REPUBLIQUE DU CAMEROUN
Paix – Travail – Patrie

MINISTERE DE L'EMPLOI ET DE LA FORMATION PROFESSIONNELLE

SECRETARIAT GENERAL

Projet d'Appui au Développement de l'Enseignement Secondaire et des Compétences Pour la Croissance et l'Emploi

REPUBLIC OF CAMEROON
Peace-Work-Fatherland

MINISTRY OF EMPLOYMENT AND VOCATIONAL TRAINING

SECRETARIAT GENERAL

Secondary Education and Skills Development Support Project

REFERENTIEL DE FORMATION PROFESSIONNELLE

Selon l'Approche Par Compétences (APC)

REFERENTIEL DE METIER-COMPETENCES (RMC)

SECTEUR : NUMERIQUE

METIER : PENTESTER

NIVEAU DE QUALIFICATION : TECHNICIEN SPECIALISÉ

EQUIPE D'ANIMATION DU RAST (RAPPORT D'ANALYSE DE SITUATION DE TRAVAIL)

N°	NOMS ET PRÉNOM	STRUCTURE	QUALIFICATION
1	Mme ZANGA MOUTONG	MINEFOP/IGF	METHODOLOGUE
2	Mme WANKY Evelyne	MINEFOP/IRF Littoral	METHODOLOGUE
3	Mme DJANDA NZUATOM Epse NDO UOH Sylvie	MINEFOP/DFOP	METHODOLOGUE

LISTE DES PARTICIPANTS AU FOCUS GROUP

N°	Noms et Prénoms	Structures	Qualifications
1	OUM Pascal Blaise	ORANGE CAMEROUN	Professionnel
2	NGANKAM NIEGUE FABO Perry	CANAL+	Professionnel
3	MBOG BABA Mathias Cyriaque	WESCO CAMEROON	Professionnel
4	NOKO Armel	CIS_F	Professionnel
5	ELOMBO ELOMBO Paul Patrick	IP_MAC	Professionnel
6	DJEUMENI NGATCHOP Ulrich	GS_TVI	Professionnel

EQUIPE DE REDACTION

Numéros	Noms et Prénoms	Structures	Qualifications
1	Mme DJANDA NZUATOM Epse NDOUOH Sylvie	MINEFOP	Méthodologue
2	M. NGANSOP Henri Michel	DIGITECH	Professionnel
3	M. TAGNE Franck	INFO-SERVICES	Professionnel
4	YALONG OSSENG VICTOR	MINEFOP	Professionnel

TABLE DES MATIÈRES

REMERCIEMENTS

Ce Référentiel de Métier - Compétence (RMC) a été élaboré et sera exploité grâce à l'impulsion de Monsieur ISSA TCHIROMA BAKARY, Ministre de l'Emploi et de la Formation Professionnelle, dans le cadre du développement des Référentiels de Formation Professionnelle selon l'Approche Par Compétences (APC) au Projet d'Appui au Développement de l'Enseignement Secondaire et des Compétences pour la Croissance et l'emploi (PADESCE). Aussi, tenons-nous à exprimer au Ministre de l'Emploi et de la Formation Professionnelle notre profonde gratitude pour cette opportunité offerte qui permettra la normalisation de la formation et la valorisation de la filière Pentester au Cameroun.

En outre, nous saluons et apprécions à sa juste valeur la collaboration avec les différents acteurs de la formation professionnelle (Experts et Entreprises) dans le cadre de l'élaboration du Référentiel Métier Compétence (RMC) et dont l'aide a été déterminante pour la bonne conduite des entretiens et la réalisation des contenus de ce Rapport.

Que ces acteurs consultés, dont les noms figurent sur la liste ci-jointe trouvent ici l'expression de nos remerciements pour leur disponibilité et leurs contributions pertinentes qui seront significatives à la production d'un Référentiel de Formation Professionnelle, de qualité pour le métier de Pentester.

ABREVIATIONS ET ACRONYMES

APC	Approche Par Compétences
APC	Approche par compétence
BT	Brevet de Technicien
CQP	Certificat de Qualification Professionnelle
CVE	Common Vulnerabilities and Exposures
CVE	Common Vulnerabilities and Exposures
DQP	Diplôme de Qualification Professionnelle
DTS	Diplôme de Technicien Spécialisé
Flux RSS	Really Simple Syndication
GIC	Groupement d'Illustrative commune
IAM	Identity and Access Management
IP	Internet Protocol
ISO	International Organization for Standardization
MINEFOP	Ministère de l'Emploi et de la Formation Professionnelle
NIDS	Network Intrusion Detection System
NIST	National Institute of Standards and Technology
OS	Open System
OWASP	Open Web Application Security Project
PAM	Privileged Access Management
RAST	Rapport Analyse de la Situation de Travail
RDP	Remote Desktop Protocol
RF	Référentiel de Formation
RMC	Référentiel de Métier Compétences
SIEM	Security Information and Event Management
SIMDUT	Système d'Information sur les Matières Dangereuses Utilisées au Travail
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SSH	Secure Shell
TCP	Transmission Control Protocol
UEBA	User and Entity Behavior Analytics

VAE	Validation des Acquis de l'Expérience
VAE	Variation d'Acquisition d'Expérience
WAF	Web Application Firewall
XSS	Cross-Site Scripting

LISTE DES PERSONNES CONSULTEES

N°	Noms et Prénoms	Structures	Qualifications
1	OUM Pascal Blaise	ORANGE CAMEROUN	Professionnel
2	NGANKAM NIEGUE FABO Perry	CANAL+	Professionnel
3	MBOG BABA Mathias Cyriaque	WESCO CAMEROON	Professionnel
4	NOKO Armel	CIS_F	Professionnel
5	ELOMBO ELOMBO Paul Patrick	IP_MAC	Professionnel
6	DJEUMENI NGATCHOP Ulrich	GS_TVI	Professionnel

INTRODUCTION

La Stratégie Nationale de Développement du Cameroun (SND30) assure que « la gouvernance est le socle sur lequel repose la transformation structurelle de l'économie du Cameroun, le développement du capital humain ainsi que l'amélioration de la situation de l'emploi. ». Elle prescrit en matière de formation professionnelle de s'orienter vers une ingénierie qui prenne en compte les politiques, les outils d'accompagnement et de planification pédagogiques. Ces politiques et outils doivent être de nature à favoriser la mise en œuvre des démarches de conception, d'organisation, d'exécution et d'évaluation des actions de formation.

Dans cette perspective, le Ministère de l'Emploi et de la Formation Professionnelle a choisi l'Approche Par Compétence (APC) comme méthode pédagogique à appliquer pour l'élaboration des Référentiels de Formation Professionnelle. Cette méthode a comme avantage d'améliorer :

- L'adéquation formation-emploi ;
- La gestion des besoins réels en ressources humaines de l'économie ;
- La définition des compétences inhérentes à l'exercice de chaque métier ;
- La contribution du monde professionnel dans l'atteinte des objectifs pédagogiques assignés.

L'objectif principal du projet est donc de développer, dans le cadre d'un partenariat novateur entre les pouvoirs publics et le secteur privé, une offre de formation professionnelle de qualité, répondant aux besoins de compétences exprimés par les Entreprises en matière d'Ouvriers et des Techniciens qualifiés.

Naturellement, la concrétisation, sur le plan opérationnel, d'une aussi grande ambition, reste largement tributaire de la conception, la planification, l'élaboration et la mise en œuvre réussie d'un plan de développement des compétences adossé sur une approche méthodologique susceptible de favoriser l'atteinte des objectifs aussi bien au niveau institutionnel, qu'à celui de la cible.

Aussi, la démarche pédagogique centrée sur l'ingénierie de la formation professionnelle suivant l'Approche Par Compétence, de par la pertinence des résultats économiques qu'elle a permis d'atteindre sous d'autres cieux, se révèle être un précieux outil sur lequel les pouvoirs publics et la communauté de la formation professionnelle au Cameroun ont jeté leur dévolu dans le processus de la recherche de la consolidation de l'accès à l'emploi décent des jeunes et autres candidats à l'insertion ou à la réinsertion professionnelle.

Cette démarche ci-dessous présentée, vise pour l'essentiel à pourvoir les candidats au très fluctuant et très exigeant marché de l'emploi, des savoirs, des savoir-faire et des savoir-être les rendant aptes à s'auto employer, ou à s'insérer efficacement dans une chaine de production des valeurs, des biens et des services nécessaires à l'amélioration des performances économiques dans un cadre local, national ou global donné et ainsi, de contribuer de manière efficiente aux transformation socio-économiques correspondantes.

Ainsi compris, le référentiel de formation et des compétences dont la présente production est méthodologiquement liée à la démarche en question, se veut un outil pratique de référence à
La disposition des formateurs dans le métier de Pentester.

A. PRESENTATION SUCCINCTE DE LA DEMARCHE DE L'INGENIERIE PEDAGOGIQUE, DU REFERENTIEL DE METIER ET DES AUTRES REFERENTIELS ET GUIDES

L'ingénierie pédagogique est centrée sur les outils et les méthodes conduisant à la conception, à la réalisation et à la mise à jour continue des Référentiels de Formation ou programmes de formation ainsi que des Guides Pédagogiques qui en facilitent la mise en œuvre. L'ingénierie pédagogique est un processus linéaire basé sur trois axes fondamentaux :

1) la détermination et la prise en compte de la réalité du marché du travail, tant sur le plan global (situation économique, structure et évolution des emplois) que sur un plan plus spécifique, liées à la description des caractéristiques d'un métier et à la formulation des compétences attendues pour l'exercer. Il s'agit du Référentiel de Métier – Compétences ;

2) le développement du support pédagogique tel que le Référentiel de Formation, le Référentiel d'Évaluation, divers documents d'accompagnement destinés à appuyer la mise en œuvre locale et à favoriser une certaine standardisation de la formation (Guides d'Organisation Pédagogiques, Guides d'Organisation Pédagogiques et Matérielle) ;

3) la mise en place, dans chaque Structure de formation, d'une approche pédagogique centrée sur la capacité de chaque apprenant à mobiliser ses connaissances dans la mise en œuvre des compétences liées à l'exercice du métier choisi.

Plus précisément, la démarche d'ingénierie en APC prend appui sur la réalité des métiers en ce qui concerne :

- Le contexte général (l'analyse du marché du travail et les études de planification) ;
- La situation de chaque métier (l'Analyse de Situation de Travail) ;
- La formulation des compétences requises et la prise en considération du contexte de réalisation propre à chaque métier (le Référentiel de Métier-Compétences) ;
- La conception de dispositifs de formation inspirés de l'environnement professionnel ;
- La détermination du niveau de performance correspondant au seuil du marché du travail ;
- L'élaboration des Référentiels de Formation et d'Évaluation basés essentiellement sur les compétences requises pour exercer chacun des métiers ciblés ;
- La production, la diffusion et l'implantation de guides et de supports pédagogiques ;
- La mise en place de diverses mesures de formation et de perfectionnement destinées à appuyer le personnel des structures de formation ;
- La révision de la démarche pédagogique (formation centrée sur l'apprenant par le développement de compétences) ;
- La disponibilité de locaux et équipements permettant de créer un environnement de formation semblable à l'environnement de travail ;
- La collaboration avec le milieu du travail (exécution des stages, alternance Ecole - Entreprise, …).

En effet, l'APC repose sur deux grands paliers conduisant successivement au Référentiel de Métier-Compétences et au Référentiel de Formation.

Les déterminants (éléments essentiels) disponibles qui mènent au premier palier sont les données générales sur le métier tirées des études de planification, l'ensemble de la documentation disponible ainsi que les résultats du RAST. Quant au deuxième palier, les déterminants sont tirés du RMC, à savoir la matrice de compétences et la table de correspondance.

En mettant à contribution ces éléments et particulièrement les descriptions des tâches, opérations, processus, habiletés, attitudes et comportements généraux, on arrive à déterminer les compétences retrouvées dans le Référentiel de Métier – Compétences et celles développées dans le Référentiel de Formation.

B. PRESENTATION SOMMAIRE DU MANDAT ET DE LA DÉMARCHE DE RÉALISATION

Le Référentiel Métier – Compétences (RMC) a comme première finalité de tracer le portrait le plus fidèle possible de la réalité d'un métier et de déterminer les compétences requises pour l'exercer. Élaboré dans le cadre du développement d'un Référentiel de formation professionnelle, le Référentiel de Métier - Compétences sert ensuite d'assise à la structure du futur référentiel de formation. Il peut également être utilisé comme document de base pour mettre en place une démarche d'apprentissage en milieu de travail. Utilisé à la fois aux fins de formation et d'apprentissage, le RMC contribue à assurer des bases similaires aux deux modes de développement des compétences (formation et apprentissage) et facilite la certification et la reconnaissance des compétences. En cette matière, il balise ainsi la voie à la mise en place d'un système de Validation des Acquis de l'Expérience (VAE).

Le Référentiel de Métier – Compétences se réalise en deux étapes :

- **la production de l'Analyse de la Situation de Travail (AST) ;**
- **la détermination des Compétences liées au métier.**

La description exhaustive des composantes et des caractéristiques d'un métier (portrait) est réalisée au moyen du RAST. Dans le cas du métier de **PENTESTER**, le RAST s'est déroulée du 01 au 15 Mars 2024 dans les régions du Littoral, du Nord, de l'extrême-Nord et de l'Ouest. Elle a regroupé treize (13) représentants d'Entreprises nationales des secteurs formel et informel.

En termes de démarche globale, il s'est agi : i) d'identifier les cibles à rencontrer (employeurs, employés, formateurs, etc.), (ii) d'élaborer des questionnaires spécifiques, sur la base du questionnaire général, (iii) de produire le RAST, (iv) d'organiser un atelier de validation des résultats du RAST, (v) de rédiger le RMC. Les membres des focus groupes sont des acteurs rencontrés et des experts-métiers invités. Chaque groupe était animé par un méthodologue.

Comme il a déjà été mentionné, l'élaboration d'une compétence résulte d'une démarche de conception ou de dérivation qui doit respecter les principaux déterminants issus des travaux antérieurs, le RAST en particulier, et présenter, sous forme d'énoncé, une compétence qui soit représentative de la démarche d'exécution d'une ou de plusieurs tâches ou qui est associée à la réalisation d'une activité de travail ou de vie professionnelle.

Les compétences présentées dans ce Référentiel de Métier – Compétences assurent une couverture complète des tâches et des opérations rattachées au métier de **PENTESTER (niveau Technicien Spécialisé)**. Cette activité est certainement l'une des plus complexes de la production d'un Référentiel de Métier – Compétences ou de la réalisation d'un programme de formation.

Deux outils ont été utilisés pour faciliter le travail de l'équipe de production et la présentation de la démarche de conception ainsi que pour documenter systématiquement chaque étape de production. Ces outils, que sont : la **Matrice des compétences** et **la Table de correspondance**, seront par la suite complétées et utilisés tout au long de la conception des référentiels de formation et d'évaluation, ainsi que des différents guides. Ils permettront de conserver l'unité de la conception et la continuité du traitement de l'information relative à chaque compétence retenue. La matrice des compétences sera par la suite transposée en matrice des objets de formation lors de la production du référentiel de formation.

Le Référentiel de Métier - Compétences mènera plus tard à la réalisation des documents pédagogiques (référentiel de formation, référentiel d'évaluation, documents et guides d'accompagnement).

Toutes les étapes de réalisation de ces documents seront confiées à une équipe de production composée de spécialistes, d'experts en méthodologie en APC, de formateurs d'expérience et de spécialistes du métier.

Le Rapport d'Analyse de Situation de Travail (RAST) est une étape importante dans le processus de développement d'un Référentiel de formation professionnelle selon l'Approche par Compétences (APC). Elle implique les professionnels qui apportent des réponses appropriées aux besoins de formation. L'Analyse de Situation de Travail est une étape importante, participative qui encourage les partenariats entre les entreprises de toutes tailles (TPE, PME PMI, etc.), les organisations professionnelles et les structures de formation professionnelle. Cette implication interpelle les différents acteurs afin qu'ils participent activement à la mise en œuvre des projets de formation professionnelle pour l'emploi.

Le présent Référentiel de Métier – Compétences décrit les activités que l'apprenant exercera dans sa vie professionnelle dès la fin de sa formation. Il sert de point de repère commun aux différents acteurs des milieux socio-professionnels, aux formateurs, aux Structures de Formation et même aux différents Services en charge de la Gestion centrale de la Formation Professionnelle. Il comprend :

Partie 1. Les résultats du Rapport d'Analyse de Situation de Travail (RAST) :

a) Les définitions,
b) Le tableau des tâches et opérations,
c) Le processus de travail,
d) Les conditions de réalisation et les critères de performance,
e) Les connaissances, habiletés et attitudes,
f) Les suggestions pour la formation.

Partie 2 : La présentation des compétences du référentiel :

a) La présentation de la notion de compétence,
b) La liste des compétences particulières,
c) La liste des compétences générales,
d) La matrice des compétences,
e) La table de correspondance.

C. PRESENTATION DU METIER ET DE SA SITUATION GENERALE SUR LE MARCHE DU TRAVAIL

"Le métier de pentester consiste à évaluer la sécurité d'un système d'information à travers différents angles d'attaques, mais toujours de manière cadrée. Le pentester va prendre la place d'un attaquant et son objectif est donc de simuler des attaques malveillantes pour identifier puis exploiter des vulnérabilités au sein du SI. Il aura également un grand rôle dans la remédiation des vulnérabilités, puisqu'il devra proposer des mesures correctives détaillées et personnalisées pour pallier à ces vulnérabilités à l'aide d'un rapport, qui à la fin du test d'intrusion, sera transmis au(x) commanditaire(s) du pentest. Il a un grand rôle de pédagogue, puisqu'il faut toujours vulgariser et savoir expliquer nos différentes trouvailles

DESCRIPTION GÉNÉRALE DU MÉTIER DE PENTESTER

TITRES	DESCRIPTIONS
Définition du métier	Un pentester est un professionnel de la cybersécurité du secteur numérique capable d'évaluer la sécurité des systèmes d'information en identifiant et en exploitant les vulnérabilités potentielles. C'est un professionnel qualifié qui utilise des méthodes et des outils spécialisés pour simuler des attaques informatiques et aider les organisations à renforcer leur sécurité en identifiant les failles et en fournissant des recommandations pour y remédier. Il a pour missions principales de : - Évaluer la sécurité des systèmes afin d'identifier les vulnérabilités potentielles qui pourraient être exploitées par des attaquants malveillants ; - Réaliser les tests d'intrusion en simulant des attaques ciblées pour mettre à l'épreuve la résistance des systèmes de l'organisation ; - Analyse des résultats et fournir des recommandations détaillées pour améliorer la sécurité ; - Rédiger les rapports ; Sensibiliser à la sécurité afin de réduire les risques d'attaques informatiques
Evolution du métier	L'évolution technologique a un impact significatif sur le métier de pentester. D'une part, elle crée des nouvelles opportunités pour les attaques et les vulnérabilités, car des nouveaux systèmes, applications et infrastructures émergent constamment. Les pentesters doivent donc rester constamment à jour sur les dernières technologies et tendances en matière de sécurité pour comprendre les nouvelles méthodes d'attaque potentielles. D'autre part, l'évolution technologique offre également des nouveaux outils et techniques aux pentesters pour renforcer la sécurité. Par exemple, l'intelligence artificielle et l'apprentissage automatique peuvent être utilisés pour détecter les anomalies et les comportements suspects, tandis que l'automatisation peut accélérer les tests de sécurité. Cependant, les technologies émergentes, telles que l'Internet des objets (IoT) et l'intelligence artificielle, présentent également des nouveaux défis en matière de sécurité, nécessitant une compréhension approfondie des risques potentiels.
Conditions d'accès à la formation	L'accès à la formation est ouvert aux personnes des deux sexes remplissant les conditions ci-après : • Être âgées d'au moins dix-sept ans ; • Avoir un BACCALAUREAT Scientifique C, D, TI ou Technique industrielle F2 ; • Avoir un BT MISE (Maintenance et Installation des Systèmes Electroniques) ; • Avoir le niveau Terminale avec VAE dans le domaine ; • Être titulaire d'un DQP en Informatique avec une expérience d'au moins 3 ans dans le domaine ; Les équivalents du sous-système anglophone sont également admis.

TITRES	DESCRIPTIONS
	• Subir avec succès à un test de sélection à l'entrée en formation.
Secteur d'activités	Selon les professionnels, le secteur d'activité d'un pentester est principalement lié à la sécurité informatique. Il travaille dans une variété d'industries, y compris les services financiers, les technologies de l'information, les entreprises de la cybersécurité, les gouvernements, les institutions de santé, les entreprises de commerce électronique, etc. Les entreprises de toutes tailles et de tous secteurs reconnaissent l'importance de protéger leurs systèmes et leurs données contre les cyberattaques. Par conséquent, le pentester a une demande croissante dans tous les secteurs où la sécurité de l'information est une priorité. Il peut être employés directement par ces organisations ou travailler en tant que consultants externes pour réaliser des tests d'intrusion, évaluer les vulnérabilités et fournir des recommandations pour renforcer la sécurité des systèmes informatiques.
Fonctions	• Gestion des risques, audit, conformité et continuité d'activités ; • Sécurité des réseaux ; • Sécurité des applications ; • Sécurité des systèmes et architecture de sécurité ; • Sécurité des données ; • Opérations de sécurité ; • Aspect juridique et règlementaire Evaluation, Correction, protection
Nature du travail	**Champ professionnel** : Cybersécurité
	Type d'emploi occupé : Technicien spécialisé
	Classification type/Catégorie : Catégorie 10
	Types de produits, de résultats ou de services : • Un système informatique sécurisé
Evolution technologique	L'évolution technologique a un impact significatif sur le métier de pentester. D'une part, elle crée de nouvelles opportunités pour les attaques et les vulnérabilités, car de nouveaux systèmes, applications et infrastructures émergent constamment. Les pentesters doivent donc rester constamment à jour sur les dernières technologies et tendances en matière de sécurité pour comprendre les nouvelles méthodes d'attaque potentielles. D'autre part, l'évolution technologique offre également de nouveaux outils et techniques aux pentesters pour renforcer la sécurité. Par exemple, l'intelligence artificielle et l'apprentissage automatique peuvent être utilisés pour détecter les anomalies et les comportements suspects, tandis que l'automatisation peut accélérer les tests de sécurité. Cependant, les technologies émergentes, telles que l'Internet des objets (IoT) et l'intelligence artificielle, présentent également de nouveaux défis en matière de sécurité, nécessitant une compréhension approfondie des risques potentiels.
Technologies utilisées	**Le pentester** utilise des logiciels de cybersécurité, les logiciels de développement d'application informatique, les logiciels de maintenance réseau, outils de connexion réseau (wifi, internet,), Il s'agit d'équipement à technologie variée comme les appareils de diagnostic…
Conditions de	**Lieux de travail** : Entreprise

TITRES	DESCRIPTIONS
travail	**Types d'entreprise** : Établissement, PME, sociétés, coopératives, GIC, etc.
	La condition de travail d'un pentester varie en fonction de plusieurs facteurs, y compris l'employeur, le type de contrat (permanent ou indépendant), et la nature des projets sur lesquels il travaille. Le pentester est souvent confronté à des horaires flexibles, car il doit s'adapter aux besoins et aux contraintes des clients. Il peut être amené à travailler en dehors des heures de travail normales pour éviter les interruptions des tests d'intrusion sur les systèmes en production. Le travail peut être intense et exigeant, car le pentester est souvent confronté à des délais serrés pour réaliser les tests de sécurité et produire des rapports détaillés. Il doit également être prêt à se maintenir constamment à jour sur les dernières techniques et outils de piratage et de sécurité.
	Environnement technique : *Processus de travail* - Planifier le travail - Effectuer le travail en respectant les mesures de sécurité ; - Contrôler la qualité du travail - Consigner et transmettre l'information **Équipements et outillages utilisés :** • Ordinateur portable … • **Systèmes d'exploitation :** (Kali Linux, Parrot OS, Windows, MacOS) • **Outils de test d'intrusion** (NAP, Metasploit Framework, Burp Suite, Wireshark, Nessus, OpenVAS, Nikto, SQLMap, Hydra, DirBuste) • **Environnements de virtualisation** (VirtualBox, VMware, QEMU…) • **Matériel réseau (**Routeurs, Commutateurs, Concentrateurs, Câbles Ethernet, Adaptateurs réseau) • **Dispositifs de capture de paquets** (Wi-Fi Pineapple, Adaptateurs USB, Matériel de piratage physique, Rubber Ducky, BadUSB) • **Outils de cryptographie** (GnuPG, OpenSSL, Hashcat, • Outils de gestion de mots de passe (KeePass, LastPass) • **Matériel de sécurité physique (**Serrures électroniques, Caméras de sécurité, Systèmes d'alarme)
	Responsabilité et autonomie C'est la taille de l'entreprise qui détermine le degré de liberté du professionnel. Dans les entreprises plus importantes, il opère sous les ordres d'un chef d'entreprise.
	Conditions d'exercice L'activité nécessite de maintenir des attitudes de concentration permanente, des positions particulières (débout, penché, accroupi, etc.). Il peut impliquer des ports de charges.
	Facteurs de stress Les sources de stress sont liées à la pression, la charge du travail et au poids des responsabilités.
	Santé et sécurité Le métier de pentester a un impact sur la santé et la sécurité des professionnels qui l'exercent. Les pentesters sont souvent confrontés à des scénarios de test

TITRES	DESCRIPTIONS
	d'intrusion qui peuvent être stressants et exigeants, car ils doivent essayer d'exploiter les vulnérabilités des systèmes pour évaluer leur sécurité. Cela peut entraîner une pression psychologique et émotionnelle importante. De plus, les pentesters sont exposés à des risques liés à la manipulation d'outils et de logiciels potentiellement dangereux, ainsi qu'à des environnements informatiques instables
Conditions d'entrée dans le marché du travail	L'accès au métier passe généralement par les offres d'emplois qui sont publiées à travers divers canaux de diffusion, notamment la presse écrite, la radio et même la télévision. De plus en plus, ces offres sont également diffusées sur le réseau Internet dans des sites spécialisés. Enfin, certaines entreprises recourent aux services de Cabinets de recrutement dont le fonctionnement est régi par une règlementation fixée par le Ministère des Postes et Télécommunications. Le technicien ou la technicienne spécialisé en pentester peut être recruté à partir : - Du DTS en pentester ; - Du CQP en sécurité informatique avec une expérience d'au moins deux ans dans le domaine ; - Les équivalents du sous-système anglophone sont également admis. En plus du diplôme requis, les employeurs peuvent également demander une expérience préalable dans le domaine de la cybersécurité.

PREMIERE PARTIE : RESULTATS DE L'ANALYSE DE SITUATION DE TRAVAIL (RAST)

I.1. DEFINITION DES TERMES USUELS

Processus de travail	Le processus de travail vise à mettre en évidence les principales étapes d'une démarche logique pour l'exécution de l'ensemble des tâches d'un métier ou d'une profession.
Tâches	Les tâches sont les actions qui correspondent aux principales activités de l'exercice du métier analysé. Une tâche est structurée, autonome et observable. Elle a un début déterminé et une fin précise. Dans l'exercice d'un métier, qu'il s'agisse d'un produit, d'un service ou d'une décision, le résultat d'une tâche doit présenter une utilité particulière et significative.
Sous-tâches	Les sous-tâches sont les décompositions d'une tâche.
Opérations	Actions qui décrivent les étapes de réalisation d'une tâche et permettent d'établir le « comment » pour l'atteinte des résultats. Elles sont liées surtout aux méthodes et aux techniques utilisées ou aux habitudes de travail existantes.
Conditions de réalisation	Elles font généralement trait à l'environnement de travail, aux données ou aux outils utilisés lors de la réalisation d'une tâche et elles ont été recueillies pour l'ensemble de la tâche et non par opération. Plus particulièrement, elles renseignent sur des aspects tels que : - Le degré d'autonomie (travail individuel, travail supervisé ou autonome); - Les références utilisées (manuels des fabricants ou des constructeurs, documents techniques, formulaires, autres) ; - Le matériel et équipement utilisés (matières premières, outils et appareils, instruments, équipement, autres) ; - Les consignes particulières (précisions techniques, bons de commande, demandes de clientes ou clients, données ou informations particulières, autres) ; - Les conditions environnementales (travail à l'intérieur ou à l'extérieur, risques d'accidents, produits toxiques, autres) ; - Les activités ou tâches préalables, parallèles ou subséquentes (préalables à la réalisation de la tâche, en coordination avec d'autres tâches, en lien avec des tâches subséquentes).
Critères de performance	Ce sont des exigences concernant la réalisation de chaque tâche. Ils permettent d'évaluer, si la tâche est effectuée de façon satisfaisante ou non. Ils sont recueillis pour l'ensemble de la tâche et non par opération. Ces critères correspondent à un ou des aspects observables et mesurables essentiels à la réalisation d'une tâche. Ils renseignent sur des aspects tels que : - La quantité et la qualité du résultat (nombre de pièces, précision du travail, seuil de tolérance, autres); - L'application des règles relatives à la santé et sécurité (respect des normes, port d'accessoires et de vêtements protecteurs, mesures de sécurité et d'hygiène, autres) ; - L'autonomie (degré de responsabilité, degré d'initiative, réaction devant les situations imprévues, autres) ; - La rapidité (vitesse de réaction, durée d'exécution, autre).

I.2. TABLEAU DES TACHES ET OPERATIONS

Le tableau des tâches et des opérations présentées ci-après est le résultat d'un consensus des professionnels du métier. Dans le tableau, les tâches (l'axe vertical), sont numérotées d'un à cinq. Les opérations associées à chacune des tâches se trouvent à l'horizontal.

Aux fins de l'exercice, le tableau des tâches et des opérations définit le portrait du métier Pentester au moment de l'analyse de la situation de travail. Le niveau de référence considéré est celui de l'entrée sur le marché de l'emploi.

Suite à l'identification des tâches et des opérations, l'ordonnancement général a été fait par consensus et proposé pour adoption par consensus. Les discussions avec les professionnels du métier laissent cependant comprendre que dans la pratique, bon nombre des tâches et opérations sont « dynamiques ». Elles sont parfois réalisées sans ordonnancement spécifique, au regard de la charge de travail journalière, des modalités prescrites par le chef d'atelier ou des priorités présentes en termes d'exécution des travaux.

Tableau des tâches.

N°	Tâches	Complexité des tâches
1.	**Analyser les vulnérabilités du système informatique**	5
2.	**Réaliser des tests d'intrusion sur les réseaux et les applications**	5
3.	**3. Elaborer des stratégies de sécurité**	3
4.	**Tester l'efficacité du système sécurité**	3
5.	**Effectuer des audits de sécurité des systèmes informatiques**	2
6.	**Assurer une veille permanente sur les menaces de piratage**	2

Tâche plus complexe =5 ; Tâche moins complexe = 1

Tableau des tâches et des opérations

TÂCHES	OPÉRATIONS			
1. Analyser les vulnérabilités du système informatique	1.1 Identifier les potentielles failles de sécurité.	1.2 Classer les vulnérabilités en fonction de leur criticité.	1.3 Documenter les résultats de l'analyse.	1.4 Présenter un rapport détaillé des vulnérabilités
2. Réaliser des tests d'intrusion sur les réseaux et les applications	2.1. Scanner les réseaux	2.2. Exploiter les failles.	2.3. Simuler des attaques	2.4. Mesurer l'efficacité des sécurités mises en place.
3. Elaborer des stratégies de sécurité	3.1. Concevoir des plans d'action.	3.1. Mettre en place des pares-feux et des systèmes de détection d'intrusion.	3.2. Configurer des politiques de sécurité.	
4. **Tester l'efficacité du système sécurité**	4.1. Coordonner des simulations d'attaques informatiques.	4.2. Apprécier la réactivité des équipes de sécurité.	4.3. Analyser les résultats des exercices.	4.4. Proposer des améliorations des systèmes de sécurité contre les cyberattaques.
5. **Effectuer des audits de sécurité des systèmes informatiques**	5.1. Vérifier la conformité des systèmes aux normes de sécurité en vigueur.	5.2. Examiner les journaux d'activité.	5.3. Déterminer l'efficacité des contrôles d'accès et des politiques de sécurité.	5.4. Recommander des mesures correctives.
6. **Assurer une veille permanente sur les menaces de piratage**	6.1. Suivre les publications spécialisées en sécurité informatique.	6.2. Effectuer la mise à jour sur les dernières tendances en matière de sécurité.	6.3. Tester de nouveaux outils de sécurité	6.4. Mettre à jour régulièrement ses connaissances

I.3. PROCESSUS DE TRAVAIL.

Le processus de travail vise à mettre en évidence les principales étapes d'une démarche logique pour l'exécution de l'ensemble des tâches d'une profession ou d'un métier.
Le processus de travail suivant est recommandé pour le métier de Pentester, en raison des tâches retenues et de leur ordonnancement par les participants au focus group. Le processus présenté est assez générique pour coller aux différentes situations de travail des diverses fonctions du domaine :

- Planifier le travail
- Effectuer le travail en respectant les mesures de sécurité ;
- Contrôler la qualité du travail
- Consigner et transmettre l'information.

I.4. CONDITIONS DE REALISATION ET LES CRITÈRES DE PERFORMANCE.

- **Les conditions de réalisation**

Les conditions de réalisation d'une tâche ont généralement trait à l'environnement de travail, aux données ou aux outils utilisés lors de la réalisation d'une tâche et elles ont été recueillies pour l'ensemble de la tâche et non par opération. Plus particulièrement, elles renseignent sur des aspects tels que :

- Le degré d'autonomie (travail individuel ou en équipe, travail supervisé ou autonome);
- Les références utilisées (manuels des fabricants ou des constructeurs, documents techniques, formulaires, autres) ;
- Le matériel et équipement utilisés (matières premières, outils et appareils, instruments, équipement, autres) ;
- Les consignes particulières (précisions techniques, bons de commande, demandes de clientes ou clients, données ou informations particulières, autres);
- Les conditions environnementales (travail à l'intérieur ou à l'extérieur, risques d'accidents, produits toxiques, autres);
- Les activités ou tâches préalables, parallèles ou subséquentes (préalables à la réalisation de la tâche, en coordination avec d'autres tâches, en lien avec des tâches subséquentes).

- **Les critères de performance**

Ce sont des exigences concernant la réalisation de chaque tâche. Ils permettent d'évaluer, si la tâche est effectuée de façon satisfaisante ou non. Ils sont recueillis pour l'ensemble de la tâche et non par opération. Ces critères correspondent à un ou des aspects observables et mesurables essentiels à la réalisation d'une tâche. Ils renseignent sur des aspects tels que :

- La quantité et la qualité du résultat (nombre de pièces, précision du travail, seuil de tolérance, autres) ;
- L'application des règles relatives à la santé et sécurité (respect des normes, port d'accessoires et de vêtements protecteurs, mesures de sécurité et d'hygiène, …) ;
- L'autonomie (degré de responsabilité, degré d'initiative, réaction devant les situations imprévues, …) ;
- La rapidité (vitesse de réaction, durée d'exécution …).

Les conditions de réalisation et critères de performance correspondant à chacune des tâches sont résumés dans les tableaux ci-après :

Tâche 1 Analyser les vulnérabilités du système informatique	
Conditions de réalisation	**Critères de performance**
Autonomie Travail individuel ou en équipe. . **Références** • Normes, • Frameworks • Publications de l'OWASP, • Guides de sécurité de l'ISO, • Rapports de vulnérabilités du NIST, etc. **Consignes particulières** Consignes spécifiques données par le client ou l'organisation. Respect des consignes et suivi des directives fournies concernant les systèmes à tester, les méthodes à utiliser, les horaires de test, les restrictions, etc **Conditions environnementales** L'accès physique aux locaux, l'accès aux systèmes informatiques, les autorisations d'utilisation des outils de test, la disponibilité des ressources réseau, etc. **Matériel/moyens** • Ordinateurs portables, • Outils de scan de vulnérabilité ; • Outils de test d'intrusion, • Logiciels spécifiques, • Environnements de test isolés, • Machines virtuelles, • Outils de capture de trafic, etc.	• Détection judicieuse d'un pourcentage de vulnérabilités, • Production correcte de rapports détaillés et clairs, • Identification judicieuse de scénarios d'attaque réalistes, • Conformité correcte aux normes de sécurité, etc.

Tâche 2– Réaliser des tests d'intrusion sur les réseaux et les applications	
Conditions de réalisation	**Critères de performance**
Autonomie Travail individuel ou en équipe. **Références** • Les publications de l'Open Web Application Security Project (OWASP), • Les guides de sécurité du National Institute of Standards and Technology (NIST), • Les rapports de vulnérabilités de Common Vulnerabilities and Exposures (CVE), **Consignes particulières** Consignes spécifiques données par le client ou	• Identification correcte du nombre de vulnérabilités, • Exploitation minutieuse des failles du système • Classification et gravité correctes des vulnérabilités, • Clarté et qualité correctes des rapports de test, • Conformité correcte aux normes de sécurité spécifiques, etc

l'organisation. Respect des consignes et suivi des directives fournies concernant les systèmes à tester, les méthodes à utiliser, les horaires de test, les restrictions, etc. **Conditions environnementales** L'accès physique aux locaux, l'accès aux systèmes informatiques, les autorisations d'utilisation des outils de test, la disponibilité des ressources réseau, etc. **Matériel/moyens** • Ordinateurs portables puissants, • Outils de scan de vulnérabilité ; • Outils de test d'intrusion spécialisés, • Logiciels de sécurité, • Environnements de test isolés, virtuelles • Outils de capture de trafic réseau, etc.	

Tâche 3– Elaborer des stratégies de sécurité	
Conditions de réalisation	**Critères de performance**
Autonomie Travail individuel ou en équipe. **Références** • Les publications de l'Open Web Application Security Project (OWASP), • Les guides de sécurité du National Institute of Standards and Technology (NIST), • Les rapports de vulnérabilités de Common Vulnerabilities and Exposures (CVE), **Consignes particulières** Consignes spécifiques données par le client ou l'organisation. Respect des consignes et suivi des directives fournies concernant les systèmes à tester, les méthodes à utiliser, les horaires de test, les restrictions, etc. **Conditions environnementales** L'accès physique aux locaux, l'accès aux systèmes informatiques, les autorisations d'utilisation des outils de test, la disponibilité des ressources réseau, etc. **Matériel/moyens** • Ordinateurs portables puissants, • Outils de test d'intrusion spécialisés, • Logiciels de sécurité, • Environnements de test isolés, virtuelles • Outils de capture de trafic réseau, etc.	• Evaluation correctes des systèmes à protéger • Réalisation cohérente des plans d'actions • Sélection correcte des solutions

Tâche 4 – Tester l'efficacité du système sécurité	
Conditions de réalisation	**Critères de performance**
Autonomie Travail individuel ou en équipe. **Références** • Sites web spécialisés dans la sécurité informatique, • Blogs de chercheurs en sécurité, • Rapports de vulnérabilités, • Conférences sur la sécurité, • Publications académiques, • Communautés de hackers éthiques, etc. **Consignes particulières** Consignes particulières données par l'organisation ou le client concernant la veille technologique. Domaines spécifiques à surveiller, Des technologies à évaluer, des tendances spécifiques à suivre, etc. **Conditions environnementales** L'accès à Internet, la disponibilité d'outils de recherche, les autorisations d'accès à des sites web spécifiques, etc. environnement de travail propice à la recherche et à la collecte d'informations. **Matériel/moyens** • Agrégateurs de flux RSS, • Moteurs de recherche spécialisés, • Outils de surveillance des vulnérabilités, • Plateformes de partage de connaissances, • Forums de discussion, etc.	• Utilisation correcte des scans de vulnérabilités • Application correcte des règles de filtrage • Evaluation correcte des configurations systèmes • Simulation minutieuse des scénarios réels

Tâche 5 – Effectuer des audits de sécurité réguliers des systèmes informatiques	
Conditions de réalisation	**Critères de performance**
Autonomie Travail individuel ou en équipe **Références** • Sites web spécialisés dans la sécurité informatique, • Blogs de chercheurs en sécurité, • Rapports de vulnérabilités, • Conférences sur la sécurité, • Publications académiques, • Communautés de hackers éthiques, etc. **Consignes particulières** Consignes particulières données par l'organisation ou le client concernant la veille technologique. Des domaines spécifiques à surveiller, Des technologies à évaluer, Des tendances spécifiques à suivre, etc. **Conditions environnementales** L'accès à Internet, la disponibilité d'outils de recherche, les autorisations d'accès à des sites web spécifiques, etc. environnement de travail propice à la recherche et à la collecte d'informations. **Matériel/moyens** • Agrégateurs de flux RSS, • Moteurs de recherche spécialisés, • Outils de surveillance des vulnérabilités, • Plateformes de partage de connaissances, • Forums de discussion, etc.	• Identification correcte des vulnérabilités courantes et points faibles • Utilisation minutieuse des outils de test automatiques • Utilisation correcte des mesures de sécurité • Application correcte des correctifs et mise à jour

Tâche 6 – Assurer une veille permanente sur les nouvelles menaces et les techniques de piratage	
Conditions de réalisation	**Critères de performance**
Autonomie Travail individuel ou en équipe. **Références** • Sites web spécialisés dans la sécurité informatique, • Blogs de chercheurs en sécurité, • Rapports de vulnérabilités, • Conférences sur la sécurité, • Publications académiques, • Communautés de hackers éthiques, etc. **Consignes particulières** Consignes particulières données par l'organisation ou le client concernant la veille technologique. Domaines spécifiques à surveiller, Identification des sources d'information pertinentes. Mise en place d'un processus de collecte et d'analyse des informations ; Diffusion des informations collectées aux pentesters. **Conditions environnementales** L'accès à Internet, la disponibilité d'outils de recherche, les autorisations d'accès à des sites web spécifiques, etc. environnement de travail propice à la recherche et à la collecte d'informations. **Matériel/moyens** • Agrégateurs de flux RSS, • Moteurs de recherche spécialisés, • Outils de surveillance des vulnérabilités, • Plateformes de partage de connaissances, • Forums de discussion, • Base de données de vulnérabilité ; • Rapport d'analyse en sécurité etc.	• Fréquence minutieuse des mises à jour, • Identification correcte des sources d'informations sur les cyberattaques, • Adoption correcte des bonnes pratiques en matière de sécurité ; • Utilisation correcte des nouveaux outils automatiques de test

I.5. CONNAISSANCES, HABILITES ET ATTITUDES.

L'atelier d'Analyse de Situation de Travail a permis entre autres, la mise en évidence des connaissances, des habiletés, et des attitudes requises ou souhaitées pour l'exécution des tâches étudiées.

Connaissances, habiletés et attitudes sont des valeurs transférables c'est-à-dire qu'elles sont applicables dans une variété de situations similaires. On ne peut donc les limiter à une seule tâche ou à une seule fonction. Ce sont des valeurs transversales entre les différentes fonctions d'un métier.

Les comportements se rapportent :

- A la dimension personnelle (compréhension de ses propres sentiments et émotions, résolution de conflits internes, autres) ;
- A la dimension interpersonnelle (communiquer avec les autres, motiver les autres et les intéresser, animer un groupe, autres) ;
- Aux attitudes ayant trait à la santé et à la sécurité, aux relations humaines, à l'éthique professionnelle, à d'autres éléments ;
- Aux attitudes ayant trait : aux réflexes physiques, aux réflexes mentaux, à la façon d'agir dans des situations de travail particulières, à d'autres éléments.

Les participants ont été unanimes pour accorder le plus haut degré d'importance aux attitudes telles que l'esprit positif, l'endurance, la persévérance, le sens de l'ordre, l'intégrité et l'honnêteté. Les attitudes telles que le calme, la discipline et la capacité d'assimilation sont considérées comme des attitudes importantes toujours au regard de la nature particulière du métier.

Le tableau suivant met en évidence les connaissances, habiletés psychomotrices, habiletés cognitives, habiletés perceptives et attitudes.

Connaissances	**Habilités**	**Attitudes**
• L'Intégration des aspects juridiques de la cybersécurité ; • La mise en place d'une politique de cybersécurité ; • Supervision de la sécurité du SI ; • Construction de la stratégie cybersécurité de l'organisation ; • Réalisation	**Habiletés cognitives**: - Résolution de problèmes, - Capacité d'analyse, - Capacité de synthèse, - Explication de modes et de principes de fonctionnement, - Conception de stratégies et de plans, - Planification d'activités, - Prise de décision, - Fréquence d'exécution, - Autres... **Habiletés psychomotrices:** - manipulation d'outils, d'appareils et d'instruments,	**Sur le plan personnel, les attitudes peuvent avoir trait:** - À la gestion du stress, - À la communication, - À la motivation des autres, - À la démonstration d'une attitude d'ouverture, - Au respect des autres - Ponctualité - Honnêteté - Intégrité - Attitude positive - Entreprenant - Passionné - Sociable - Rigoureux

Connaissances	Habilités	Attitudes
d'une rétro-ingénierie	- assemblage d'objets, - manœuvre spécialisées, - degré de dextérité, - degré de coordination, - qualité des réflexes, - autres. **Habiletés perceptives**: - Perception de couleurs, de formes, de signes, de signaux, de codes; - perception d'odeurs afin de reconnaître un danger , de diagnostiquer l'état d'un danger , de percevoir un danger; - Perception, distinction de variations d'un fini, d'aspérités, d'uniformité ; - Reconnaissance des sons afin de diagnostiquer un problème	- Responsable - Recherche de perfectionnement - Esprit d'initiative / Autonomie/ - contrôle de ses sentiments et émotions, - Résolution de conflits internes ; - Autres…

I.6. SUGGESTIONS POUR LA FORMATION.

L'Analyse de Situation de Travail a permis de recueillir des suggestions concernant la formation au métier de Pentester. Les principaux aspects qui ont fait l'objet de suggestions sont les suivants :

- Les modalités de formation (moyens didactiques, informatique, activités des apprenants, etc.).
- Les stages en entreprise (modalités, durée, fréquence).
- Les connaissances fondamentales.
- L'évaluation et la reconnaissance des acquis de l'expérience qui est une autre voie d'accès à la certification.
- La formation initiale qui regroupe un contenu de formation obligatoire.

Ainsi, il a été mentionné que :

- La formation doit être davantage axée sur la pratique et les réalités de la cyber sécurité.
- Les formateurs doivent être des professionnels ayant de l'expérience.
- Le matériel et l'équipement utilisés au centre doivent être représentatifs des pratiques en entreprises.
- Les apprenants doivent se familiariser avec la réalité du terrain par le biais de visites et de stages en entreprise.
- Appliquer les règles de conduite en entreprise au centre de formation, et développer l'autodiscipline, la responsabilisation des apprenants.
- Développer chez les futurs lauréats le souci de concilier la qualité et le rendement satisfaisant des prestations.
- Développer chez les apprenants le sens de l'initiative et l'autonomie.

- Former les apprenants à s'adapter au changement et à l'innovation.
- Développer leur capacité à être responsable de tout ce qui se passe sur les postes de travail.
- Montrer la meilleure méthode et manière pendant qu'ils effectuent les opérations.
- Développer la polyvalence dans la formation, pour permettre aux apprenants d'exécuter différentes opérations sur une variété d'équipements.
- Les formateurs doivent suivre des formations continues en entreprises et dans les structures spécialisées pour être à jour des innovations technologiques et pédagogiques.
- Tous sont d'avis qu'une ou qu'un lauréat a besoin d'une période d'intégration dans l'entreprise avant de pouvoir prendre en charge la totale responsabilité de son poste de travail.
- La connaissance de l'anglais et du français ainsi que la capacité de pouvoir lire et comprendre des documents écrits et technique sont des éléments importants pour exercer le métier, sans oublier les connaissances fondamentales de secourisme et de premiers soins, les connaissances en calculs professionnels sont incontournables.

Aussi, les entreprises sont disposées à recevoir les apprenants pour des stages d'imprégnation, d'une durée variant d'un (01) à trois (03) mois. Certaines d'entre elles en reçoivent déjà dans le cadre de stages académiques et professionnels.

DEUXIEME PARTIE : PRESENTATION DES COMPETENCES

II.1. PRESENTATION DE LA NOTION DE COMPETENCE GENERALE ET DE COMPETENCE PARTICULIERE

La compétence correspond à un savoir agir reconnu dans un environnement et dans le cadre d'une méthodologie définie.
Les professionnels du métier expriment leurs manières d'agir, autrement dit leurs compétences, à travers des actes opératoires qui leur paraissent clés pour répondre aux enjeux de la situation.

Les compétences générales correspondent à des activités plus vastes qui vont au-delà des tâches, mais qui contribuent généralement à leur exécution. Elles requièrent habituellement des apprentissages de nature plus fondamentale. (Par exemple une compétence liée à la santé et à la sécurité au travail) et doivent donc correspondre à des activités de travail à la « périphérie » des tâches, tout en y étant étroitement liées ou associées.

Les compétences particulières renvoient à des aspects concrets, pratiques, circonscrits et directement liés à l'exercice d'un métier. Elles sont directement liées à l'exécution des tâches et à une évolution appropriée dans le contexte du travail et visent surtout à rendre la personne efficace dans l'exercice d'un métier.

II.2. LISTE DES COMPETENCES GENERALES.

Suite aux informations présentées dans le RAST, les compétences générales suivantes et correspondantes aux attitudes, habiletés et comportements attendus ont été retenues :

N°	Compétences générales	Tâches liées
01	Communiquer en milieu professionnel	1, 2, 3, 4, 5 ; 6
02	Appliquer les principes de la sécurité des comptes	1, 2, 3, 4, 5, 6
03	Exploiter l'architecture des systèmes informatiques des réseaux et des protocoles	1, 2, 3, 4, 5, 6
04	Configurer les systèmes d'exploitation	1, 2, 3, 4, 5, 6
05	Utiliser les langages de programmation	1, 2, 3, 4, 5, 6

II.3. LISTE DES COMPETENCES PARTICULIERES.

Les compétences particulières identifiées pour le technicien Spécialisé en Pentester sont les suivantes :

N°	Compétences particulières	Taches liées
06	Identifier les vulnérabilités potentielles dans les Systèmes informatiques	1, 2, 3, 4, 5, 6
07	Configurer les outils de test de pénétration des systèmes d'exploitation	1, 2, 3, 4, 5, 6
08	Tester la vulnérabilité sur les Réseaux, les applications, site web et les systèmes d'exploitation	1, 2, 3, 4, 5, 6
09	Proposer les stratégies d'atténuation	1, 2, 3, 4, 5, 6
10	Configurer les pares-feux et des systèmes de détection d'intrusions	1, 2, 3, 4, 5, 6
11	Assurer la veille technologique en cyberattaque	1, 2, 3, 4, 5

II.4. MATRICE DES COMPETENCES.

- **Présentation générale de la matrice.**

La matrice des compétences présente l'ensemble structuré des compétences générales et particulières dans un lien dynamique. Elle comprend :

- Les compétences générales qui portent sur des activités communes à différentes tâches ou à différentes situations. Elles portent, notamment, sur l'application de principes scientifiques et technologiques liés à la fonction de travail ;
- Les compétences particulières qui visent l'exécution des tâches et des activités à l'intérieur de la fonction de travail et de la vie professionnelle ;
- Le processus de travail qui porte sur les étapes les plus significatives de la réalisation des tâches de la profession.

La matrice des compétences permet de voir les liens qui existent entre les compétences générales, placées à l'horizontale, et les compétences particulières, placées à la verticale.

Le symbole (O) indique la présence d'un lien entre une compétence générale et une compétence particulière.

Le symbole (Δ) indique la présence d'un lien entre les compétences particulières et une étape du processus.

La logique suivie au moment de la conception d'une matrice influe sur la séquence d'acquisition des compétences. Ainsi, la conception de la matrice s'est réalisée de manière à permettre d'une part une progression dans la complexité des compétences à acquérir et, d'autre part, l'établissement de liens favorisant l'intégration des compétences.

- **Matrice des compétences**.

MATRICE DES COMPÉTENCES												
			Compétences générales					Processus				
Pentester (Technicien spécialisé) **Compétences particulières**	**Numéro de la compétence**	Niveau de complexité / 10	Communiquer en milieu professionnel	Appliquer les principes de la sécurité des comptes	Exploiter l' architecture des systèmes informatiques des réseaux et des protocoles	Configurer les systèmes d' exploitation	Utiliser les langages de programmation	Planifier le travail	Exécuter le travail en adoptant les mesures de sécurité	Contrôler la qualité du travail	Consigner et transmettre l' information	**Nombre de compétences**
Numéro de la compétence			**01**	**02**	**03**	**04**	**05**					**05**
Niveau de complexité / 5			8	8		8	8					
Identifier les vulnérabilités potentielles dans les Systèmes informatiques	**06**	9	O	O	O	O	O	Δ	Δ	Δ	Δ	
Tester la vulnérabilité sur les réseaux des applications site web et les systèmes d'exploitation	**07**	6	O	O	O	O	O	Δ	Δ	Δ	Δ	
Configurer les outils de test de pénétration des systèmes d'exploitation	**08**	10	O	O	O	O	O	Δ	Δ	Δ	Δ	
Proposer les stratégies d'atténuation	**09**	9	O	O	O	O	O	Δ	Δ	Δ	Δ	
Configurer les pares-feux et des systèmes de détection d'intrusions	**10**	9	O	O	O	O	O	Δ	Δ	Δ	Δ	
Assurer la veille technologique en cyberattaque	**11**	7	O	O	O	O		O	O	Δ	Δ	
Nombre de compétences	**06**											**11**
		Légende : Le symbole (O) indique la présence d'un lien entre une compétence générale et une compétence particulière.										
		Le symbole (Δ) indique la présence d'un lien entre les compétences particulières et une étape d'un processus.										

II.5. TABLE DE CORRESPONDANCE

- **Présentation générale de la table**

La table de correspondance ci-après présente onze (11) compétences retenues pour le métier de technicien Spécialisé Pentester. Elle présente de façon détaillée chacune des compétences en identifiant précisément les éléments qui la caractérisent, de même que les déterminants tels que les connaissances et les habiletés. La table de correspondance contient diverses informations relatives au projet de formation. La première colonne présente, dans l'ordre, les compétences telles qu'elles apparaissent dans la matrice.

Dans la deuxième colonne, on retrouve, pour chacune des compétences, des indications sur la compétence de façon à baliser celle-ci et en préciser la teneur. Ces données sont présentées à titre indicatif de façon à rendre plus explicite l'énoncé de compétence. Il est important de retenir que ces indications constituent avant tout un premier déblayage pour mieux cerner la compétence. Ces indications ne sont pas nécessairement exhaustives. De plus, elles peuvent référer tant à des éléments de contenu, à des notions liées à l'acquisition de la compétence qu'à des éléments de cette compétence.

- **Présentation du contenu de la table de correspondance.**

COMPÉTENCE 01: Communiquer en milieu professionnel	
Indications sur la compétence	**Déterminants**
1. Traiter les informations 2. Produire les messages indispensables à la vie professionnelle et sociale 3. Communiquer oralement 4. Rendre compte de son activité	**AST** **Tâches : 1, 2, 3, 4, 5 ,6** **Connaissances :** Communication orale Rédaction des rapports, compte rendu etc.. **Savoir-être et qualités :** s'exprimer avec clarté, Éloquence. Capacité d'écoute dans les relations avec le personnel ; capacité à gérer le stress et le temps ; esprit d'analyse et de synthèse, autonomie, capacité d'observation, intuition…

COMPÉTENCE 02 : Appliquer les principes de la sécurité des comptes	
Indications sur la compétence	**Déterminants**
1. Gérer les identités 2. Sécuriser les mots de passe 3. Contrôler les accès 4. Détecter les activités anormales 5. Élaborer la Journalisation et traçabilité 6. Gérer les incidents	**Tâches : 2 3, 4, 5,6** **Connaissances :** - Méthodes de gestion centralisée des identités - Gestion des droits d'accès et des autorisations - Principes d'authentification forte (2FA, biométrie...) - Politiques de mots de passe complexes et uniques - Stockage et hachage sécurisés des mdp - Solutions de gestion des mots de passe **Savoir-être et qualités :** habilités motrices et perceptives, vigilance, organisation et méthode. - Implémentation des contrôles d'accès logiques - Principes des listes de contrôle d'accès - Solutions de PAM/IAM - paramétrage des alertes et alarmes - Corrélation des logs et détection d'intrusions - Solutions de SIEM/UEBA

COMPÉTENCE 03 : Exploiter l'architecture des systèmes informatiques des réseaux et des protocoles	
Indications sur la compétence	**Déterminants**
1. Utiliser l'architecture des systèmes informatiques 2. Utiliser l'architecture système et applicative 3. Utiliser les réseaux 4. Appliquer les protocoles de communication	**Tâches :1, 2, 3, 4, 5,6** **Connaissances :** Architecture matérielle et logicielle, protocoles réseaux, équipements réseaux, fonctionnement des principaux protocoles, architecture logicielle **Savoir-être et qualités :** habilités motrices et perceptives, vigilance, organisation et méthode.

COMPÉTENCE 04 : Configurer les systèmes d'exploitation	
Indications sur la compétence	**Déterminants**
1. Effectuer l'administration système ; 2. Gérer les utilisateurs et les droits ; 3. Gérer la sécurité des systèmes d'exploitation ; 4. Gérer la sécurité OS: 5. Gérer les périphériques :	**Tâches :1, 2,3, 4, 5,6** **Connaissances :** Installation, configuration et maintenance des systèmes d'exploitation, Création et gestion des comptes utilisateurs, des groupes et des droits d'accès **Savoir-être et qualités :** habilités motrices et perceptives, vigilance, organisation et méthode.

COMPÉTENCE 05 : Utiliser les langages de programmation	
Indications sur la compétence	**Déterminants**
1. Identifier le langage de programmation généralistes ; 2. Acquérir les notions en Développement web et applicatif : 3. Acquérir les notions d'algorithmie et structures de données : 4. Utiliser la programmation système : 5. Sécuriser le code source	**RAST : Tâches 3, 4, 5** **Connaissances : -** C/C++, Java, Python, **P**HP, Javascript etc, Concepts de programmation orientée objet/procédurale, HTML/CSS, comme React , Angular, Langages serveur comme PHP, Node.js ; boîtes à outils comme .NET, Swift, Android, Interfaces graphiques, bases de données, Tableaux, listes, piles, files, arbres, graphes, Algorithmes de tri, recherche, cryptog, Langages bas niveau comme C, assemblage **Habiletés :** adopter un comportement de sécurité, dextérité, concentration

COMPÉTENCE 06 : Identifier les vulnérabilités potentielles dans les Systèmes informatiques	
Indications sur la compétence	**Déterminants**
1. Acquerir les connaissances approfondies en sécurité informatique ; 2. Décrire un audit de configuration ; 3. Effectuer une analyse statique et dynamique de code source ; 4. Effectuer les tests d'intrusion ("penetration testing") ; 5. Veiller sur les vulnérabilités :	**RAST: tâches 1,2,3,4,5,6** **Connaissances :** - Méthodologies d'analyse de risques et de vulnérabilités, Techniques d'attaque, modèles de menaces, Analyse de la configuration système, réseaux, applications, Détection de mauvaises pratiques et déviations de baselines ; Revue de code, détection de failles dans les applications, Connaissance de langages/frameworks courants, Outils de scan de vulnérabilités (nmap, nessus, burp suite etc.), Exploitation de failles pour validation , Simulation d'attaques ciblées en boite noire ou boite grise, Suivi des bases de données CVE, exploit-db, Compréhension des impacts business **Savoir-être et qualités:** utilisation des outils, respect des procédures etc…

COMPÉTENCE 07 : Tester la vulnérabilité sur les Réseaux des applications, site web et les systèmes d'exploitation	
Indications sur la compétence	**Déterminants**
1. Décrire les outils de tests de vulnérabilités ; 2. Tester l'efficacité du réseau et des applications ; 3. Tester les systèmes d'exploitation	**RAST: Tâches 1, 2,3,4, 5,6** **Connaissances :** - Scanners de vulnérabilités réseaux/applications , Outils de tests d'intrusion/pentesting (Kali Linux, Metasploit etc.), Cartographie, détection de services, énumération, Vulnérabilités TCP/IP (SNMP, RDP, SSH, firewalls etc.), Injection SQL, XSS, débordements tampons, Détection de failles dans les APIs, services web, Privilèges, configurations sécurité, patchs manquants, Exploitation de vulnérabilités OS (Windows, Linux, mobile etc.), Définition de périmètre, plan de test, gestion des vulnérabilités, **Savoir-être et qualités:** Travail avec précision, de manière ordonnée et méthodique ; respect des conditions d'utilisation et des règles de sécurité.

COMPÉTENCE 08: Configurer les outils de test de pénétration des systèmes d'exploitation	
Indications sur la compétence	**Déterminants**
1. Utiliser des outils de tests de pénétration/intrusion : 2. Configurer les outils : 3. Configurer les systèmes d'exploitation cibles 4. Elaborer les Scripts intelligents	**RAST** **Tâches : 1,2, 3, 4, 5,6** **Connaissances :** - Kali Linux, Metasploit Framework, Burp Suite, nmap, nikto, etc. Installation et mise à jour des outils, Paramétrage des options, plugins, bases de données, Personnalisation des profils d'analyse, Architecture, services, protocoles réseaux, Fonctionnement des principaux OS (Windows, Linux, mobile etc.), Développement de scripts de tests (Python, Ruby etc.) **Habiletés :** Dextérité, esprit d'analyse et de synthèse, sens de l'organisation, les règles d'éthique et déontologiques ; esprit d'équipe ; rigueur, constance, Efficacité. Sens de l'observation. Perception visuelle. Perception tactile. Perception auditive,

COMPÉTENCE 9 : Proposer les stratégies d'atténuation	
Indications sur la compétence	**Déterminants**
1. Analyser la topologie et les flux réseau ; 2. Identifier les vecteurs d'intrusion réseau ; 3. Évaluer la propagation latérale de l'attaquant ; 4. Utiliser les outils et techniques de forensics réseau ; 5. Concevoir des scénarios de segmentation réseau	**Tâches :1, 2, 3, 4, 5,6** **Connaissances** : - Architecture réseau et périmètre de sécurité, Protocoles, services et ports utilisés, Outils de détection et de prévention réseau, Modèles de menaces et TTP réseau (MITRE ATT&CK), Techniques d'investigation réseau (analyse de logs, de paquets...), Principes de segmentation, de filtrage et de micro-segmentation, Solutions de détection d'intrusion réseau (NIDS, WAF...), Isolation d'hôtes et de VLANs compromis, Restauration et durcissement de la configuration réseau, Plans de continuité applicative, Aspects légaux et conformité réseau **Habiletés :** Dextérité, esprit d'analyse et de

	synthèse, sens de l'organisation, les règles d'éthique et déontologiques ; esprit d'équipe; rigueur, constance, Efficacité. Sens de l'observation. Perception visuelle. Perception tactile. Perception auditive, équipements, Utiliser les consommables etc…

COMPÉTENCE 10 : Configurer les pares-feux et des systèmes de détection d'intrusions	
Indications sur la compétence	**Déterminants**
1. Configurer les pare-feux et des IDS/IPS ; 2. Implémenter une politique de filtrage et de détection 3. Gérer les règles, les signatures et les listes blanches/noires 4. Superviser les événements de sécurité générés	**RAST: tâches 2,3,4, 5,6** **Connaissances :** Architecture réseau, fonctionnement des pare-feux et IDS/IPS - Langages de configuration (iptables, pf, Cisco ASA, Snort, Suricata, Bro, etc.), Interfaces de configuration graphique et ligne de commande, Mécanismes de filtrage et de détection (états de connexion, signatures, comportements anormaux), Méthodologie de définition d'une politique de sécurité réseau, Principes de filtrage et de détection (autorisations, restrictions, alertes), Typologie des règles (autorisées, refusées, alertes), Langages et moteurs de règles/signatures , Mécanismes d'activation/désactivation, de priorisation, Gestion centralisée via une console de supervision, Catégories d'adresses et services réseau, Interprétation des logs et alertes, Corrélation avec les politiques appliquées, Principes de gestion des événements de sécurité **Savoir-être et qualités:** Travail avec précision, de manière ordonnée et méthodique ; respect des conditions d'utilisation et des règles de sécurité.

COMPÉTENCE 11 : assurer la veille technologique en cyberattaque	
Indications sur la compétence	**Déterminants**
1. Assurer la veille technologique et sécuritaire 2. Analyser les nouvelles techniques d'attaques 3. Évaluer l'impact sur l'architecture existante 4. Préconiser des mesures correctives 5. Valider la réponse apportée	**RAST: 1,2,3,4,5 ,6** **Connaissances :** - Sources d'information sur les vulnérabilités et menaces émergentes, Méthodologie de veille (mots-clés, agrégateurs, forums...), Analyse de tendances et évaluation des risques potentiels, Méthodologies d'analyse (modèles d'attaque MITRE ATT&CK...), Fonctionnement des familles de malwares/ransomwares, Techniques de phishing/hameçonnage évoluées, Outils et services des acteurs de la menace, Architecture réseau, systèmes et sécurité en place, Évaluation des risques en fonction des vulnérabilités, Scénarios d'attaque possibles, Tests d'intrusion et détection de surfaces d'attaque, Solutions techniques de protection existantes et émergentes - Paramétrages et déploiements recommandés - Plans de formation et sensibilisation adaptés - Exercices de simulation et de gestion de crise - Méthodes de tests (intrusion, détection...) - Tableaux de bord et reporting - Plans d'amélioration continue - Retour d'expérience et documentation **Savoir-être et qualités:** Travail avec précision, de manière ordonnée et méthodique ; respect des conditions d'utilisation et des règles de sécurité.

REFERENCES BIBLIOGRAPHIQUES

1 Yassine Maleh, 2023, Guide pratique pour devenir un Pentester Professionnel », Eyrolles, Vol.1, 512 pages

2 Damien BANCAL, Franck EBEL, Frédéric VICOGNE, Guillaume FORTUNATO, Jacques BEIRNAERT-HUVELLE, Jérôme HENNECART, Joffrey CLARHAUT, Laurent SCHALKWIJK, Raphaël RAULT, Rémi DUBOURGNOUX, Robert CROCFER, Sébastien LASSON, 12 janvier 2022, « Ethical hacking : apprendre l'attaque pour mieux se défendre », ENI, 6e édition, 970 pages.

3 Nir Yehoshua, Uriel Kosayev, 2021, «Learn practical techniques and tactics to combat, bypass, and evade antivirus software», Packt Publishing, 100 pages.

4 David Kennedy, Jim O'Gorman, Devon Kearns, Mati Aharoni, 2013, HACKING, SÉCURITÉ ET « Tests d'intrusion avec METASPLOIT », Pearson, Vol.1, 400 pages, ISBN: 2744025976, 9782744025976

5 Anne Lupfer, 1er septembre 2010, « Gestion des risques en sécurité de l'information », Eyrolles ,1re édition, 230 pages.

6 Géorgie Weidman, 2014, « Tests de pénétration », Presse à amidon, 1ere Édition, 766 pages.

7 Bruno Favre, Pierre-Alain Goupille, 1er octobre 2005, « Guide pratique de sécurité informatique » DUNOD, 1re édition, 254 pages.

8 Moïse LABONNE, Paul MAGRONG, Yvan OUSTALET, SEPTEMBRE 2006 « L'approche par Compétences dans l'enseignement technique et la formation professionnelle, BÉNIN - BURKINA FASO – MALI » BUREAU RÉGIONAL de L'UNESCO à Dakar (BREDA)

9 République du Cameroun, 2012, Des curricula pour la formation professionnelle initiale, 2010 ARRETE N° 2010/0015/A/MINEPIA DU 30 AOUT 2010 Portant cahier de charges précisant les conditions et les modalités d'exercice des compétences transférées par l'État aux Communes en matière de promotion des activités de production pastorale et piscicole »

10 Document de politique nationale genre (version préliminaire) Yaoundé,74 pages.

11 Commission nationale pour l'UNESCO, 2008, « Tendances récentes et situation actuelle de l'éducation et de la formation des adultes » , Ed.FoA Yaoundé,22 pages.

12 Samurçay R. et Pastré, P. (2004), Stratégie de la formation professionnelle, République du Cameroun, Toulouse : Octarès, 187 pages.

13 Organisation Internationale de la Francophonie (2007), Les guides méthodologiques d'appui à la mise en œuvre de l'approche par compétences en formation professionnelle, Guide - Conception et réalisation des études sectorielles et préliminaires, 77 pages.

14 Organisation Internationale de la Francophonie (2007), Les guides méthodologiques d'appui à la mise en œuvre de l'approche par compétences en formation professionnelle, Guide - Conception et réalisation d'un référentiel de métier-compétences, 83 pages.

15 Organisation Internationale de la Francophonie (2007), Les guides méthodologiques d'appui à la mise en œuvre de l'approche par compétences en formation professionnelle, Guide - Conception et production d'un guide pédagogique, 61 pages.

16 Organisation Internationale de la Francophonie (2007), Les guides méthodologiques d'appui à la mise en œuvre de l'approche par compétences en formation professionnelle, Guides - Conception et production d'un guide d'évaluation, 86 pages.
17 Organisation Internationale de la Francophonie (2007), Les guides méthodologiques d'appui à la mise en œuvre de l'approche par compétences en formation professionnelle, Guides - Conception et production d'un guide d'organisation pédagogique et matérielle, 69 pages.

WEBOGRAPHIE.

https://www.plb.fr/formation/securite/formation-tests-intrusion,24-853.php
https://openclassrooms.com/fr/courses/7727176-realisez-un-test-dintrusion-web/7915475-adoptez-la-posture-d-un-pentester
https://www.doussou-formation.com/formation/formation-en-cybersecurite-et-tests-dintrusion/
https://www.hetic.net/debouches-insertions/metiers-web-internet/pentester
https://www.m2iformation.fr/diplomes-et-certifications/formations/m2i-securite-pentesting/
https://formation-cn.fr/formation/formation-en-cybersecurite/pentest/tests-d-intrusion-niv1/
https://pecb.com/fr/education-and-certification-for-individuals/penetration-testing