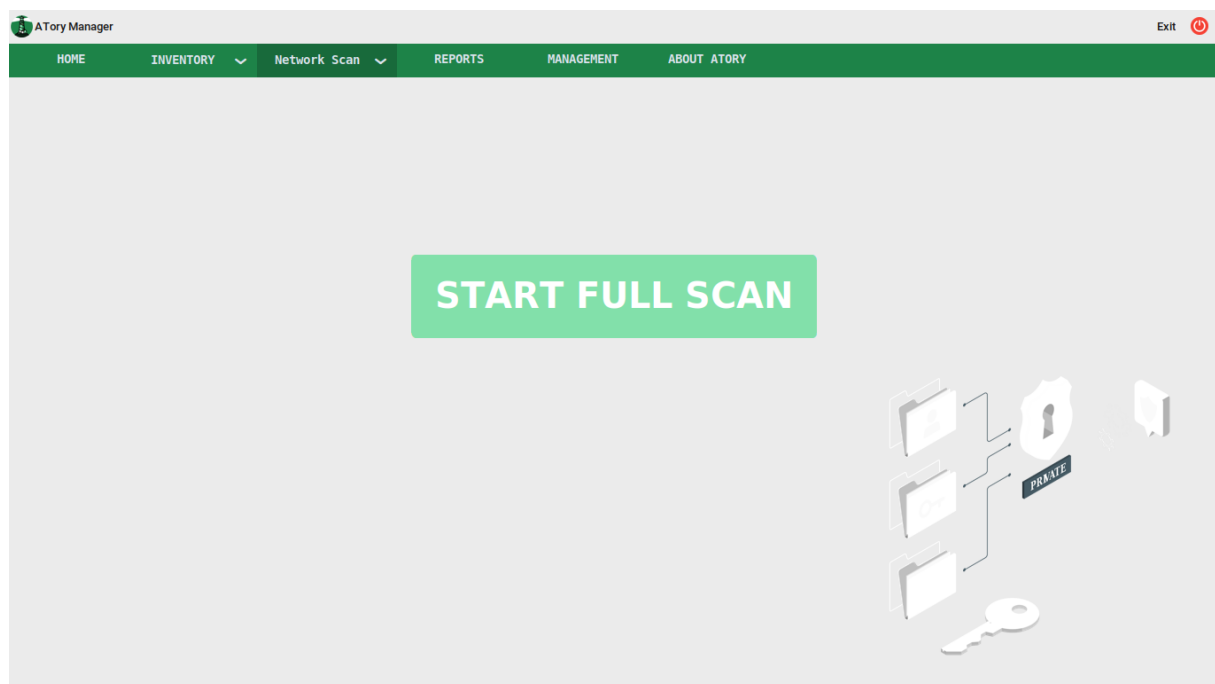


FIG. 3.19 : Scanner tout le réseau

Chapitre 3. Implementation

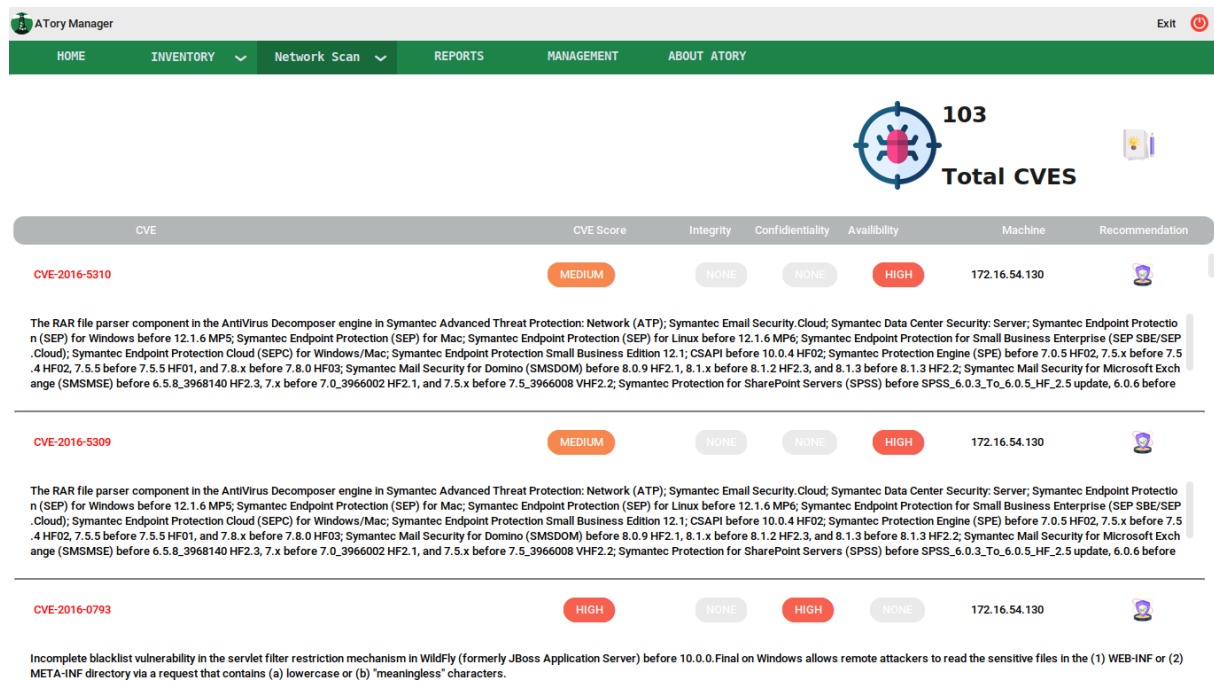


FIG. 3.20 : Le résultat du Scan total

Le bouton "Rapports" permet de consulter et de télécharger les rapports d'inventaire et de scan précédemment générés. La liste est classée par ordre de date de création. Cette fonctionnalité facilite l'accès à l'historique des rapports, ce qui fournit des références utiles pour l'analyse et le suivi.

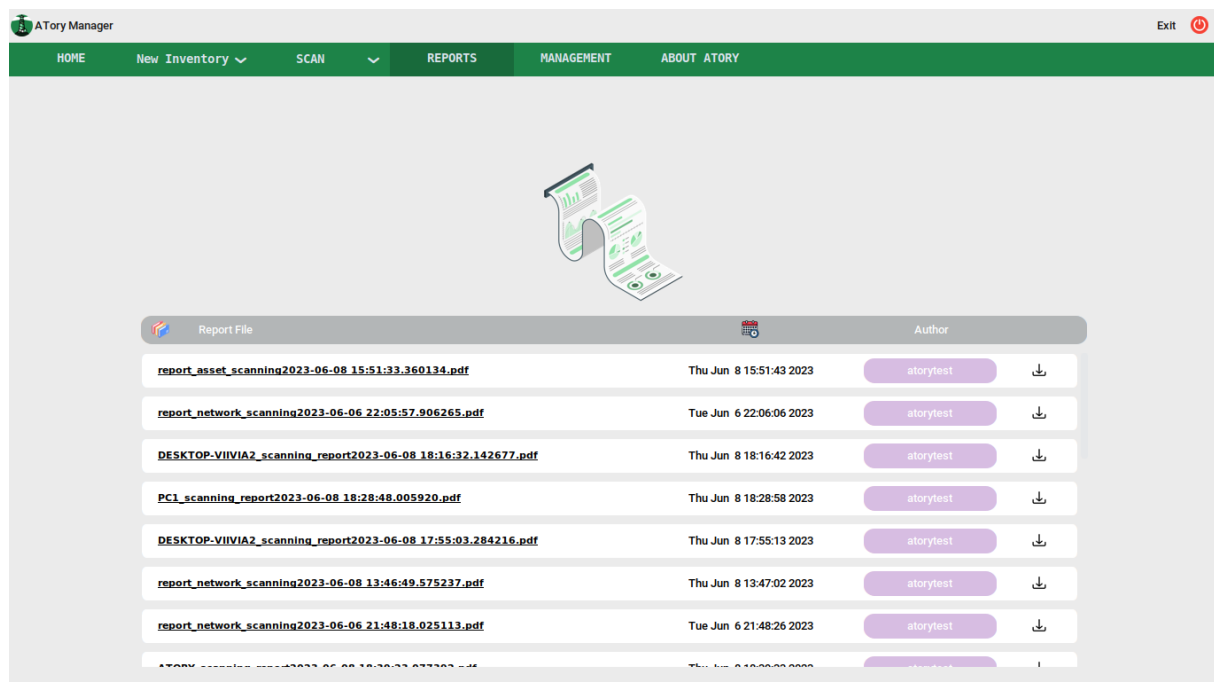


FIG. 3.21 : La liste des rapports générés

Quand il s'agit du "Management", on a 3 fonctions principales pour faciliter la gestion

et la configuration des actifs automatiquement.

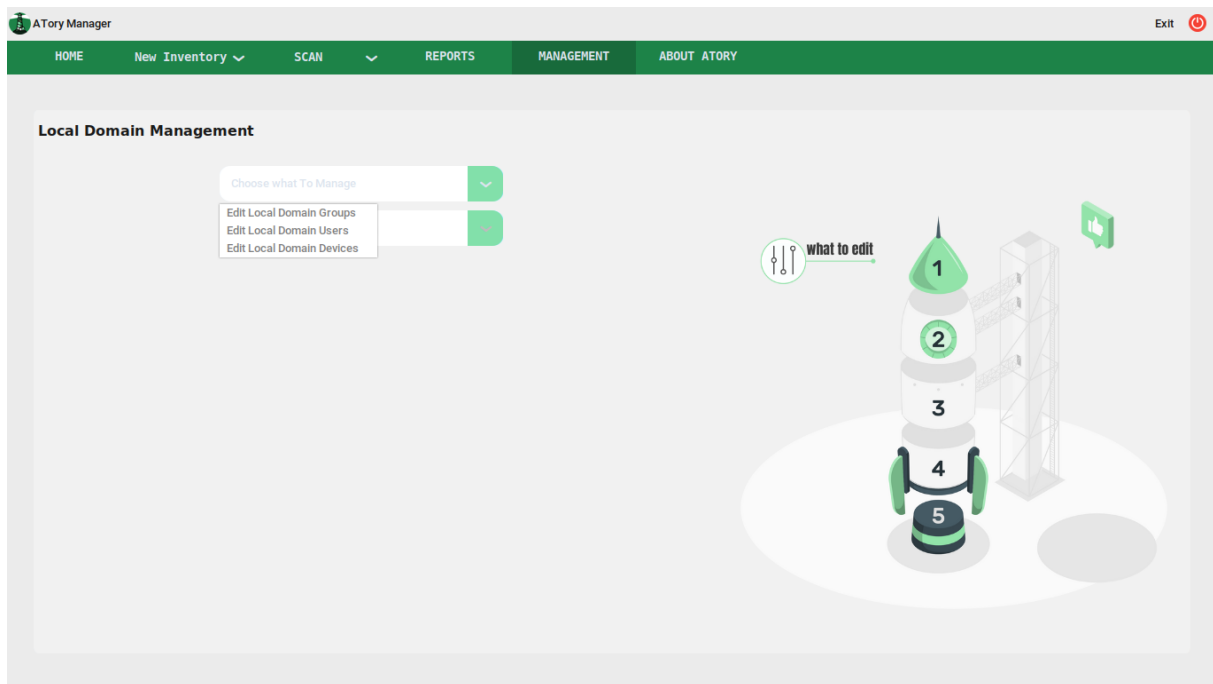


FIG. 3.22 : L'interface de la gestion

La première fonctionnalité 'Edit local domain groupe' permet d'ajouter de nouveau groupe dans le domaine local du réseau.

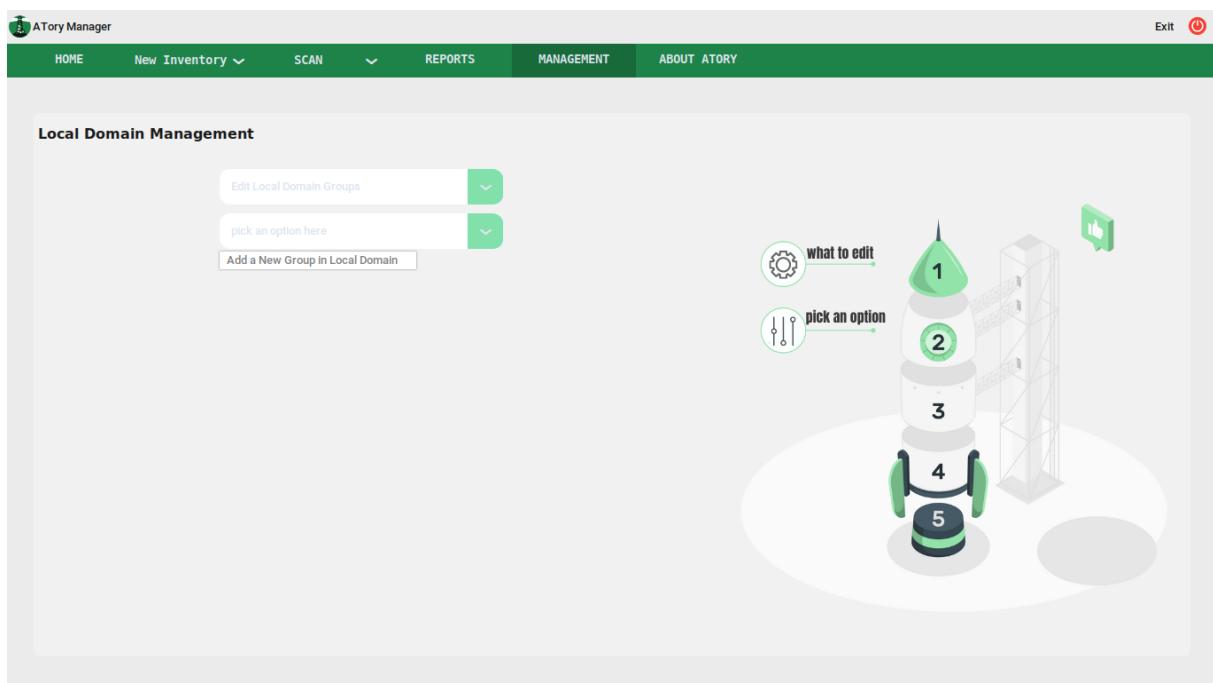


FIG. 3.23 : La gestion des groupes

La deuxième fonctionnalité 'Edit local domain users' permet d'ajouter ou supprimer un utilisateur dans le domaine local, ou bien de changer son groupe.

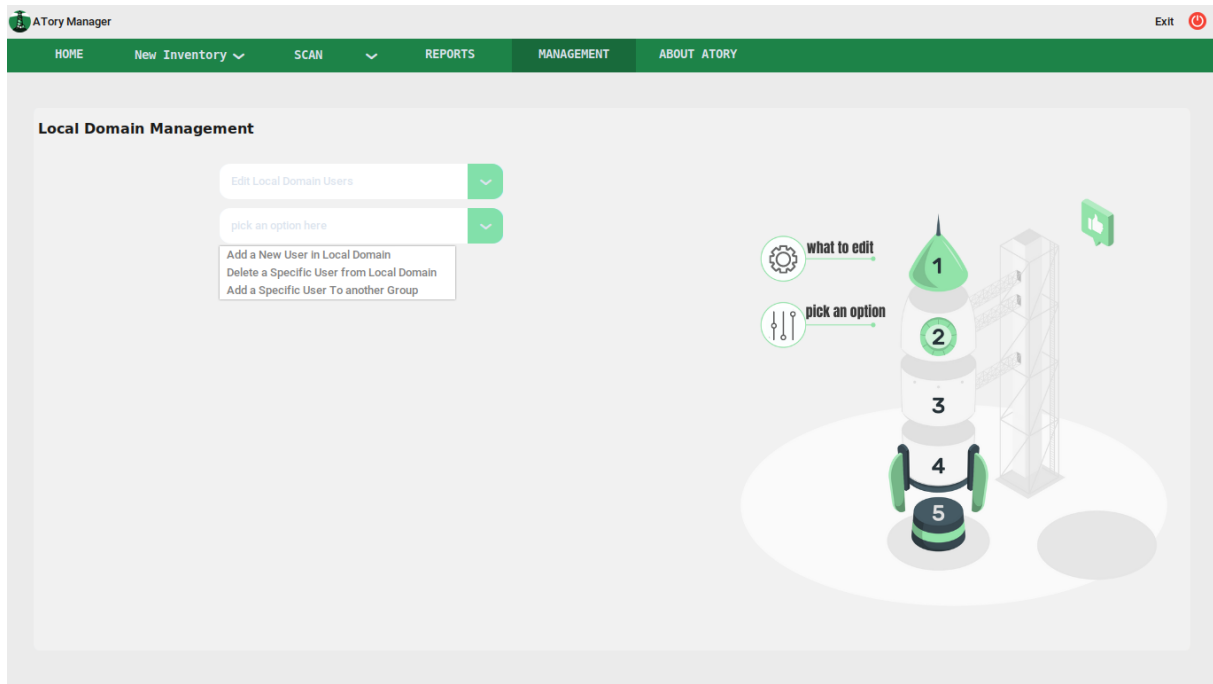


FIG. 3.24 : La gestion des utilisateurs

La troisième fonctionnalité 'Edit local domain devices' permet de changer la valeur critique d'un actif ,changer son administrateur, ou encore ajouter un actif à un groupe spécifié.

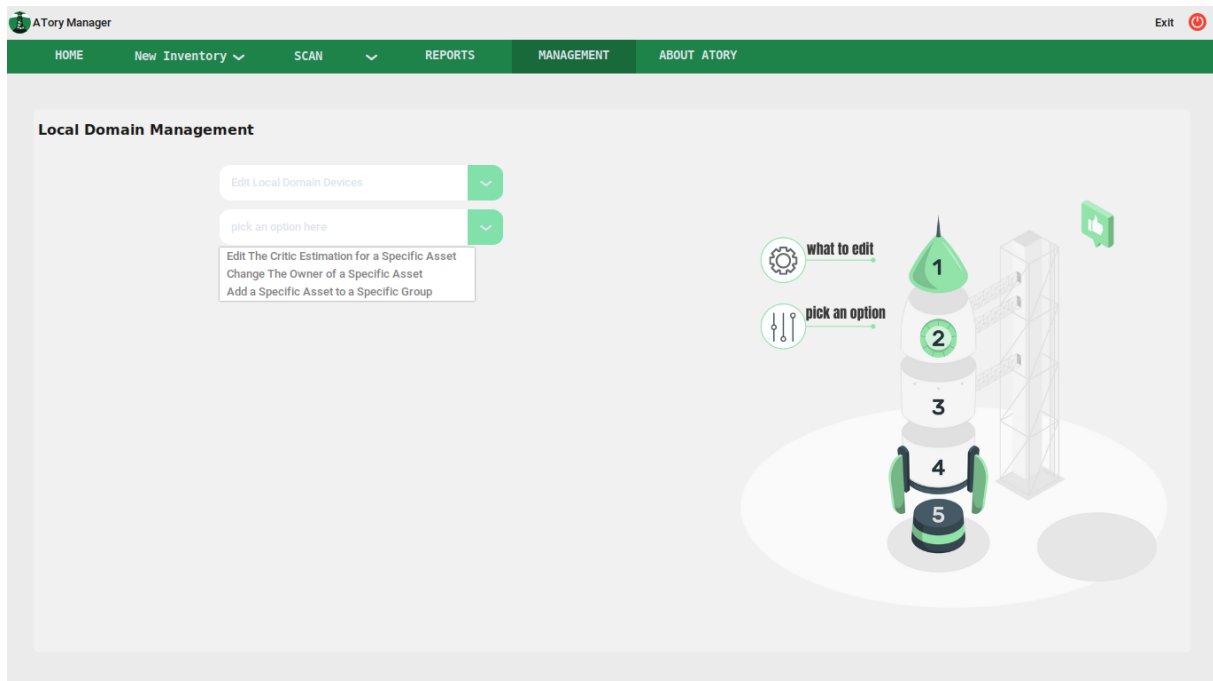


FIG. 3.25 : La gestion des actifs informatiques

En cliquant sur le bouton 'Submit' toute modification faite sera enregistrée automatiquement dans l'active directory.

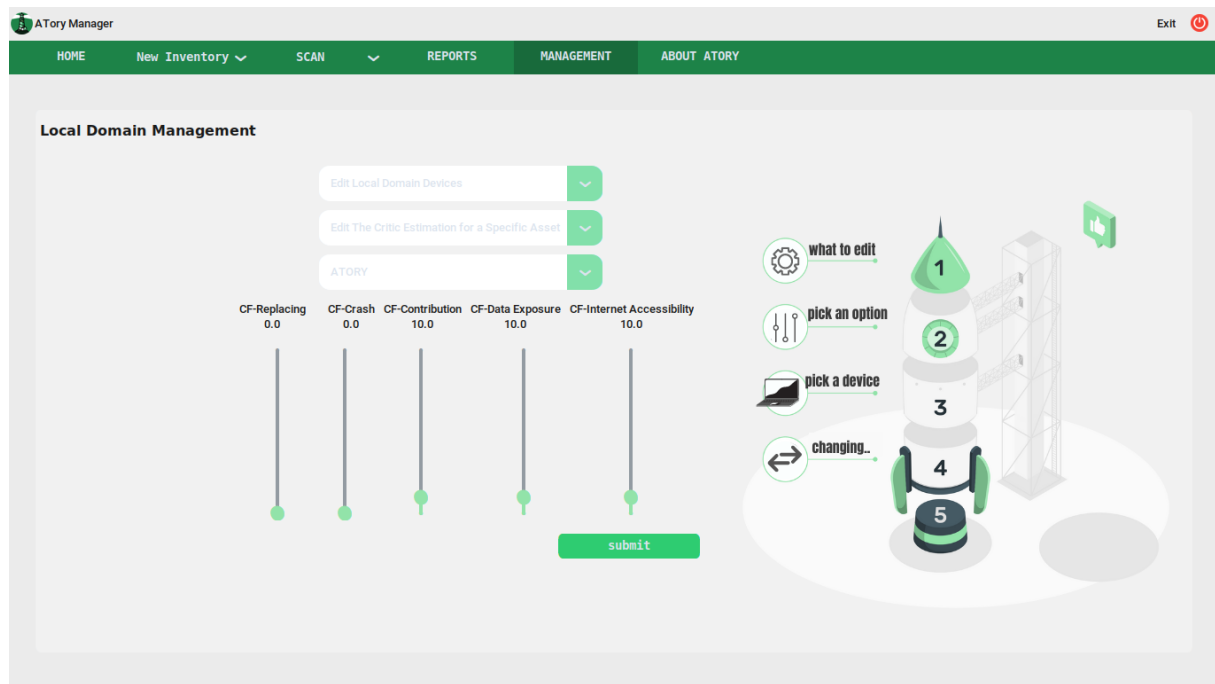


FIG. 3.26 : L'enregistrement des changements

La page "À propos" présente des détails sur l'application contenant une documentation sur l'application, son importance, et ces objectifs.

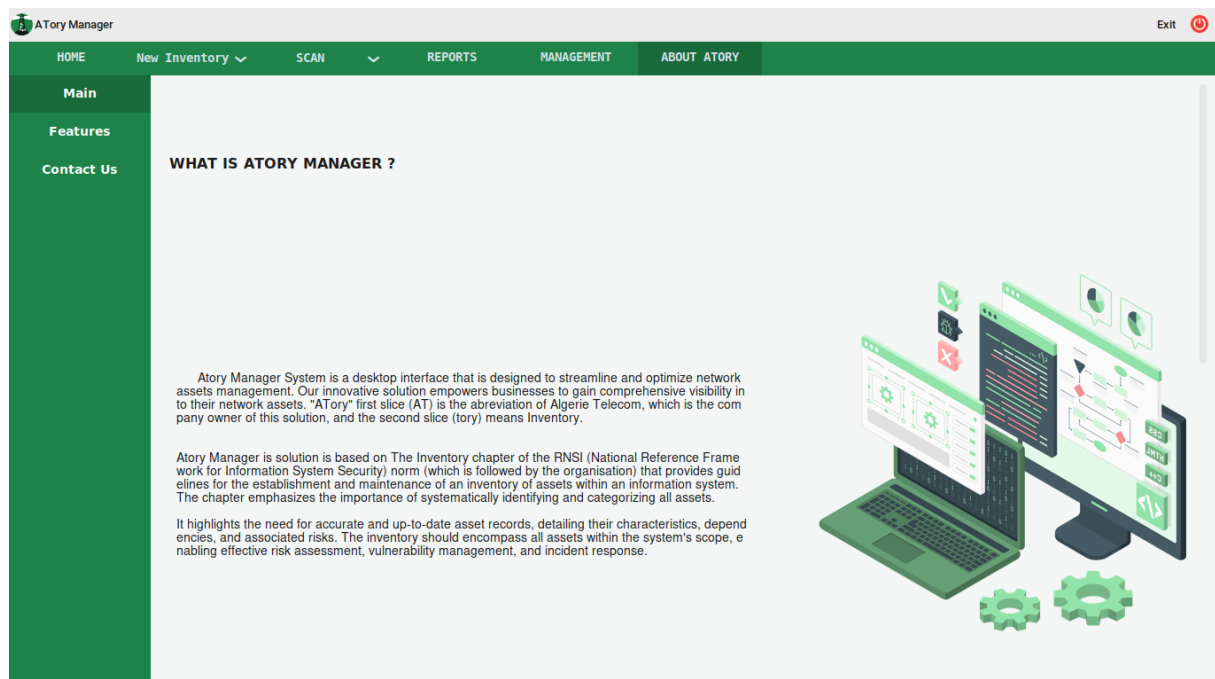


FIG. 3.27 : À propos de Atory

Et pour bien comprendre et tracer le comportement des utilisateur afin de détecter les problèmes techniques, améliorer l'utilisation du système. On a opté pour un enregistrement

de chaque action l'utilisateur fasse pendant son utilisation du système. Ce dernier, est un fichier qui doit contenir le nom de l'acteur, la date de l'action et une description d'action.

	A	B	C
1	ACTION	ACTOR	DATE
2	Login to Atory Manager Interface	atorytest	2023-06-06 23:15:50.013523
3	Established a Network Vulnerability scanning	atorytest	2023-06-06 23:19:22.152736
4	Generated a Network Scanning Report	atorytest	2023-06-06 23:19:56.507615
5	Established a vulnerability scan on ATORY asset with the ip address of 172.16.54.131	atorytest	2023-06-06 23:22:29.126069
6	Generated an Asset Scanning Report for ' ATORY ' asset	atorytest	2023-06-06 23:22:47.907115
7	Added A new User in local domain under the name of ' chahinezzz '.	atorytest	2023-06-06 23:27:28.121480
8	Changed The administrator of ' DESKTOP-VIIVIA2 ' asset to ' chahinezzz '.	atorytest	2023-06-06 23:27:57.649389
9	Edited The Critic Value of ' PC1 ' asset	atorytest	2023-06-06 23:28:44.255114
10	Added a new Group in local domain under the name of ' clients vip '.	atorytest	2023-06-06 23:30:03.289585
11	Exit Atory Manager Interface	atorytest	2023-06-06 23:39:55.884181
12	Login to Atory Manager Interface	administrator	2023-06-06 23:43:28.289959
13	Exit Atory Manager Interface	administrator	2023-06-06 23:46:17.740025
14	Login to Atory Manager Interface	atorytest	2023-06-07 20:32:28.196752
15	Generated an Inventory Report	atorytest	2023-06-07 20:42:24.533343
16	Exit Atory Manager Interface	atorytest	2023-06-07 20:42:29.865414
17	Login to Atory Manager Interface	atorytest	2023-06-07 21:52:37.795212
18	Exit Atory Manager Interface	atorytest	2023-06-07 21:53:08.919626
19	Login to Atory Manager Interface	atorytest	2023-06-07 21:54:44.575446
20	Established an Inventory process in the local network	atorytest	2023-06-07 21:54:56.080549
21	Exit Atory Manager Interface	atorytest	2023-06-07 21:55:14.630044
22	Login to Atory Manager Interface	atorytest	2023-06-07 21:55:51.107763
23	Established an Inventory process in the local network	atorytest	2023-06-07 21:56:01.542809
24	Established an Inventory process in the local network	atorytest	2023-06-07 21:56:13.516915
25	Exit Atory Manager Interface	atorytest	2023-06-07 21:56:19.757754
26	Login to Atory Manager Interface	atorytest	2023-06-07 21:56:54.496593
27	Established an Inventory process in the local network	atorytest	2023-06-07 21:57:06.416831
28	Exit Atory Manager Interface	atorytest	2023-06-07 21:57:11.949887
29	Login to Atory Manager Interface	atorytest	2023-06-07 21:57:45.164206
30	Established an Inventory process in the local network	atorytest	2023-06-07 21:57:55.784225
31	Exit Atory Manager Interface	atorytest	2023-06-07 22:00:44.094657

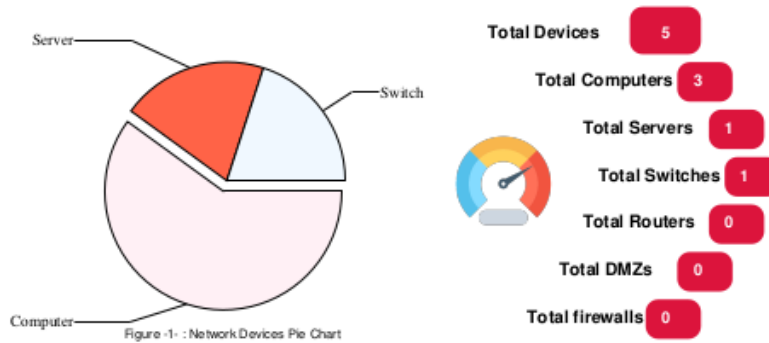
FIG. 3.28 : Le rapport des logs des actions des utilisateurs

3.5 Présentation des points les plus importants des rapports générés

Les figures suivantes montrent les résultats détaillés du processus d'inventaire et du scan également, sous forme de visualisations, des sections, etc. afin de faciliter la compréhension de ces derniers.

Cette partie du rapport d'inventaire présente la cartographie du réseau. Ainsi qu'un graphe montrant les différentes mesures sur lesquelles on a classifié les différents actifs informatiques.

EXECUTIVE SUMMARY



This bar chart represents the number of devices per the different measures to take in consideration for calculating the degree of criticism of each device in the network (High,Medium,Low)

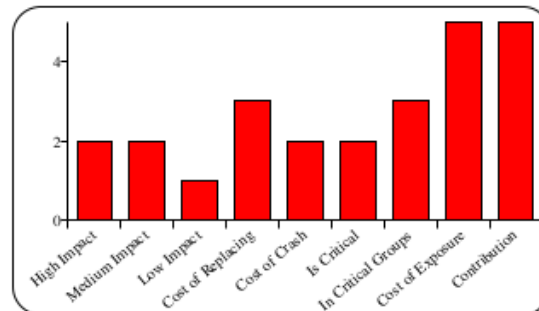


Figure -2: Network Critic Evaluation Bar Chart

FIG. 3.29 : Une page du document de rapport d'inventaire qui représente la cartographie

Cette partie du rapport d'inventaire montrent la cartographie d'un actif informatique, avec la liste des ports ouverts dans ce dernier et sa classification dans le réseau. De plus, des informations sur l'ensemble des erreurs ou des avertissement apparus.



FIG. 3.30 : La cartographie d'un actif informatique WINSERVER du rapport d'inventaire

Cette partie du rapport d'évaluation d'un actif selon choix couvre le nombre de toutes les faiblesses potentielles identifiées. Classifiées selon leur degré d'impact sur l'intégrité, la confidentialité et la disponibilité.

EXECUTIVE SUMMARY

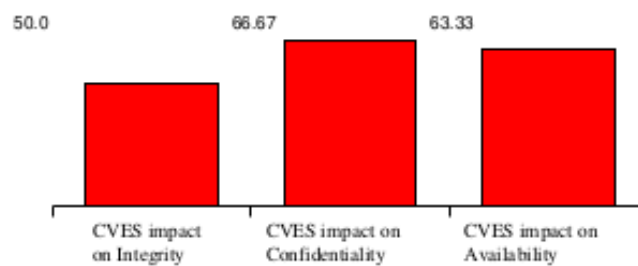
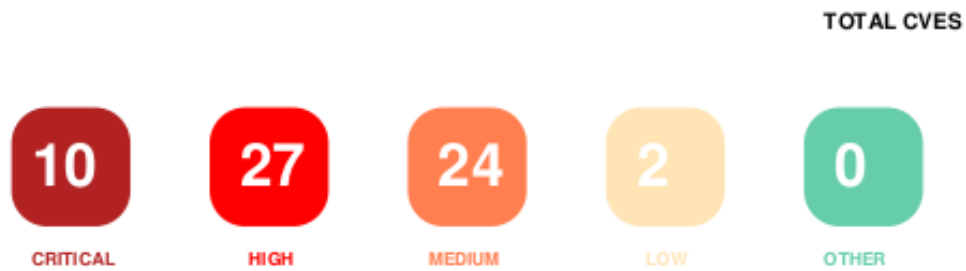


Figure -1 - : cves impact on CIA graph

This bar graph represents cves impact percentage on Integrity, Confidentiality and Availability on this asset.

FIG. 3.31 : Des statistiques sur l'ensemble des vulnérabilités détectées lors du scan

Cette partie du rapport d'évaluation indique pour chaque actif informatique la liste des vulnérabilités identifiées, une description détaillée de chaque vulnérabilité accompagnée par son degré d'impact potentiel, et une liste des recommandations.

 04

FINDINGS

device :WINSERVER

CVE ID CVE-2023-0465

Description:

Applications that use a non-default option when verifying certificates may be vulnerable to an attack from a malicious CA to circumvent certain checks. Invalid certificate policies in leaf certificates are silently ignored by OpenSSL and other certificate policy checks are skipped for that certificate. A malicious CA could use this to deliberately assert invalid certificate policies in order to circumvent policy checking on the certificate altogether. Policy processing is disabled by default but can be enabled by passing the '-policy' argument to the command line utilities or by calling the 'X509_VERIFY_PARAM_set1_policies()' function. ...

Recommendation:

[click me](#) [click me](#) [click me](#) [click me](#) [click me](#) [click me](#) [click me](#) [click me](#)

CVE ID CVE-2023-25746

Description:

Mozilla developers Philipp and Gabriele Svelto reported memory safety bugs present in Firefox ESR 102.7. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Thunderbird < 102.8 and Firefox ESR < 102.8.

Recommendation:

[click me](#) [click me](#) [click me](#)

Metrics:

CVE score  **MEDIUM**

Integrity Impact **LOW**

Confidentiality Impact **NONE**

Availability Impact **NONE**

Metrics:

CVE score  **HIGH**

Integrity Impact **HIGH**

Confidentiality Impact **HIGH**

Availability Impact **HIGH**

FIG. 3.32 : Une description détaillée d'une vulnérabilité identifiée d'un actif informatique WINSERVER

3.6 Conclusion

Nous avons présenté dans ce chapitre l'implémentation du processus Atory qui vise à identifier les actifs informatiques et évaluer les vulnérabilités dans un réseau LAN . Nous avons commencé par présenter la maquette du réseau du test et introduire les différents outils utilisés pour la réalisation de notre application, et en fin, des interfaces graphiques et des échantillons sur les rapports obtenus.

Conclusion et perspectives

Le suivi et la gestion des actifs informatiques d'une entreprise sont primordiaux pour la détection des dangers qui menacent et affectent la sécurité de cette dernière. Cependant lorsqu'il s'agit d'un suivi manuel, le processus devient plus long et parfois mène à négliger des points très importants.

Afin de faire face à ce défi. La solution proposée consiste à assurer l'automatisation de ce processus et l'utilisation avec efficacité des ressources des réseaux, qui se manifeste par la possibilité de

- Faire un inventaire automatique sur les actifs informatiques existants.
- Créer plusieurs groupes à travers lesquels on peut ajouter des actifs informatiques.
- Créer plusieurs utilisateurs et les affecter aux actifs informatiques.
- Établir une classification des actifs informatiques.
- Changer les valeurs de classification des actifs informatiques.
- Faire un scan sur les vulnérabilités des actifs informatiques selon le choix de l'utilisateur.
- Générer un rapport automatique d'inventaire et du scan selon la demande de l'utilisateur.

Cette solution assure donc la simplification de la gestion des actifs informatiques. Ce qui nous amène à une bonne compréhension des composants du réseau, ainsi que les mises à jour automatiques qui dégagent un gain de temps appréciable. Et ceci dans le but de rester conforme aux normes et exigences de l'entreprise.

Notre travail offre de nombreuses perspectives d'évolution, notamment dans le cadre d'implémentation du travail et l'algorithme d'orchestration. Il en est de même pour leurs extensions afin de rendre ce système plus performant. Il existe d'autres perspectives pour les travaux futurs notamment :

La vérification de la conformité de chaque actif informatique

Procéder à une analyse de conformité relative aux configurations automatiques des actifs informatiques dans le réseau en se basant sur les politiques et exigences de conformité spécifiques.

L'établissement d'une fonction des alerts

Les alertes servent à rappeler l'utilisateur par les incidents non vus, ou bien des configurations non rectifiées, ou même des vérifications non faites. Afin de rester à jour avec tous les scénarios possibles.

L'établissement d'une fonction de gestion du processus d'inventaire

Pour que la visibilité de l'infrastructure du réseau ne soit pas dévoilée pour tous les utilisateurs du système, chaque catégorie d'utilisateur à l'accès à une partie spécifique de l'infrastructure. À titre d'exemple, les administrateurs des réseaux ont accès seulement aux nœuds intermédiaires.

L'établissement d'une fonction de remédiation automatique

Pour prendre rapidement en charge les pannes et dysfonctionnements des actifs informatiques et améliorer leurs performances en les réparant automatiquement.

Bibliographie

- [1] *Présentation du groupe Algérie Télécom*. URL : https://www.itu.int/dms_pub/itu-d/md/06/dap2b.1.3.7/inf/D06-DAP2B.1.3.7-INF-0025!!PDF-F.pdf (visité le 10/06/2023).
- [2] *Référentiel National de Sécurité de l'Information*. URL : <https://www.webservices.dz/images/pdf/RNSSI-2020.pdf> (visité le 05/02/2023).
- [3] Michael E WHITMAN et al. *Principles of Information Security, International Edition*. 2012.
- [4] *Information technology – Security techniques – Information security risk management*. Standard. Geneva, CH : International Organization for Standardization, 2018.
- [5] Stéphane GILL. “Type d’attaques”. In : *Document soumis à la licence GNU FDL*. http://sgill.ep.profweb.qc.ca/spip/IMG/pdf/02_TypeAttaque.pdf (2003), p. 37.
- [6] Subhangani PANDEY et Anita CHAUDHARY. “Vulnerability Scanning”. In : (2022).
- [7] Eric CHEVIGNY et Bernard BELLAMY. “Outil de cartographie et d’inventaire”. In : *Actes du congrès JRES 2005* (2005).
- [8] Mohcene FARES et Djamel BENYAHY. “Conception et réalisation d’un système pour l’évaluation des menaces et des risques dans les réseaux Informatiques”. Université des Sciences et de Technologie Houari Boumediene, 2005.
- [9] Vladimir Lucian MIHAILESCU. “Risk analysis and risk management using MEHARI”. In : *J. Appl. Bus. Inf. Syst* 3.4 (2012), p. 143-162.
- [10] Jean-Philippe HUMBERT. “La méthode EBIOS : présentation et perspective d’utilisation pour la certification ISO 27001”. In : ()
- [11] Richard A CARALLI et al. “Introducing octave allegro : Improving the information security risk assessment process”. In : *Hansom AFB, MA* (2007).
- [12] *Définition de l’actif*. URL : <https://www.larousse.fr/dictionnaires/francais/actif/888> (visité le 10/06/2023).
- [13] *Gestion des vulnérabilités informatiques : Vers une meilleure gestion des risques opérationnels*. URL : https://clusif.fr/wp-content/uploads/2016/04/clusif-2015-gt-gestionvulnerabilites-tome2_vf.pdf (visité le 14/05/2023).
- [14] *Community-cookbook EVE-NG*. URL : <https://www.eve-ng.net/index.php/documentation/community-cookbook/> (visité le 18/02/2023).

- [15] *Python*. URL : <https://www.machaon.fr/isn/resume-cours/python/muniglia/resume.html> (visité le 10/06/2023).
- [16] *Customtkinter*. URL : <https://customtkinter.tomschimansky.com/documentation/> (visité le 10/06/2023).
- [17] *Tkinter*. URL : <https://docs.python.org/3/library/tkinter.html> (visité le 25/03/2023).
- [18] Brian DESMOND et al. *Active Directory : Designing, Deploying, and Running Active Directory*. " O'Reilly Media, Inc.", 2008.
- [19] Robbie ALLEN et Alistair LOWE-NORRIS. *Active directory*. " O'Reilly Media, Inc.", 2003.
- [20] *Remote Procedure Call (RPC)*. URL : <https://www.techtarget.com/searcharchitecture/definition/Remote-Procedure-Call-RPC> (visité le 17/04/2023).
- [21] *Nmap_python*. URL : [Pypi.org/project/python-nmap](https://pypi.org/project/python-nmap) (visité le 20/05/2023).
- [22] *Netmiko*. URL : <https://pypi.org/project/netmiko/#description> (visité le 20/05/2023).
- [23] *Matplotlib*. URL : <https://matplotlib.org/stable/index.html> (visité le 25/05/2023).
- [24] *Reportlab*. URL : <https://pypi.org/project/reportlab/#description> (visité le 02/06/2023).
- [25] *NIST CVE*. URL : <https://nvd.nist.gov/general/cve-process> (visité le 05/03/2023).
- [26] *Visual Studio Code*. URL : <https://code.visualstudio.com/docs> (visité le 10/06/2023).
- [27] *MySQL*. URL : <https://dev.mysql.com/doc/> (visité le 10/06/2023).
- [28] *DrawIO*. URL : <https://www.drawio.com/about> (visité le 10/06/2023).