Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université de Blida 1
Faculté des Sciences
Département de l'informatique
Mémoire de Master
Filière : Informatique
Spécialité : SSI

Thème

Conception et Implémentation d'un Outil d'Assistance aux Tests d'Intrusion dans un environnement d'Entreprise

Sujet Proposé par :
Mare Nostrum Advising Groupe

Réalisé par :
LISRI Maroua
MERAD Khaoula

Soutenu le 24/ 06 /2023 Devant le jury composé de :

Mme.BEY Fella	Présidente
Mr CHERIF ZAHAR Sid Ahmed Amine	Examinateur
Mme.AROUSSI Sana	Promotrice
Mr BELARBI Mohamed Abdou	Encadreur

Année universitaire : 2022/2023

Résumé

Les conséquences désastreuses de la cybercriminalité sur les activités des entreprises incitent ces dernières à mettre en œuvre une stratégie solide en matière de cybersécurité ainsi qu'un plan d'atténuation et de détection robuste si elles souhaitent rester à flot face aux cyberattaques. Parmi les mesures mises en place, la sous-traitance des tests d'intrusion (ou de pénétration) à des équipes spécialisées en Red Team (équipes de simulation d'attaques) est devenue courante. Notre projet consiste à développer un outil d'assistance pour les équipes Red Team afin d'effectuer des tests d'intrusion dans un réseau d'entreprise. Cela permet de réduire le temps nécessaire pour mener les tests en automatisant certaines tâches, ainsi que de générer des rapports faciles à lire et à interpréter. Par ailleurs, les tests d'intrusion reposent sur une méthodologie bien définie qui constitue une feuille de route, dont certaines étapes peuvent être automatisées. Ainsi, dans notre solution, nous proposons d'intégrer le processus PTES (Penetration Testing Execution Standard) déjà déployé par l'entreprise d'accueil Mare Nostrum Advising Groupe avec les TTP (**T**actiques, **T**echniques, **P**rocédures) extraites du framework MITRE ATT&CK qui s'agit d'une base de connaissances accessible basée sur des observations réelles des attaques.

Mots clés : cybersécurité, Red Team, tests d'intrusion, ou pénétration, PTES, TTP, MITRE ATT&CK.

Abstract

The disastrous impact of cybercrime on companies activities means that they companies need to implement a solid cybersecurity strategy, as well as a robust mitigation and detection plan, if they are to stay afloat in the face of cyberattacks. Among the measures implemented, outsourcing penetration testing to specialized Red Team teams (attack simulation teams) has become commonplace. Our project involves developing a tool to assist Red Team teams in carrying out penetration tests on a corporate network. This reduces the time needed to carry out tests by automating certain tasks, as well as generating reports that are easy to read and interpret. In addition, penetration testing is based on a well-defined methodology that forms a roadmap, some steps of which can be automated. Thus, in our solution, we propose to integrate the PTES (Penetration Testing Execution Standard) process already deployed by host company Mare Nostrum Advising Groupe with the TTPs (Tactics, Techniques, Procedures) extracted from the MITRE ATT&CK framework, which is an accessible knowledge base based on actual observations of attacks.

Keywords: Red Team, Penetration testing, MITRE ATT&CK, Attack simulation, Pentest, cybersecurity

ملخص

تتسبب آثار الجرائم السيبرانية المدمرة على أنشطة الشركات في دفع هذه الشركات لتنفيذ استراتيجية قوية في مجال الأمان السيبراني وخطة قوية للتخفيف والكشف عنها ومواجهتها. ومن بين الإجراءات المتخذة، تفويض اختبارات الاختراق لفرق الأمن الحمراء المتخصصة (فرق محاكاة الهجمات) .

تستند اختبارات الاختراق التي تقوم بها فرق الأمن الحمراء إلى منهجية محددة تشكل خارطة طريق، يتضمن مشروعنا تطوير أداة لمساعدة فرق الاختراق الحمراء في إجراء اختبارات الاختراق على شبكة الشركة. هذا يقلل من الوقت اللازم لإجراء الاختبارات من خلال أتمتة مهام معينة ، بالإضافة إلى إنشاء تقارير سهلة القراءة والتفسير. بالإضافة إلى ذلك ، يعتمد اختبار الاختراق على منهجية محددة جيدًا تشكل خريطة طريق ، حيث يمكن أن تتم بعض المراحل بشكل الي وبالتالي ، في حلنا ، نقترح دمج PTES (عملية تنفيذ اختبار الاختراق) التي تم نشرها بالفعل من قبل الشركة المضيفة Mare Nostrum Advising Groupe مع التكتيكات والتقنيات, الإجراءات المستخرجة من إطار MITRE ATT&CK ، وهو قاعدة معرفية يمكن الوصول إليها بناءً على الملاحظات الفعلية للهجمات.

كلمات مفتاحية: فريق الاختراق الأحمر، اختبار الاختراق ، محاكاة الهجوم، أمن المعلومات

Remerciement

Nous tenons tout d'abord à exprimer notre gratitude envers Dieu le Tout-Puissant et Miséricordieux, qui nous a donné la force, le courage, la volonté et la santé pour accomplir ce travail.

Nous souhaitons exprimer notre profonde gratitude envers notre promotrice, Madame AROUSSI Sana, pour avoir accepté de nous encadrer et pour sa disponibilité tout au long de la réalisation de ce mémoire. Ses précieux conseils nous ont permis de mener à bien ce travail, et nous avons bénéficié de son expérience et de sa sagesse.

Nous tenons également à remercier notre encadreur, Monsieur BELARBI Mohamed Abdou, pour la confiance qu'il nous a accordée en proposant ce travail. Son encadrement attentif et le temps précieux qu'il nous a consacré ont été d'une grande aide durant la réalisation de ce projet.

Nous exprimons notre profonde gratitude envers Monsieur NABAOUI ZERROUGUI Faiçal et Monsieur BOUTENARTE Zaki pour leur précieuse aide. Leur contribution a été d'une valeur inestimable et a joué un rôle essentiel dans la réalisation de ce travail. Nous tenons à remercier Monsieur HANNOUN Abdeldjalil et Monsieur ANOU Amir pour leur présence et leur disponibilité pour répondre à nos questions et partager leur expérience avec nous.

Nos sincères remerciements vont également aux membres du jury pour l'intérêt qu'ils ont porté à notre travail en l'examinant minutieusement et pour leurs suggestions qui ont enrichi notre mémoire. Enfin, nous souhaitons exprimer nos remerciements les plus sincères à toutes les personnes qui ont contribué de près ou de loin à l'élaboration de ce mémoire. Votre soutien et votre collaboration ont été d'une importance capitale pour nous, et nous sommes extrêmement reconnaissants.

Dédicace

Je dédie ce modeste travail en signe de respect, de reconnaissance et de remerciement :

À ma lumière, mon idole, celle qui a veillé à mes côtés depuis mon jeune âge jusqu'à aujourd'hui, tu n'es pas seulement une mère pour moi, mais une meilleure amie, une sœur, tout simplement mon tout. Sache que tous les mots du monde ne suffisent pas pour décrire à quel point je t'aime.

Au roi de mon cœur, mon père, l'épaule sur qui je peux compter, tu as su me guider tout au long de mon parcours et as su me soutenir même quand on n'était pas du même avis. Ta unique fille qui t'aime.

À ma chère grand-mère, une source d'amour inconditionnel et de soutien constant. Ta présence bienveillante a été une inspiration pour moi, et je te suis infiniment reconnaissante pour tout ce que tu as fait.

À la personne qui m'a soutenue toute l'année, ma binôme Khaoula, et à mon amie, un grand merci pour ton soutien inébranlable. Ta présence à mes côtés a été d'une valeur inestimable, et je suis profondément reconnaissante de t'avoir comme binôme et amie.

À mes chers frères Idris, Abdelrahim et Yakob, en reconnaissance de leur affection toujours présente, je tiens à exprimer combien votre présence a enrichi ma vie. Vous êtes des sources de joie, de bonheur et de complicité

Chère Tante Zohra, qui m'a toujours encouragée et a été présente à mes côtés tout au long de mon parcours, je souhaite te dire combien ta présence a été précieuse et enrichissante pour moi.

À ma cousine Imen Sabrina, qui a été une grande sœur et qui a toujours été là pour moi, je suis infiniment reconnaissante de t'avoir dans ma vie.

À mes sœurs de cœur Amani et Manar, qui ont toujours été là pour moi.Merci d'avoir partagé les bons moments, d'avoir séché mes larmes et d'avoir toujours été là pour moi. je vous aime énormément .

À mes chères amies Rania, Serine, Fella et Meriem, Et à tous ceux qui me sont chers, votre présence dans ma vie est précieuse et je vous suis reconnaissante pour votre soutien constant. Que chacun de vous trouve ici l'expression de ma gratitude et de mon amour sincère.

LISRI Maroua

Dédicace

Je voudrais exprimer ma plus profonde gratitude à ma mère, la plus compréhensive et la plus incroyable du monde. Sans elle, je n'aurais jamais pu accomplir ce que j'ai réalisé jusqu'à présent.

À mon cher père, je veux te dire combien je suis reconnaissante pour tout ce que tu as fait pour moi. Ta présence, ton soutien et tes précieux conseils ont été essentiels à ma réussite.

À mes grands frères et sœurs Saliha, Ibrahim, Mustapha et Sabrina, je tiens à vous remercier du fond du cœur d'avoir toujours été là pour moi, de m'avoir soutenue inconditionnellement.

À ma chère tante Farida, qui a toujours été là pour moi, je tiens à la remercier du fond du cœur.

Je dédie cette phrase à mon amie Maroua, depuis le lycée, en espérant que notre amitié perdure et que tous ses projets rencontrent le succès tout au long de sa vie.

Je souhaite exprimer ma profonde gratitude envers tous mes amies, depuis mes années à l'école primaire jusqu'à l'université.

Je suis profondément reconnaissante envers tous ceux qui ont joué un rôle dans ma vie et qui ont contribué à mon épanouissement. Je sais que je ne serais pas là où je suis aujourd'hui sans votre amour, votre soutien et vos encouragements constants. Je vous suis vraiment reconnaissante.

MERAD Khaoula

Table de Matière

Introduction Générale 1
CHAPITRE I : TESTS D'INTRUSION dans les RÉSEAUX 2
1 Introduction 2
2 Cybersécurité 2
2.1 Principales menaces liées à la cybersecurité : 2
2.2 Approches de Sécurité de l'information 3
2.3 Types des équipes de sécurité 3
3 Généralités sur les Tests d'intrusion 4
3.1 Les types de tests d'intrusion 5
3.2 L'automatisation des tests d'intrusion 5
4 Processus des tests d'intrusion 7
4.1 La Cyber Kill Chain 7
4.2 PTES 8
4.3 MITRE ATT&CK 8
4.4 La différence entre MITRE ATT&CK, PTES et Cyber Kill Chain 10
5 Les outils d'automatisation des tests d'intrusion existants 12
5.1 vPENTEST 12
5.2 Core Impact 13
5.3 Comparaison entre vPENTEST et Core Impact 13
6 Conclusion 14
CHAPITRE II : CONCEPTION 15
1 Introduction 15
2 Description de la solution proposée 15
2.1 Notre Processus de test d'intrusion 15
2.2 Techniques choisies 18
2.3 Génération de rapport : 19
3 Etude Conceptuelle de notre application 22
3.1 Diagramme de cas d'utilisation 22
3.2 Diagramme de Classe : 24
3.3 Diagramme d'activité 26
4 Conclusion 26

CHAPITRE III : REALISATION, TESTS & RESULTATS 27
1 Introduction 27
2 Environnement de développement 27
3 Procédures 29
4 Implémentation de l'application 32
4.1 Espace administrateur 32
4.2 Espace Pentester 33
5 Tests et résultats 33
5.1 Environnement de test 34
5.2 Scénarios de test 34
5.2.1 Collecte des propriétés du domaine(T1590.001) 34
5.2.2 Reconnaissance DNS 35
5.2.3 Collecte des AdressesIP 36
5.2.4 Découverte d'informations sur le système 36
5.2.5 Scan de Vulnérabilités 37
5.2.6 Empoisonnement du cache ARP 38
5.2.7 Génération de rapport 39
6 Conclusion 40
CONCLUSION GÉNÉRALE & PERSPECTIVES 41
Annexes 44

Liste des Figures

Figure 1:Matrice Réseau MITRE ATT&CK 9
Figure 2:vPENTEST 12
Figure 3:Core Impact 13
Figure 4:Notre processus de test d'intrusion 16
Figure 5:Diagramme de cas d'utilisation globale 23
Figure 6:Diagrammes de cas d'utilisation de gestion du projet et gestion d'attaque 23
Figure 7:Diagramme de classe 25
Figure 8:Diagramme d'activités 26
Figure 9:Environnement de développement 27
Figure 10:WHOIS 29
Figure 11:Dnsrecon 29
Figure 12:Scapy 30
Figure 13:Collecte des AdressesIP 30
Figure 14:Découverte d'informations sur le système 31
Figure 15:NSE 32
Figure 16:Espace Administrateur 33
Figure 17:Espace Pentester 33
Figure 18: Environnement de test 34
Figure 19:Scenario de test (Propriétés du domaine) 35
Figure 20:Scenario de test (Reconnaissance DNS) 35
Figure 21:Scenario de test (Collect des addresses IP) 36
Figure 22: Scenario de test (Découverte d'informations sur le système) 37
Figure 23:Scenario de test (Scan de vulnérabilités) 37
Figure 24:Scenario de test (d'Empoisonnement du cache ARP) 38
Figure 25:Analyse des paquets 39
Figure 26:Generation de rapport 39

Liste des Tableaux

Table 1:Différences entre les tests d'intrusion manuels et les tests d'intrusion automatisés ...6
Table 2:Les avantages et les limites d'automatisation des tests d'intrusion ….....7
Table 3:La différence entre MITRE ATT&CK et Cyber KILL Chain 11
Table 4:Comparaison entre vPENTEST et Core Impact 14
Table 5:TTPs choisies 17
Table 6:Generation de rapport 20
Table 7:Langages de programmation 28
Table 8:Les échelles de la difficulté d'exploitation……....40

Liste des abréviations

ARP Address Resolution Protocol
CSS Cascading Style Sheet
CVE Common Vulnerabilities and Exposures
CVSS Common Vulnerability Scoring System
DNS Domain Name System
DNSSEC Domain Name System Security Extensions
DOS Denial of Service attaque
HTML Hyper Text Markup Language
ICMP Internet Control Message Protocol
MITM Man in the middle attack
NIST National Institute of Standards and Technology
Nmap Network Mapper
NSE Nmap Scripting Engine
NVD National Vulnerability Database
PTES Penetration Testing Execution Standard, Penetration Testing Execution Standard
TCP Transmission Control Protocol
TTP Tactiques, Techniques et Procédures
UDP User Datagram Protocol

Introduction Générale

La sécurité informatique est devenue un enjeu majeur pour les entreprises en raison du développement rapide des technologies et des réseaux de communication. Les attaques informatiques sont devenues de plus en plus complexes, ce qui expose les entreprises à des risques importants tels que l'accès non autorisé à des informations sensibles, le vol de données et les perturbations des opérations.

Dans ce contexte, les tests d'intrusion (ou de pénétration) jouent un rôle crucial. Ils consistent à simuler des attaques informatiques pour évaluer la sécurité d'un système. Ces tests sont effectués par des experts en sécurité qui utilisent des méthodologies spécifiques pour identifier les vulnérabilités. La réalisation régulière de tests d'intrusion offre plusieurs avantages aux entreprises. Elle permet de détecter et de corriger les vulnérabilités avant qu'elles ne soient exploitées par des attaquants réels. Cela contribue à améliorer la sécurité globale en renforçant les défenses et en appliquant les correctifs nécessaires. Pour cela, les entreprises font appel à des spécialistes pour mener des tests d'intrusion afin d'évaluer le niveau de sécurité actuel et de mettre en place des améliorations selon les recommandations des rapports finaux fournis par les consultants.

Cependant, lors de ces tests d'intrusion, une part importante du temps est consacrée à des tâches répétitives telles que la reconnaissance et l'identification des éléments vulnérables, ainsi que la rédaction des rapports détaillés comprenant les travaux réalisés, les vulnérabilités identifiées, les techniques d'exploitation utilisées et les recommandations de mitigation. Cette situation limite le temps disponible pour les experts (testeurs ou Pentesteurs) fin d'exploiter pleinement les failles identifiées et de tirer le meilleur parti de leurs compétences techniques. D'autre part, la durée des engagements est prédéfinie et limitée par le client, ce qui ajoute une contrainte de temps supplémentaire.

Effectué au sien de l'entreprise Mare Nostrum Advising Groupe (MNA Groupe)1, l'objectif de notre projet de fin d'études est de développer un outil d'assistance permettant d'effectuer des tests d'intrusion dans un environnement d'entreprise (client). Cet outil doit permettre aux consultants du MNA Groupe (formant des Red Teams (équipes rouges)[2]) de réduire le temps d'engagement en automatisant certains tests, ainsi que d'automatiser l'analyse des résultats des

[1] C'est une entreprise renommée dans le domaine de la sécurité de l'information. Dotée d'une équipe de professionnels hautement qualifiés et expérimentés, elle se distingue par sa spécialisation en audit, conseil et accompagnement en cybersécurité. Implantée dans plusieurs régions stratégiques, notamment en France (Paris et Marseille), en Afrique du Nord (Algérie) et en Afrique de l'Ouest (Sénégal), l'entreprise est en mesure de répondre aux besoins de sa clientèle dans ces différentes zones géographiques. Elle dispose également d'une structure dédiée et certifiée QUA-LIOPI, connue sous le nom de « MN Advising Cert », qui offre des programmes de formation de haut niveau. Grâce à leur expertise et à l'utilisation d'outils adaptés, les consultants de l'entreprise sont en mesure de former efficacement les collaborateurs des organisations clientes, en améliorant leurs compétences en matière de sécurité de l'information.

[2] C'est un groupe externe de Pentesters qui sont des testeurs de pénétration.

différentes étapes. Cela leur permettra de prendre des décisions éclairées sur les actions à entreprendre dans les prochaines étapes et d'accumuler progressivement d'autres scénarios d'attaques possibles.

Pour expliquer bien notre travail, le mémoire est divisé en trois chapitres comme suite:

- **Chapitre 1** : où nous couvrons les notions de base sur lesquelles notre projet se repose : le types et les équipes des tests d'intrusion, les méthodologies (ou processus) utilisées dans les tests d'intrusion, notamment le PTES (Penetration Testing Execution Standard) et MITRE ATT&CK, et enfin, une synthèse sur les outils de tests déjà réalisés.
- **Chapitre 2** : où nous allons décrire notre solution : processus suivi, TTPs choisis et les fonctionnalités de notre application à travers les diagrammes UML.
- **Chapitre 3** : où nous allons montrer les outils utilisés afin de développer notre application, les procédures choisis, le déroulement de notre application et les tests effectuées, une discussion des résultats obtenus.

Et à la fin, nous terminons par une conclusion générale et nous suggérons quelques perspectives.

CHAPITRE I : TESTS D'INTRUSION dans les RÉSEAUX

1 Introduction

Dans ce chapitre, nous allons présenter les différents éléments clés de notre projet, tels que la cybersécurité, les types, les équipes et l'automatisation des tests d'intrusion. Nous allons également discuté des processus méthodologies utilisées dans les tests d'intrusion, notamment la Cyber Kill Chain , le PTES et le MITRE ATT&CK. Enfin, nous allons présenter une synthèse des outils déjà réalisés.

2 Cybersécurité

La cybersécurité englobe toutes les mesures, politiques et pratiques visant à protéger les systèmes informatiques, les réseaux et les données contre les attaques, les intrusions et les incidents de sécurité [1]. Son objectif est de garantir la confidentialité, l'intégrité et la disponibilité des informations sensibles [2]:

- **Confidentialité** : se réfère à la protection des informations contre les accès et utilisations non autorisés. Elle assure que seules les personnes autorisées ont accès aux informations sensibles.
- **Intégrité** : garantit que les informations restent complètes, exactes et inchangées tout au long de leur cycle de vie. Elle prévient toute modification ou altération non autorisée des données.
- **Disponibilité** : assure que les informations et les ressources sont accessibles et utilisables lorsque nécessaire.

2.1 Principales menaces liées à la cybersecurité :

Les réseaux d'entreprises sont vulnérables à une variété d'attaques qui peuvent avoir de graves conséquences. Dans notre projet, nous nous intéressons aux attaques suivantes :

- **Spoofing** (Usurpation d'identité) est l'action de déguiser une communication ou une identité de manière à ce qu'elle semble être associée à une source autorisée et de confiance. Les attaques spoofing peuvent prendre de nombreuses formes, qu'il s'agisse d'attaques par usurpation d'adresse e-mail déployées dans le cadre de campagnes d'hameçonnage ou d'attaques par spoofing de l'appelant, souvent utilisées pour commettre des fraudes. Les attaquants peuvent également cibler des éléments plus techniques du réseau d'une entreprise, tels qu'une adresse IP, un

serveur DNS[3] (Domain Name System) ou un service ARP[4] (Address Resolution Protocol), dans le cadre d'une attaque par usurpation d'identité [3].

- **Attaque de l'homme du milieu (MITM, Man in the middle)** : C'est une forme d'attaque par laquelle l'adversaire se place entre l'utilisateur et le système afin d'intercepter et de modifier les données qui passent entre eux [4] .
- **Déni de service (DOS, Denial of Service):**Une attaque par déni de service (abrégé en Dos attaque pour attaque en anglais) l'une des attaques les plus courantes dans le monde de l'informatique sont les attaques Dos, visant à empêcher ou à affecter la disponibilité des services d'un système informatique. Les attaques par déni de service sont généralement réalisées en envoyant un grand nombre de requêtes à un serveur afin de le surcharger et de le rendre indisponible pour ses utilisateurs légitimes [4].

2.2 Approches de Sécurité de l'information

Dans le domaine de la sécurité de l'information, deux approches distinctes sont couramment utilisées pour garantir la protection des systèmes et des données :

- **Défensive** : La cybersécurité défensive est une stratégie et des pratiques de sécurité qui sont mises en place pour empêcher et détecter les menaces et les attaques sur un système informatique [5]. Elle vise à limiter la surface d'attaque en identifiant et en corrigeant les vulnérabilités, et en mettant en œuvre des stratégies de contrôle d'accès et de surveillance. Les outils de cybersécurité défensive comprennent des systèmes de prévention des intrusions, des pare-feux, des outils de détection et des outils de chiffrement. Ces outils peuvent être utilisés pour détecter et répondre aux menaces en temps réel, et pour aider à prévenir les attaques.
- **Offensive** : La cybersécurité offensive est une approche proactive de la sécurité des systèmes information qui consiste à identifier et à exploiter les vulnérabilités d'un système ou d'un réseau informatique avant qu'elles ne puissent être exploitées par des attaquants malveillants. L'objectif de la cybersécurité offensive est de simuler des attaques réelles afin de trouver les faiblesses de sécurité et de les corriger avant qu'elles ne soient utilisées par des cybercriminels. *Les tests d'intrusion (ou de pénétration) sont un élément essentiel d'une stratégie de cybersécurité efficace et sont recommandés par les principaux organismes de cybersécurité tels que le National Institute of Standards and Technology (NIST)* [6] . *Dans la section suivante (section 3), nous nous focalisons sur les tests d'intrusion qui font l'objet de notre projet de fin d'étude.*

2.3 Types des équipes de sécurité

Dans le domaine de la cybersécurité, différentes équipes jouent un rôle essentiel pour garantir la protection des systèmes et des données. Le National Institute of Standards and Technology(NIST) définit trois types d'équipes comme suit :

[3] **DNS** (Domain Name System) est un système qui traduit les noms de domaine en adresses IP
[4] **ARP** (Address Resolution Protocol) est un protocole utilisé pour résoudre les adresses IP en adresses MAC dans un réseau local.

- **Red Team** : un groupe de personnes autorisées et organisées pour émuler les capacités d'attaque ou d'exploitation d'un adversaire potentiel contre la posture de sécurité d'une entreprise". Red Team joue le rôle de l'attaquant dans le but d'identifier les vulnérabilités d'un système [7].
- **Blue Team** : un groupe responsable de la défense de l'utilisation des systèmes d'information d'une entreprise en maintenant sa posture de sécurité contre un groupe d'attaquants fictifs". Si le Red Team joue l'offensive, Blue Team joue la défense pour protéger les actifs critiques d'une organisation. Cette équipe est chargée de défendre l'entreprise. Elle a la responsabilité de repousser les attaques de Red Team, notamment en vérifiant l'infrastructure, en mettant à jour les logiciels et en empêchant les tentatives d'ingénierie sociale d'aboutir [8].
- **Purple Team** : une équipe interdisciplinaire d'experts qui se réunissent pour adopter une approche offensive et défensive de la cybersécurité. L'équipe veille à ce que les mesures de sécurité d'une organisation soient solides et efficaces en testant les défenses du système et en recherchant activement les faiblesses ou les vulnérabilités. L'équipe contribue à la sensibilisation l'organisation aux meilleures pratiques en matière de sécurité, afin qu'elle puisse rester à l'abri des cyberattaques [9] .

Rappelons que notre objectif est de développer un outil d'assistance destiné à une Red Team (équipe rouge) lors des tests d'intrusion d'un réseau d'entreprise. Cet outil permet ainsi de mettre en place le processus suivi par Red Team qui « consiste à utiliser des Tactiques, Techniques et Procédures (TTP) pour émuler une menace réelle dans le but de former et de mesurer l'efficacité des personnes, des processus et des technologies utilisés pour défendre un environnement » [10]. Les TTP englobent toutes les étapes d'une attaque simulée, de la reconnaissance initiale à l'exécution d'actions spécifiques sur les objectifs [11] :

- **Tactique:** fait référence à la stratégie ou à l'approche globale utilisée par le Red Team lors d'une attaque simulée. Il s'agir de décisions concernant les cibles à viser, les méthodes de reconnaissance à utiliser et les tactiques les plus efficaces pour atteindre les objectifs.
- **Techniques:** font référence aux méthodes spécifiques utilisées pour réaliser chaque étape de l'attaque. Par exemple, une technique peut consister en l'utilisation d'un exploit particulier, d'un courriel d'hameçonnage ou d'une méthode spécifique de déplacement latéral au sein d'un réseau.
- **Procédures:** il s'agit de la description, étape par étape, de la manière dont l'attaquant prévoit d'atteindre son objectif. En d'autres termes, comment les techniques générales seront exécutées en détail.

Dans ce qui suit, nous détaillons les tests d'intrusion du réseau effectués par les Red Teams.

3 Généralités sur les Tests d'intrusion

Un test d'intrusion (ou test de pénétration ou Penetration Testing) appeler aussi pentest, est un test complet d'un système informatique (réseau complet, serveur, application). Pour identifier les points faibles qui pourraient être exploités par des attaquants. Ces tests sont effectués par des professionnels de la sécurité informatique tentent d'identifier les failles de sécurité informatique et proposer un plan d'action cohérentes pour les corriger [12].

Les tests d'intrusion offrent de nombreux avantages [12]:

- ✓ Ils peuvent identifier les vulnérabilités cachées dans un système, donner une vue complète de la sécurité du système et aider à créer des mesures de sécurité plus efficaces.
- ✓ Les tests d'intrusion peuvent également aider à identifier les processus et les pratiques qui permettent aux attaquants de pénétrer dans un système, et peuvent être utilisés pour créer des plans de réponse aux incidents.
- ✓ Les tests d'intrusion peuvent être utilisés pour surveiller le système et ses performances sur une période prolongée, permettant aux administrateurs système d'identifier des anomalies et de réagir rapidement.

3.1 Les types de tests d'intrusion

Il existe un certain nombre de méthodes de test d'intrusion différentes qui peuvent être réalisées, chacune ayant ses propres objectifs et buts. Dans une entreprise, on peut distinguer entre [12]:

- **Test d'intrusion externe** : Ce type de test est effectué à partir d'une position extérieure à l'entreprise et vise à identifier les vulnérabilités qui pourraient être exploitées par un attaquant extérieur.
- **Test d'intrusion interne** : Ce type de test est effectué à partir d'une position interne à l'entreprise et vise à identifier les vulnérabilités qui pourraient être exploitées par un utilisateur malveillant ou un employé malveillant.

Ces derniers peuvent être effectués en trois manières différentes :

- ➢ **En boîte noire** : Un test d'intrusion en boîte noire (Black Box) simule une tentative de piratage. Le test commence par le fait que le tester ne reçoit aucune information sur les réseaux ou les systèmes de l'organisation.
- ➢ **En boîte blanche**: Un test de la boîte blanche (White box) reproduit une tentative de piratage. Les testeurs simulent un initié malveillant qui connaît la configuration des systèmes de l'organisation.
- ➢ **En boîte grise** : Un test d'intrusion en boîte grise (Grey Box) est une technique de test de sécurité qui se situe entre un test d'intrusion en boîte blanche (où le testeur a une connaissance approfondie du système et de son architecture) et un test d'intrusion en boîte noire (où le testeur n'a aucune connaissance préalable du système à tester).

Dans le cadre de notre projet, nous nous intéressons au test d'intrusion interne en boîte grise, afin d'identifier les vulnérabilités qui pourraient être exploitées par un utilisateur malveillant ou un employé mal intentionné, tout en ayant une connaissance partielle du réseau d'entreprise. Cette approche nous permettra d'évaluer la sécurité interne et de prendre des mesures préventives pour renforcer la posture de sécurité.

3.2 L'automatisation des tests d'intrusion

Les tests d'intrusion peuvent être réalisés à l'aide des techniques d'attaque manuelles ou automatisées. Le tableau suivant résumé la différence entre ces deux techniques [13]:

	Les tests manuels	Les tests automatisés
Moyens utilisés	- L'utilisation d'experts humains formés qui inspectent manuellement les réseaux et les systèmes à la recherche de faiblesses et de vulnérabilités.	- L'utilisation des outils et des logiciels automatisés pour rechercher les vulnérabilités et identifier tout risque potentiel.
Temps et efforts fournis	- Demandent plus de temps et d'efforts et impliquent des tests plus approfondis et plus complets.	- Sont généralement plus rapides et nécessitent moins de temps et d'efforts humains pour être menés à bien.
Type de vulnérabilités/failles détectées	- Sont plus susceptibles de découvrir des vulnérabilités plus subtiles et obscures. - Détectent les failles importantes.	- Sont plus susceptibles de manquer des vulnérabilités plus subtiles et obscures. - Ils découvrent les failles de sécurité les plus courantes, comme l'absence de mise à jour, des règles d'autorisation erronées ou des défauts de configuration

Table 1:Différences entre les tests d'intrusion manuels et les tests d'intrusion automatisés

Les tests d'intrusion manuels et automatisés ont tous les deux leur propre signification. Les tests automatisés sont rapides et faciles à utiliser lorsqu'ils sont associés à une analyse manuelle. Les tests d'intrusion manuels sont idéaux pour évaluer l'impact de l'exploitation d'une vulnérabilité [13].

L'objectif de notre projet est d'automatiser certains tests d'intrusion dans le but de bénéficier des avantages de cette technique tout en considérant ses limites. Les principaux avantages et limites de l'automatisation des tests d'intrusion sont présentés dans le tableau suivant [14]:

Les avantages	Les limites
• **Gain de temps :** les tests automatisés peuvent être exécutés rapidement et de manière répétitive, ce qui permet de couvrir un grand nombre de scénarios de test en un temps relativement court	• **Faux positifs** : les outils automatisés peuvent générer un nombre élevé de faux positifs, ce qui peut entraîner des investigations inutiles et une perte de temps.
• **Précision :** les outils automatisés peuvent être configurés pour effectuer des tests précis et répétitifs, ce qui permet de détecter rapidement les vulnérabilités.	• **Portée limitée** : les outils automatisés peuvent ne pas être en mesure d'identifier toutes les vulnérabilités, et la portée des tests peut être limitée par rapport aux tests manuels.
• **Réduction des coûts** : l'automatisation des tests réduit les coûts liés à la main-d'œuvre humaine, car il n'est pas	• **Manque de créativité** : les outils automatisés reposent sur des règles et des scripts prédéfinis, qui peuvent ne pas

nécessaire de payer des experts en sécurité pour effectuer ces tests manuellement.	être en mesure de simuler la créativité et l'ingéniosité des attaquants humains.
• **Préparation aux attaques réelles** : en automatisant les tests d'intrusion, les entreprises peuvent simuler des attaques réelles et se préparer à les gérer efficacement en cas de besoin.	• **Compréhension limitée du système :** les outils automatisés peuvent ne pas être en mesure de comprendre le contexte d'un système et ses processus opérationnels sous-jacents, ce qui peut conduire à l'oubli de vulnérabilités.
• **Meilleure couverture des tests**: l'automatisation des tests d'intrusion permet de couvrir un plus grand nombre de scénarios et de cas d'utilisation, ce qui augmente les chances de détecter les vulnérabilités.	• **Rapports limités** : les outils automatisés peuvent ne pas fournir de rapports aussi détaillés ou complets que les tests manuels, ce qui peut rendre difficile la compréhension de la portée et de l'impact complets des vulnérabilités.

Table 2:Les avantages et les limites d'automatisation des tests d'intrusion [14].

4 Processus des tests d'intrusion

Le processus des tests d'intrusion se basent sur des frameworks de référence bien établis permettant de catégoriser les tactiques et techniques utilisées par les attaquants ainsi que de décrire les différentes étapes d'une cyberattaque. Les Frameworks les plus utilisés sont le Framework Cyber Kill Chain [15], le Framework PTES [16]et le Framework MITRE ATT&CK [17].

4.1 La Cyber Kill Chain

La "Cyber Kill Chain" est un cadre développé par Lockheed Martin, dans le cadre du modèle "Intelligence Driven Defense", pour l'identification et la prévention des cyber-intrusions. Le modèle identifie ce que les adversaires doivent accomplir pour atteindre leurs objectifs

La "cyber kill chain" comprend sept phases principales, qui sont les suivantes [15]:

- **Reconnaissance** : L'attaquant recueille des informations sur la cible, notamment ses vulnérabilités, ses actifs et ses utilisateurs. Ces informations sont utilisées pour déterminer la meilleure approche pour l'attaque.
- **Armement** : L'attaquant crée un moyen pour lancer l'attaque, tel qu'un exploit ou un logiciel malveillant. Il peut s'agir d'écrire un code, de rédiger un courriel malveillant ou de préparer l'attaque d'une autre manière.
- **Transmission** : L'attaquant transmet l'attaque à la cible, par exemple en envoyant un courriel ou en téléchargeant un fichier sur un site Web.
- **Exploitation** : L'attaquant exécute l'attaque et utilise la vulnérabilité pour accéder au système ou au réseau cible.
- **Installation** : L'attaquant installe des logiciels malveillants ou des outils sur le système cible pour maintenir l'accès et effectuer d'autres actions.

- **Commandement et contrôle** : L'attaquant établit un canal de communication avec la cible pour garder le contrôle du système et exécuter d'autres actions.
- **Actions sur les objectifs** : L'attaquant atteint son objectif final, comme l'exfiltration de données sensibles, la perturbation des opérations ou la compromission d'autres systèmes. Cette phase peut impliquer la collecte d'informations, la modification de données ou l'exécution d'autres actions pour atteindre les objectifs de l'attaquant.

4.2 PTES

Le Penetration Testing Execution Standard (PTES) est un ensemble des normes utilisées dans le domaine des tests d’intrusion. Il fournit un cadre complet pour planifier, exécuter et gérer les tests d’intrusion, qui sont des évaluations de sécurité visant à identifier les vulnérabilités et à tester la résistance d'un système ou d'un réseau aux attaques. PTES est divisée en sept phases principales qui englobent tous les aspects d'un test d’intrusion [16]:

- **Interactions pré-engagement** : Établir une communication avec l'organisation concernée. Il s'agit de comprendre les objectifs du test, d'établir les accords et de discuter des contraintes, des délais et des ressources nécessaires.
- **Collecte de renseignements** : Rassembler une recherche approfondie sur l'organisation cible. Cela peut inclure l'identification des infrastructures, des systèmes, des technologies utilisées, des contacts internes, etc.
- **Modélisation des menaces** : Dans cette étape, le testeur analyse les informations recueillies lors de la phase précédente afin de comprendre les différentes menaces potentielles pour l'organisation. Cela permet de prioriser les domaines d'investigation pour les tests ultérieurs.
- **Analyse des vulnérabilités** : Identifier et évaluer les vulnérabilités techniques de l'infrastructure de l'organisation.
- **Exploitation** : Utiliser les vulnérabilités identifiées pour accéder aux systèmes et aux données sensibles.
- **Post-exploitation** : Explorer davantage les systèmes compromis pour élargir l'accès et évaluer les risques supplémentaires.
- **Rédaction du rapport** : Présenter les résultats du test d’intrusion dans un rapport détaillé, incluant les vulnérabilités identifiées, les mesures correctives recommandées et les informations nécessaires pour la prise de décision.

4.3 MITRE ATT&CK

MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) est une base de connaissances des Tactiques et Techniques et Procédures (TTP) des adversaires basés sur des observations du monde réel. Il est conçu pour fournir une vue d'ensemble des diverses méthodes utilisées par les acteurs malveillants pour pénétrer dans les réseaux et mener des attaques, ainsi que pour offrir aux équipes un plan directeur sur la façon de concentrer leurs efforts de sécurité [17]. Il est également ouvert au public et régulièrement mis à jour avec de nouvelles informations**.**

Le Framework est divisé en tactiques (les colonnes) et techniques (les lignes) qui décrivent les moyens par lesquels les adversaires atteignent leurs objectifs. Ces lignes et colonnes forment trois matrices distincts : Entreprise, Mobile et ICS (pour les systèmes de contrôle industriels).

Ces matrices sont conçues pour couvrir des domaines spécifiques et fournir des informations détaillées sur les techniques d'attaque et les comportements observés dans chaque contexte. Dans ce qui suit, nous présentons la matrice d'entreprise et notamment la sous matrice du réseau (Figure 1)

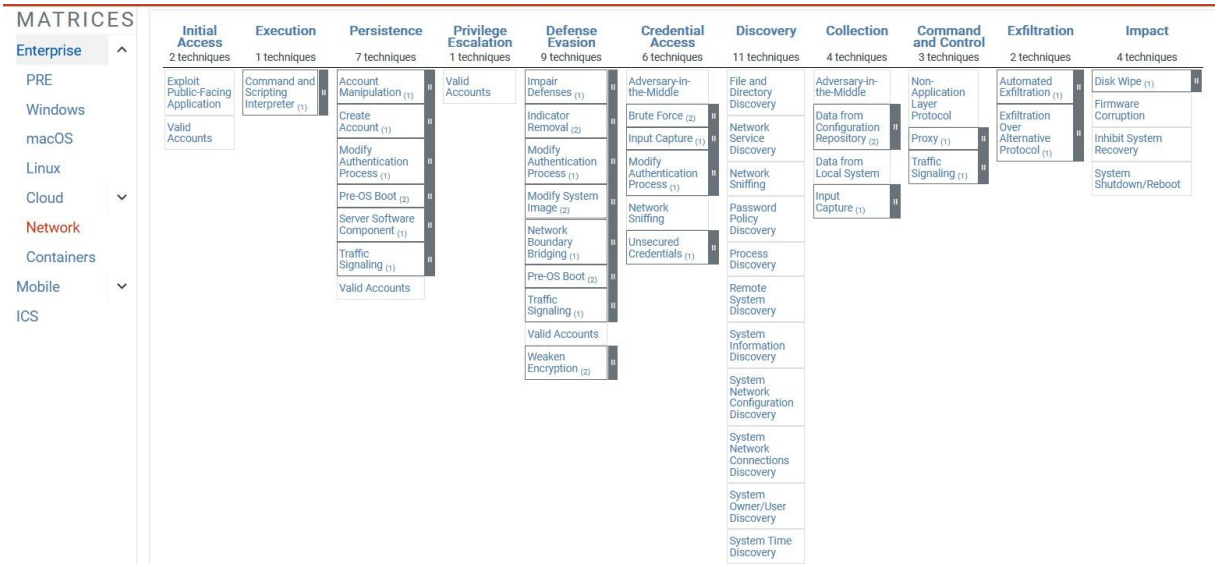

Figure 1:Matrice Réseau MITRE ATT&CK

Comme illustré dans la figure 1, Les tactiques de MITRE ATT&CK sont un ensemble de comportements utilisés par les adversaires pendant les cyberattaques pour atteindre leurs objectifs. Dans chaque tactique de la matrice ATT&CK de MITRE, il y a des techniques adverses, qui décrivent l'activité réelle menée par l'adversaire. Certaines techniques comportent des sous-techniques qui expliquent comment l'adversaire exécute une technique spécifique de manière plus détaillée.

Ces tactiques et techniques sont les suivants [17] :

- **Reconnaissance** : La reconnaissance consiste à recueillir des informations sur la cible, son infrastructure, ses systèmes et ses utilisateurs. Les techniques utilisées pour la reconnaissance peuvent inclure la recherche d'informations sur les sites web, les réseaux sociaux, les moteurs de recherche, l'analyse des noms de domaine, des adresses IP, des ports ouverts et des services actifs.
- **Accès initial** : Il s'agit des techniques utilisées par les attaquants pour s'introduire pour la première fois dans un système cible. Il peut s'agir de techniques telles que l'hameçonnage, l'exploitation de vulnérabilités, l'utilisation d'informations d'identification volées ou l'accès physique.
- **Exécution** : Une fois que l'attaquant a obtenu un accès initial, l'étape suivante consiste à exécuter un code malveillant sur le système cible. Il peut s'agir de techniques telles que l'utilisation de PowerShell ou d'autres langages de script.
- **La persistance** : La persistance consiste à maintenir un pied sur le système cible même après un redémarrage ou une autre interruption. Les techniques utilisées pour la persistance peuvent inclure la modification du registre ou des tâches planifiées, la création de fichiers ou de répertoires, ou l'installation d'un nouveau service.

- **Escalade de privilèges** : Il s'agit des méthodes utilisées par les attaquants pour obtenir des niveaux d'accès plus élevés à un système cible, tels que les privilèges d'administrateur ou de racine. Il peut s'agir d'exploiter des vulnérabilités, de recourir à l'ingénierie sociale ou d'utiliser des informations d'identification volées.
- **Évasion de défense** : L'évasion de défense consiste à éviter la détection par les outils et le personnel de sécurité. Les techniques utilisées pour échapper à la défense peuvent inclure la modification des propriétés des fichiers ou des processus, l'utilisation du cryptage, ou la désactivation des fonctions de sécurité.
- **Accès aux informations d'identification** : Il s'agit des méthodes utilisées par les attaquants pour voler ou obtenir des informations d'identification, telles que des mots de passe, des clés cryptographiques ou des jetons. Il peut s'agir de techniques telles que le craquage de hachages, l'utilisation de keyloggers ou l'utilisation d'une attaque de type "pass-the-hash".
- **Découverte** : La découverte consiste à recueillir des informations sur le système cible et son environnement. Les techniques utilisées pour la découverte peuvent inclure l'analyse du réseau, le profilage du système ou l'examen des journaux ou des métadonnées.
- **Mouvement latéral** : Le mouvement latéral consiste à se déplacer au sein d'un réseau pour accéder à d'autres systèmes. Les techniques utilisées pour le mouvement latéral peuvent inclure l'exploitation des relations de confiance, l'utilisation de procédures d'appel à distance ou l'utilisation de services à distance.

- **Collecte** : La collecte consiste à recueillir des données à partir du système cible. Les techniques utilisées pour la collecte peuvent inclure le grattage d'écran, l'exfiltration de données ou l'utilisation d'un outil d'accès à distance.
- **Commandement et contrôle** : Le commandement et le contrôle consistent à établir et à maintenir le contrôle d'un système cible. Les techniques utilisées pour le commandement et le contrôle peuvent inclure l'utilisation d'un reverse shell, d'un proxy ou d'un tunnel, ou l'utilisation d'un protocole personnalisé.
- **Exfiltration** : L'exfiltration consiste à extraire des données d'un système cible et à les envoyer à un emplacement distant. Les techniques utilisées pour l'exfiltration peuvent inclure l'utilisation d'un canal secret, d'un dispositif de stockage externe ou du cloud.
- **Impact** : L'impact consiste à causer des dommages au système cible et à son environnement. Les techniques utilisées pour l'impact peuvent inclure la destruction de données, l'arrêt du système ou la demande de rançon.

Les procédures MITRE ATT&CK sont des exemples de techniques spécifiques utilisées par les attaquants pour accomplir une étape ou une activité dans une tactique donnée.

4.4 La différence entre MITRE ATT&CK, PTES et Cyber Kill Chain

MITRE ATT&CK, PTES et Cyber Kill Chain sont des cadres d'évaluation de la sécurité informatique, chacun se concentrant sur des domaines distincts :

	MITRE ATT&CK	**PTES**	**Cyber Kill Chain**
Description	-Cadre de référence des tactiques et techniques d'attaques	-Procédures normalisées pour les tests d'intrusion	-Modèle décrivant les étapes d'une attaque ciblée
Objectif	-Comprendre les actions des attaquants et renforcer les défenses	-Effectuer des tests d'intrusion et évaluer la sécurité	-Comprendre le processus d'une attaque et organiser la défense
Focus	-Tactiques et techniques d'attaques spécifiques	-Phases d'un test d'intrusion	-Étapes d'une attaque ciblée
Utilisation	-Analyse de sécurité et renforcement des défenses	-Réalisation de tests d'intrusion	-Détection, prévention et réponse aux incidents
Points Forts	-Offre un cadre de référence complet des tactiques et techniques d'attaques utilisées par les attaquants. -Aide à comprendre les actions des attaquants et à renforcer les défenses en conséquence.	-Établit des procédures normalisées pour les tests d'intrusion, offrant une approche structurée et méthodique. -Permet d'effectuer des tests d'intrusion complets et d'évaluer la sécurité de manière systématique.	-Fournit un modèle décrivant les étapes d'une attaque ciblée, ce qui aide à comprendre le processus global de l'attaque. -Aide à organiser les défenses en se concentrant sur la détection, la prévention et la réponse aux incidents.
Points Faibles	-Nécessite une mise à jour régulière pour suivre l'évolution des tactiques d'attaques. -Complexité de détermination de la malveillance, toutes les techniques répertoriées ne sont pas exclusivement utilisées à des fins malveillantes.	-Peut-être rigide et ne pas s'adapter à tous les scénarios de tests d'intrusion. -Nécessite une adaptation pour s'aligner sur les spécificités et les objectifs de chaque organisation.	-Peut être considéré comme une approche linéaire de l'attaque, alors que les attaques réelles peuvent être plus complexes. -Peut négliger certaines tactiques d'attaque moins courantes.

Table 3:La différence entre MITRE ATT&CK et Cyber KILL Chain

Notre thème est proposé par l'organisme MNA Groupe où ses équipes suivent un processus basé sur PTES. Nous suggérons de combiner les phases de PTES avec les TTP de MITRE ATT&CK afin de bénéficier de la connaissance approfondie des techniques d'attaque de MITRE ATT&CK. Cette hybridation nous permet de détecter les menaces potentielles, d'identifier les failles de sécurité et de recommander des mesures de prévention et de correction adaptées à notre environnement spécifique.

5 Les outils d'automatisation des tests d'intrusion existants

Il existe une variété d'outils disponibles pour l'automatisation des tests d'intrusion, chacun ayant ses propres caractéristiques et fonctionnalités. Ces outils offrent des solutions complètes pour les tests automatisés et manuels. Par la suite, nous présentons les outils les plus connus :

5.1 vPENTEST

vPENTEST est un outil d'évaluation de vulnérabilités et de test d'intrusion basé sur le cloud développé par Vonahi Security. vPenTest peut effectuer des simulations avant et après une intrusion à tout moment dans des environnements internes et externes d'un réseau

Il offre une suite complète de fonctionnalités de test automatisées et manuelles, notamment l'analyse des vulnérabilités, l'analyse des applications Web, la cartographie du réseau et les tests d'intrusion manuels [18]. Il offre également d'autres fonctionnalités [18]:

- Établir des rapports et des analyses pour aider les organisations à mieux comprendre leur posture de sécurité**.**
- Utilisation d'un agent de sécurité Vonahi pour communiquer avec vPenTest sur des canaux cryptés.
- Effectuer de manière cohérente la découverte, l'énumération, l'exploitation, et post-exploitation
- Tâches basées sur le cadre d'attaque de MITRE, et Vonahi Cadre de test de pénétration de la sécurité
- Mises à jour du statut en temps réel et notifications pour les activités et menaces identifiées
- VPentest offre des recommandations de sécurité pour aider à protéger le réseau.
- La possibilité de générer des rapports détaillés.

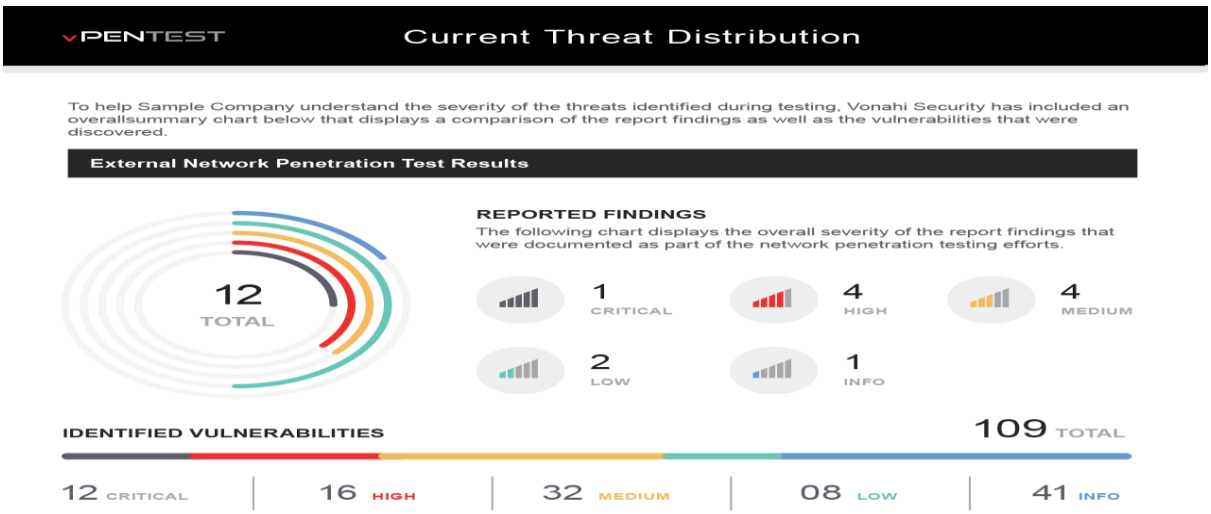

Figure 2:vPENTEST

5.2 Core Impact

Core Impact est un outil commercial de test d'intrusion conçu pour permettre aux équipes de sécurité de mener facilement des tests de pénétration avancés. . L'outil comprend différentes fonctionnalités telles que la reproduction des attaques sur l'infrastructure réseau, les terminaux, le Web et les applications pour révéler les vulnérabilités exploitées, ce qui vous permet de remédier immédiatement aux risques [19].

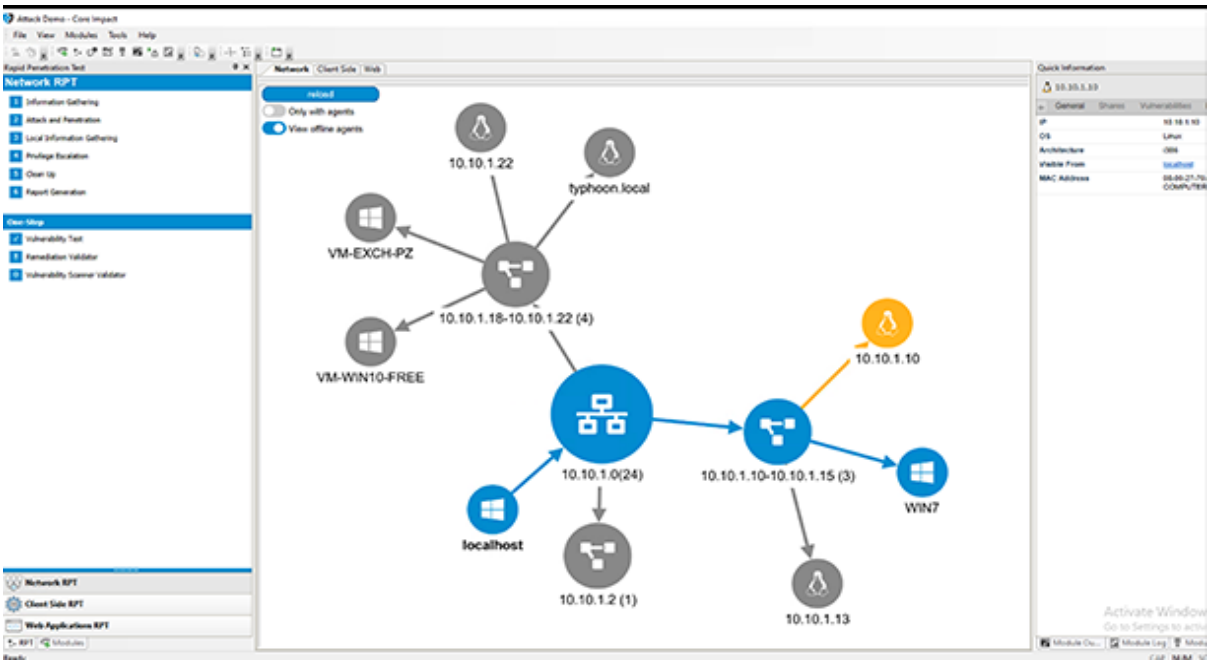

Figure 3:Core Impact

5.3 Comparaison entre vPENTEST et Core Impact

vPENTEST [18] et Core Impact [19]offrent des fonctionnalités similaires, mais présentent également des différences distinctes comme illustré dans le tableau suivant :

	vPENTEST	**Core Impact**
Fonctionnalités	Suite complète de tests automatisés et manuels incluant analyse de vulnérabilités, applications Web, cartographie réseau et tests d'intrusion.	Automatisation des tests d'intrusion, découverte de vulnérabilités, exploitation et évaluation de l'impact. Prise en charge multi système d'exploitation et protocoles réseau.
Déploiement	C'est un outil commercial basé sur le Cloud, ce qui permet de réaliser des simulations avant et après une intrusion à tout moment dans des environnements internes et externes d'un réseau.	Un outil commercial qui est généralement déployé localement sur une machine Windows avec une base de données SQL intégrée, sur un système physique ou virtuel.

Les Développeurs	Développé par Vonahi Security, avec un support et des mises à jour régulières pour maintenir l'outil à jour avec les dernières vulnérabilités et techniques d'attaque.	Développé par Core Security Technologies, Core Impact propose également un support et des mises à jour régulières pour garantir une efficacité optimale.
Interface et les fonctionnalités de rapport	L'interface conviviale et les fonctions de rapport et d'analyse simplifient l'utilisation de l'outil et la présentation des résultats.	L'interface utilisateur peut nécessiter une certaine familiarité avec les tests d'intrusion et les rapports pour une utilisation efficace
Processus	Tâches basées sur le framework MITRE ATT&CK, l'expérience et le framework de tests dintrusion de Vonahi Security.	Utiliser des Tests d'intrusion Rapides automatisés.

Table 4:Comparaison entre vPENTEST et Core Impact

Dans le cadre de notre projet, nous avons bénéficié des avantages et des fonctionnalités offertes par les deux outils, vPENTEST et Core Impact, pour créer une application similaire. Nous nous sommes inspirés de ces deux outils pour améliorer plusieurs aspects de notre application notamment coté interface graphique.

6 Conclusion

Dans ce chapitre, nous avons présenté les éléments clés que nous allons utiliser dans notre projet, tels que les équipes de sécurités (RedTeam), les types de test d'intruction (interne en boite grise), l'automatisation des tests d'instrusion ainsi que les processus de tests d'intruction (PTES et MITRE ATT&CK). En combinant tous ces éléments, nous proposons une solution qui permet d'automatiser les tests d'intrusion d'une RedTeam dans un environnement d'entreprise. La description de la solution fait l'objet du chapitre suivant.

CHAPITRE II : CONCEPTION

1 Introduction

La conception préalable d'une solution est essentielle avant sa mise en place. Dans ce chapitre, nous débutons par une description générale de notre solution. Ensuite, nous expliquerons le processus adopté pour les tests d'intrusion, les tactiques, techniques et procédures (TTP) mises en œuvre dans notre solution, ainsi que les fonctionnalités de notre application. Nous utiliserons également des diagrammes UML pour illustrer ces fonctionnalités.

2 Description de la solution proposée

Dans le but de réduire le temps humain considérable consacré aux tests d'intrusion, d'éliminer les tâches répétitives et augmenter la productivité des membres de la Red Team, nous proposons une solution permet d'automatiser les tests d'intrusion de réseau en boîte grise (Grey Box) dans un environnement d'entreprise. Cette solution permet d'effectuer les principales TTP (Tactiques, Techniques et Procédures) de MITRE ATT&CK et d'élaborer des rapports contenant des résultats détaillés sur les tests effectués afin de mesurer le niveau de sécurité de l'entreprise et de fournir ainsi des recommandations de sécurité et des mesures correctives pour renforcer la posture de sécurité de l'entreprise.

2.1 Notre Processus de test d'intrusion

Dans notre projet, nous avons adopté le processus de tests d'intrusion des équipes RedTeam de MNA Groupe. Basé sur le processus PTES, les membres de la RedTeam suivent une approche structurée qui constitue une feuille de route des étapes à simuler durant l'engagement afin d'identifier le maximum de failles et de vulnérabilités présentes dans l'environnement du client. Les principales phases dans leurs engagements sont généralement les suivantes [16]:

a. **Reconnaissance** : C'est la phase où la RedTeam recueille des informations sur la cible à évaluer. Cela peut inclure la collecte d'informations publiques, l'identification des systèmes en ligne, la recherche d'adresses IP, l'exploration de noms de domaine, etc. L'objectif est d'obtenir une compréhension approfondie de l'environnement de la cible.
b. **Analyse des vulnérabilités**: Une fois que la RedTeam dispose d'informations sur la cible, elle effectue des scans de vulnérabilité pour identifier les faiblesses potentielles. Cela peut impliquer l'utilisation d'outils automatisés pour rechercher des vulnérabilités connues dans les systèmes, les applications ou les services de la cible. Les résultats du scan aident à prioriser les vulnérabilités et à planifier les activités d'exploitation.
c. **Exploitation** : Après avoir identifié les vulnérabilités, la RedTeam tente de les exploiter pour obtenir un accès non autorisé ou des privilèges plus élevés. L'objectif de cette phase est de démontrer les risques réels que les vulnérabilités peuvent présenter pour la cible. Les techniques d'exploitation peuvent varier en fonction des vulnérabilités découvertes

et peuvent inclure l'utilisation de codes malveillants, d'attaques réseau, de techniques de phishing, etc.

d. **Génération de rapport** : Une fois les tests d'intrusion ou l'évaluation de la vulnérabilité terminée, la RedTeam compile les résultats dans un rapport détaillé. Ce rapport décrit les vulnérabilités identifiées, les méthodes d'exploitation utilisées, les preuves d'exploitation réussies et les recommandations pour remédier aux vulnérabilités. Le rapport est remis à l'organisation cliente pour l'aider à améliorer sa sécurité en corrigeant les vulnérabilités découvertes.

Nous proposons de combiner cette feuille de route avec les principales tactiques, techniques et procédures extraites du Framework MITRE ATT&CK comme illustré dans la figure suivante :

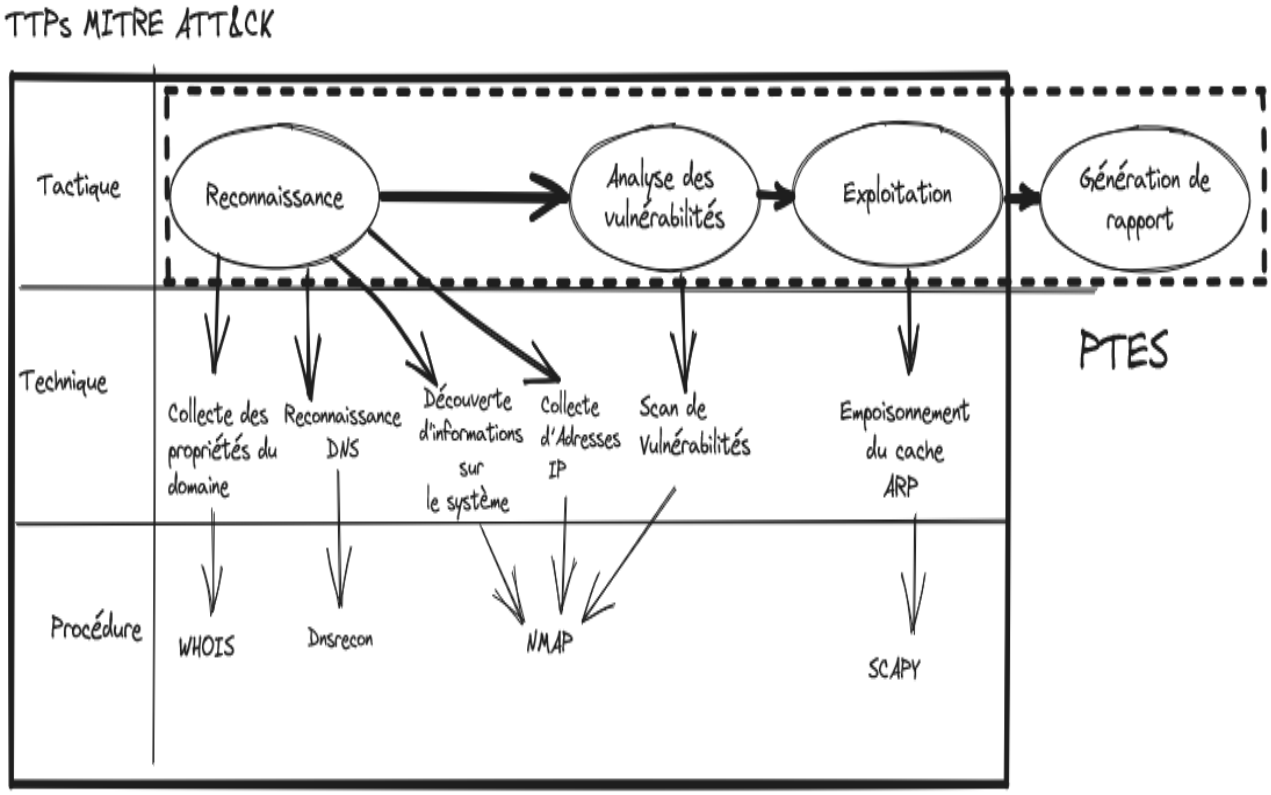

***Figure** 4:Notre processus de test d'intrusion*

Dans notre processus, une tactique du Framework MITRE ATT&CK correspond à une phase de PTES et chaque tactique contient un ou plusieurs techniques et procédures. Ces TTPs sont décrites dans le Tableau 5**.**

Tactique	Technique		Procédure
Reconnaissance	**Recueillir des informations sur le réseau de victimes (T1590)** : Les attaquants peuvent recueillir des informations sur les réseaux de la victime qui peuvent être utilisées pour le ciblage.	**Collecte des propriétés du domaine (T1590.001)** Les attaquants peuvent collecter des informations sur le(s) domaine(s) du réseau de la victime.	**Whois**
		Reconnaissance DNS (T1590.002) Les attaquants peuvent collecter des informations sur les DNS de la victime qui peuvent être utilisées pour le ciblage.	**DNSRecon**
		Collecte d'Adresses IP (T1590.005) Les attaquants peuvent collecter les adresses IP de la victime qui peuvent être utilisées pour le ciblage.	**Nmap**
	Découverte (TA0007) : La découverte consiste en des techniques qu'un attaquant peut utiliser pour obtenir des informations sur le système et le réseau interne.	**Découverte d'informations sur le système (T1082)** Un attaquant peut tenter de récupérer des informations détaillées sur le système d'exploitation et le matériel.	
Analyse des vulnérabilités	**Active Scanning (T1595) :** Les adversaires peuvent effectuer des scans de reconnaissance actifs afin de recueillir des informations qui peuvent être utilisées lors du ciblage.	**Scan de Vulnérabilités (T1595.002)** Les attaquants peuvent scanner les victimes à la recherche de vulnérabilités qui peuvent être utilisées lors du ciblage.	
Exploitation	**Adversaire au milieu (T1557)** :Les adversaires peuvent tenter de se positionner entre deux ou plusieurs dispositifs en réseau à l'aide d'un adversaire au milieu(adversary-in-the-middle AiTM)	**Empoisonnement du cache ARP (T1557.002)** Les adversaires peuvent empoisonner les caches du protocole de résolution d'adresses (ARP) pour se positionner entre les communications de deux ou plusieurs appareils en réseau.	**SCAPY**

Table 5:TTPs choisies

2.2 Techniques choisies

Etant donné que nos tests s'effectuent en interne en boite grise, nous supossons avoir les informations suivantes sur l'entreprise : nom de domaine (exemple.com), adresse IP de réseau cible (192.168.254.0/24), Ces informations nous permettent de lancer les techniques suivantes :

- **La technique « Propriétés du domaine (T1590.001) »**

Cette technique interroge des bases de données spécifiques et d'autres sources d'informations pour récupérer les détails du nom de domaine ciblé comme le titulaire, les coordonnées du registraire, les serveurs de noms, les dates d'enregistrement et d'expiration, etc. Afin de vérifier la validité et la disponibilité d'un domaine

- **La technique de la reconnaissance « DNS (T1590.002) »**

La procédure de la reconnaissance DNS permet aux pentesteurs de détecter les vulnérabilités potentielles en obtenant des informations détaillées sur les infrastructures DNS telles que les requêtes pour les enregistrements A (adresses IPv4), les enregistrements AAAA (adresses IPv6), les enregistrements MX (serveurs de messagerie), les enregistrements TXT (texte arbitraire associé à un domaine), les enregistrements SRV (service), etc. Elle peut également détecter si DNSSEC est configuré. Des recherches récursives sont également effectuées pour récupérer des informations sur les serveurs DNS autoritaires du domaine et les enregistrements associés. Les résultats sont récupérés en utilisant une expression régulière, sont stockés dans une base de données.

- **La technique de « Collecte des AdressesIP(T1590.005) »**

En utilisant le protocole ICMP[5], cette technique se déroule comme suit :

1) L'utilisateur saisit une plage d'adresses IP valide
2) Des paquets ICMP Echo Request sont envoyés à une plage d'adresses IP spécifiée afin de vérifier l'état de connectivité des hôtes.
3) Lorsqu'un hôte répond avec un paquet ICMP Echo Reply, cela confirme que l'hôte est actif et connecté au réseau. Si un hôte ne répond pas, cela peut indiquer qu'il est éteint, qu'il filtre les requêtes ICMP ou qu'il est inaccessible.
4) Lorsqu'un hôte répond avec un paquet ICMP Echo Reply, les informations suivantes sont extraites : l'adresse IP de l'hôte, l'adresse, l'état et le nom de la technologie de l'hôte. Ces informations seront ensuite stockées dans la base de données et affichées à l'utilisateur.

- **La technique « Découverte d'informations sur le système (T1082) »**

Cette technique permet de scanner les systèmes d'exploitations, les ports ouverts et/ou afficher les services associés d'une machine cible après avoir spécifié

- Une adresse IP unique valide
- Le protocole de la couche transport TCP (Transmission Control Protocol) ou UDP (User Datagram Protocol) utilisé.
- Le niveau d'agressivité (de T1 le plus lent à T4 le plus rapide (par défaut))

- **La technique « Scan de Vulnérabilités (T1595.002) »**

[5] **ICMP** (Internet Control Message Protocol) est un protocole de communication réseau utilisé pour envoyer des messages de contrôle et de diagnostic entre les périphériques d'un réseau IP, tels que les routeurs et les hôtes.

Cette technique opère en scrutant le réseau afin de détecter d'éventuelles vulnérabilités pouvant affecter les services déployés sur les différents composants du réseau. Son processus consiste à réaliser les étapes suivantes :

1) Collecter des empreintes digitales des services qui fournissent des informations telles que la version du logiciel ou du service, le système d'exploitation sous-jacent, les fonctionnalités spécifiques prises en charge, les configurations par défaut, ainsi que d'autres détails pertinents pour la détection des vulnérabilités
2) Comparer ces empreintes à une ou plusieurs bases de données de vulnérabilités connues. Ces bases de données contiennent des informations détaillées sur les vulnérabilités répertoriées et les versions de logiciels ou de services associées. Si une correspondance est trouvée, cela indique qu'une vulnérabilité spécifique peut être présente dans la version du service concerné.

Cette technique de scan de vulnérabilités permet d'identifier les failles potentielles dans les services déployés sur le réseau, ce qui permet aux administrateurs de prendre les mesures appropriées pour remédier à ces vulnérabilités et renforcer la sécurité de leur système.

- **La technique « d'empoisonnement du cache ARP (T1557.002) »**

Cette technique consiste à envoyer des paquets ARP falsifiés pour tromper les appareils cibles. Elle prend en paramètres l'adresse IP de la cible et l'adresse IP de la passerelle/routeur, et elle se déroule comme suit :

1) Récupération des adresses MAC correspondantes aux adresses IP de la cible et du routeur. Cela permet de spécifier correctement les adresses de destination dans les paquets ARP falsifiés.
2) La création de paquets ARP falsifiés, implique la modification ou la falsification des adresses MAC et IP dans les paquets ARP. Cela permet à l'attaquant de tromper les appareils du réseau en leur faisant croire qu'il est un autre appareil légitime.
3) Lorsqu'un appareil cible reçoit des paquets ARP falsifiés, il mettra à jour sa table ARP en conséquence avec les adresses MAC fausses fournies par l'attaquant. Cela signifie que le cible associera incorrectement les adresses IP aux adresses MAC incorrectes, ce qui peut entraîner des problèmes de connectivité réseau et permettre à l'attaquant de rediriger ou d'intercepter le trafic à son avantage.
4) L'attaquant peut décider de mettre fin à l'attaque à tout moment. Cela peut être fait en restaurant les tables ARP originales sur les appareils ciblés ou en arrêtant l'envoi des faux messages ARP.

Notons ici que les procédures seront détaillées dans le chapitre suivant (section 2).

2.3 Génération de rapport :

Notre application intègre une fonctionnalité de génération de rapports détaillés qui regroupe les résultats des différentes techniques utilisées lors des tests d'intrusion. Les rapports générés fournissent une vue complète de la relation entre les techniques, les procédures employées, les menaces potentielles et les vulnérabilités détectées, ainsi que des consignes et des recommandations pour améliorer la posture de sécurit

Table 6:Generation de rapport

Technique	**Procédure utilisée**	**Informations collectées**	**Exemples des Menaces potentielles**	**Recommandations**
Propriétés du domaine (T1590.001)	WHOIS	- Informations sensibles liées au domaine, telles que les noms de domaine, le nom du titulaire du domaine, les adresses e-mail, les numéros de téléphone.	-Vol de noms de domaine pour compromettre la réputation de l'organisation. -Vol d'identité : Les informations sensibles peuvent être utilisées pour voler l'identité de la victime.	- Être vigilant face aux tentatives de phishing ou d'ingénierie sociale visant à obtenir des informations supplémentaires sur le domaine suspecte. - Limiter l'accès aux informations sensibles du domaine.
Reconnaissance DNS(T1590.002)	DNSRecon	-Configuration DNS exposée. - Enregistrements DNS mal configurés. -Vulnérabilités des serveurs DNS.	-Injection de fausses entrées DNS (DNS spoofing) pour tromper les utilisateurs ou intercepter des communications. -Attaques par déni de service (DNS DDoS) pour rendre les services DNS inaccessibles.	- Mettre en place des configurations DNS sécurisées, y compris l'utilisation de protocoles de sécurité tels que DNSSEC (Domain Name System Security Extensions). - Effectuer des audits réguliers de sécurité sur les serveurs DNS.
Collecte d'Adresses IP (T1590.005)	Nmap	- les adresses IP et les adresses MAC et les fournisseurs de matériel (vendors) attribuées aux machines dans le réseau local de l'organisation. Cela peut inclure les adresses des ordinateurs, des serveurs, des imprimantes, des routeurs, etc., qui sont accessibles au sein du réseau interne.	-Balayage de ports pour identifier des services vulnérables. -Attaques de déni de service distribué (DDoS) visant les adresses IP exposées. -Utilisation d'adresses IP sensibles pour cibler les systèmes internes.	-Mettre en place des pare-feu pour limiter l'exposition des adresses IP sensibles. -Utiliser des listes de contrôle d'accès pour restreindre l'accès aux ressources réseau. -Appliquer les meilleures pratiques de segmentation réseau pour isoler les systèmes sensibles.
Découverte d'informations sur le système (T1082)		- Configuration du système exposée. - Informations sensibles sur le système d'exploitation. - Vulnérabilités connues. - Versions logicielles obsolètes.	-Exploitation de vulnérabilités connues sur des systèmes dont les versions logicielles sont obsolètes.	- Mettre en œuvre des pratiques de sécurité telles que la gestion des correctifs et les mises à jour régulières du système d'exploitation. - Utiliser des outils de détection d'intrusions pour surveiller les activités suspectes.

			-Utilisation d'informations sensibles sur le système pour mener des attaques ciblées.	
Scan de vulnérabilité (T1595.002)		- Vulnérabilités identifiées. -Configuration faible ou non sécurisée.	-Exploitation de vulnérabilités identifiées pour obtenir un accès non autorisé aux systèmes. -Exfiltration de données sensibles à travers des vulnérabilités non corrigées.	- Effectuer régulièrement des scans de vulnérabilités pour identifier les faiblesses du système. - Corriger les vulnérabilités détectées en appliquant les correctifs appropriés. - Fermer les services et les ports non nécessaires pour réduire l'exposition.
Empoisonnement du cache ARP (T1557.002)	SCAPY	-Les associations entre adresses IP et adresses MAC légitimes des machines présentes sur le réseau	-Intercepter et manipuler les communications réseau pour mener des attaques d'usurpation d'identité. -Capturer et analyser le trafic réseau pour récupérer des informations sensibles. -Faciliter les attaques de l'homme du milieu (Man-in-the-Middle) pour intercepter les communications.	- Mettre en place des mesures de sécurité pour détecter et prévenir les attaques d'empoisonnement de cache ARP. - Utiliser des mécanismes d'authentification et de chiffrement pour sécuriser les communications.

3 Etude Conceptuelle de notre application

Afin d'automatiser les tests d'intrusion, nous avons conçu une application permettant de répondre aux besoins suivants :

- **Authentification sécurisée** permettant aux utilisateurs autorisés d'accéder aux fonctionnalités et aux données appropriées.
- **Gestion des projets de tests d'intrusion** permettant de créer des projets, organiser les tests par projet, suivre l'état d'avancement et enregistrer les résultats associés à chaque projet à des fins de génération de rapport ultérieure.
- **Gestion des attaques automatisées** permettant aux utilisateurs de sélectionner les techniques d'attaque à exécuter, spécifier les cibles, définir les paramètres de l'attaque et lancer les tests. Les résultats des attaques sont enregistrés et présentées de manière claire et structurée.

3.1 Diagramme de cas d'utilisation

Un diagramme de cas d'utilisation est un moyen de décrire et de représenter l'interaction et les relations entre les acteurs et les différents cas d'utilisation.

- **Un acteur :** est une entité, telle qu'une personne, une entreprise ou un système, qui interagit avec les fonctionnalités offertes par le système.
- **Un cas d'utilisation** : représente une série d'actions que le système doit effectuer pour répondre aux besoins de l'utilisateur.

Dans le cas de notre système, nous pouvons distinguer les acteurs suivants :

- **Administrateur** : qui gère les projets et les utilisateurs
- **Un Pentester:** qui lance les attaques

Les diagrammes suivants (**Figure 5 et Figure 6**) regroupent les principales fonctionnalités établies par les utilisateurs de l'application. Il est suivi d'une description détaillée des chacune d'elle.

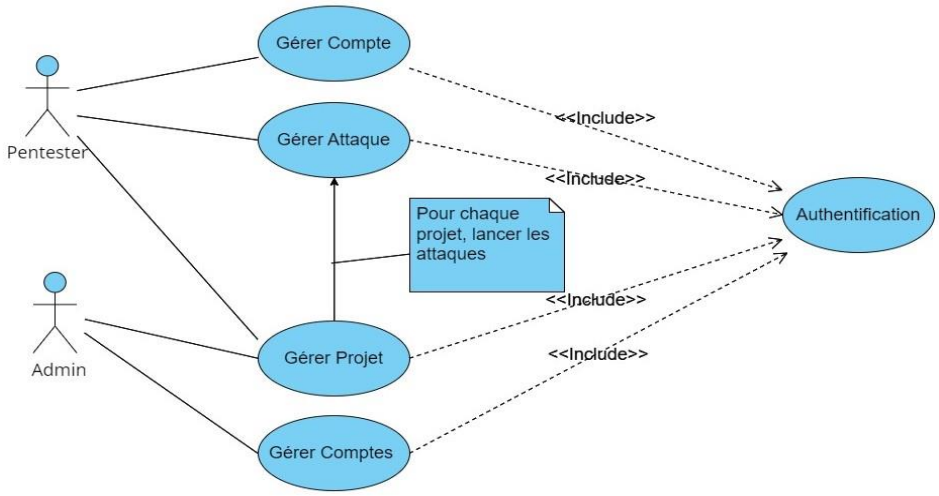

Figure 5:Diagramme de cas d'utilisation globale

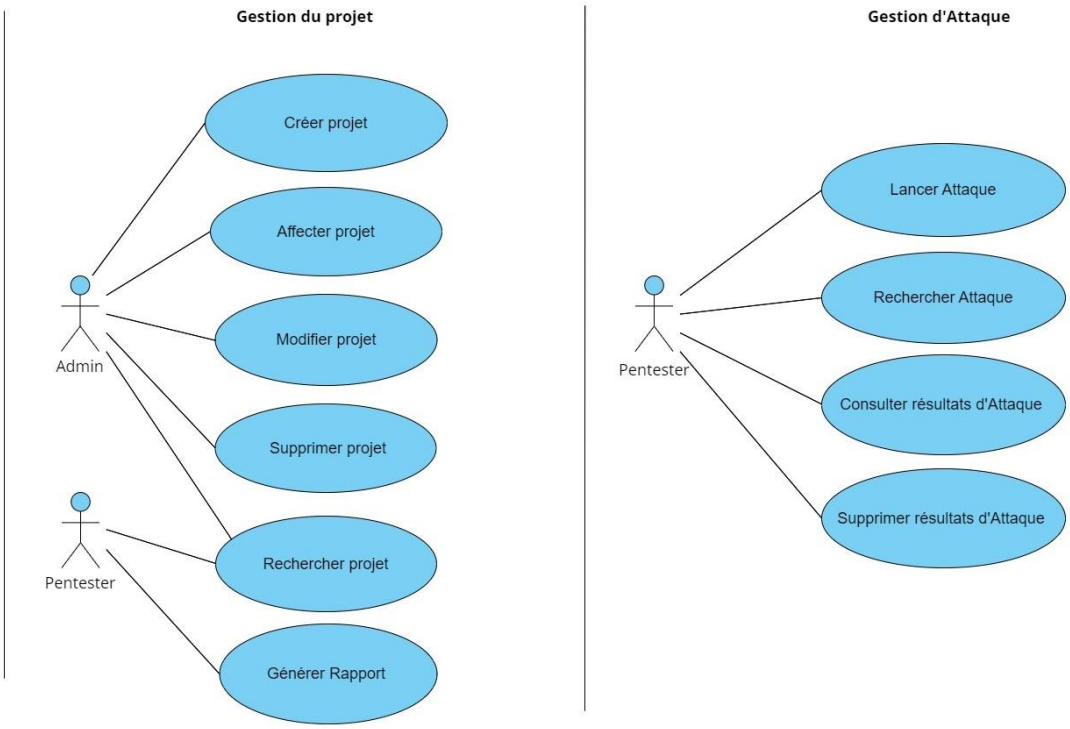

Figure 6:Diagrammes de cas d'utilisation de gestion du projet et gestion d'attaque

Cas d'utilisation		**Acteur**	**Description de cas d'utilisation**
S'authentifier		Administrateur Pentester	Les acteurs peuvent se connecter au système en fournissant leurs identifiants pour accéder aux fonctionnalités
Gestion du Projet	Créer Projet	Administrateur	L'administrateur peut créer un nouveau projet en spécifiant les détails et les paramètres requis.
	Affecter Projet		L'administrateur peut attribuer un projet spécifique à un Pentester pour qu'il puisse y travailler.
	Modifier Projet		L'administrateur peut apporter des modifications aux détails et aux paramètres d'un projet existant.
	Supprimer Projet		L'administrateur peut supprimer un projet existant du système.
	Rechercher Projet	Administrateur Pentester	L'administrateur et le Pentesteur peuvent rechercher et accéder à des projets spécifiques en utilisant des critères de recherche.
	Générer Rapport	Pentester	Le Pentester peut générer un rapport détaillé sur les résultats des attaques
Gestion d'Attack	Lancer Attaque	Pentester	Le Pentester peut exécuter des attaques spécifiques dans le cadre d'un projet.
	Consulter Résultat d'attaque		Le Pentester peut consulter les résultats
	Rechercher Attaque		Le Pentester peut effectuer des recherches pour trouver des informations
	Supprimer Résultat d'attaque		Le Pentester peut supprimer des informations relatives à une attaque.

Tableau 3-1: Description des cas d'utilisation du diagramme globale

3.2 Diagramme de Classe :

Le diagramme de classe est une représentation graphique utilisée pour visualiser les classes et les interfaces d'un système, ainsi que les relations qui existent entre elles. Nous présentons ci-dessous (Figure ***7)*** notre diagramme de classe, accompagnée d'une description détaillée dans le tableau 7 et suivi du schéma relationnel correspondant.

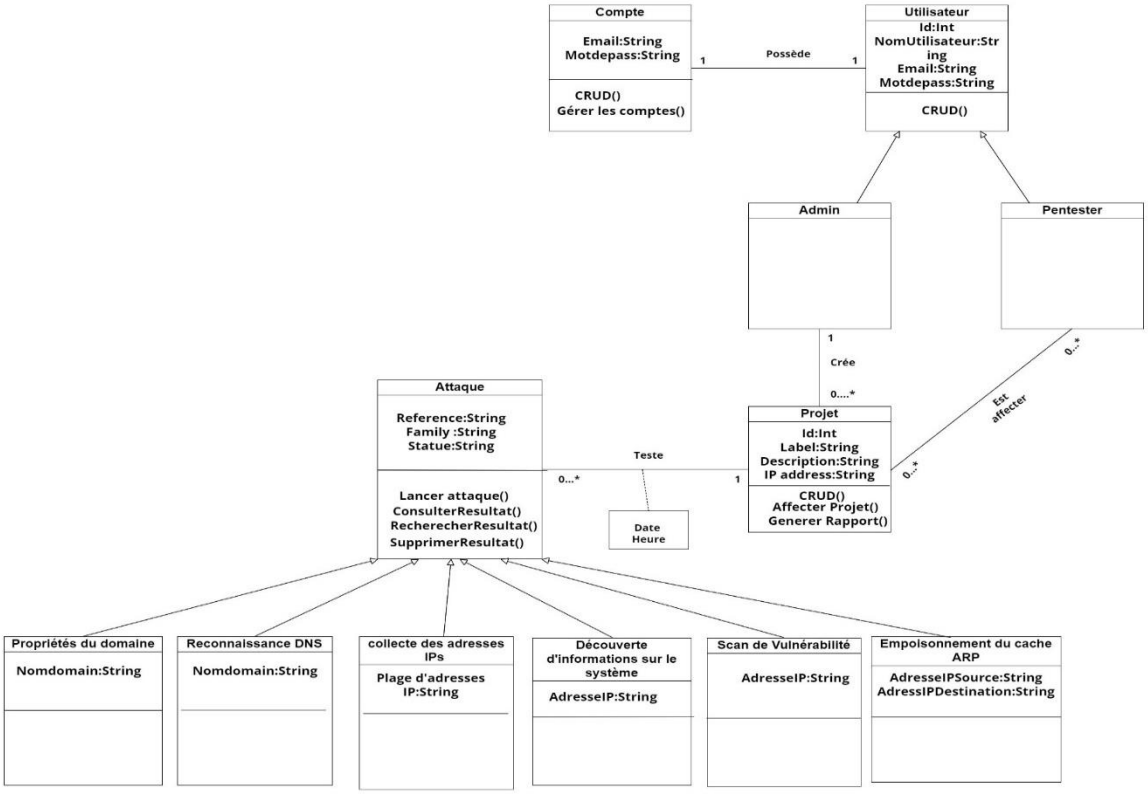

Figure 7:Diagramme de classe

Classe	Attribut	Type	Désignation	Méthode
Utilisateur	Id	Int	Identifiant Utilisateur	CRUD()
	NomUtilisateur	String	Nom d'Utilisateur	
	Email	String	Email d'Utilisateur	
	Motdepass	String	Mot de passe d'Utilisateur	
Admin				
Pentester				
Projet	Id	Int	Id projet	CRUD () Affecter projet ()
	Label	String	Nom du projet	
	Description	String	Description du projet	
	IP Adresse	String	IP Adresse de réseau cible	
Attaque	Reference	String	Reference dans MITRE ATT&CK	CRUD () Lancer attaque () Rechercher attaque () Résultats d'attaque () Génération de rapport ()
	Famille	String	Tactique dans MITRE ATT&CK	
	Statue	String	Statue de l'Attaque	
Compte	Email	String	Email de compte	CRUD () Gérer les comptes ()
	Motdepass	String	Mot de passe de compte	

Tableau 7: Tableau descriptif des classes, attributs et méthodes

3.3 Diagramme d'activité

Le diagramme d'activité représente les étapes séquentielles d'un processus ou d'un système sous forme de symboles et de flèches.

Comme illustré dans la figure ci-dessous, l'administrateur pourra créer un projet qui regroupe toutes les informations et les actions relatives aux engagements spécifiques lors d'un test d'intrusion. Ensuite, il doit attribuer ce projet à des pentesteurs existants. Puis, chaque Pentester peut sélectionner une ou plusieurs attaques à exécuter. Enfin, le rapport final est généré.

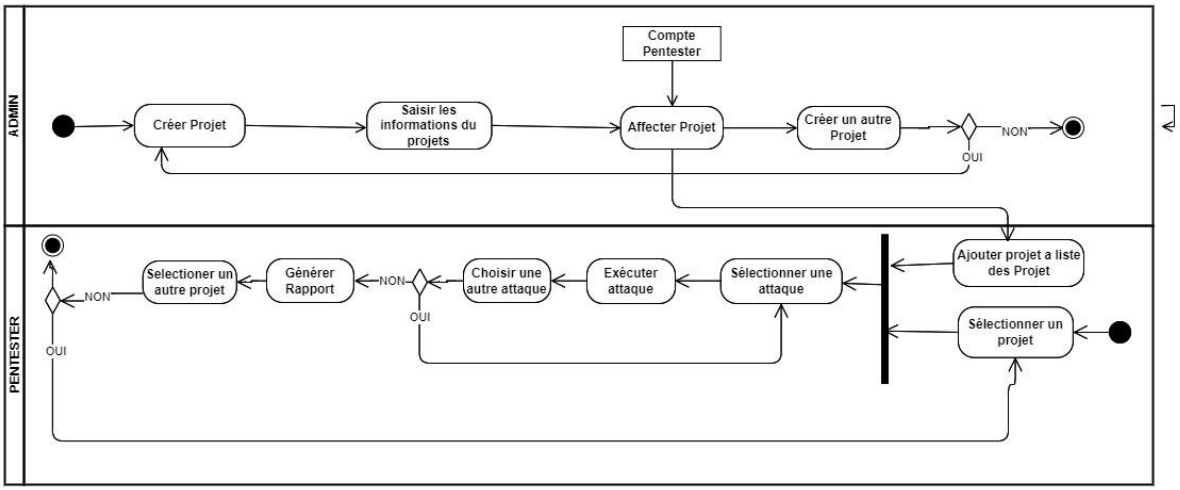

Figure 8:Diagramme d'activités

4 Conclusion

Dans ce chapitre, nous avons fourni une description générale de notre solution, ainsi qu'une explication détaillée de la méthodologie de test d'intrusion que nous avons adoptée. Nous avons également présenté les tactiques, techniques et procédures (TTP) que nous avons mises en œuvre pour renforcer la sécurité de notre application. De plus, nous avons utilisé des diagrammes UML pour illustrer les fonctionnalités clés de notre application. Cette approche nous a permis de créer une solution solide et sécurisée, répondant aux besoins de l'organisme d'accueil.

CHAPITRE III : REALISATION, TESTS & RESULTATS

1 Introduction

Ce chapitre est dédié à notre application, mettant en avant ses fonctionnalités principales. Nous commençons par présenter l'environnement de développement, les langages de programmation et les procédures utilisées. Ensuite, nous décrivons les différentes interfaces de l'application. Enfin, nous réaliserons des tests d'intrusion interne incluant les attaques implémentées et les résultats obtenus, soutenus par des captures d'écran.

2 Environnement de développement

Dans le développement de notre application web, nous avons utilisé une machine hébergeant le système d'exploitation Kali-Linux, qui est divisé en deux parties distinctes (figure 9**,**Tableau 2-1) : le FRONT-END et le BACK-END.

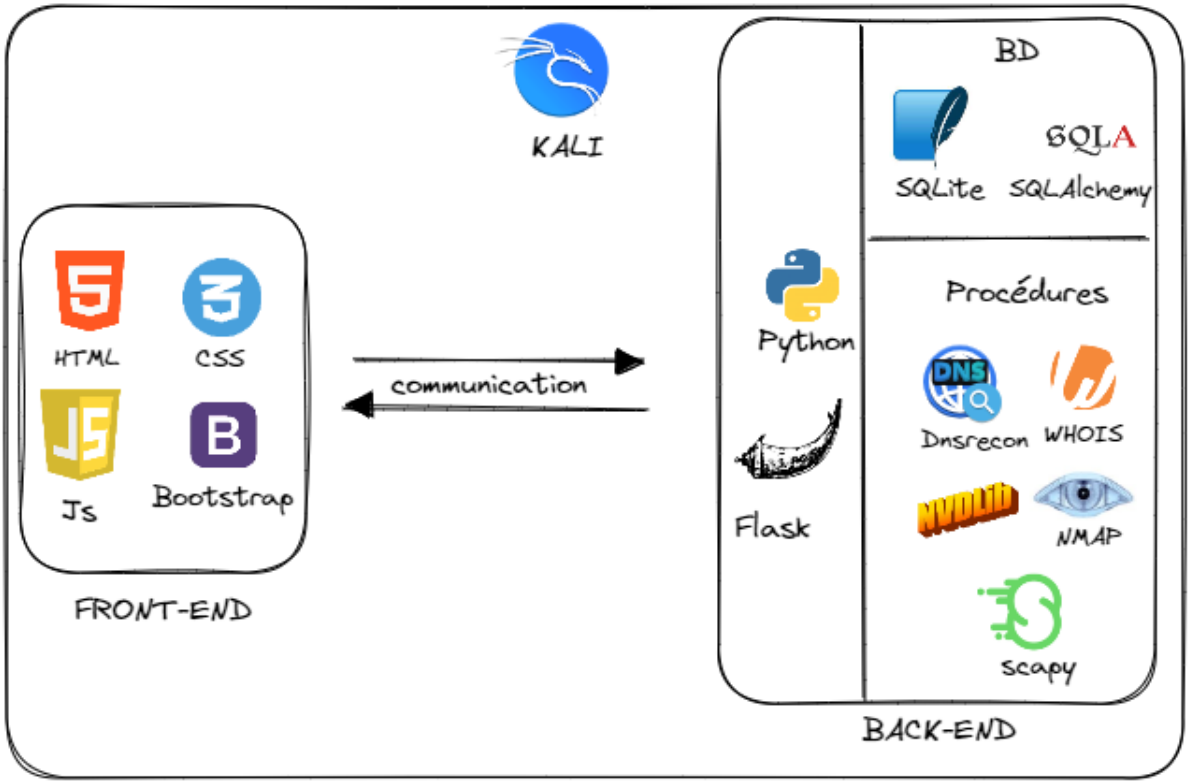

Figure 9:Environnement de développement

- **Le FRONT-END** de notre application web est développé en utilisant les langages et les technologies web fondamentaux tels que HTML (Hyper Text Markup Language), CSS (Cascading Style Sheet) et JavaScript. Ces langages nous permettent de structurer et de présenter les informations de manière interactive dans le navigateur des utilisateurs.

Pour améliorer l'efficacité et la facilité de développement, nous avons également utilisé le framework Bootstrap.

- **Le BACK-END** de notre application est basé sur une architecture de serveur-client. Nous avons développé le serveur en utilisant le langage de programmation Python et le framework Flask. Flask nous a permis de mettre en place des routes pour gérer les requêtes des utilisateurs et effectuer les opérations nécessaires sur les données. Nous avons utilisé une base de données SQLite pour stocker les données de l'application.

Langage	Description
HTML	Langage de balisage utilisé pour structurer le contenu d'une page web [20].
CSS	Langage de style permettant de définir l'apparence et la mise en forme des éléments HTML [21].
JavaScript	Langage de programmation utilisé pour rendre les pages web interactives en ajoutant des fonctionnalités dynamiques et des comportements. [22]
Bootstrap	Collection d'outils utiles à la création du design, graphisme, animation et interactions avec la page dans le navigateur [23].
Python	Langage de programmation interprété, polyvalent et convivial. Il est réputé pour sa syntaxe claire et lisible. il est largement utilisé dans le développement web, l'automatisation de tâches, l'analyse de données, l'intelligence artificielle et bien d'autres domaines [24].
Flask	Framework web minimaliste et léger pour Python. Il est conçu pour faciliter le développement rapide d'applications web. Flask offre une grande flexibilité et permet de créer des applications de petite à moyenne taille. Il fournit des fonctionnalités de base pour le routage, la gestion des requêtes HTTP, la gestion des cookies, etc [25].
SQLite	Système de gestion de base de données relationnelle (SGBDR) qui fonctionne sans serveur. Il est intégré directement dans l'application et stocke les données dans un fichier unique. SQLite prend en charge la plupart des fonctionnalités SQL standard et est facile à utiliser avec de nombreuses bibliothèques et langages de programmation, y compris Python [26].
SQLAlchemy	Bibliothèque Python qui fournit un ensemble d'outils pour travailler avec des bases de données relationnelles. Elle offre une interface de haut niveau pour interagir avec les bases de données, tout en fournissant une couche d'abstraction qui permet de travailler avec différents types de bases de données (comme SQLite, MySQL, PostgreSQL, etc.) de manière transparente. SQLAlchemy facilite la création et l'exécution de requêtes SQL, ainsi que la gestion des relations entre les tables [27].

Table 7:Langages de programmation

3 Procédures

Dans cette section, nous allons présenter les procédures que nous avons choisies dans notre processus TTPs. Pour chaque procédure, nous montrons un exemple d'application dans une figure.

- **Whois**

Un outil permet d'obtenir des informations sur un nom de domaine spécifique. Il interroge les bases de données WHOIS publiques pour récupérer des détails sur le propriétaire du domaine, les contacts administratifs, les serveurs de noms, les dates d'enregistrement et d'expiration, etc [28]. La figure suivante montre un exemple d'application :

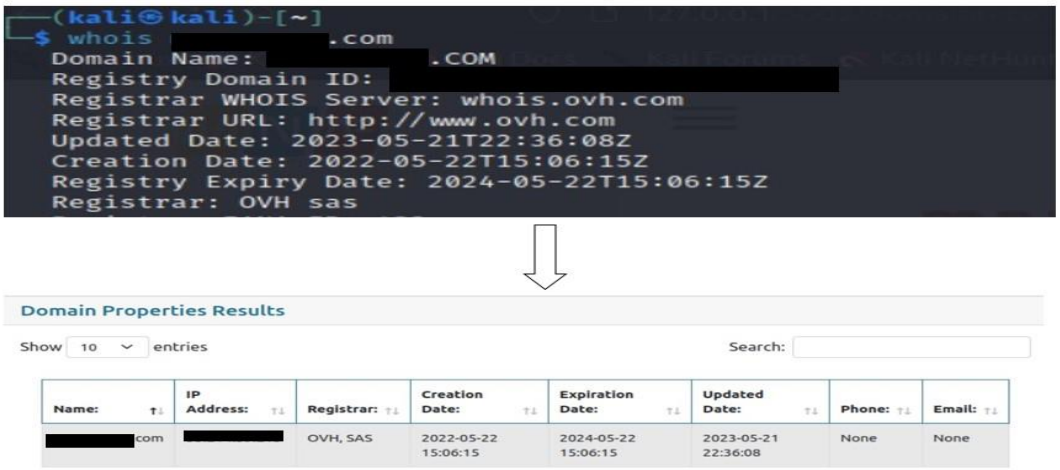

Figure 10:WHOIS

- **DNSRecon**

C'est un outil de reconnaissance de DNS (Domain Name System) qui permet de collecter des informations sur les enregistrements DNS d'un domaine donné. Il effectue diverses requêtes DNS telles que les enregistrements A, MX, NS, TXT, etc afin de découvrir des informations sur l'infrastructure réseau d'un domaine. Il peut également être utilisé pour détecter des serveurs DNS ouverts, des enregistrements cachés, des vulnérabilités potentielles ou pour effectuer des tests d'intrusion ciblant les serveurs DNS [29].

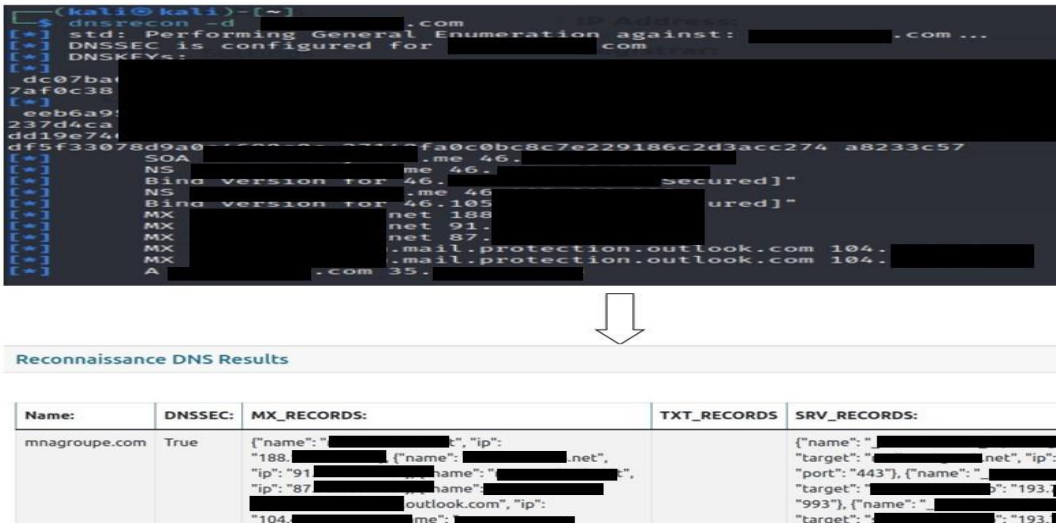

Figure 11:Dnsrecon

- **Scapy**

C’est une bibliothèque Python puissante et flexible pour la manipulation de paquets réseau. Scapy permet de créer, d’envoyer, capturer et analyser des paquets réseau, ce qui est utile pour le développement d'outils de sécurité et de diagnostic réseau [30]

```
def perform_spoof(target_ip, target_mac, gateway_ip, gateway_mac):
    while spoofing_started:
        packet_to_target = scapy.ARP(op=2, pdst=target_ip, hwdst=target_mac, psrc=gateway_ip)
        packet_to_gateway = scapy.ARP(op=2, pdst=gateway_ip, hwdst=gateway_mac, psrc=target_ip)

        scapy.send(packet_to_target, verbose=False)
        scapy.send(packet_to_gateway, verbose=False)
```

Figure 12:Scapy

- **Nmap**

Network Mapper est un outil de découverte de réseau et de sécurité. Il est utilisé pour analyser les hôtes et les services sur un réseau, ainsi que pour détecter les vulnérabilités potentielles. Nmap utilise des techniques avancées de balayage de port pour détecter les services en cours d'exécution sur un hôte, le système d'exploitation utilisé et d'autres informations pertinentes [31].

Dans notre solution, nous avons utilisé le Nmap pour implémenter trois techniques comme suit:

- **Collecte des AdressesIP** : La commande nmap -sP <cible> effectue une recherche d'hôtes à l'aide de requêtes ICMP (ping scan). L'objectif de cette commande est d'identifier rapidement les hôtes actifs et réactifs sur un réseau donné. Elle est généralement utilisée comme étape préliminaire avant de procéder à d'autres analyses ou évaluations du réseau.

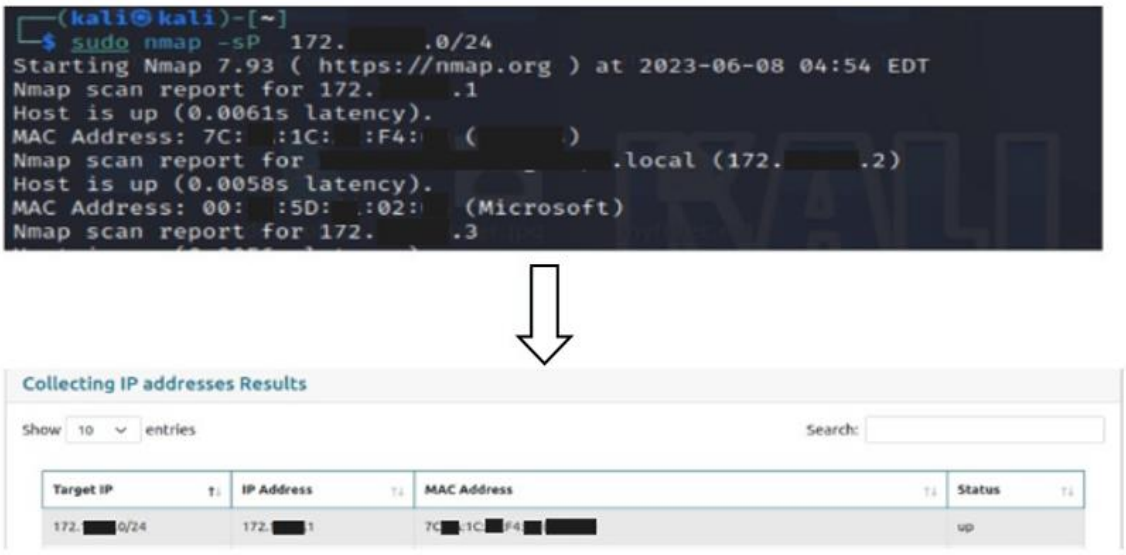

Figure 13:Collecte des AdressesIP

- **Découverte d'informations sur le système** : La commande "nmap -sS -T4 -O -Pn <cible>" est une commande Nmap complète qui effectue un scan SYN agressif pour

les ports (il s'agit des options de synchronisation comme T1, T2, T3 et T4, elles permettent de contrôler la vitesse d'envoi des paquets), active la détection des systèmes d'exploitation, et désactive la découverte de l'hôte par ping(-Pn). Elle permet d'obtenir des informations détaillées sur les ports ouverts(-sS), les services des ports et les systèmes d'exploitation des hôtes cibles(-O).

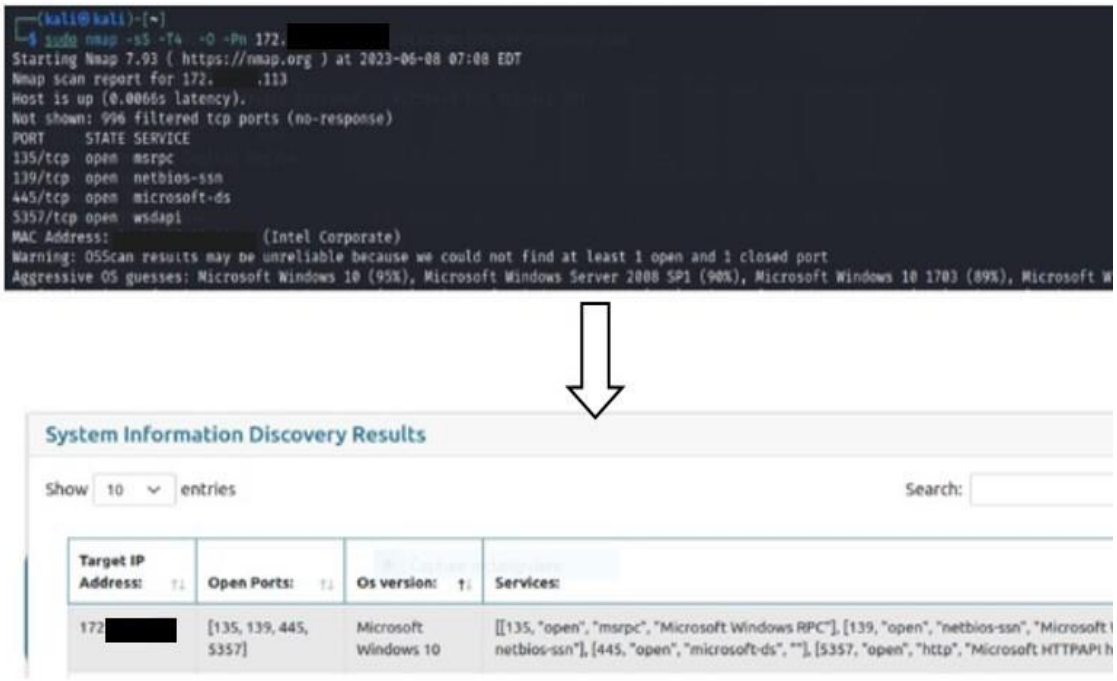

Figure 14:Découverte d'informations sur le système

- **Scan de vulnérabilités** : Les scripts NSE (Nmap Scripting Engine), tels que "nmap-vulners[6]" et "vuln[7]", sont conçus pour effectuer des analyses de vulnérabilités sur les systèmes cibles. Après avoir réalisé une première phase de scan pour identifier les ports ouverts et les services actifs, ces scripts sont utilisés pour détecter les vulnérabilités connues liées à ces services en consultant des sources d'informations fiables. Dans notre application, nous avons opté pour la base de données NVD (National Vulnerability Database) et notamment la bibliothèque "nvdlib[8]" qui permet de rechercher des vulnérabilités par ID CVE (Common Vulnerabilities and Exposures) ou par d'autres critères spécifiques, et de récupérer les informations détaillées associées à ces vulnérabilités.

[6] Il se base sur une base de données de vulnérabilités connues afin de vérifier si les services identifiés présentent des failles spécifiques. Il compare les versions des services avec les références des vulnérabilités connues pour identifier d'éventuelles failles potentielles.

[7] En utilisant des scripts dédiés à chaque service pour effectuer des analyses plus approfondies, Il peut exécuter des tests d'exploitation et autres vérifications pour évaluer si une vulnérabilité est réellement exploitable.

[8] Bibliothèque Python qui fournit une interface pour accéder à la base de données nationale des vulnérabilités (NVD). La base de données NVD contient des informations sur les vulnérabilités logicielles connues, y compris les descriptions, les niveaux de gravité, les références, etc. NVDLib permet aux développeurs de récupérer les données de la NVD et de les utiliser pour la recherche, l'analyse et la gestion des vulnérabilités dans leurs applications [32]

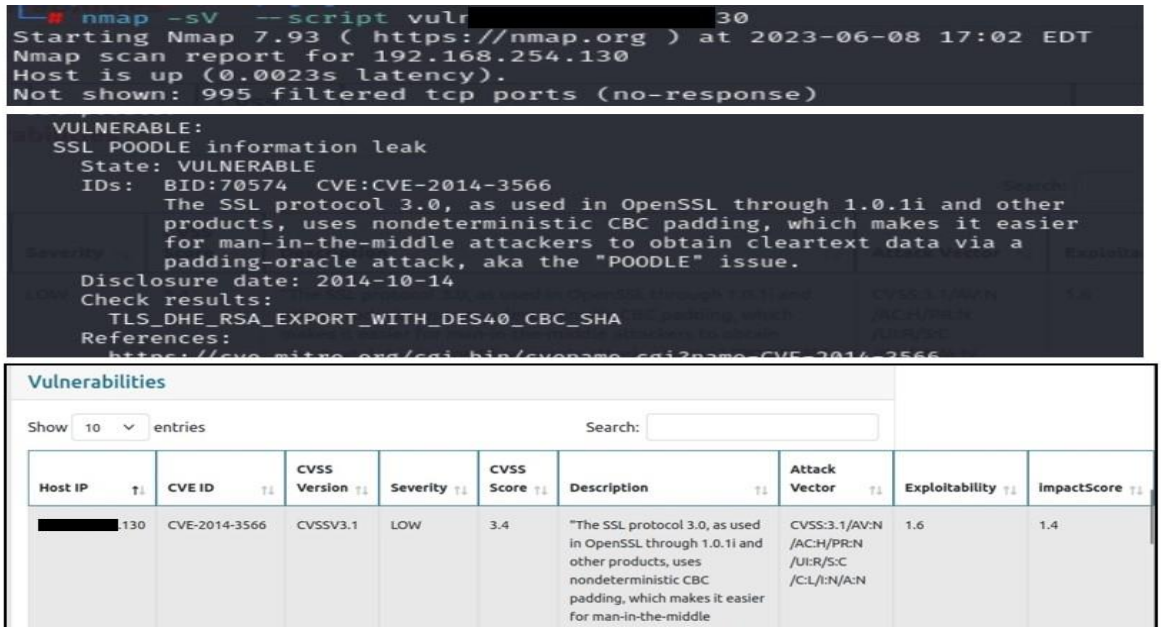

Figure 15:NSE

4 Implémentation de l'application

Notre application intègre un système d'authentification permettant aux utilisateurs de se connecter en tant qu'administrateur ou pentester, leur donnant ainsi accès aux fonctionnalités spécifiques correspondantes à leur rôle respectif. Lors de la phase d'authentification, les utilisateurs doivent fournir leurs identifiants (email et mot de passe) pour accéder à l'application. Ainsi, nous distinguons deux types d'espace :

4.1 Espace administrateur

Dans l'espace administrateur (figure 16), l'administrateur dispose de fonctionnalités avancées lui permettant de gérer efficacement les projets en cours. Tout d'abord, il peut accéder à une liste complète des projets déjà créés, leur permettant ainsi d'avoir une vue d'ensemble de toutes les activités en cours. L'administrateur peut créer de nouveaux projets en fournissant les paramètres requis, puis les attribuer à un ou plusieurs pentesters spécifique. De plus, l'administrateur a la possibilité de consulter à tout moment l'état d'avancement de chaque projet.

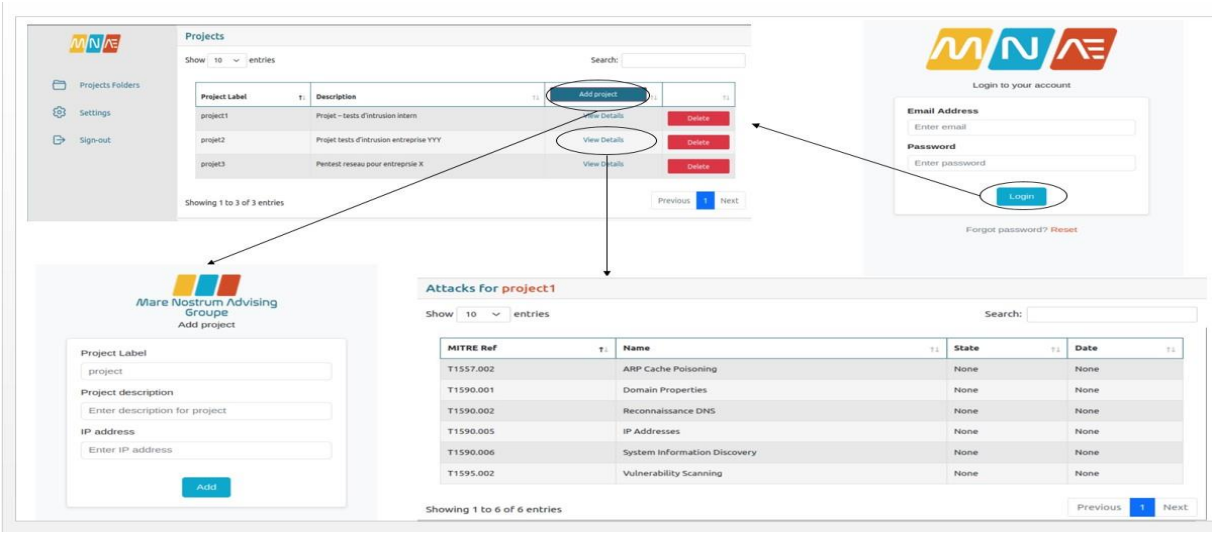

Figure 16:Espace Administrateur

4.2 Espace Pentester

Dans l'espace Pentester (Figure17), le Pentester a la possibilité de consulter les projets qui lui ont été attribués par l'administrateur. Une fois qu'un projet lui est assigné, le Pentester peut lancer un ou plusieurs attaques et tests de sécurité pour évaluer les vulnérabilités du système. Il utilise les outils disponibles dans l'application pour mener à bien ces attaques et collecter des informations pertinentes. Il peut à la fin des tests générer un rapport détaillé comprenant les vulnérabilités détectées, accompagnées de recommandations de sécurité.

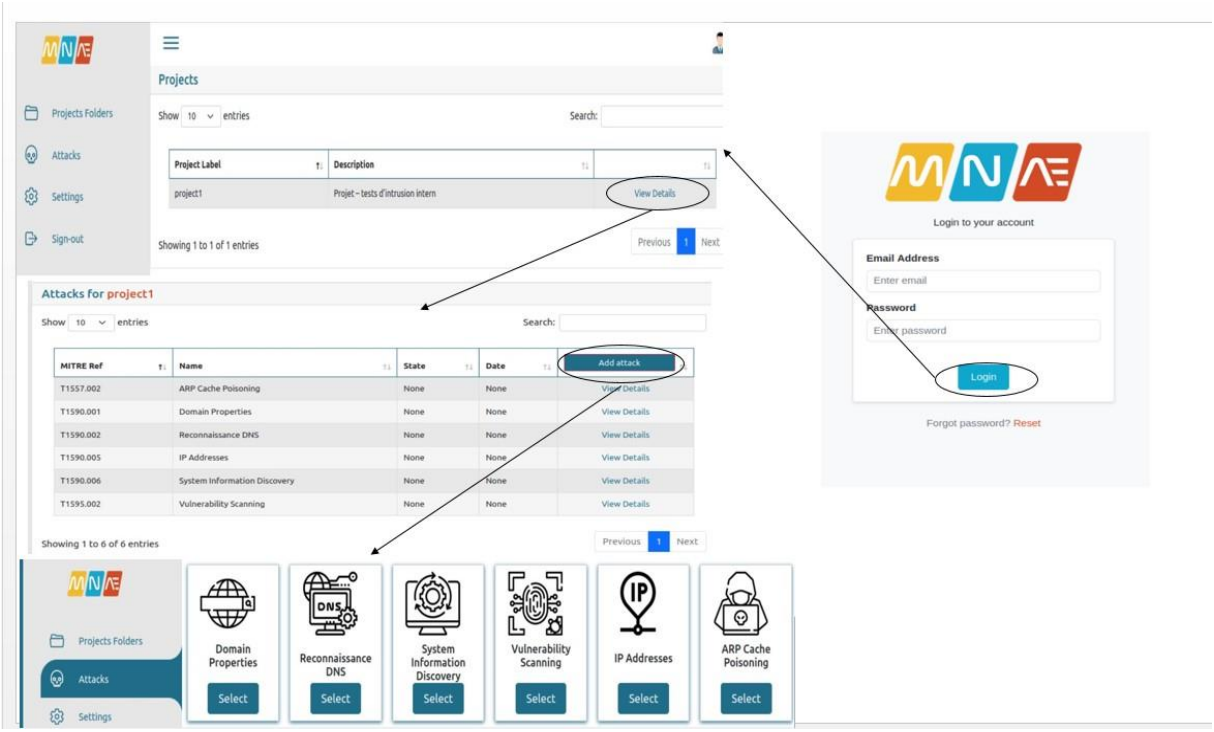

Figure 17:Espace Pentester

5 Tests et résultats

Dans cette section, nous aborderons les tests effectués ainsi que les résultats obtenus.

5.1 Environnement de test

Dans le cadre de notre projet, nous avons réalisé des tests dans un environnement réel au sein de l'entreprise MNA Groupe. Cet environnement de test a permis de simuler des situations réelles et de mettre à l'épreuve notre solution dans des conditions proches de la réalité. Comme illustré dans la figure 17, l'environnement est composé des hôtes (pcs bureau ou portable), des serveurs (Windows et Linux) et des équipements réseaux (commutateurs, routeurs, points d'accès et pare feu). Nous avons testé le réseau interne de l'entreprise ainsi que son site web public, qui est accessible depuis Internet.

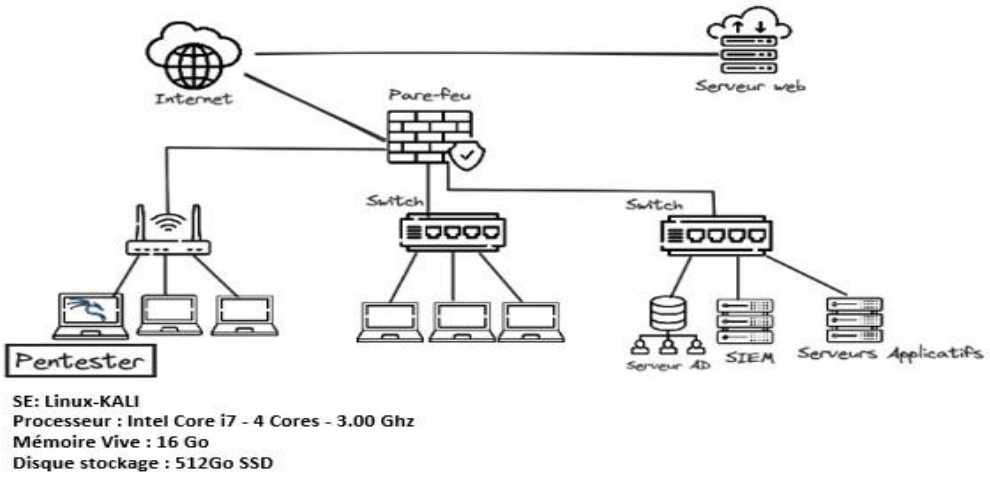

Figure 18: Environnement de test

5.2 Scénarios de test

En respectant les lois et les réglementations en matière de sécurité des données, de confidentialité et de protection des informations sensibles, nous nous sommes assurés de mener les tests dans le respect des politiques et des obligations légales en vigueur. Et c'est pourquoi, nous allons masquer la configuration du réseau de l'entreprise MNA Groupe dans les figures de cette section où nous allons simuler les techniques choisies.

5.2.1 Collecte des propriétés du domaine(T1590.001)

Une fois que le Pentester a sélectionné la technique de "Collecte des propriétés du domaine" parmi les différentes options disponibles, un formulaire lui est présenté afin de recueillir les informations nécessaires. Ce formulaire permet au Pentester de saisir le domaine cible (exemple.com) pour lequel il souhaite collecter différentes informations, telles que l'adresse IP associée au domaine, le registre du domaine, la date d'enregistrement et la date d'expiration du domaine, et d'autres détails pertinents. Cependant, il est important de noter que, pour des raisons de confidentialité, il n'est pas toujours possible de recueillir des informations telles que les adresses e-mail et les numéros de téléphone liés au domaine.

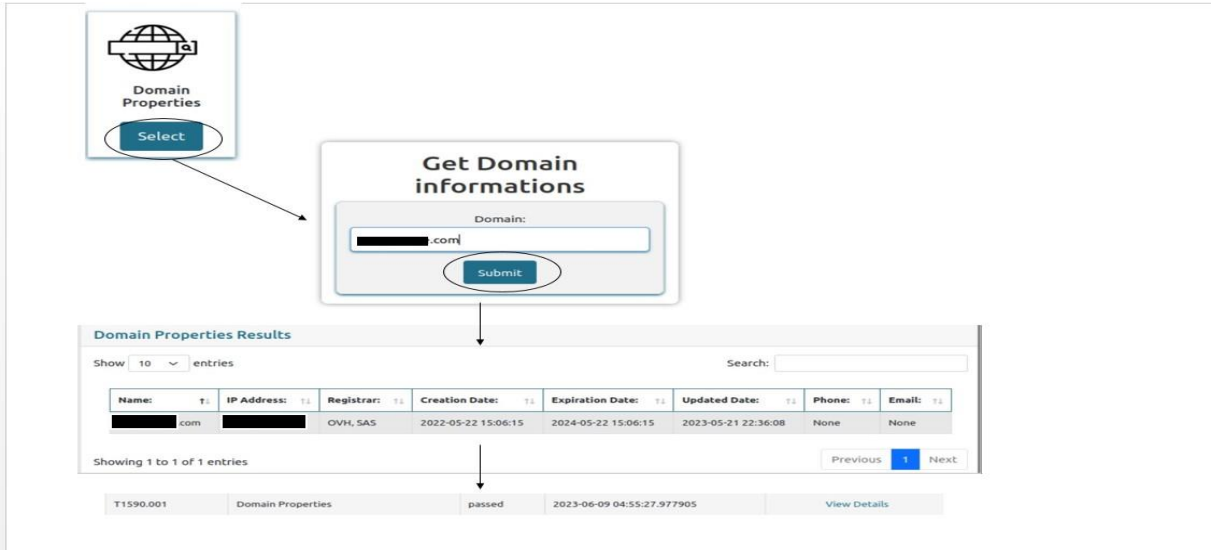

Figure 19:Scenario de test (Propriétés du domaine)

5.2.2 Reconnaissance DNS

Cette technique permet au Pentester de collecter des informations relatives au DNS en saisissant un domaine donné, tel que "exemple.com", dans un formulaire dédié. Une fois que le Pentester soumet le domaine, l'application lance une analyse DNS pour récupérer les différents enregistrements associés à ce domaine. Cela peut inclure entre autres des enregistrements A (adresses IP), des enregistrements MX (serveurs de messagerie), des enregistrements NS (serveurs de noms), des enregistrements TXT (informations de texte). Les informations collectées fournissent au Pentester une compréhension approfondie de la configuration du DNS pour le domaine spécifié. Ces données peuvent être utilisées pour évaluer la sécurité du DNS, identifier d'éventuelles vulnérabilités et prendre des mesures pour renforcer la résilience du système.

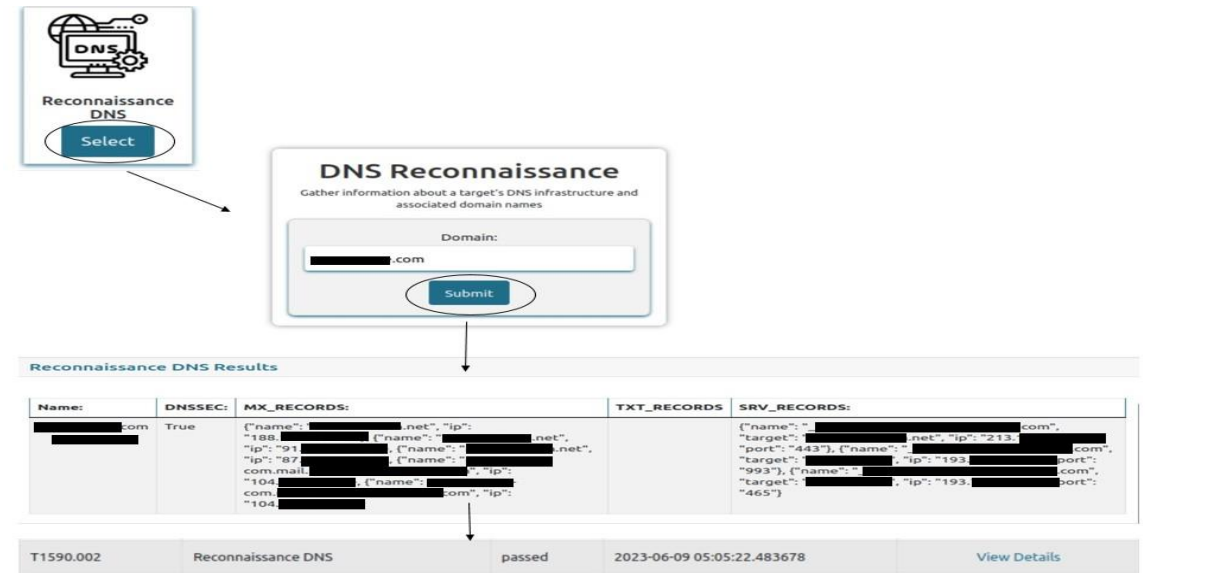

Figure 20:Scenario de test (Reconnaissance DNS)

5.2.3 Collecte des AdressesIP

Un formulaire est mis à la disposition du Pentester pour qu'il puisse saisir l'adresse réseau souhaitée, par exemple, 192.168.254.0 /24. En utilisant cette information, le Pentester lance une analyse qui lui permet de collecter les adresses IP associées à ce réseau, ainsi que les adresses MAC correspondantes et les fournisseurs des machines. Ces données fournissent une vue approfondie des actifs présents sur le réseau, facilitant ainsi l'identification d'éventuelles vulnérabilités et la prise de mesures appropriées pour renforcer la sécurité. Cette technique de collecte des adresses IP et des adresses MAC offre au Pentester une visibilité essentielle pour une évaluation complète de l'environnement réseau et une identification précise des machines actives.

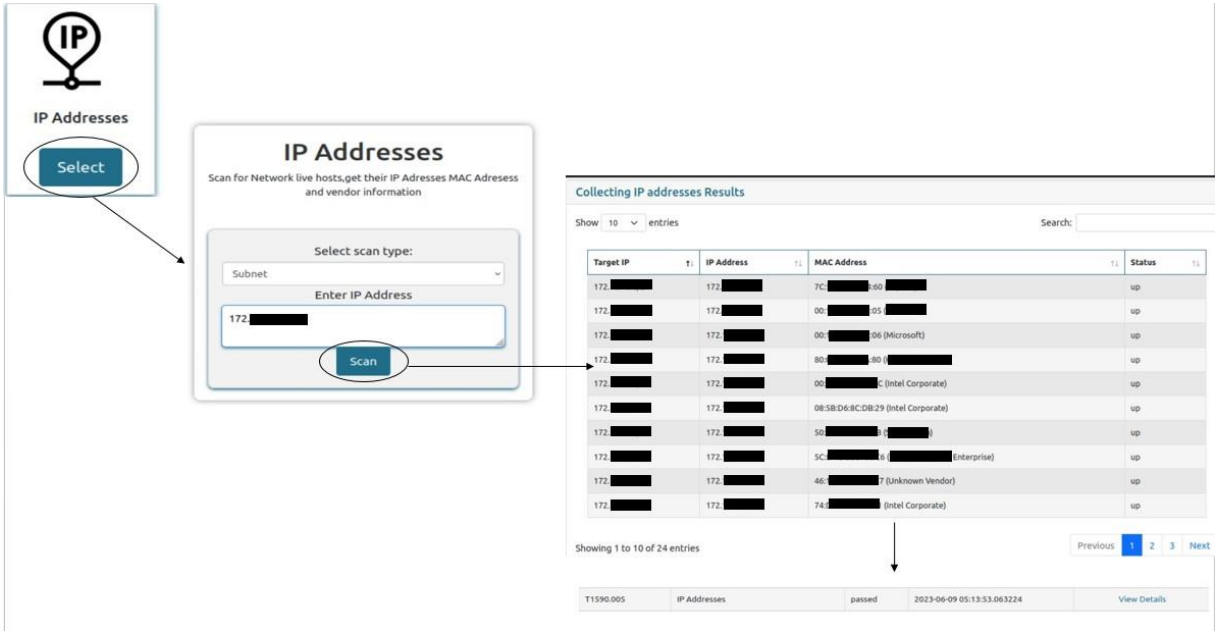

Figure 21:Scenario de test (Collect des addresses IP)

5.2.4 Découverte d'informations sur le système

Cette technique permet au Pentester d'explorer et de collecter des informations sur une machine spécifique en saisissant son adresse IP dans un formulaire dédié. Lors de cette phase, le Pentester a la possibilité de régler le niveau d'agressivité du scan, allant de T1 à T4, afin d'adapter l'intensité du processus de découverte. De plus, le Pentester peut choisir le type de scan à effectuer, que ce soit un scan des ports ouverts et de leurs services associés en utilisant les protocoles UDP ou TCP.

Une fois que les paramètres appropriés ont été définis, le Pentester lance le scan. L'application effectue alors une analyse approfondie de la machine cible, en explorant les ports ouverts et les services qui y sont associés. Les résultats obtenus incluent des informations telles que le système d'exploitation de la machine, les ports ouverts et les services actifs. Ces données permettent au Pentester de mieux comprendre la configuration et la topologie du système cible, facilitant ainsi l'identification de potentielles vulnérabilités et la planification des tests de sécurité ultérieurs.

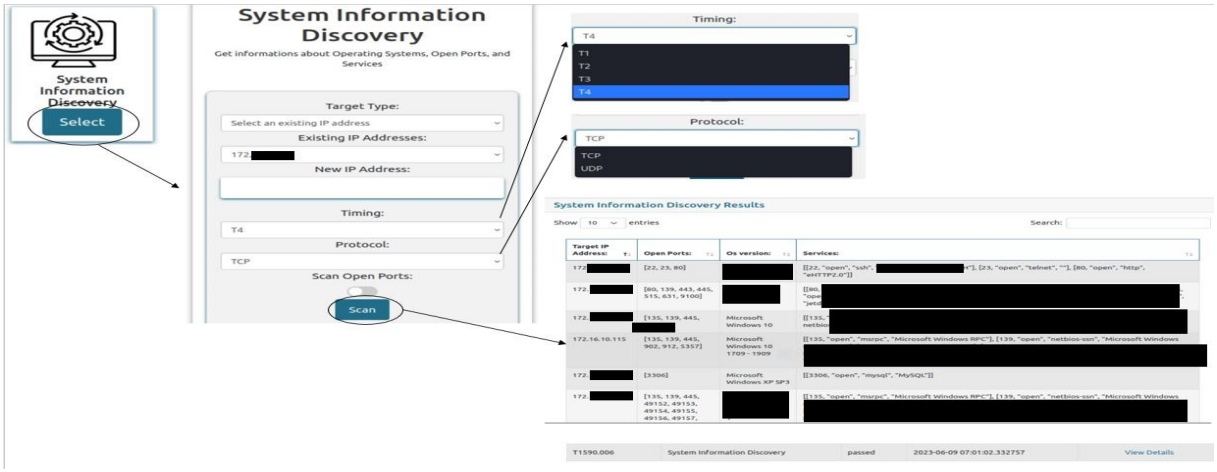

Figure 22: Scenario de test (Découverte d'informations sur le système)

5.2.5 Scan de Vulnérabilités

La technique du Scan de Vulnérabilités permet au Pentester de lancer un scan de vulnérabilités en spécifiant une adresse cible dans un formulaire dédié. Ce scan est conçu pour identifier les failles de sécurité potentielles présentes sur le système cible. Une fois le scan effectué, les résultats obtenus fournissent des informations détaillées sur les CVE (Common Vulnerabilities and Exposures) découvertes lors du processus.

Les résultats du scan de vulnérabilités incluent des informations telles que le CVE-ID, la version CVSS (Common Vulnerability Scoring System), l'impact de la vulnérabilité, la description détaillée de la faille, ainsi que le vecteur d'attaque potentiel. Ces informations permettent au Pentester d'évaluer la gravité des vulnérabilités identifiées et de prendre des mesures appropriées pour les corriger ou les atténuer.

L'objectif principal de la technique du scan de vulnérabilités est de fournir une évaluation complète des vulnérabilités du système cible, permettant ainsi de renforcer la sécurité et de réduire les risques potentiels.

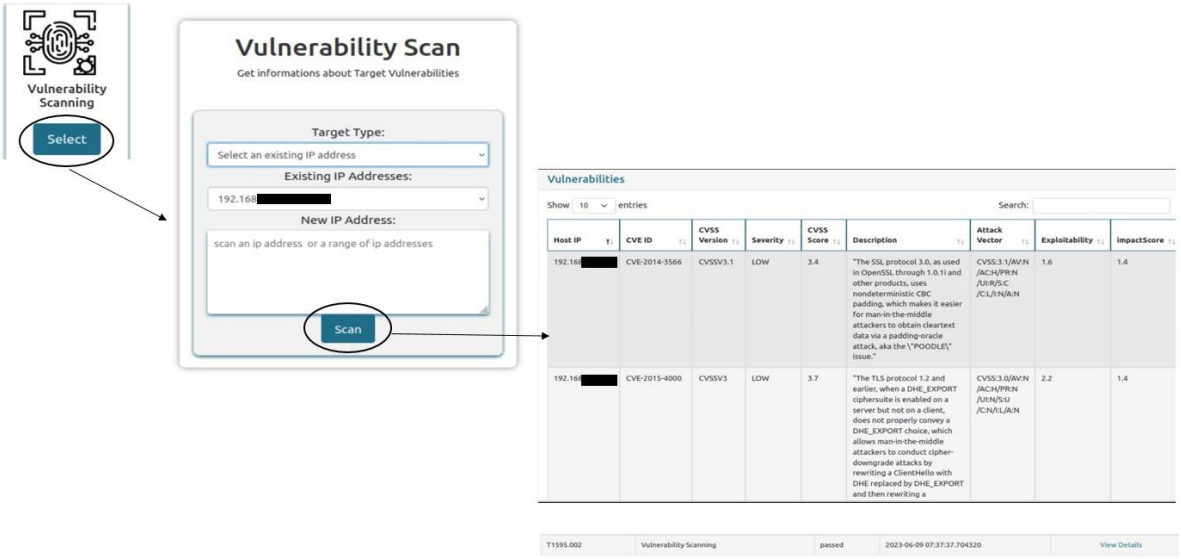

Figure 23:Scenario de test (Scan de vulnérabilités)

5.2.6 Empoisonnement du cache ARP

Dans cette attaque, le Pentester utilise un formulaire pour spécifier l'adresse IP de la cible et l'adresse IP de la passerelle. L'objectif de l'attaque d'empoisonnement du cache ARP est de tromper les systèmes cibles en leur faisant croire que l'adresse MAC associée à l'adresse IP de la passerelle est celle contrôlée par le Pentester. Ainsi, lorsque la machine cible reçoit une réponse ARP falsifiée prétendant provenir de la passerelle légitime, elle met à jour son

cache ARP en associant l'adresse IP de la passerelle à l'adresse MAC falsifiée. Cela permet au Pentester de rediriger le trafic destiné à la passerelle vers une machine contrôlée, lui donnant ainsi la possibilité de surveiller, intercepter ou modifier les paquets transitant entre la cible et la passerelle.

Figure 24:Scenario de test (d'Empoisonnement du cache ARP)

Dans le cadre de l'attaque, le Pentester peut utiliser des outils tels que Wireshark[9] pour l'analyse des paquets et la surveillance du trafic réseau. L'analyse des paquets capturés avec Wireshark permet au Pentester de surveiller les échanges entre la cible et d'autres machines du réseau, d'identifier les informations sensibles qui sont transmises, de détecter des anomalies ou des comportements suspects, et d'intercepter les paquets.

[9] **Wireshark** est un outil d'analyse de réseau open-source. Il permet de capturer, d'analyser et de visualiser le trafic réseau en temps réel, offrant ainsi des informations détaillées sur les protocoles, les paquets et les données échangées sur le réseau. [33]

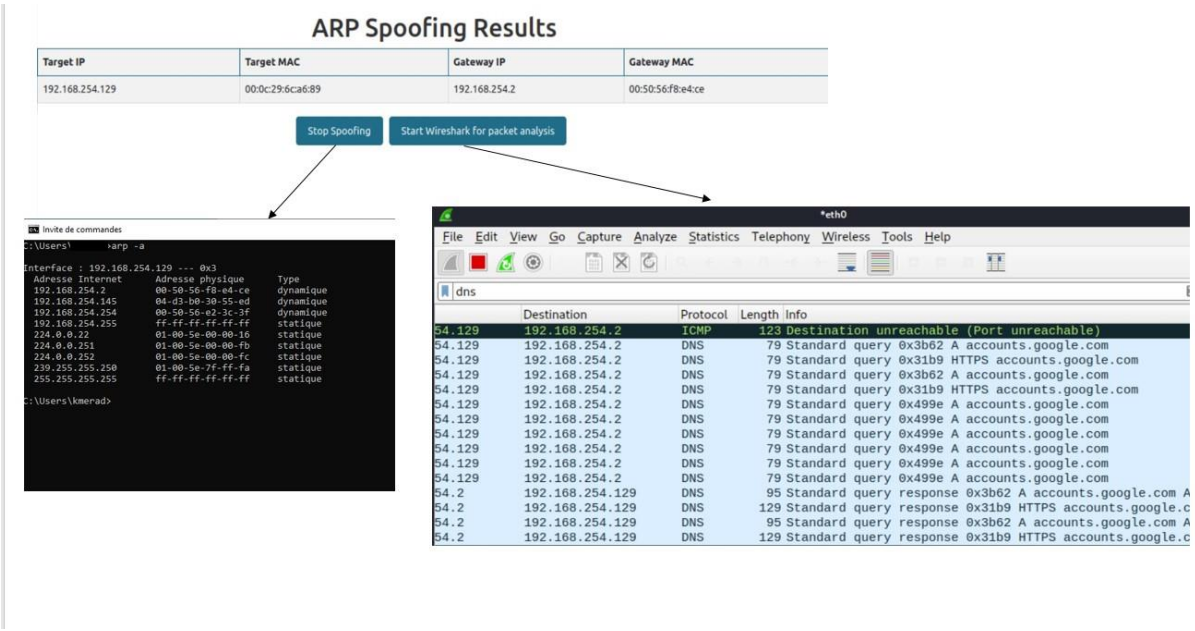

Figure 25:Analyse des paquets

5.2.7 Génération de rapport

Dans la phase finale du test, le Pentester peut générer un rapport détaillé regroupant les résultats des différentes techniques utilisées. Ce rapport comprend une analyse complète des vulnérabilités identifiées, les résultats des scans effectués, les informations sur les adresses IP et le système, ainsi que d'autres détails pertinents. Chaque technique est documentée en détail, offrant une vue d'ensemble des résultats obtenus. De plus, le rapport contient des recommandations spécifiques pour améliorer la sécurité du système en remédiant aux vulnérabilités détectées.

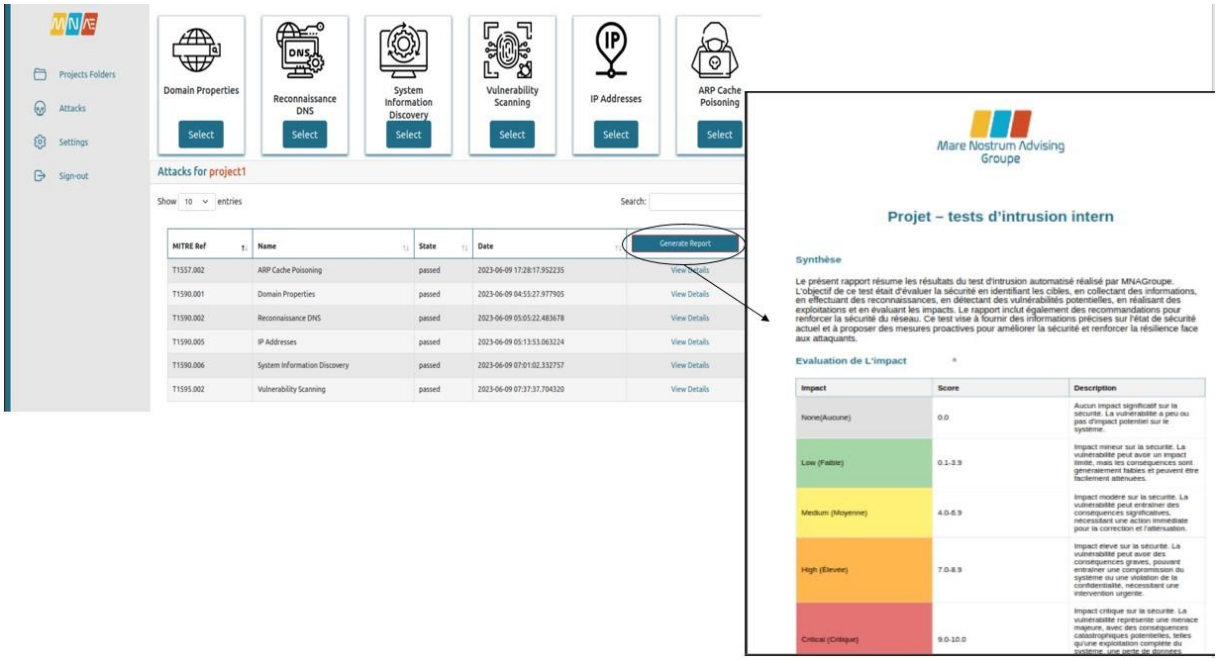

Figure 26:Generation de rapport

Le rapport présente également une échelle d'évaluation de l'impact des vulnérabilités sur la sécurité, en se basant sur les catégories de scores et les descriptions correspondantes. Voici une explication plus détaillée de chaque catégorie (Table 8)

Impact	Description
None(Aucune)	Cette catégorie indique qu'il n'y a aucun impact significatif sur la sécurité. La vulnérabilité en question a peu ou pas d'impact potentiel sur le système.
Low (Faible)	Une vulnérabilité classée comme "Faible" a un impact mineur sur la sécurité. Bien qu'elle puisse avoir un impact limité, les conséquences sont généralement faibles et peuvent être facilement atténuées.
Medium (Moyenne)	Les vulnérabilités classées comme "Moyenne" ont un impact modéré sur la sécurité. Elles peuvent entraîner des conséquences significatives, nécessitant une action immédiate pour la correction et l'atténuation.
High (Elevée)	Les vulnérabilités classées comme "Élevée" ont un impact élevé sur la sécurité. Elles peuvent avoir des conséquences graves, pouvant entraîner une compromission du système ou une violation de la confidentialité. Une intervention urgente est nécessaire pour les traiter.
Critical (Critique)	Les vulnérabilités classées comme "Critique" représentent une menace majeure pour la sécurité. Elles ont des conséquences catastrophiques potentielles, telles qu'une exploitation complète du système, une perte de données sensibles ou un accès non autorisé à des informations sensibles. Ces vulnérabilités nécessitent une attention et une intervention immédiate.

Table 8 : Les échelles de la difficulté d'exploitation

6 Conclusion

En conclusion, ce chapitre a fourni une vue d'ensemble de notre application en mettant l'accent sur ses fonctionnalités, son environnement de développement et de test, ainsi que ses interfaces. De plus, nous avons effectué des tests d'intrusion interne en utilisant une approche de type boîte grise, illustrant les attaques mises en œuvre et les résultats obtenus.

CONCLUSION GÉNÉRALE & PERSPECTIVES

En conclusion, ce projet de fin d'études sur le développement d'un outil d'assistance aux tests d'intrusion dans un environnement d'entreprise a été mené en suivant une approche méthodique et rigoureuse. Nous avons réalisé une étude bibliographique approfondie pour acquérir les connaissances nécessaires à la conception de notre solution. Dans notre premier chapitre, nous avons exploré les fondamentaux des tests d'intrusion, y compris les différents types et équipes impliquées, ainsi que les méthodologies telles que le PTES et MITRE ATT&CK. Nous avons également examiné les outils de tests existants pour comprendre leur fonctionnement et identifier les lacunes. Dans le deuxième chapitre, nous avons décrit en détail notre solution, mettant en évidence le processus suivi, les tactiques, techniques et procédures (TTPs) que nous avons sélectionnées, ainsi que les fonctionnalités de notre application à travers les diagrammes UML. Cette étape nous a permis de concevoir une solution complète et adaptée aux besoins des Pentesters. Dans le troisième chapitre, nous avons présenté les outils que nous avons utilisés pour développer notre application, les procédures que nous avons mises en place, ainsi que les tests effectués et les résultats obtenus. Nous avons également inclus une discussion approfondie sur ces résultats, ce qui nous a permis d'évaluer l'efficacité de notre solution.

En résumé, notre outil offre aux Pentesters la capacité d'adopter les tactiques, techniques et procédures utilisées par les acteurs malveillants pour détecter les vulnérabilités dans les configurations de l'infrastructure avant qu'un adversaire ne les exploite. Il permet également aux Pentesters d'économiser du temps en automatisant les tâches répétitives, tout en offrant une exploitation manuelle pour une flexibilité maximale. La génération de rapports détaillés assure un suivi précis et détaillé des activités de test d'intrusion.

Parmi les exigences que nous avions fixées dès le début du projet, nous sommes parvenus à respecter l'objectif d'extensibilité de la solution proposée. Cependant, il est important de souligner que tout projet peut toujours bénéficier d’améliorations, Des perspectives d’amélioration et d’extension peuvent donc être envisagées afin d’enrichir et améliorer, dans l’avenir, notre solution. Nous proposons :

- Enrichir l'outil avec plus de tactiques, techniques et procédures de la base de connaissances MITRE ATT&CK, notamment dans la phase d'exploitation.
- Elargir le périmètre de notre outil afin de permettre la simulation d'attaques sur des machines Linux et des machines Windows.
- Améliorer le développement sécurisé de l’application et renforcer les lignes de sécurité.
- Ajouter une documentation afin d’expliquer comment utiliser cette application par l’utilisateur.
- Améliorer les interfaces afin d'offrir aux utilisateurs une meilleure expérience.

Références

[1] *CSRC Content Editor. (s. d.). cybersecurity - Glossary | CSRC. Consulté le 6 juin 2023, à l'adresse https://csrc.nist.gov/glossary/term/cybersecurity*

[2] Executive Summary — NIST SP 1800-25 documentation. (s. d.). Consulté le 2 juin 2023, à l'adresse https://www.nccoe.nist.gov/publication/1800-25/VolA/index.html

[3] CrowdStrike. (2023, 8 juin). *What is Spoofing ? Spoofing Attacks Defined - CrowdStrike*. crowdstrike.com. Consulté le 13 juin 2023, à l'adresse https://www.crowdstrike.com/cybersecurity-101/spoofing-attacks/

[4] *Erickson, J. (2003). Hacking : The Art of Exploitation. O'Reilly Japan.*

[5] *Dorigny, M. (2022, 12 septembre). Cybersécurité : Qu'est ce que la défense en profondeur ? IT-Connect. Consulté le 24 janvier 2023, à l'adresse https://www.it-connect.fr/cybersecurite-defense-en-profondeur/.*

[6] *National Institute of Standards and Technology (NIST). (2013). Technical Guide to Information Security Testing and Assessment (Special Publication 800-115). Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf*

[7] Red Team vs. Blue Team in Cybersecurity. (2022, 1 novembre). Coursera. Consulté le 17 janvier 2023, à l'adresse https://www.coursera.org/articles/red-team-vs-blue-team RED TEAM

[8] Red Team vs. Blue Team vs. Purple Team Compared – What's the Difference ? (2022, 11 décembre). US Cybersecurity Inc. Consulté le 17 janvier 2023, à l'adresse https://www.uscybersecurity.com/blogs/red-team-vs-blue-team-vs-purple-team BLEUE

[9] What Is the Purpose of the Purple Team ? (2022, 30 novembre). Coursera. Consulté le 17 janvier 2023, à l'adresse https://www.coursera.org/articles/purple-team

[10] Red Team Development and Operations. (s. d.-b). Consulté le 4 février 2023, à l'adresse https://redteam.guide/docs/definitions/

[11] *Zenko, M., & Lane, C. (2016). Red Team: How to Succeed By Thinking Like the Enemy (Unabridged). Brilliance Audio.*

[12] *What is Penetration Testing ? Types and Benefits. (s. d.). Fortinet. Consulté le 25 janvier 2023, à l'adresse https://www.fortinet.com/resources/cyberglossary/penetration-testing*

[13] *Keshri, A. (2022, 25 avril). NIST Penetration Testing : Guide,Framework and How to Achieve Security Compliance. Astra Security Blog. Consulté le 29 janvier 2023, à l'adresse https://www.getastra.com/blog/security-audit/automated-penetration-testing/*

[14] *Kiprin, B. (2022, 26 septembre). Automated Penetration Testing .Benefits and Tools. Crashtest Security. Consulté le 4 juin 2023, à l'adresse https://crashtest-security.com/best-automated-penetration-testing/.*

[15] *Cyber Kill Chain®. (s. d.). Lockheed Martin. Consulté le 4 juin 2023, à l'adresse https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html*

[16] The Penetration Testing Execution Standard. (s. d.). Consulté le 30 mai 2023, à l'adresse http://www.pentest-standard.org/index.php/Main_Page

[17] *CrowdStrike. (2022b, octobre 13). What is the Mitre Attack Framework ? | CrowdStrike. crowdstrike.com. Consulté le 24 janvier 2023, à l'adresse https://www.crowdstrike.com/cybersecurity-101/mitre-attack-framework/*

[18] *Network Penetration Testing for 2023 | vPenTest. (s. d.). Vonahi Security : Automated Penetration Testing & Cyber Security Services. Consulté le 28 janvier 2023, à l'adresse https://www.vonahi.io/services/network-penetration-testing*

[19] *Comprehensive Penetration Testing to Prioritize Risks That Matter. (s. d.). Consulté le 29 janvier 2023, à l'adresse https://www.coresecurity.com*

[20] *HTML (HyperText Markup Language) | MDN. (2022, 17 octobre). Consulté le 1 juin 2023, à l'adresse https://developer.mozilla.org/fr/docs/Web/HTML*

[21] *CSS : Feuilles de style en cascade | MDN. (2022, 21 septembre). Consulté le 1 juin 2023, à l'adresse https://developer.mozilla.org/fr/docs/Web/CSS*

[22] *JavaScript | MDN. (2022, 21 septembre). Consulté le 1 juin 2023, à l'adresse https://developer.mozilla.org/fr/docs/Web/JavaScript*

[23] *Bootstrap Get Started. (s. d.). Consulté le 1 juin 2023, à l'adresse https://www.w3schools.com/bootstrap/bootstrap_get_started.asp*

[24] *Welcome to Python.org. (2023, 31 mai). Python.org. Consulté le 1 juin 2023, à l'adresse https://www.python.org/*

[25] *Welcome to Flask — Flask Documentation (2.3.x). (s. d.). Consulté le 1 juin 2023, à l'adresse https://flask.palletsprojects.com/en/2.3.x/*

[26] *SQLite Home Page. (s. d.). Consulté le 1 juin 2023, à l'adresse https://sqlite.org/index.html.*

[27] *SQLAlchemy. (s. d.). Consulté le 1 juin 2023, à l'adresse https://www.sqlalchemy.org/*

[28] *Whois.com - Free Whois Lookup*. (n.d.). Retrieved June 13, 2023, from https://www.whois.com/whois/

[29] *dnsrecon | Kali Linux Tools*. (n.d.). Kali Linux. Retrieved June 13, 2023, from https://www.kali.org/tools/dnsrecon/

[30] *Scapy. (s. d.). Consulté le 1 juin 2023, à l'adresse https://scapy.net/*

[31] *Nmap : the Network Mapper - Free Security Scanner. (s. d.-b). Consulté le 1 juin 2023, à l'adresse https://nmap.org/*

[32] *NVDLib : : NVDLib : NIST National Vulnerability Database API Wrapper. (s. d.). Consulté le 1 juin 2023, à l'adresse https://nvdlib.com/en/latest/*

[33] Wireshark · Go Deep. (s. d.). Wireshark. Consulté le 13 juin 2023, à l'adresse https://www.wireshark.org/

Annexes

1 Présentation de l'organisme d'accueil

Mare Nostrum Advising Groupe est une entreprise renommée dans le domaine de la sécurité de l'information. Dotée d'une équipe de professionnels hautement qualifiés et expérimentés, ellese distingue par sa spécialisation en audit, conseil et accompagnement en cybersécurité.

Implantée dans plusieurs régions stratégiques, notamment en France (Paris et Marseille), en Afrique du Nord (Algérie) et en Afrique de l'Ouest (Sénégal), l'entreprise est en mesure de répondre aux besoins de sa clientèle dans ces différentes zones géographiques.

Mare Nostrum Advising Groupe dispose également d'une structure dédiée et certifiée QUA- LIOPI, connue sous le nom de « MN Advising Cert », qui offre des programmes de formation de haut niveau. Grâce à leur expertise et à l'utilisation d'outils adaptés, les consultants de l'entreprise sont en mesure de former efficacement les collaborateurs des organisations clientes, en améliorant leurs compétences en matière de sécurité de l'information.

2 Services offerts par Mare Nostrum Advising Groupe

- **Stratégie et gouvernance Cybersécurité**
  - Apport d'expertise aux Directions Générales.
  - Évaluation de la maturité Cybersécurité ou Privacy de l'entreprise.
  - Définition de schémas directeurs et de roadmaps Cyber.
  - Mise en place de SMSI (ISO 27 00x).
  - Optimisation du pilotage et reporting Cyber.
- **Cyber résilience et gestion de crise**
  - Définition de stratégie et de plan de continuité ou de reprise d'activité.
  - Revue de la cyber résilience de l'entreprise ou d'un processus métier.
  - Accompagnement à la réponse aux incidents Cybersécurité.
  - Accompagnement à la mise en place d'une gestion de crise.
- **Accompagnement de la fonction Cybersécurité**
  - Définition de fonctions Cyber d'excellence.

- Mise en œuvre de programmes de Cybersécurité.
- Aide au choix et déploiement d'outils, services, solutions Cyber.
- Accompagnement à la mise en place d'une cyber assurance.
- Sécurisation des projets.
- Sensibilisation à la cybersécurité.

- **Gestion des risques Cybersécurité**
  - Cartographies globales des risques et des menaces Cyber.
  - Classification des actifs.
  - Analyse de risques Cyber : entreprise / IT / projet.
  - Analyse de l'évolution des menaces (Threat Intelligence).
- **Audit Cybersécurité**
  - Audit des fonctions Cybersécurité.
  - État des lieux du niveau de sécurité du SI.
  - Audit Cybersécurité de tiers (fournisseurs, prestataires, hébergeurs).
  - Audit des accès et revue des habilitations.