RÉPUBLIQUE TUNISIENNE
MINISTÉRE DE L'ENSEIGNEMENT SUPÉRIEUR
ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITÉ DE CARTHAGE

INSTITUT SUPÉRIEUR DES TECHNOLOGIES DE
L'INFORMATION ET DE LA COMMUNICATION

RAPPORT DE PROJET DE FIN D'ETUDES

**Présenté en vue de l'obtention de la**
LICENCE FONDAMENTALE EN SCIENCES ET TECHNOLOGIES

**Mention : Sciences de l'Informatique**
**Spécialité : Sciences de l'Informatique**

# Création des scripts d'analyse des rapports de pentest

*Par*
NADIM NAGATI & AMENI HAZEMI

Réalisé au sein de la société O2

Soutenu publiquement le 24 mai 2021 devant le jury composé de :

| | |
|---|---|
| Président : | Prénom NOM, University Relations Leader, IBM |
| Rapporteur : | Prénom NOM, Enseignant, ISTIC |
| Examinateur : | Prénom NOM, Enseignant, ISTIC |
| Encadrant professionnel : | Yann Chartier, Résponsable de sécurité d'intormations , O2 |
| Encadrant académique : | Wassim Abessi, Enseignant, ISTIC |

Année Universitaire : 2020-2021

RÉPUBLIQUE TUNISIENNE
MINISTÉRE DE L'ENSEIGNEMENT SUPÉRIEUR
ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITÉ DE CARTHAGE

INSTITUT SUPÉRIEUR DES TECHNOLOGIES DE
L'INFORMATION ET DE LA COMMUNICATION

RAPPORT DE PROJET DE FIN D'ETUDES

**Présenté en vue de l'obtention de la**
LICENCE FONDAMENTALE EN SCIENCES ET TECHNOLOGIES

**Mention : Sciences de l'Informatique**
**Spécialité : Sciences de l'Informatique**

# Création des scripts d'analyse des rapports de pentest

*Par*
NADIM NAGATI & AMENI HAZEMI

Réalisé au sein de la société O2

**AUTORISATION DE DÉPÔT DU RAPPORT DE PROJET DE FIN D'ETUDES :**

| | |
|---|---|
| Encadrant professionnel : | Encadrant académique : |
| Le : | Le : |
| Signature : | Signature : |

# Table des matières

# Table des figures

# Liste des tableaux

# Liste des abréviations

— O2 :

# Dédicaces

**A mes parents**

Pour tous leur amour , leur tendresse, leur soutien et leur sacrifice tout au long de mes études.

**A mes frères et soeurs**

Pour leur encouragement et surtout pour leur soutien moral. Je vous souhaite un bon avenir plein de joie, de bonheur et de réussite .

**A mes amis**

Je vous remercie pour tous les moments et les aventures que nous avons vécu ensemble pendant toute ces années et je vous souhaite tout le bonheur et tout le succés du monde.

**Ameni Hazemi**

**Je dédie ce travail :**

A mes parents, qui ont toujours été là pour moi. Pour tout les sacrifices que vous aviez fait pour moi, jamais je ne l'oublierai. Vous avez été mon soutien, ma source d'inspiration et mon bonheur. C'est grâce â vous que j'ai pu en arriver lá.

A mon petit frère, petit taquineur que tu es, tu n'as raté aucune chance pour m'embeter mais je sais très bien que c'est ta manière de me montrer ton affection. Mes journées seraient tellement ennuyeuse sans toi ! Je n'aurais pas pu avoir mieux comme frangin.

A ma meilleure amie, Inès, tu as été la personne la plus supportive et celle qui m'a aidé le plus. Je voudrais t'offrir ce travail qui n'aurait jamais vu le jour sans ton aide.

*Nadim Nagati*

# Remerciements

On profite par le biais de ce rapport, d'exprimer nos remerciements les plus chalheureux à toute personne qui a participé à l'elaboration de ce travail que ce soit de près ou de loin.

On tient à remercier dans un premier temps, monsieur Wassim Abassi, notre encadreur académique. On le remercie pour tout le soutien qu'il nous a apporté et pour nous avoir remis sur les rails à chaque fois que nous dévions.

On présente nos sincères gratitudes à monsieur Yann Chartier, notre encadreur professionel, pour nous avoir suivi et soutenu tout au long de cette periode. On a appris beaucoup de choses à ses cotés et sans lui, ce travail n'aurait pas pu aboutir.

Finalement, on tient apporter nos remerciements à tout les membres de O2, qui malgré la distance qui nous sépre, ont su nous montrer leur bienveillance. Nous remercions également tout nos professeurs de l'institut, qui ont toujours été présent pour nous et qui nous ont guider tout au long de cette année universitaire.

# Introduction Générale

Nul ne peut nier que la sécurité informatique est un domaine qui prend de plus en plus d'ampleur chez les entreprises d'ou une bonne entreprise est celle qui présente une bonne sécurité informatique et assure que ces ressources matérielles ou logicielles sont uniquement utilisées dans le cadre prévu .

Un test d'intrusion (pentest) est une étape clé dans le processus de renforcement du niveau de cyber-sécurité de toute entreprise. En confrontant les protections mise en place á une épreuve réelle, le pentest permet d'identifier trés concrétement les risques et d'apporter des réponses opérationnelles d'ou le résultat final d'un pentest est un rapport présentant les vulnérabilités ainsi que la façon de les corriger . Le résultat du pentest est un niveau de protection pour l'entreprise qui investit dans un pentest afin de diminuer son niveau d'exposition au risque et de renforcer sa valeur.

l'utilisation de différent outils de pentest et la récupération de différent rapport puis l'agrégation des rapports en un seul pour a la fin analyser les correction appropriés prend beaucoup de temp et effort . Durant notre stage de projet de fin d'étude notre mission est de mettre en place la réalisation des scripts d'analyse des rapports de pentest afin de facilité la recupération des rapports de pentest et diminuer le temp de réponse pour facilité cette tâche.

Afin de mieux exposer notre projet, nous présentons les éléments de notre solution dans ce présent rapport qui est composé de trois chapitres :

— Le premier chapitre va présenter le cadre général de notre projet en commençant par l'organisme d'accueil, ensuite l'étude préalable .

— Le deuxiéme chapitre va présenter l'environnement de travail , ses avantages et les outils choisie .

— Le dernier chapitre va présenter la partie de réalisation de notre solution .

# Chapitre 1

# Cadre général de projet

## 1.1 Introduction

Dans ce chapitre nous allons présenté le cadre général de notre projet . Tout d'abord nous commencant par présenté l'organisme d'acceuil ensuite l'étude préalable .

## 1.2 Présentation de l'organisme d'accueil

Nous introduisons dans cette partie la présentation de la société O2 et ses services .

### 1.2.1 Présentation

L'origine de l'entreprise O2 remonte á 19961 avec la création respective á Lille et á Paris des sociétés Unipôles et At Home. En 2007, le groupe compte désormais une présence nationale avec 93 agences succursalistes et avec un peu moins de 2 000 salariés.
Deux ans plus tard, l'entreprise signe une convention de partenariat avec le Pôle emploi et le Ministére de l'économie, de l'industrie et de l'emploi puis en 2010, elle signe une convention nationale avec l'Agefiph .
En 2012, l'entreprise ouvre un réseau de franchises et elle fonde un institut de recherches.
En 2015, le groupe compte 150 agences succursalistes et 75 franchises. En 2016, le groupe O2 acquiert Apef Services, entreprise basé á Montpellier qui avait un chiffre d'affaires de 43 millions d'euros, comparé á celui de O2 qui était de 152 millions d'euros.
Fin 2016, le groupe se renomme Oui Care. En août 2017, Oui Care annonce l'acquisition d'Interdomicilio, une entreprise espagnole de services à la personne employant 450 personnes également présent au Portugal et en Amérique latine .[1]

### 1.2.2 Fiche d'identité

**Raison sociale** :Société française de services á domicile .

**Activité** :Services á domicile de ménage-repassage , garde d'enfant, accompagnement pour les seniors et personnes dépendantes , jardinage et bricolage.

**Siege social** :85 boulevard Marie et Alexandre Oyon CS85533 72055 Le Mans Cedex 2 .

**Téléphone** :+33 02 43 72 02 02

**Site web** : www.o2.fr

### 1.2.3 Les services

La société o2 propose plusieurs type de services dans les domaines suivants :

1. Garde d'enfant
2. Accompagnement du handicap
3. Soutien scolaire
4. Ménage et repassage á domicile
5. Jardinage
6. Bricolage
7. Aide aux personnes âgées

## 1.3 Étude Préalable

Nous allons commencer par expliquer tout d'abord le pentest , ensuite nous présenterons la méthode utilisée par la société et enfin la solution proposée.

### 1.3.1 Pentest

Nous allons commencer par présenté le pentest ensuite les on va cité les phases et les types de pentest.

#### Présentation

Un test d'intrusion (pentest) est une méthode importante pour le renforcement du niveau de sécurité de toute entreprise d'ou il permet d'analyser une cible qui peut être une ip , une application , un réseau complet ou un serveur web et d'identifier dans un rapport détaillé les risques , les faiblesses , les vulnérabilité et propose des mesures correctives pour corriger les failles trouvées .

#### Objectifs de faire les pentest

Les objectifs sont :

1. Connaître les vulnérabilités des aplications et systéme informatique
2. Évaluer le degré de risque des failles trouvée
3. Proposer des correctifs [2]

**Quand faire un pentest**

Les pentest peuvent être fait a différents situations :

1. Lors de conception d'un nouveau projet pour eliminer les eventuelles attaques
2. Pendant l'utilisation de la cible
3. Suite á une cyberattaque afin que ça ne se reproduise pas . [3]

**Les phases de réalisation d'un pentest**

La réalisation d'un pentest se résume en 4 phases que nous allons présenter et expliquer :

1. Phase de planification : cette phase consiste a définir notre cible
2. Phase de découverte : cette phase consiste a choisir le bon outil et découvrir son fonctionnement pour la réalisation du pentest sur notre cible
3. phase d'attaque : cette phase consiste a scanner la cible par l'outil choisie
4. Phase de rapport : cette phase consiste á analyser le rapport fourni par l'outil de pentest a la fin du scann afin de corriger les vulnérabilités trouvées .

**Les types de pentest**

Voici les 3 type de pentest :

1. Test d'intrusion en boite noire :
   C'est un type qui permet d'attaquer une cible sans savoir son fonctionnement interne . Les pentesters connaissent uniquement l'IP ou l'URL de la cible donc ce type laisse une liberté de choix de la cible .

2. Test d'intrusion en boite blanche :
   Dans ce type il faut connaitre le fonctionnement de la cible pour comprendre exactement d'ou proviennent les failles de sécurité .

3. Test d'intrusion en boite grise :
   Dans ce type les pentesters connaissent certaines informations sur la cible et cela permet de comprendre le contexte et faire un test approfondi donc on dit que c'est un test du point de vue d'utilisateur standard .

## 1.4 Méthodologie

Dans cette partie nous allons définir la méthodologie et citer ensuite les méthodologies choisies pour notre travail .

### 1.4.1 Présentation

La méthodologie est une méthode de travail standard et rigoureuse utilisée par l'entreprise pour analyser ses systémes en s'appuyant sur des outils de pentest afin d'optimiser et arriver á ses buts plus rapidement et efficacement .

### 1.4.2 Méthodologie choisie

Nous avons choisie les deux méthodes qui sont les plus appropriée et populaire et qui conviennent par rapport aux outils que nous allons utiliser , d'ou la présentation de ces deux méthodes .

**OSSTMM (manuel de méthodologie de test de sécurité open source) :**

C'est une des normes reconnues comme méthodologie de test d'intrusion réseau afin d'identifier les vulnérabilités pour sécuriser le réseau et ses composants et donner un aperçu de niveau de cybersécurité du réseau avec des solutions qui aide vos intervenants a sécuriser vos réseaux .

**ISSAF (cadre d'évaluation de la sécurité des systémes d'information) :**

Les spécialistes en pentest utilisent la combinaison de différent outils parmis lesquels se trouve ISSAF . C'est une méthodologie pertinente parce qu'elle permet de lier chaque étape d'analyse á un outil particulier qui permet de donner des informations sur les risques ce qui garantit á l'entreprise une sécurité des systémes contre les cyberattaques .

### 1.4.3 Etude de l'existant

Nous avons remarqué qu'au sein de la société O2 le responsable de SI a besoin de faire quotidiennement des pentest avec des différents outils afin d'analyser une cible pour connaitre les vulnérabilités, évaluer les risques et analyser les correctifs appropriés.Cette opération se divise en 3 étapes et dure huit heures Ce qui est fatigant, ennuyeux et prend beaucoup de temps .
Voici la figure ci-dessous présente le temps et les étapes de la méthode utilisée .

### 1.4.4 Solution proposée

Dans le but d'apporter une valeur ajoutée au service informatique de o2, nous allons développer des scripts qui permettent d'automatiser des outils de pentest pour scanner une cible et récupérer enfin un rapport de pentest qui regroupe tout les rapports résultant de chaque outil utilisé et cette solution est rapide et fournit des résultats en un temps minimum qui est de quatre heures au lieu de huit heures .
La figure ci-dessous présente le temp et les étapes de la solution proposée .

| Temps | étape |
|---|---|
| 2 heures | · Lancements des outils de pentest |
| 4 heures | · Récupération des différents rapports .<br>· Analyses des rapports |
| 2 heures | · Agrégation des rapports en un seul<br>· Analyse des corrections appropriés |

FIGURE 1.1 – Les étapes de solution utilisée

| Temps | étape |
|---|---|
| 2 heures | · Lancement des scripts |
| 2 heures | · Analyse des corrections appropriés |

FIGURE 1.2 – Les étapes de solution proposée

## 1.5 Conclusion

Ce chapitre nous a permis d'avoir une idée sur la problématique et la solution proposée . Le prochain chapitre va présenter les outils de pentest .

# Chapitre 2

# Les outils de pentest

## 2.1 Introduction

Dans ce chapitre nous allons présenter notre environnement de travail ainsi que les méthodologies sur lequelles nous allons nous appuyer . Ensuite nous allons présenter les choix des outils de pentest .

## 2.2 Environnement de travail

Dans cette partie nous allons définir notre environnement de travail choisie et citer ses avantages.

### 2.2.1 Présentation de kali linux

Kali linux et appelé aussi boite a outils pour pentest , C'est une distribution GNU/linux basée sur debian et sortie en 13 mars 2013. Cette distribution regroupe tous les outils importants pour réaliser les tests de sécurité du systéme informatique et surtout les tests d'intrusion .

### 2.2.2 Les avantages

Kali linux présente beaucoup d'avantages dont :

- Une grande communauté
- logiciel libre et customisable
- Systéme d'exploitation résistant a toute épreuve
- Espace de travail sécurisé
- Panel d'outils pour les tests d'instrusion

## 2.3 Choix des outils

Le choix des outils dépend de la cible du pentest et puisque nous allons faire des tests d'intrusion sur le réseau , ip ,systéme informatique , nous avons choisir les outils les

plus populaires et qui présentent des interface graphique simple et facile a l'utilisation et qui sont même les plus utilisé par les pentesteurs d'ou ils permettent de faire parfaitement les tests . Nous allons commencer cette partie par la présentation des outils de pentest ensuite nous allons définir ces outils un par un et présenter enfin les fonctionnalités de chacun .

### 2.3.1 Présentation

Les outils de pentest utilisés par les entreprises pour détecter les failles , les vulnérabilités , les faiblesses et même les risques réels d'une cible qui peut être un systéme d'exploitation ,réseau , application , ip ou site web et de recevoir a fin de cette analyse un rapport qui détaille toutes ses informations avec des corrections appropriées afin de corriger les problémes trouvés rapidement et efficacement .

### 2.3.2 Owasp zap

#### Définition

Zed Attack Proxy (zap) est un outil de pentest qui est installé par défaut sur kali linux et il est utilisé pour la sécurité des applications ouvertes (OWASP) . Il est donc trés utilisé par les entreprises et les professionnels pour la sécurité des sites et des applications web afin de détecter les vulnérabilités et les failles .

#### Fonctionnalité de owasp zap

Zap présente 4 modes : safe , standard ,protected et attack . Ce qui nous intrésse c'est le mode attaque car il le permet de scanner les applications et site web et de fournir a la fin de cette scan un rapport qui peut être soit en forme html , markdown , json ou xml .

### 2.3.3 Lynis

#### définition

C'est un logiciel libre , trés complet et populaire , il est disponisble sur ubunto , debian , fedora et openSUSE . Il permet de scanner un systéme en cherchant les erreurs de configuration et les problémes de sécurité .

#### Fonctionnalité de lynis

Lynis permet de rechercher et analyser tous les logiciels installés sur votre ordinateur pour finir par un rapport sous différentes formes qui présentent tous les détails necessaires pour corriger les problémes trouvés et garantir un systéme sécurisé .

### 2.3.4 openVAS

#### Définition

OpenVAS est un outil de sécurité informatique , c'est un fork de nessus , il est developpé par tenable network security , il est né en 2005 lorsque nessus est passé sous licence propriétaire .

#### Fonctionnalité de openVAS

OpenVAS est capable de scanner une machine , un matériel réseau , un ensemble d'équipements , un réseau entier ou globalement tout ce qui présente une adresse et il fournit enfin un rapport de scan sous différentes formes qui présentent les vulnérabilités avec une description et une méthode ou bien un lien pour corriger les problémes détectés .

### 2.3.5 Nikto

#### Définition

Nikto est un outil libre , open-source et trés pratique , il permet de scanner les failles du serveur web et son exécution est trés rapide .

#### Fonctionnalités de nikto

Nikto permet de vérifier la version du serveur , du logiciel si elle est obsoléte et permet aussi de scanner les répertoires qui contiennent les informations sensibles et aussi de tester prés de 6000 fichiers vulnérables et de supporter les connexions ssl .

### 2.3.6 Conclusion

Ce chapitre nous a permis de présenter les méthodologies et les outils de pentest utilisés . La suite de ce document va présenter la réalisation de notre solution .

# Chapitre 3

# Réalisation

## 3.1 Introduction

## 3.2 Conclusion

# Conclusion Générale

Nous espérons que ce document vous a aidé à rédiger votre rapport convenablement. Ce document vise à aider les étudiants à rédiger des rapports en Latex. Ce document vise à aider les étudiants à rédiger des rapports en Latex. Ce document vise à aider les étudiants à rédiger des rapports en Latex. Ce document vise à aider les étudiants à rédiger des rapports en Latex.
Ce document vise à aider les étudiants à rédiger des rapports en Latex.Ce document vise à aider les étudiants à rédiger des rapports en Latex.Ce document vise à aider les étudiants à rédiger des rapports en Latex.
Ce document vise à aider les étudiants à rédiger des rapports en Latex.Ce document vise à aider les étudiants à rédiger des rapports en Latex.Ce document vise à aider les étudiants à rédiger des rapports en Latex.
Ce document vise à aider les étudiants à rédiger des rapports en Latex.Ce document vise à aider les étudiants à rédiger des rapports en Latex.Ce document vise à aider les étudiants à rédiger des rapports en Latex.Ce document vise à aider les étudiants à rédiger des rapports en Latex.
Ce document vise à aider les étudiants à rédiger des rapports en Latex.Ce document vise à aider les étudiants à rédiger des rapports en Latex.
Ce document vise à aider les étudiants à rédiger des rapports en Latex. Ce document vise à aider les étudiants à rédiger des rapports en Latex. Ce document vise à aider les étudiants à rédiger des rapports en Latex. Ce document vise à aider les étudiants à rédiger des rapports en Latex.
Ce document vise à aider les étudiants à rédiger des rapports en Latex.Ce document vise à aider les étudiants à rédiger des rapports en Latex.Ce document vise à aider les étudiants à rédiger des rapports en Latex.
Ce document vise à aider les étudiants à rédiger des rapports en Latex.Ce document vise à aider les étudiants à rédiger des rapports en Latex.Ce document vise à aider les étudiants à rédiger des rapports en Latex.
Ce document vise à aider les étudiants à rédiger des rapports en Latex.Ce document vise à aider les étudiants à rédiger des rapports en Latex.Ce document vise à aider les étudiants à rédiger des rapports en Latex.Ce document vise à aider les étudiants à rédiger des rapports en Latex.
Ce document vise à aider les étudiants à rédiger des rapports en Latex.Ce document vise à aider les étudiants à rédiger des rapports en Latex.
Ce document vise à aider les étudiants à rédiger des rapports en Latex. Ce document vise à aider les étudiants à rédiger des rapports en Latex. Ce document vise à aider les étudiants à rédiger des rapports en Latex. Ce document vise à aider les étudiants à rédiger des rapports en Latex.
Ce document vise à aider les étudiants à rédiger des rapports en Latex.Ce document vise à aider les étudiants à rédiger des rapports en Latex.Ce document vise à aider les

étudiants à rédiger des rapports en Latex.
Ce document vise à aider les étudiants à rédiger des rapports en Latex.Ce document vise à aider les étudiants à rédiger des rapports en Latex.Ce document vise à aider les étudiants à rédiger des rapports en Latex.
Ce document vise à aider les étudiants à rédiger des rapports en Latex.Ce document vise à aider les étudiants à rédiger des rapports en Latex.Ce document vise à aider les étudiants à rédiger des rapports en Latex.Ce document vise à aider les étudiants à rédiger des rapports en Latex.
Ce document vise à aider les étudiants à rédiger des rapports en Latex.Ce document vise à aider les étudiants à rédiger des rapports en Latex.

# Bibliographie

# Bibliographie


[1] Présentation o2 :
https://fr.wikipedia.org/wiki/Oui$_C$$are$
$consultéle$14/04/2021

[2] Objectifs de faire les pentest :
https://theexpert.squad.fr/theexpert/security/le-pentest-en-pratique/
consulté le 20/05/2021

[3] Quand faire un pentest :
https://theexpert.squad.fr/theexpert/security/le-pentest-en-pratique/
consulté le 20/05/2021

[4] Rôle de owasp zap :
https://www.consultingit.fr/en/owasp-zap-et-son-mode-attaque-en-test-de
consulté le 18/04/2021

# Annexe 1