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
---
COORDINATION TECHNIQUE DE LA COMPOSANTE II

REPUBLIC OF CAMEROON
Peace-Work-Fatherland

MINISTRY OF EMPLOYMENT AND VOCATIONAL TRAINING

SECRETARIAT GENERAL

Secondary Education and Skills Development Support Project

TECHNICAL COORDINATION OF COMPONENT 2

REFERENTIEL DE FORMATION PROFESSIONNELLE

Selon l'Approche Par Compétences (APC)

SECTEUR : NUMERIQUE

METIER : PENTESTER

NIVEAU DE QUALIFICATION : TECHNICIEN SPECIALISE

Edition 2024



Préface

Afin d'atteindre son objectif de développement à l'horizon 2035, le Gouvernement camerounais a placé la formation professionnelle comme un levier essentiel pour son développement économique et social. Il s'est engagé pour la période 2020-2030 dans un processus ambitieux de réformes et d'investissements visant à améliorer durablement l'accès à une éducation inclusive, équitable et de qualité, tout en renforçant l'efficacité de son pilotage sectoriel.

Eu égard aux défis identifiés, le Gouvernement de la République du Cameroun a reçu un crédit de l'Association Internationale pour le Développement (IDA) dans le but de financer les activités du Projet d'Appui au Développement de l'Enseignement Secondaire et des Compétences pour la Croissance et l'Emploi (PADESCE / P 170561).

C'est dans cette perspective que quarante-cinq (45) référentiels de formation ont été élaborés selon l'Approche Par Compétences dans les secteurs de l'Energie, le Numérique, l'Agro-alimentaire et les Bâtiments et Travaux Publics (BTP) et implantés dans certaines structures de formation professionnelle. A date, lesdits référentiels sont prêts à être mis en œuvre dans les structures de formation professionnelles.

Le présent référentiel de formation est donc un document de référence pour le dispositif de Développement de Compétences Techniques et Professionnelle au Cameroun.

Nous exhortons les acteurs de la formation professionnelle à contribuer à sa mise en œuvre.

Contenu

- ✓ **Rapport de l'Analyse de Situation de Travail (RAST)**
- ✓ **Référentiel de Métier-Compétences (RMC)**
- ✓ **Référentiel de Formation (RF)**
- ✓ **Référentiel d'Evaluation et de Certification (REC)**
- ✓ **Guide Pédagogique (GP)**
- ✓ **Guide d'Organisation Pédagogique et Matérielle (GOPM)**

EQUIPE D'ANIMATION DE L'AST (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

N°	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

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

REMERCIEMENTS

Ce Référentiel de formation 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 de ce Référentiel et dont l'aide a été déterminante pour la bonne conduite des entretiens et la réalisation des contenus de ce Référentiel.

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.

TABLE DES MATIERES

PRÉFACE 2
EQUIPE D'ANIMATION DE L'AST (ANALYSE DE SITUATION DE TRAVAIL) 4
EQUIPE DE REDACTION 4
LISTE DES PERSONNES CONSULTEES 4
REMERCIEMENTS 5
RAPPORT DE L'ANALYSE DE SITUATION DE TRAVAIL (RAST) 11
ABREVIATIONS ET ACRONYMES 11
INTRODUCTION 13
PREMIERE PARTIE : DESCRIPTION GÉNÉRALE DE LA PROFESSION 14
1. DEFINITION DE LA FONCTION DE TRAVAIL 15
2. CONTEXTE PROFESSIONNEL 15
2.1. DESCRIPTION DE L'ENVIRONNEMENT DE TRAVAIL 15
2.2. ÉVOLUTION TECHNOLOGIQUE ET FACTEURS D'INTÉRÊT POUR L'EXERCICE DE LA PROFESSION 16
a) Évolution technologique et conséquences 16
b) Facteurs d'intérêt pour l'exercice de la profession 16
3. APPELLATIONS COURANTES DE LA FONCTION DE TRAVAIL 16
4. PERSPECTIVES ET CHEMINEMENT D'EMPLOI 17
5. CONDITIONS D'EMBAUCHE, REMUNERATION ET HORAIRES DE TRAVAIL – CONDITIONS D'ACCES A LA FORMATION 17
a) Conditions d'embauche, rémunération et horaires de travail 17
b) Conditions d'accès à la formation 18
6. ACCESSIBILITE DES FEMMES AU METIER 18
7. IMPACT DU METIER SUR L'ENVIRONNEMENT 18
a) Au niveau de la santé et de la sécurité 18
b) Au niveau de l'environnement 19
8. FORMATION EN MILIEU DE TRAVAIL 19
DEUXIEME PARTIE : DESCRIPTION DU TRAVAIL 20
1. CONCEPTS ET DEFINITIONS 21
2. DETERMINATION DES TACHES ET DES OPERATIONS 22
3. TABLEAU DES TÂCHES ET DES OPÉRATIONS DU PENTESTER 23
4. CONDITIONS DE REALISATION DES TACHES ET CRITERES DE PERFORMANCE 24
5. IMPORTANCE RELATIVE, FREQUENCE ET COMPLEXITE DES TACHES 28
6. CONSEQUENCES DE L'EVOLUTION TECHNOLOGIQUE SUR LA FONCTION DE TRAVAIL 29
7. CONNAISSANCES, HABILETES ET ATTITUDES 30
REFERENCES BIBLIOGRAPHIQUES 34
REFERENTIEL DE METIER – COMPETENCES (RMC) 35
ABREVIATIONS ET ACRONYMES 36
A. PRESENTATION SUCCINCTE DE LA DEMARCHE DE L'INGENIERIE PEDAGOGIQUE, DU REFERENTIEL DE METIER ET DES AUTRES REFERENTIELS ET GUIDES 39
B. PRESENTATION SOMMAIRE DU MANDAT ET DE LA DÉMARCHE DE RÉALISATION 40
C. PRESENTATION DU METIER ET DE SA SITUATION GENERALE SUR LE MARCHE DU TRAVAIL 42
PREMIERE PARTIE : RESULTATS DE L'ANALYSE DE SITUATION DE TRAVAIL (RAST) 47

I.1.1. DEFINITION DES TERMES USUELS 48
I.1.2. TABLEAU DES TACHES ET OPERATIONS 49
I.1.3. PROCESSUS DE TRAVAIL 51
I.1.4. CONDITIONS DE REALISATION ET LES CRITÈRES DE PERFORMANCE. 51
I.1.5. CONNAISSANCES, HABILITES ET ATTITUDES 57
I.1.6. SUGGESTIONS POUR LA FORMATION 58
DEUXIEME PARTIE : PRESENTATION DES COMPETENCES 60
I.2.1. PRESENTATION DE LA NOTION DE COMPETENCE GENERALE ET DE COMPETENCE PARTICULIERE 61
I.2.2. LISTE DES COMPETENCES GENERALES. 61
I.2.3. LISTE DES COMPETENCES PARTICULIERES 61
I.2.4. MATRICE DES COMPETENCES 62
I.2.5. TABLE DE CORRESPONDANCE 64
COMPÉTENCE 01 : COMMUNIQUER EN MILIEU PROFESSIONNEL 64
COMPÉTENCE 02 : APPLIQUER LES PRINCIPES DE LA SÉCURITÉ DES COMPTES 65
COMPÉTENCE 03 : EXPLOITER L'ARCHITECTURE DES SYSTÈMES INFORMATIQUES DES RÉSEAUX ET DES PROTOCOLES 65
COMPÉTENCE 04 : CONFIGURER LES SYSTÈMES D'EXPLOITATION 65
COMPÉTENCE 05 : UTILISER LES LANGAGES DE PROGRAMMATION 66
COMPÉTENCE 06 : IDENTIFIER LES VULNÉRABILITÉS POTENTIELLES DANS LES SYSTÈMES INFORMATIQUES 66
COMPÉTENCE 07 : TESTER LA VULNÉRABILITÉ SUR LES RÉSEAUX DES APPLICATIONS, SITE WEB ET LES SYSTÈMES D'EXPLOITATION 67
COMPÉTENCE 08 : CONFIGURER LES OUTILS DE TEST DE PÉNÉTRATION DES SYSTÈMES D'EXPLOITATION 67
COMPÉTENCE 9 : PROPOSER LES STRATÉGIES D'ATTÉNUATION 68
COMPÉTENCE 10 : CONFIGURER LES PARES-FEUX ET DES SYSTÈMES DE DÉTECTION D'INTRUSIONS 68
COMPÉTENCE 11 : ASSURER LA VEILLE TECHNOLOGIQUE EN CYBERATTAQUE 69
REFERENCES BIBLIOGRAPHIQUES 70
REFERENTIEL DE FORMATION(RF) 72
ABREVIATIONS ET ACRONYMES 73
II.1. PRESENTATION D'UN REFERENTIEL DE FORMATION 74
II.2. PRÉSENTATION DES CONCEPTS ET DES PRINCIPALES DÉFINITIONS 75
II.3. DESCRIPTION SYNTHESE DU REFERENTIEL DE FORMATION 76
PREMIERE PARTIE : OBJETS DE LA FORMATION 80
II.4. BUTS DU REFERENTIEL 81
II.5. ÉNONCE DES COMPETENCES 82
II.6. MATRICE DES OBJETS DE FORMATION 82
II.7. LOGIGRAMME 85
DEUXIEME PARTIE : PRESENTATION DETAILLEE DES COMPETENCES DU REFERENTIEL 86
Module N°1 : Métier et formation 87
Module N°2 : Communication en milieu professionnel 89
MODULE N°03 : Application des principes de la sécurité des comptes 90

MODULE N° 04 : Exploitation de l'architecture des systèmes informatiques des réseaux et des protocoles 92
MODULE N° 05 : Configuration du système d'exploitation 94
MODULE N° 06 : Utilisation des langages de programmation 96
MODULE N° 07 : Identification des vulnérabilités potentielles dans les Systèmes informatiques 98
MODULE N° 08 : Configuration des outils de test de pénétration des systèmes d'exploitation .. 99
MODULE N° 09 : Tests de vulnérabilité, sur les Réseaux, les applications, site web et les systèmes d'exploitation 100
MODULE N°10 : Proposition des stratégies d'atténuation 102
MODULE Nº 11 : Configuration des pares-feux et des systèmes de détection d'intrusions..... 104
MODULE N°12 : Veille technologique en cyberattaque 105
Module 13 : Entrepreneuriat 107
Module 14 : Stage professionnel 108
RÉFÉRENCES BIBLIOGRAPHIQUES 111
REFERENTIEL D'EVALUATION ET DE CERTIFICATION(REC) 113
III.1. PRESENTATION D'UN REFERENTIEL D'EVALUATION 114
a) Nature 114
b) Structure 114
c) Finalités 114
d) Modalités d'évaluation des compétences 115
e) Eléments prescriptifs 115
III.2. PRÉSENTATION DES CONCEPTS ET DES PRINCIPALES DÉFINITIONS 115
a) Concepts 115
b) Principales définitions 116
III.3. DESCRIPTION SYNTHÈSE DU RÉFÉRENTIEL DE FORMATION 117
III.4. PRESENTATION DES OUTILS 124
a) Tableau de spécifications 124
b) Description de l'épreuve 124
c) Fiche d'évaluation 124
III.5. ÉVALUATION DES COMPÉTENCES 125
COMPÉTENCES TRADUITES EN SITUATIONS 129
Compétence 01: Se situer au regard du métier et de la formation 130
Durée d'apprentissage : 130
30 h 130
COMPÉTENCE 02 : COMMUNIQUER EN MILIEU PROFESSIONNEL 133
DURÉE D'APPRENTISSAGE 133
45H 133
COMPÉTENCES TRADUITES EN COMPORTEMENT 145
REFERENCES BIBLIOGRAPHIQUES 190
GUIDE PEDAGOGIQUE(GP) 192
ABREVIATIONS ET ACRONYMES 193
PREMIERE PARTIE : STRATEGIES DE FORMATION 195
IV.1. PRÉSENTATION GENERALE DU GUIDE 196
1. Nature 196
2. Buts 196

IV.2. PRINCIPES PÉDAGOGIQUES....197
IV.3. PROJET DE FORMATION ET INTENTIONS PÉDAGOGIQUES....197
IV.4. PRÉSENTATION GÉNÉRALE DU RÉFÉRENTIEL DE FORMATION....198
IV.5. LISTE DES COMPÉTENCES....199
IV.6. STRATEGIES PEDAGOGIQUES....202
IV.7. PRÉSENTATION DU CHRONOGRAMME....203
DEUXIEME PARTIE : SUGGESTIONS PEDAGOGIQUES....206
IV.8. PRESENTATION DES FICHES DE SUGGESTION PEDAGOGIQUES....207
COMPETENCE N°1 : Se situer au regard du métier et de la formation....208
COMPETENCE 02 : Communiquer en milieu professionnel....210
COMPETENCE 03 : Appliquer le principe de la sécurité des comptes....213
COMPETENCE 04 Exploiter l'architecture des systèmes informatiques des réseaux et des protocoles....219
COMPETENCE 05 : Configurer les systèmes d'exploitation....224
COMPETENCE 06 : Utiliser les langages de programmation....230
COMPETENCE 07 : Identifier les vulnérabilités potentielles dans les Systèmes informatiques238
COMPETENCE 08 : Configurer les outils de test de pénétration des systèmes d'exploitation.241
COMPETENCE 09 : Tester la vulnérabilité sur les Réseaux des applications, site web et les systèmes d'exploitation....245
COMPETENCE 10 : Proposer les stratégies d'atténuation....250
COMPETENCE 11 : Configurer les pares-feux et des systèmes de détection d'intrusions....256
COMPÉTENCE 12 : Assurer la veille technologique en cyberattaque....260
COMPETENCE N°13 : Rechercher un emploi....263
COMPETENCE 14 : S'intégrer en milieu professionnel....265
REFERENCES BIBLIOGRAPHIQUES....268
GUIDE D'ORGANISATION PEDAGOGIQUE ET MATERIELLE(GOPM)....270
ABREVIATIONS ET ACRONYMES....271
V.1. INTRODUCTION ET PRÉSENTATION DU GUIDE D'ORGANISATION PÉDAGOGIQUE ET MATÉRIELLE....273
V.2. BUTS DU RÉFÉRENTIEL DE FORMATION....274
V.3. DESCRIPTION DU REFERENTIEL DE FORMATION....274
V.4. ORGANISATION DE LA FORMATION....278
1. Conditions d'admission....278
2. Présentation du logigramme....279
3. Présentation du chronogramme....281
4. Modes d'organisation à privilégier....284
5. Promotion du programme....288
V.5.RESSOURCES HUMAINES....289
1. Qualifications professionnelles....289
2. Besoins quantitatifs en matière de ressources humaines....290
3. Orientation du recrutement et compétences recherchées....290
4. Perfectionnement des formateurs....291
V.6. ORGANISATION PHYSIQUE ET MATÉRIELLE....293
6.1. RESSOURCES MATERIELLES....293
6.1.1. Machinerie, équipement et accessoires....294
6.1.2. Outils et instruments....297

6.1.3. Matériels de sécurité 300
6.1.4. Matière d'œuvre et matière première.....303
6.1.5. Mobilier et équipement de bureau 304
6.1.6. Matériel audiovisuel et informatique. 305
6.1.7. Matériel didactique 306
6.2. RESSOURCES PHYSIQUES.....309
6.2.1. Types d'aménagement physique à considérer.....309
6.2.2. SCENARIO DE RECHANGE 309
RÉFÉRENCES BIBLIOGRAPHIQUES.....312
ANNEXES.....314
A- PLAN D'AMENAGEMENT (PROPOSITION) D'UNE SALLE DE CLASSE.....315
B- EXEMPLE DE PLAN DE MASSE D'UNE STRUCTURE DE FORMATION.....316
C- EXEMPLE DE PLAN D'OCCUPATION D'SCS, DU METIER PENTESTER 317

RAPPORT DE L'ANALYSE DE SITUATION DE TRAVAIL (RAST)

ABREVIATIONS ET ACRONYMES

APC	Approche Par Compétences
RAST	Rapport de l'Analyse de la Situation de Travail
CQP	Certificat de Qualification Professionnelle
CVE	Common Vulnerabilities and Exposures
DFOP	Direction de la Formation et de l'Orientation Professionnelles
DQP	Diplôme de Qualification Professionnelle
DTS	Diplôme de Technicien Spécialisé
ISO	International Organization for Standardization
NIST	National Institute of Standards and Technology

OWASP	Open Web Application Security Project
PME	Petite et Moyenne Entreprise
RSS	Really Simple Syndication
SA	Société Anonyme
SARL	Société à Responsabilité Limité
VAE	Validation des Acquis de l'Expérience

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 prend 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'Analyse de Situation de Travail (AST) est une étape cruciale dans le développement des référentiels successifs (Référentiel de Formation ; Référentiel d'Évaluation), des outils d'accompagnement et de planification (Guide Pédagogique ; Guide d'Organisation Pédagogique et Matérielle) liés au métier**.**

La valeur ajoutée de la présente Analyse de Situation de Travail est garantie par la qualité des études sectorielles menées (enquêtes et bases de données consultées) et la diversité d'origine des professionnels qui ont été invités à apporter leur contribution.

Le présent Rapport d'Analyse de Situation de Travail (RAST) rend compte des résultats de la mission d'Analyse de Situation de Travail et des rencontres sous forme de groupes de travail, d'entretiens qui se sont déroulés 01 au 15 mars 2024, dans les régions du littoral, Nord, Extrême-Nord, Ouest et centre.

PREMIERE PARTIE : DESCRIPTION GÉNÉRALE DE LA PROFESSION

1. DEFINITION DE LA FONCTION DE TRAVAIL

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.

2. CONTEXTE PROFESSIONNEL

2.1.Description de l'environnement de travail

L'environnement de travail d'un pentester, ou testeur d'intrusion, est dynamique et axé sur la résolution de problèmes. Les pentesters travaillent dans des entreprises spécialisées en sécurité informatique, des cabinets de conseil ou en tant que consultants indépendants. Ils peuvent se déplacer fréquemment pour effectuer des tests d'intrusion sur site chez les clients, ou bien travailler à distance en utilisant des outils de test et des logiciels spécialisés. Les pentesters doivent être à l'aise avec les technologies de réseau, les systèmes d'exploitation, les protocoles de sécurité et les vulnérabilités courantes. Ils doivent également être capables de travailler de manière autonome, de gérer leur temps et de communiquer efficacement avec les clients pour comprendre leurs besoins et présenter les résultats de leurs tests d'intrusion. En raison de la nature du travail, les pentesters doivent respecter les normes éthiques et légales en matière de tests de sécurité, tout en étant constamment à jour sur les dernières techniques et tendances en matière de piratage et de sécurité informatique.

Secteur d'activité

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.

Condition de travail

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.

2.2.Évolution technologique et facteurs d'intérêt pour l'exercice de la profession

a) Évolution technologique et conséquences

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.

b) Facteurs d'intérêt pour l'exercice de la profession

Plusieurs facteurs peuvent susciter un fort intérêt pour l'exercice de la profession de pentester. Tout d'abord, le domaine de la cyber sécurité est en constante évolution et offre un environnement dynamique et stimulant. Les pentesters sont constamment confrontés à de nouveaux défis et doivent constamment se tenir à jour sur les dernières techniques de piratage et de défense. Cela permet de développer et d'affiner en permanence leurs compétences techniques. De plus, la profession offre une grande variété de projets et d'entreprises à travers lesquels les pentesters peuvent travailler. Chaque test d'intrusion présente des systèmes et des configurations uniques, ce qui rend le travail intéressant et diversifié. Par ailleurs, le rôle des pentesters dans la protection des systèmes informatiques et la prévention des cyberattaques est crucial dans un monde de plus en plus connecté. Contribuer à renforcer la sécurité et à protéger les données confidentielles des entreprises est une motivation importante pour exercer cette profession. Enfin, les pentesters ont l'opportunité de travailler avec des professionnels talentueux et de collaborer étroitement avec des équipes de sécurité informatique, ce qui favorise l'apprentissage continu et le développement professionnel.

3. APPELLATIONS COURANTES DE LA FONCTION DE TRAVAIL

Les appellations courantes de la fonction de travail d'un pentester peuvent être **:**

- Testeur d'intrusion ;
- Analyste en sécurité des systèmes d'information ;
- Auditeur en sécurité des réseaux ;
- Technicien en cyberdéfense ;
- Analyste de vulnérabilité ;
- Hacker éthique.

4. PERSPECTIVES ET CHEMINEMENT D'EMPLOI

Les perspectives d'emploi dans le métier de pentester sont prometteuses et en constante croissance. Avec la montée en puissance des cyberattaques et la prise de conscience croissante de l'importance de la sécurité informatique, la demande de professionnels de la sécurité qualifiés, y compris les pentesters, ne cesse d'augmenter. Les entreprises de tous les secteurs cherchent à renforcer leurs défenses contre les cybermenaces, ce qui crée un besoin continu de services de tests d'intrusion. En termes de cheminement de carrière, les pentesters peuvent progresser en acquérant de l'expérience et en développant leurs compétences techniques. Ils peuvent évoluer vers des rôles de gestion de la sécurité ou de conseil en sécurité. Obtenir des certifications pertinentes, telles que CEH (Certified Ethical Hacker) ou OSCP (Offensive Security Certified Professional), peut également renforcer les perspectives d'emploi et l'employabilité. En clair, les pentesters peuvent envisager un avenir prometteur dans un domaine en pleine expansion, avec de nombreuses possibilités d'avancement professionnel et de développement de carrière.

5. CONDITIONS D'EMBAUCHE, REMUNERATION ET HORAIRES DE TRAVAIL – CONDITIONS D'ACCES A LA FORMATION

a) Conditions d'embauche, rémunération et horaires de travail

Conditions d'embauche

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 des 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.

Rémunération

En dépit de l'absence ou de la non-disponibilité d'une convention collective pour le secteur, l'offre de rémunération est généralement très attrayante et les conditions de rémunération sont fixées en accord avec les parties entre l'entreprise et la personne recrutée. Catégorie 10 du BIT

Horaires de travail

Quant aux horaires de travail, ils sont définis par la règlementation en vigueur. Le technicien pentester travaille généralement pendant 8 à 12 heures de travail par jour. Toutefois, ces durées peuvent être influencées par l'affluence et les conditions de travail, les heures supplémentaires sont rémunérées. Le

travail nécessite parfois des horaires adaptés (temps perdu pendant une panne du réseau, intempéries etc.…).

b) 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 ;
- Subir avec succès à un test de sélection à l'entrée en formation.

Les équivalents du sous-système anglophone sont également admis.

6. ACCESSIBILITE DES FEMMES AU METIER

Les professionnels sont unanimes que l'accessibilité des femmes dans le métier de pentester est faible en raison des traditions culturelles, les stéréotypes de genre et les préjugés persistants. Historiquement, le domaine de la sécurité informatique a été largement dominé par les hommes, ce qui a créé des barrières et des déséquilibres de genre. Cependant, au fil du temps, il y a eu une prise de conscience croissante de l'importance de la diversité et de l'inclusion dans ce secteur. Des initiatives visant à encourager les femmes à poursuivre des carrières techniques et à briser les stéréotypes ont été mises en place régulièrement dans les entreprises. Dans certaines entreprises, il existe des programmes de mentorat, des initiatives de sensibilisation et des efforts pour créer un environnement de travail plus égalitaire. Bien que des progrès aient été réalisés, il reste encore du travail à faire pour surmonter les obstacles et créer des opportunités égales pour les femmes dans le métier de pentester.

7. IMPACT DU METIER SUR L'ENVIRONNEMENT

a) Au niveau de la santé et de la 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 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.

Il est donc essentiel que les pentesters prennent des mesures pour garantir leur propre sécurité, telles que l'utilisation d'environnements de test isolés et sécurisés, ainsi que l'application de meilleures pratiques en matière de sécurité lors de l'exécution des tests.

Les entreprises et les organisations qui emploient des pentesters doivent également s'assurer de fournir un environnement de travail sûr, en veillant à la santé mentale et à la sécurité physique des professionnels de la sécurité informatique.

b) Au niveau de l'environnement

Le métier de pentester en lui-même n'a pas d'impact direct sur l'environnement. Les activités de test d'intrusion se concentrent sur l'évaluation de la sécurité des systèmes informatiques et des réseaux, sans générer de déchets ou de polluants physiques. Cependant, il est important de noter que l'utilisation d'infrastructures informatiques et de ressources énergétiques nécessaires au fonctionnement des systèmes de test peut avoir un impact indirect sur l'environnement. Par exemple, les serveurs, les équipements de réseau et les dispositifs de test utilisent de l'électricité, et leur utilisation peut contribuer à la consommation d'énergie et aux émissions de carbone associées. Les pentesters et les organisations qui les emploient peuvent prendre des mesures pour minimiser leur empreinte environnementale, telles que l'utilisation d'équipements écoénergétiques, la mise en place de politiques de gestion de l'énergie et la promotion de pratiques de travail durable, comme le télétravail lorsque cela est possible. Ainsi, bien que le métier de pentester n'ait pas d'impact direct sur l'environnement, la prise de conscience des enjeux environnementaux reste importante pour promouvoir des pratiques plus durables dans l'ensemble du secteur de la sécurité informatique.

8. FORMATION EN MILIEU DE TRAVAIL

La formation en milieu de travail est essentielle pour un pentester afin de développer et d'améliorer ses compétences techniques et ses connaissances en matière de sécurité informatique. En raison de la nature évolutive du domaine, de nombreuses compétences nécessaires pour être un pentester efficace sont acquises grâce à une expérience pratique sur le terrain. La formation en milieu de travail peut prendre différentes formes, telles que des mentorats, des projets pratiques, des missions d'équipe, des formations internes ou des programmes de développement professionnel. Les pentesters bénéficient souvent d'une exposition à une variété de systèmes, de réseaux et de technologies, ce qui leur permet d'acquérir une expérience diversifiée et une compréhension approfondie des vulnérabilités et des méthodes d'attaque. La formation en milieu de travail est généralement complétée par des certifications professionnelles spécifiques à la sécurité, telles que CEH (Certified Ethical Hacker), OSCP (Offensive Security Certified Professional) ou CISSP (Certified Information Systems Security Professional), qui renforcent la crédibilité et les compétences du pentester.

DEUXIEME PARTIE : DESCRIPTION DU TRAVAIL

Sont présentés dans cette partie, les définitions usuelles, le processus de travail, les tâches et opérations, les conditions de réalisation et les critères de performance rattachés au métier de Technicien spécialisé en pentester.

1. CONCEPTS ET DEFINITIONS

Quelques définitions sont consignées dans cette partie pour faciliter la compréhension des aspects ci-dessus évoqués.

Les tâches :

- sont les principales activités qu'une personne doit mener dans l'exercice de sa profession ;
- sont les différents types de travaux qui sont exécutés de façon régulière ou ponctuelle ;
- correspondent à un ensemble d'actions permettant d'obtenir un résultat précis, un service ou un produit particulier.

Les opérations :

- correspondent aux étapes à franchir pour remplir une tâche donnée;
- décrivent de quelle manière est exécutée une tâche.

Les conditions de réalisation :

- renvoient à la situation dans laquelle la tâche s'effectue;
- précisent le degré d'autonomie entourant l'exécution de la tâche, les consignes et les normes à respecter;
- renseignent sur les lieux de travail, les conditions environnementales et l'équipement utilisé pour exécuter une tâche;
- indiquent les références à consulter et le matériel nécessaire à l'exécution d'une tâche donnée.

Les critères de performance :

- indiquent les caractéristiques observables et mesurables pour évaluer les éléments essentiels d'une réalisation satisfaisante d'une tâche;
- indiquent les caractéristiques observables et mesurables pour évaluer les produits réalisés pendant le processus de réalisation d'une tâche;
- sont énoncés sous forme d'exigences, de normes de qualité et de règles qui permettent de voir que la tâche est bien exécutée.

- **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. Le processus de travail suivant est couramment observé et est assez générique pour coller aux différentes situations de travail :

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

2. DETERMINATION DES TACHES ET DES OPERATIONS

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.
Les informations recueillies permis de :

- Déterminer les tâches principales qui structurent l'activité de pentester.
- Établir les opérations correspondant à chacune des tâches, c'est-à-dire les actions qu'implique la réalisation de cette tâche.
- Ordonnancer les tâches et les opérations.

L'exercice de détermination des tâches a permis de proposer ce qui suit :

3. Tableau des tâches et des opérations du Pentester

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 les 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 les politiques de sécurité.	
4. **Tester l'efficacité du système sécurité**	4.1. Coordonner les simulations d'attaques informatiques.	4.2. Apprécier la réactivité des équipes de sécurité.	4.3. Interpréter 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

4. CONDITIONS DE REALISATION DES TACHES ET CRITERES DE PERFORMANCE

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 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).

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	• 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.

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.	

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 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.	• 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

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.	• Utilisation correcte des scans de vulnérabilités • Application correcte des règles de filtrage • Evaluation correcte des configurations systèmes • Simulation minutieuse des scénarios réels

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.	

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,	• Fréquence minutieuse des mises à jour, • Identification correcte des sources d'informations sur les cyberattaques,

• 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.	• Adoption correcte des bonnes pratiques en matière de sécurité ; • Utilisation correcte des nouveaux outils automatiques de test

IMPORTANCE RELATIVE, FREQUENCE ET COMPLEXITE DES TACHES

IMPORTANCE

L'importance de la tâche est exprimée selon une échelle variant de très important à peu important en comparant les tâches les unes aux autres. Les données obtenues sont converties en pourcentage selon l'information reçue des professionnels de façon individuelle.
On constate que les tâches énumérées sont toutes très importantes ou moyennement importantes, cela justifie évidemment leur choix au sein du métier.
Sachant que l'importance de la tâche est déterminée par les conséquences plus ou moins fâcheuses que peut avoir le fait de mal l'exécuter ou de ne pas l'exécuter du tout, il est logique que certaines tâches soient celles nettement considérées plus importantes. En fait, elles apparaissent comme des tâches qui sont au cœur du métier.

FRÉQUENCE

La fréquence de la tâche est habituellement exprimée en pourcentage du temps consacré au travail sur une période d'une semaine ou d'une durée convenable à la réalisation de l'ensemble des tâches identifiées pour le métier.

COMPLEXITE DES TACHES

Le degré de complexité des tâches est exprimé selon une référence variant de très complexe à peu complexe en considérant la nature des difficultés, des problèmes ou des situations rencontrées et la possibilité de les surmonter dans un contexte normal d'exécution. Si les risques d'erreur dans l'exécution de la tâche sont minimes, la tâche est considérée comme facile, alors que s'ils sont élevés, la tâche est considérée comme complexe.

Les professionnels du secteur présents à l'AST ont évalué la complexité de chacune des tâches. Les données présentées dans le tableau suivant correspondent aux moyennes des résultats obtenus pour chacun des éléments identifiés. Les données sur le degré de complexité des tâches, fréquence sont présentées dans le tableau ci-dessus. Les professionnels présents à l'AST ont évalué la fréquence relative des tâches et leur importance. Les données présentées dans le tableau suivant correspondent aux moyennes des résultats obtenus pour chacun des éléments identifiés.

N°	Tâches	Importance	Fréquence	Degré de complexité
1	Analyser les vulnérabilités du système informatique	Très : 80% Moyen : 20 % Peu : 0%	Très : X	3
2	Réaliser des tests d'intrusion sur les réseaux et les applications	Très : 100 % Moyen : 0% Peu :0%	Très : X	5
3	Elaborer des stratégies de sécurité	Très : 100 % Moyen : 0 % Peu : 0%	Très : X	4
4	Tester l'efficacité du système sécurité	Très : 100 % Moyen : 0 % Peu : 0%	Très : X	5
5	Effectuer des audits de sécurité des systèmes informatiques	Très : 100 % Moyen : 0 % Peu : 0%	Très : X	5
6	Assurer une veille permanente sur les menaces de piratage	Très : 100 % Moyen : 0 % Peu : 0%	Très : X	4

X= mode sélectionné ; Tâche complexe =5 et 1 = tâche d'exécution simple

6. CONSEQUENCES DE L'EVOLUTION TECHNOLOGIQUE SUR LA FONCTION DE TRAVAIL

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), l'intelligence artificielle et le Big Data, présentent également de nouveaux défis en matière de sécurité, nécessitant une compréhension approfondie des risques potentiels.

7. CONNAISSANCES, HABILETES 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.

Ci-dessous sont présentés les éléments détaillés liés aux connaissances, habiletés et attitudes nécessaires pour l'accomplissement des tâches par le Pentester. Ces éléments ont été unanimement validés par les participants au focus group.

8. Connaissances

Le Pentester doit avoir des capacités d'écoute pour comprendre et apprendre, la capacité de résolution logique de problèmes, la compréhension des concepts fondamentaux de la sécurité informatique est nécessaire, y compris les principes de base des réseaux, des systèmes d'exploitation, des protocoles de communication et des architectures de sécurité. Les pentesters doivent également avoir une connaissance approfondie des différentes techniques d'attaque et des vulnérabilités courantes, telles que les attaques par injection, les attaques par déni de service, les attaques de force brute, etc. Ils doivent être familiers avec les outils et les logiciels utilisés pour effectuer des tests d'intrusion, tels que les scanners de vulnérabilités, les outils d'analyse de code, les frameworks d'exploitation, etc. De plus, des compétences en programmation sont souvent nécessaires, notamment dans des langages tels que Python, Ruby, Java, C/C++, etc., afin de comprendre et de manipuler les systèmes informatiques de manière efficace. Enfin, les pentesters doivent avoir de solides compétences en résolution de problèmes, en analyse des risques et en communication, car ils doivent être en mesure de documenter et de rapporter les résultats de leurs tests de manière claire et professionnelle.

. Il peut aussi avoir les connaissances dans les domaines suivants :

- 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 d'une rétro-ingénierie ;

. Habiletés

Le Pentester doit être apte dans la résolution des problèmes et la planification du service qu'il offre. Il connait l'utilisation des techniques d'intrusion et de résolution des problèmes en matière de sécurité informatique. Il a des aptitudes à la compréhension des menaces en cybersécurité, l'exploitation des sources ouvertes de manière sécurisé, la détection, la qualification et l'analyse d'informations pertinentes à la réussite de la mission. Cette activité est au cœur de sa mission. Le Pentester doit être capable de travailler à des horaires non traditionnels et utiliser des équipements appropriés à cet effet (transport). Il doit avoir un relationnel avec ses entreprises (PME, SA, SARL etc…). Il doit être capable de travailler en équipe et avoir une oreille attentive sur tout ce qui entoure son métier.

Attitudes

Comme attitudes, de l'Analyse de la Situation de Travail permet entre autres la mise en évidence des connaissances, des habiletés, et des attitudes requises ou souhaitées pour l'exécution des tâches étudiées.

Les 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.

Ci-dessous sont présentés les éléments détaillés liés aux connaissances, habiletés et attitudes nécessaires pour l'accomplissement des tâches par le pentester. Ces éléments ont été unanimement validés par les participants au focus group.

ATTITUDES ET COMPORTEMENTS	**Très Important**	**Important**	**Moyen**	**Négligeable**
Capacité de gérer le temps (et ponctualité)	X			
Honnêteté	X			
Intégrité	X			
Attitude positive		X		
Responsable /Sens des responsabilités		X		
Recherche de perfectionnement	X			
Esprit d'initiative / Autonomie/ Débrouillardise	X			
Persévérance /Endurance physique/ Adaptabilité	X			
Créativité	X			
Discrétion	X			
Calme		X		
Discipline		X		
Capacité d'assimilation		X		
Sens de l'ordre		X		
TRAVAIL EN ÉQUIPE ET/OU INSERTION	**Très important**	**Important**	**Moyen**	**Négligeable**
Capacité de participer aux discussions		X		

Capacité de travailler en équipe / Entraide / Esprit d'équipe		X		
Respect des directives		X		
CONNAISSANCES ET/OU APPRENTISSAGE	**Très important**	**Important**	**Moyen**	**Négligeable**
Connaissance des techniques	X			
Capacité d'écoute pour comprendre et apprendre		X		
Lire, comprendre et utiliser des documents écrits		X		
Capacité de résolution logique de problème		X		
Capacité de rédaction			X	
Connaissances en mathématiques, sciences physiques			X	
Connaissance de la langue anglaise			X	
Connaissance du secourisme et des règles de sécurité			X	
Connaissance des équipements		X		
Connaissance de l'informatique (Initiation)		X		
Connaissance des systèmes experts		X		
Connaissance de l'électronique	X			
Connaissance sur les mesures de sécurité	X			

9. SUGGESTIONS CONCERNANT 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.

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 Les guides méthodologiques d'appui à la mise en œuvre de l'approche par les compétences en formation professionnelle/ Organisation internationale de Francophonie – 2009.

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.

REFERENTIEL DE METIER – COMPETENCES (RMC)

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

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 tiré 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 Baccalauréat 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. • Subir avec succès à un test de sélection à l'entrée en formation.

TITRES	DESCRIPTIONS
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 travail	**Lieux de travail** : Entreprise
	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

TITRES	DESCRIPTIONS
	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 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.

TITRES	DESCRIPTIONS
	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.1.1. 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.1.2. 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 six. 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.	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.	3.2 Mettre en place des pares-feux et des systèmes de détection d'intrusion.	3.3 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.1.3. 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.1.4. 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),	• 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

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 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.1.5. 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 :

- À la dimension personnelle (compréhension de ses propres sentiments et émotions, résolution de conflits internes, autres) ;
- À 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 d'une rétro-ingénierie	**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, - 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	**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 - Responsable - Recherche de perfectionnement - Esprit d'initiative / Autonomie/ - contrôle de ses sentiments et émotions, - Résolution de conflits internes ; - Autres…

I.1.6. 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

I.2.1. 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.

I.2.2. 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

I.2.3. 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

I.2.4. 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 / 10			8	8	6	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	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.												

I.2.5. 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:	**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

5. Gérer les périphériques :	**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

COMPÉTENCE 10 : Configurer les pares-feux et des systèmes de détection d'intrusions	
Indications sur la compétence	**Déterminants**
	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

REFERENTIEL DE FORMATION(RF)

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

II.1. PRESENTATION D'UN REFERENTIEL DE FORMATION

Nature

Le Référentiel de Formation ou Programme présente un ensemble cohérent et significatif de compétences à acquérir. Il est conçu selon une démarche qui tient compte à la fois de facteurs tels que les besoins de formation, la situation de travail, les buts ainsi que les moyens pour réaliser la formation.

Le référentiel de formation constitue un outil de référence dont une partie ou la totalité a un caractère prescriptif, c'est-à-dire obligatoire.

Les compétences du référentiel incluent une description des résultats attendus au terme de la formation, elles ont une influence directe sur le choix des activités pratiques et théoriques d'enseignement et d'apprentissage. Cependant, le référentiel de formation ne comprend ni les activités pratiques, ni les contenus de cours, ni les stratégies, ni même les moyens d'enseignement et de formation. Le référentiel d'évaluation et les guides pédagogiques et d'organisation pédagogique et matérielle apportent plus de précisions en ces domaines et suggèrent diverses approches et divers contenus de formation. Le référentiel de formation est également un outil de référence pour l'évaluation des apprentissages et la validation des acquis de l'expérience (VAE). Ainsi, pour obtenir leur Diplôme de fin de formation, les apprenants doivent démontrer qu'ils ont maîtrisé les compétences inscrites dans le référentiel de formation. Les instruments d'évaluation de la formation et de validation des acquis sont conçus en fonction de ce document.

En somme, le référentiel de formation est une source d'information exhaustive sur les compétences attendues pour l'exercice d'un métier, au seuil du marché du travail.

Structure

Le référentiel de formation se divise en deux parties. La première, d'intérêt général, contient quatre éléments : les buts du référentiel, les énoncés des compétences (compétences générales, compétences spécifiques), la matrice des objets de formation et le logigramme. Dans la deuxième partie du référentiel, on décrit les composantes de chacune des compétences retenues pour la formation.

Finalité

Le Référentiel de formation a pour finalité de permettre la formation des personnes aptes à exercer le métier pour lequel le Référentiel a été élaboré avec l'appui de méthodologues, de professionnels de formation et d'experts-métiers.

Dans un Référentiel de formation, la description générale du métier visé est une synthèse des tâches et opérations qui y sont associées. Elle porte de plus sur les principaux champs et secteurs d'activité, les différents outils techniques ou technologies utilisés et les principales responsabilités qui s'y rattachent. Cette synthèse est constituée à partir de l'information contenue dans le Rapport d'Analyse de Situation de Travail (RST) et des choix effectués au moment de la détermination des compétences. Les buts du référentiel de formation traduisent les orientations particulières en matière de formation professionnelle pour l'emploi.

Éléments prescriptifs

Le Référentiel de formation professionnelle au Cameroun comprend : le Référentiel métier-compétences (RMC), le Référentiel de formation (REF), le Référentiel d'évaluation (REV), le Guide

pédagogique (GPE), le Guide d'organisation pédagogique et matérielle (GPM), avec une distinction entre les différents documents. C'est ainsi qu'on peut distinguer : les référentiels et les guides.

Essentiellement, ce qui distingue les Référentiels des autres documents est le fait qu'ils devraient comporter des éléments prescriptifs ou d'application obligatoire pour toutes des Structures de formation.

Les guides et autres documents présentent des informations facultatives, élaborées et rendues disponibles pour faciliter la réalisation de la formation. Les compétences issues du Référentiel de métier-compétences (RMC) et celles retenues dans le scénario de formation du Référentiel de formation (REF) constituent l'essence même de la formation. Au Cameroun, leur application n'est ni facultative ni optionnelle.

En résumé, ont un caractère prescriptif :

- la liste des compétences ;
- chaque compétence traduite en comportement : l'énoncé de la compétence, les éléments de la compétence, le contexte de réalisation, les critères de performance ;
- chaque compétence traduite en situation : l'énoncé de la compétence, les éléments de la compétence, le contexte de réalisation, la situation de mise en œuvre de la compétence, les critères d'engagement dans la démarche ;
- la durée totale du référentiel de formation (la durée de la formation liée à chaque module reste facultative pour accorder une certaine souplesse aux structures de formation et aux équipes de formateurs / enseignants pour prendre en considération le contexte, le rythme d'apprentissage et les besoins des apprenants) ;
- le temps de réalisation de l'évaluation.
- Présentation des concepts et des principales définitions.

II.2. PRÉSENTATION DES CONCEPTS ET DES PRINCIPALES DÉFINITIONS

a. Compétence

Regroupement ou ensemble intégré de connaissances, d'habiletés et d'attitudes permettant de faire, avec succès, une action ou un ensemble d'actions telles qu'une tâche ou une activité de travail.

b. Compétences particulières

Compétences directement liées à l'exécution des tâches et à une évolution appropriée dans le contexte du travail. Elles renvoient à des aspects concrets, pratiques, circonscrits et directement liés à l'exercice d'un métier.

c. Compétences générales

Compétences correspondant à des activités plus vastes qui vont au-delà des tâches, mais qui contribuent à leur exécution. Ces activités sont généralement communes à plusieurs tâches et transférables à plusieurs situations de travail. Elles requièrent habituellement des apprentissages de nature plus fondamentale.

d. Compétence traduite en comportement

Se prête surtout aux apprentissages faciles à circonscrire et pour lesquels on possède des données objectives. Cette méthode s'applique bien à la définition de comportements relatifs aux tâches ou aux productions propres à un métier.

e. Compétence traduite en situation

Présente une démarche dans laquelle s'inscrit une personne en vue d'un développement personnel et professionnel. Cette méthode s'applique mieux s'il s'agit de viser particulièrement l'acquisition de compétences qui présentent une forte composante liée à des attitudes ou à des savoir-être. Elle permet de prendre en compte les dimensions profondes de la personnalité, des valeurs et des attitudes.

f. Contexte de réalisation

Renseigne sur la situation de mise en œuvre de la compétence au seuil du marché du travail. Il permet de circonscrire et de mieux comprendre l'ampleur, l'importance et le champ d'application de la compétence. Il contribue à en fixer les limites et à saisir son degré de complexité.

g. Critères de performance

Définissent les exigences qui permettront de juger de l'atteinte des éléments de la compétence et, par ricochet, de la compétence elle-même.

h. Critères d'engagement dans la démarche

Sont à la compétence traduite en situation ce que les critères de performance sont à la compétence traduite en comportement. Ils permettent de porter un jugement sur l'acquisition de la compétence.

II.3. DESCRIPTION SYNTHESE DU REFERENTIEL DE FORMATION

Le scénario de formation se trouve au cœur du référentiel de formation. Il consiste à présenter les choix qui ont résulté de la définition des compétences issues du Référentiel de Métier-Compétences (elles-mêmes découlant de l'AST). Ces compétences sont traduites en actions observables et en résultats mesurables, éléments sur lesquels reposent l'acquisition des compétences par l'apprenant et leurs évaluations. Le scénario de formation est complété par deux autres éléments :

- la détermination du nombre d'heures d'enseignement de chaque compétence ;
- l'établissement d'une séquence d'apprentissage qui détermine l'ordre logique d'acquisition de la compétence.

En plus de mettre en évidence la liste des compétences requises pour exercer un métier, le référentiel de formation les décrit de manière exhaustive et pose des balises qui déterminent une démarche d'acquisition desdites compétence.

L'exercice d'un métier met à contribution un ensemble de compétences en interrelation à un moment donné de l'exécution des tâches et des opérations. Ces interrelations sont mises en évidence dans la matrice des compétences contenue dans le Référentiel de Métier-Compétences. Le référentiel de formation prend en considération ces interrelations et les transpose dans la description des compétences qui constitue son essence même.

Cette transposition conduit à un référentiel de formation qui est d'abord pertinent, c'est-à-dire qui respecte les caractéristiques et les exigences du métier. Il est aussi cohérent, pour maintenir un équilibre entre les composantes et être applicable et réalisable. Ces dernières caractéristiques signifient que les compétences d'un référentiel doivent prendre en considération les moyens accessibles, mais qu'elles doivent également être formulées de façon à faciliter leur acquisition par l'apprenant. En conséquence, selon les modalités de réalisation de la compétence, le référentiel de formation mise sur deux techniques différentes pour décrire les compétences : la traduction en comportement et la traduction en situation.

Enfin, il importe de bien prendre en considération les liens entre les diverses compétences d'une part, et entre les compétences et le processus de travail d'autre part, pour bien décrire les compétences et la nature des relations qui les unissent.

En se servant des deux outils de base utilisés pour l'élaboration du référentiel de métier-compétences, à savoir la matrice des compétences et la table de correspondance, il est possible de produire un scénario de formation sous la forme de la matrice des objets de formation, le logigramme de la séquence d'acquisition des compétences et une description détaillée des compétences en comportement ou en situation.

DONNEES ADMINISTRATIVES

Niveau de qualification : **Technicien spécialisé**
Année d'approbation :2024

Type de sanction :	**Technicien spécialisé**
Nombre d'unités :	94
Volume horaire lié aux compétences générales	360
Volume horaire lié aux compétences particulières	1005
Durée totale :	1365
Conditions d'accès à la formation	Être âgée au moins de dix-sept ans, justifiant d'un niveau scolaire de Baccalauréat Scientifique, Technique industrielle

Liste des compétences du référentiel de formation

N°	Énoncé de la compétence	Durée	CP	CG	Unités	Types d'objets	Types de compétences	Titre du Module
1	Se situer au regard du métier et de la formation	30	0	30	2	S	G	Métier et Formation
2	Communiquer en milieu professionnel	45	0	45	3	S	G	Communication en milieu professionnel
3	Appliquer le principe de la sécurité des comptes	60	0	60	4	S	G	Application du principe de sécurité des comptes
4	Exploiter l'architecture des systèmes informatiques des réseaux et des protocoles	60	0	60	4	C	G	Exploitation de l'architecture des systèmes informatiques des réseaux et des protocoles
5	Configurer les systèmes d'exploitation	60	0	60	4	C	G	Configuration des systèmes d'exploitation
6	Utiliser les langages de programmation	60	0	60	4	C	G	Utilisation des langages de programmation
7	Identifier les vulnérabilités potentielles dans les Systèmes informatiques	90	90	0	6	C	P	Identification des vulnérabilités potentielles dans les Systèmes informatiques
8	Configurer les outils de test de pénétration des systèmes d'exploitation	120	120	0	8	C	P	Configuration des outils de test de pénétration des systèmes d'exploitation
9	Tester la vulnérabilité sur les réseaux, les applications, site web et les systèmes d'exploitation	150	150	0	10	C	P	Tests de la vulnérabilité, sur les Réseaux, les applications, site web et les systèmes d'exploitation
10	Proposer les stratégies d'atténuation	120	120	0	8	C	P	Proposition des stratégies d'atténuation

11	Configurer les pares-feux et des systèmes de détection d'intrusions	120	120	0	8	C	P	Configuration des pares-feux et des systèmes de détection d'intrusions
12	Assurer la veille technologique en cyberattaque	90	90	0	6	C	P	Veille technologique en cyberattaque
13	Rechercher un emploi	45	0	45	3	S	G	Entreprenariat
14	S'intégrer en milieu professionnel	315	315	/	21	S	P	Stage
	Total	**1365**	**1005**	**360**	**94**			
			73,62%	**26,38%**				

Une unité = 15 heures

PREMIERE PARTIE : OBJETS DE LA FORMATION

II.4. BUTS DU REFERENTIEL

Les buts du référentiel de formation traduisent les orientations particulières en matière de formation professionnelle pour l'emploi. Il reprend aussi les buts généraux de formation professionnelle. Le Référentiel de formation prépare donc la personne à devenir un travailleur du secteur de la cybersécurité pouvant mener des activités de Pentester seul, en équipe ou sous supervision, pour le compte d'une entreprise ou en auto emploi.

La nature du travail et les caractéristiques de l'environnement imposent au Pentester de respecter strictement les règles et les consignes de sécurité autant pour la protection des travailleurs que de celle de l'environnement. Il doit aussi maîtriser les techniques de secourisme et de survie.

Étant donné que le pentester travaille souvent en équipe ou supervision, il doit démontrer de bonnes attitudes relationnelles, tout en veillant à préserver l'image de l'entreprise pour laquelle il réalise les activités d'évaluation de la sécurité d'un système, la réalisation des tests d'intrusion, l'analyse des résultats, la rédaction des rapports et la Sensibilisation à la sécurité informatique.

Outre les compétences liées directement au métier de Pentester, le référentiel de formation vise, conformément aux buts généraux de la formation professionnelle, à :

- Rendre la personne efficace dans l'exercice de son métier, soit :
  - Lui permettre, dès l'entrée sur le marché du travail, de jouer les rôles, d'exercer les fonctions et d'exécuter les tâches et les activités associées à son métier ;
  - Lui permettre d'évoluer adéquatement dans un milieu de travail (ce qui implique des connaissances et des habiletés techniques et technologiques en matière de communication, de résolution de problèmes, de prise de décisions, d'éthique, de santé et de sécurité, etc.).
- Favoriser l'intégration de la personne à la vie professionnelle, soit :
  - Lui faire connaître le marché du travail en général ainsi que le contexte particulier de son métier ;
  - Lui faire connaître ses droits et responsabilités comme travailleur ou travailleuse ;
- Favoriser l'évolution de la personne et l'approfondissement de savoirs professionnels, soit :
  - Lui permettre de développer son autonomie et sa capacité d'apprendre ainsi que d'acquérir des méthodes de travail ;
  - Lui permettre de comprendre les principes sous-jacents aux techniques et aux technologies utilisées ;
  - Lui permettre de développer sa faculté d'expression, sa créativité, son sens de l'initiative et son esprit d'entreprise ;
  - Lui permettre d'adopter des attitudes essentielles à son succès professionnel, de développer son sens des responsabilités et de viser l'excellence.
- Assurer la mobilité professionnelle de la personne, soit :
  - Lui permettre d'adopter une attitude positive à l'égard des changements ;
  - Lui permettre de se donner des moyens pour gérer sa carrière, notamment par le développement de ses habiletés interpersonnelles et celles liées au travail d'équipe et à la gestion des responsabilités au sein d'une équipe.

II.5. ÉNONCE DES COMPETENCES

a) Compétences générales

N°	Compétences générales	Tâches liées
01	Se situer au regard du métier et de la formation	1
02	Communiquer en milieu professionnel	1, 2, 3, 4, 5,6
03	Appliquer le principe de la sécurité des comptes	1, 2, 3, 4, 5,6
04	Exploiter l'architecture des systèmes informatiques des réseaux et des protocoles	1, 2, 3, 4, 5,6
05	Configurer les systèmes d'exploitation	1, 2, 3, 4, 5,6
06	Utiliser les langages de programmation	1, 2, 3, 4, 5,6
13	Rechercher un emploi	1, 2, 3, 4, 5,6

b) Compétences particulières

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

II.6. MATRICE DES OBJETS DE FORMATION

C'est un tableau à double entrée. Il s'agit d'une matrice qui permet de voir les liens qui unissent des éléments placés à l'horizontale et des éléments placés à la verticale.

Le lien fonctionnel (●) entre une compétence particulière et une compétence générale indique que, dans le référentiel de formation, la relation qui existe dans le marché de travail est prise en compte.

Le lien fonctionnel (▲) entre une compétence particulière et une ou plusieurs étapes du processus de travail annonce qu'au cours de l'acquisition de cette compétence, les étapes sont intégrées.

Malgré les liens existants sur le marché du travail, les symboles □ et △ ne sont pas noircis, indiquant que ceux-ci ne sont pas pris en considération dans la formation, c'est-à-dire dans l'acquisition des compétences particulières.

La matrice des objets de formation présente également les durées de formation retenues pour l'enseignement technologique, l'apprentissage pratique de chacune des compétences et leur évaluation.

Les compétences sont placées dans la matrice des objets de formation selon un ordre séquentiel, allant du premier module au dernier.

Les indications (C) et (S) présentent une compétence traduite en comportement et une compétence traduite en situation respectivement.

De manière globale, la matrice des objets de formation ci-dessous présente une démarche intégrée de la formation qui est reprise schématiquement dans le logigramme de la séquence d'acquisition des compétences.

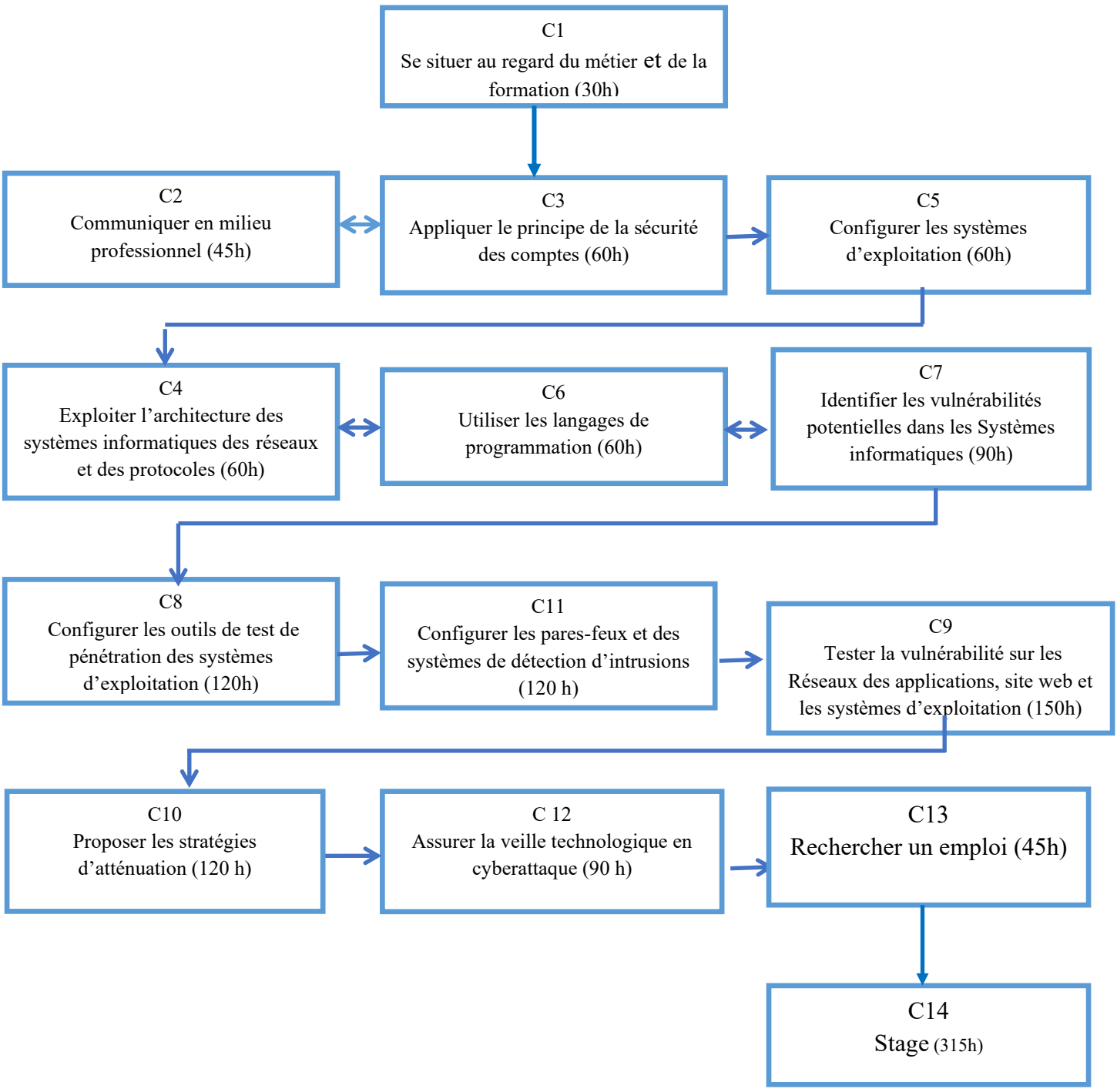
La logique qui a présidé à la conception de la matrice influe sur la séquence d'enseignement des modules. De façon générale, on prend en considération une certaine progression dans la complexité des apprentissages et le développement de l'autonomie de l'apprenant. De ce fait, l'axe vertical présente les compétences particulières dans l'ordre à privilégier pour la formation et sert de point de départ pour l'agencement de l'ensemble des modules. Certains deviennent ainsi préalables à d'autres ou doivent être vus en parallèle.

Pentester (Technicien) Compétences particulières	**Compétences générales**										**Processus de travail**			**Durée (heures)**	**Nombre**
	Numéro de la compétence	**Type d' objectif**	**Durée (heure)**	Se situer au regard du métier et de la formation	Communiquer en milieu professionnel	Appliquer le principe 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	Rechercher un emploi	Planifier le travail à réaliser	Exécuter le travail en adoptant les mesures de sécurité	Contrôler la qualité du travail.		
Numéro de la compétence				1	2	3	4	5	6	13					**7**
Type d'objectif				S	S	S	C	C	C	S					
Durée (heure)				30	45	60	60	60	60	45				**360**	
COMPÉTENCES PARTICULIÈRES															
Identifier les vulnérabilités potentielles dans les Systèmes informatiques	7	C	90	○	●	●	●	●	●	●	▲	▲	▲		
Configurer les outils de test de pénétration des systèmes d'exploitation	8	C	120	○	●	●	●	●	●	●	▲	▲	▲		
Tester la vulnérabilité, sur les réseaux, les applications, site web et les systèmes d'exploitation	9	C	150	○	●	●	●	●	●	●	▲	▲	▲		
Proposer les stratégies d'atténuation	10	C	120	○	●	●	●	●	●	●	▲	▲	▲		
Configurer les pares-feux et des systèmes de détection d'intrusions	11	C	120	○	●	●	●	●	●	●	▲	▲	▲		
Assurer la veille technologique en cyberattaque	12	C	90	○	●	●	●	●	●	●	▲	▲	▲		
S'intégrer en milieu professionnel	14	S	315	○	●	●	●	●	●	●	▲	▲	▲		
Durée de la formation (heures)			**1005**											**1365**	
Nombre de compétences	**7**														**14**

II.7. LOGIGRAMME

Le logigramme est une représentation schématique de l'ordre d'acquisition des compétences. Celles-ci peuvent être distribuées par semestre en tenant compte de leur niveau de complexité et des liens établis entre elles.

Le logigramme assure une planification globale de l'ensemble des compétences du référentiel de formation et permet de voir l'articulation qui existe entre les compétences.



DEUXIEME PARTIE : PRESENTATION DETAILLEE DES COMPETENCES DU REFERENTIEL

Module N°1 : Métier et formation	**Code** : **MEF01**	**Durée** : **30 h**
Énoncé de la compétence traduite en situation : se situer au regard du métier et de la formation		
CONTEXTE DE RÉALISATION • À l'aide des données à jour sur le métier ; • Au contact de personnes ressources du métier ou en milieu de travail ; • À l'occasion d'une démarche d'orientation ou de réorientation professionnelle.		
ELEMENTS DE COMPETENCE	**MISE EN ŒUVRE DE LA COMPETENCE**	**CRITERES D'ENGAGEMENT DANS LA DEMARCHE**
1. S'informer sur le métier	1.1 S'informer à propos du marché du travail : perspectives d'emploi, rémunération, possibilités d'avancement et de mutation, critères et processus de sélection des candidats et des candidates 1.2 S'informer de la nature et des exigences de l'emploi (tâches, conditions de travail, critères d'évaluation, droits et responsabilités) au cours de visites, d'entrevues, de rencontres d'information animées par un représentant ou une représentante de l'industrie, d'examens de documentation, etc. 1.3 Inventorier les habiletés, aptitudes, attitudes et connaissances nécessaires pour pratiquer le métier 1.4 Présenter les données collectées et discuter de sa perception du métier	• Description judicieuse de la nature et exigences de l'emploi • Inventaire judicieux les habiletés, aptitudes, attitudes nécessaires pour pratiquer le métier • Identification correcte des particularités du milieu professionnel
2. S'informer sur le programme de formation et engagement de la démarche	2.1 Présentation du contenu de la formation ; 2.2 Présentation de la démarche de formation ; 2.3 Présentation des modalités de l'évaluation de sanction 2.4 Faire part de ses premières réactions en ce qui a trait à la formation	• Présentation correcte du contenu de la formation ; • Présentation correcte de la démarche de formation ; • Présentation correcte des modalités de l'évaluation de sanction

3.Évaluer et confirmer son engagement	3.1 Faire un bilan de ses goûts, de ses aptitudes, de ses connaissances du domaine et de ses qualités personnelles 3.2 Comparer son bilan avec les exigences liées à la formation et à l'exercice du travail ; 3.3 Reconnaître les forces qui faciliteront son travail ainsi que les faiblesses qu'il faudra palier 3.4 Donner les raisons qui motivent son choix de poursuivre ou non la démarche de formation 3.5 Examiner la possibilité de créer son entreprise ou de travailler à son compte	• Présentation correcte d'un bilan de ses goûts, aptitudes, connaissances du domaine ainsi que de ses qualités personnelles • Justification de sa décision quant au fait de poursuivre ou non le programme de formation • Détermination correcte de son attirance pour l'auto-emploi

Module N°2 : Communication en milieu professionnel	Code :COM 02	Durée :45 heures
Enoncé de la compétence traduite en situation : Communiquer en milieu professionnel		
CONTEXTE DE REALISATION À partir des documents et ressources techniques ; À partir des principes de communication ; À l'aide des matériels et outillages appropriés ; À partir d'une situation de travail.		

ELEMENTS DE COMPETENCE	MISE EN ŒUVRE DE LA COMPETENCE	CRITERES D'ENGAGEMENT DANS LA DEMARCHE
1- Utiliser les termes et expressions indispensables pour la communication en milieu de travail	1.1 Appréhender le langage professionnel 1.2 Utiliser les connaissances du lexique professionnel.	• Traduction correcte du sens général et des idées essentielles d'un message • Interprétation exacte du sens général et des idées principales d'un texte.
2-Traiter les informations	2.1 Relever les propos essentiels du texte 2.2 Repérer et classer les thèmes du texte	• Reformulation juste des éléments importants des propos du texte • Classement approprié des principales manifestations thématiques.
3- Produire les messages indispensables à la vie professionnelle et sociale	3.1 Présenter une pratique professionnelle 3.2 Présenter une situation de travail 3.3 Expérimenter des situations de communication.	• Production judicieuse d'un message. • Élaboration conforme d'un plan de rédaction.
4- Communiquer oralement	4.1 S'informer des principes généraux de la communication orale 4.2 Exprimer oralement un message sur des sujets à portée professionnelle.	• Appropriation parfaite des principes de communication • Expression avec éloquence des sujets.
5- Rendre compte de son activité	5.1 Rendre compte du résultat d'une activité 5.2 Faire part d'une situation inhabituelle.	• Application correcte des techniques de rédaction • Rédaction correcte compte rendu

MODULE N°03 : Application des principes de la sécurité des comptes	Code : APS03	Durée : 60h

Enoncé de la Compétence traduite en situation : Appliquer le principe de la sécurité des comptes

CONTEXTE DE REALISATION :

- Dans toute situation comportant des risques pour la santé et la sécurité de l'intervenant et de la clientèle.
- A partir :
  - des lois, des règlements et des normes relatives à santé, à la sécurité au travail, à l'hygiène, à la salubrité et à la préservation de l'environnement ;
  - de consignes et d'instructions.
- À l'aide :
  - D'accessoires et équipements de protection individuelle (EPI) et collective (EPC) ;
  - d'une trousse de premiers soins ;
  - de notices, de guides et de manuels d'utilisation.

CRITERES GENERAUX DE PERFORMANCE :

- Disponibilité des services et capacité à assurer la continuité d'activité.
- Rapidité d'exécution des tâches et traitements.
- Faculté d'évolution et d'adaptation aux changements
- Respect des lois, des règlements et des normes.
- Application correcte des mesures d'hygiène, de salubrité, de sécurité, de santé et de protection de l'environnement.
- Intervention judicieuse en cas d'urgence.

Éléments de compétence		Critères particuliers de performance
1.	S'informer des lois et des règlements sur la santé et la sécurité au travail.	• Interprétation juste de la législation du travail. • Relevé approprié des normes et des procédures de santé et de sécurité au travail. • Repérage adéquat de l'information dans les documents et les pictogrammes.
2.	Gérer les identités	• Respect judicieux du nombre d'identités • Respect judicieux du délai de provisioning d'une nouvelle identité • Renouvellement approprié des mots de passe
3.	Contrôler les mots de passe	• Sécurisation correcte des mots de passe • Respect de la complexité des mots de passe • Respect du délai de réinitialisation d'un mot de passe oublié/compromis

4.	Contrôler les accès	• Authentification correcte des accès ; • Respect strict du délai d'approbation d'une demande d'accès • Détection correcte du Nombre de violations.
5	Détecter les activités anormales	• Respect strict du délai entre la survenue et détection d'un incident • Génération efficace des alertes ; • Analyse approfondie du trafic réseau.
6	Élaborer la Journalisation et traçabilité	• Gestion efficace du délai d'agrégation des logs dans l'outil de SIEM ; • Gestion efficace des logs ; • Gestion efficace de la traçabilité.
7	Gérer les incidents	• Détections et résolution efficace des compromissions ; • Détermination correcte du taux de réussite des plans de reprise d'activité testés • Evaluation correcte de la maturité par des audits et la certification ;

MODULE N° 04 : Exploitation de l'architecture des systèmes informatiques des réseaux et des protocoles	Code : EAS04	Durée : 60 h

Énoncé de la compétence traduite en comportement : ***Exploiter l'architecture des systèmes informatiques des réseaux et des protocoles***

CONTEXTE DE REALISATION

- À l'intérieur, dans un bureau
- Travail effectué individuellement ou en équipe ou sous supervision.

À partir :

- de problèmes réels ou simulés
- de consignes et d'instructions
- de situations propres à une intrusion

À l'aide :

- d'un ordinateur,

CRITÈRES GÉNÉRAUX DE PERFORMANCE :

- taux de disponibilité des services et capacité à assurer la continuité d'activité ;
- débit maximal pouvant être atteint, notamment pour les réseaux ;
- temps de réponse des systèmes et des communications réseau ;
- capacité du système à supporter une augmentation de charge ;
- rapidité d'exécution des tâches et traitements ;
- faculté d'évolution et d'adaptation aux changements ;
- capacité des systèmes à communiquer entre eux ;
- niveau de robustesse contre les attaques et protection des informations.
- facilité d'administration, de maintenance et de dépannage ;
- efficience dans l'utilisation des ressources matérielles et logicielles ;
- - équilibrage de l'activité sur l'ensemble des composants ;
- possibilité de faire évoluer les capacités de manière proportionnée aux besoins ;
- capacité à retracer les opérations et flux de données de bout en bout ;
- facilité de contrôle et de certification de la conformité du système.

Éléments de compétence		Critères particuliers de performance
1	Identifier les composants des systèmes informatiques	• Choix exact du matériel • Identification correcte des données • Identification correcte des logiciels

2	Utiliser l'architecture système et applicative	• Utilisation correcte de l'architecture système et applicative • Suivi correct de l'architecture système et applicative • Isolation/Sécurisation correcte des applications.
3	Utiliser les réseaux	• Contrôle efficace des latences des communications • Gestion appropriée de la fiabilité des transmissions • Sécurité et confidentialité correctes des échanges.
4	Appliquer les protocoles de communication	• Identification judicieuse des types de protocole • Contrôle correct de la charge réseau • Vérification de la Robustesse et résistance efficace aux aléas.

MODULE N° 05 : Configuration du système d'exploitation	Code : CSE05	Durée : 60h

Enoncé de la compétence traduite en comportement : *Configurer les systèmes d'exploitation*

CONTEXTE DE REALISATION

- À l'intérieur, dans un bureau
- Travail effectué individuellement ou en équipe ou sous supervision.

À partir :

- de problèmes réels ou simulés
- de consignes et d'instructions
- de situations propres à une intrusion

À l'aide :

- D'un ordinateur,

CRITERES GENERAUX DE PERFORMANCE :

- Respect des bonnes pratiques de configuration ;
- Stabilité et robustesse ;
- Performance des paramètres systèmes pour maximiser les ressources et accélérer les traitements ;
- -Sécurité de la configuration par des mesures techniques pour se prémunir des failles et attaques ;
- Disponibilité des mécanismes de haute disponibilité et de reprise sur incident ;
- Supervision des outils de surveillance pour contrôler l'état des systèmes et détecter les dysfonctionnements ;
- Maintenance et l'évolution des systèmes par des configurations standardisées et documentées ;
- Portabilité à la compatibilité des configurations sur différentes versions ou distributions d'un même système ;
- Audibilité pour justifier la conformité aux politiques en vigueur ;
- Documentation technique décrivant les règles de configuration

Éléments de compétence		*Critères particuliers de performance*
1	Effectuer l'administration système :	• Gestion efficace de l'administration système ; • Suivi correct des actions d'administration système ; • Respect des procédures d'administration système.
2	Organiser les utilisateurs et les droits	• Supervision efficace des mécanismes d'authentification ; • Supervision efficace de l'Intégrité des comptes utilisateurs ;

		• Suivi correct des actions sur les comptes.
3	Appliquer la sécurité des systèmes d'exploitation	• Gestion efficace de protection contre les vulnérabilités ; • Résistance efficace aux attaques ciblées ; • Détection correcte des compromissions.
4	Contrôler la sécurité des systèmes d'exploitation :	• Gestion efficace des mécanismes de défense ; • Détection correcte des menaces avancées ; • Détermination correcte du Journal des événements de sécurité ; • Réponses efficaces aux incidents.
5	Gérer les périphériques :	• Échanges efficaces avec les périphériques ; • Échange minutieuse des données ; • Vérification correcte de l'intégrité des données échangées ; • Suivi correct des actions sur les périphériques.

MODULE N° 06 : Utilisation des langages de programmation	**Code : ULP06**	**Durée : 60 h**

Enoncé de la compétence traduite en comportement : *Utiliser les langages de programmation*

CONTEXTE DE REALISATION

- A l'intérieur, dans un bureau
- Travail effectué individuellement ou en équipe ou sous supervision.

À partir :

- De problèmes réels ou simulés
- De consignes et d'instructions
- De situations propres à une intrusion

À l'aide :

- D'un ordinateur
- Les logiciels de programmation.

CRITERES GENERAUX DE PERFORMANCE :

- Maîtrise technique du/des langage(s) ;
- Qualité et robustesse du code ;
- Performance applicative, Maintenabilité, Portabilité, Sécurité ;
- Tests et validation ;
- Documentation technique et des commentaires dans le code ;
- Méthodologie des principes et processus de développement (versioning, revue de code etc.) ;

Éléments de compétence		***Critères particuliers de performance***
1	Identifier le langage de programmation	• Identification correcte des caractéristiques et spécificités ; • Comparaison minutieuse des langages entre eux ; • Gestion efficace sur les évolutions et nouveaux langages.
2	Acquérir les notions d'algorithmie et structures de données :	• Gestion efficace de la complexité des algorithmes ; • Implémentation correcte d'algorithmes courants ; • Analyse et optimisation efficace d'algorithmes.
3	Acquérir les notions en Développement web, applicatif et base de données	• Acquisition correcte du HTML/CSS, frameworks front-end comme React, Angular, Langages serveur comme PHP, Node.js, language base de données ; • Acquisition correcte du développement défensif ;

		• Gestion correcte des vulnérabilités ; • Acquisition correcte de la Cryptographie ; • Gestion correcte des identités ;
4	Utiliser la programmation système :	• Utilisation appropriée de la mémoire et threads ; • Langages bas niveau comme C, assemblage ; • Utilisation appropriée du Développement embarqué/temps réel.
5	Sécuriser le code source :	• Exécution correcte des tests de vulnérabilités ; • Attribution appropriée des droits et permissions ; • Utilisation correcte du développement défensif ; • Gestion efficace des vulnérabilités ; • Utilisation judicieuse de la Cryptographie.

MODULE N° 07 : Identification des vulnérabilités potentielles dans les Systèmes informatiques	**Code : IVP07**	**Durée : 90 h**

Enoncé de la compétence traduite en comportement : *Identifier les vulnérabilités potentielles dans les Systèmes informatiques*

CONTEXTE DE REALISATION

- A l'intérieur, dans un bureau
- Travail effectué individuellement ou en équipe ou sous supervision.

À partir :

- De problèmes réels ou simulés
- De consignes et d'instructions
- De situations propres à une intrusion

À l'aide :

- D'un ordinateur,
- Outils de scanne.

CRITERES GENERAUX DE PERFORMANCE :

- Couverture des systèmes et composants analysés ;
- Maîtrise des techniques et outils de détection des vulnérabilités :
- Précision du référencement des vulnérabilités identifiées :
- Pertinence de la classification des vulnérabilités par criticité :
- Exhaustivité de la documentation des résultats ;
- Mise à jour régulière en fonction des évolutions techniques ;
- Communication claire sur les vulnérabilités aux équipes concernées.

Éléments de compétence		***Critères particuliers de performance***
1	Acquérir les connaissances approfondies en sécurité informatique	• Acquisition parfaite des concepts, modèles et normes de référence ; • Identification correcte des nouvelles menaces ; • Transmission correcte des connaissances. • Contrôle exact de l'évolution des connaissances
2	Décrire un audit de configuration	• Vérification correcte du périmètre couvert • Vérification correcte des tests réalisé ; • Précision -pertinente du rapport d'audit produit.

3	Effectuer une analyse statique et dynamique de code source	• Détection correcte des vulnérabilités ; • Précision pertinente des résultats produits ; • Détermination Pertinente des recommandation
4	Effectuer les tests d'intrusion ("penetration testing")	• Exploitation correcte des vulnérabilités ; • Détermination correcte des résultats ; • Exécution correcte du plan d'amélioration.
5	Veiller sur les vulnérabilités	• Identification judicieuse des sources de veille ; • Exploitation correcte des alertes sur les vulnérabilités. • Contextualisation efficace par rapport au système audité

MODULE N° 08 : Configuration des outils de test de pénétration des systèmes d'exploitation	**Code : COTP08**	**Durée : 120h**

Enoncé de la compétence traduite en comportement : *Configurer les outils de test de pénétration des systèmes d'exploitation*

CONTEXTE DE REALISATION

- A l'intérieur, dans un bureau
- Travail effectué individuellement ou en équipe ou sous supervision.

À partir :

- De problèmes réels ou simulés
- De consignes et d'instructions
- De situations propres à une intrusion

À l'aide :

- D'un ordinateur,
- Outils de test ;

CRITERES GENERAUX DE PERFORMANCE :

- Maîtrise technique des outils de tests d'intrusion (Kali Linux, Metasploit, Nmap, Hydra, etc.) ;
- Capacité à personnaliser/paramétrer les outils en fonction du test à réaliser ;
- Exhaustivité de la configuration des modules, plugins et options des outils ;

- Automatisation et planification efficace des tests de pénétration ;
- Gestion avancée des vulnérabilités identifiées (classification, priorisation, remédiation) ;
- Qualité de la documentation des configurations réalisées ;
- Sécurisation des outils pour éviter les détournements ;
- Respect des bonnes pratiques éthiques du pentesting ;
- Rapidité d'analyse et de réaction face à de nouvelles vulnérabilités ;
- Veille technique sur les mises à jour des outils de test.

Éléments de compétence		***Critères particuliers de performance***
1	Utiliser des outils de tests de pénétration d'intrusion :	• Exploitation efficace des fonctionnalités des outils ; • Choix pertinent des outils en fonction des tests ; • Documentation pertinente des résultats.
2	Configurer les outils :	• Sélection pertinente des options/modules ; • Exécution appropriée des tâches de configuration.
3	Configurer les systèmes d'exploitation cibles	• Spécification efficace des OS ciblés ; • Documentation pertinente des services et ports testés ; • Exploitation efficace des mises à jour des configurations
4	Elaborer les Scripts	• Gestion Pertinente des fonctionnalités ; • Vérification correcte de l'efficacité des scripts ; • Documentation pertinente des techniques des scripts

MODULE N° 09 : Tests de vulnérabilité, sur les Réseaux, les applications, site web et les systèmes d'exploitation	**Code : TVR09**	**Durée : 150 h**
Enoncé de la compétence traduite en comportement : *Tester la vulnérabilité, sur les Réseaux, les applications, site web et les systèmes d'exploitation*		
CONTEXTE DE REALISATION ▪ A l'intérieur, dans un bureau ▪ Travail effectué individuellement ou en équipe ou sous supervision. À partir : ▪ De problèmes réels ou simulés		

- De consignes et d'instructions
- De situations propres à une intrusion

À l'aide :

- D'un ordinateur,

CRITERES GENERAUX DE PERFORMANCE :

- Méthodologie rigoureuse dans la planification et la conduite des tests ;
- Connaissance approfondie des techniques d'attaque (intrusion, injection, déni de service, escalade de privilèges...) ;
- Maîtrise des outils de tests de vulnérabilités (scanners réseau, web, applications ;
- Analyse technique experte des résultats pour qualifier les vulnérabilités ;
- Exhaustivité de la couverture des vecteurs d'attaque testés sur le périmètre ;
- Qualité de la documentation produite (rapports précis localisant les failles) ;
- Recommandations pertinentes et applicables pour renforcer la sécurité ;
- Respect de la méthodologie et des règles éthiques du test ;
- Culture de la sécurité (veille technique et réglementaire, bonnes pratiques) ;
- Capacité à expliquer et présenter les résultats de manière pédagogique.

Éléments de compétence		***Critères particuliers de performance***
1	Analyser la topologie et les flux réseau	• collecte judicieuse des informations ; • Visualisation pertinente des flux ; • Evaluation correcte des métriques réseau. • collecte judicieuse des traces réseau ; • recherche appropriée des preuves réseau ; • application correcte de la méthodologique
2	Identifier les vecteurs d'intrusion réseau	• Identification correcte des techniques d'attaque réseau ; • Analyse appropriée des logs et alertes ; • Collecte minutieuse des vecteurs potentiels couverts.
3	Décrire les outils de tests de vulnérabilités :	• Présentation correcte des outils de tests d'intrusion/pentesting ; • Description parfaite des fonctionnalités ; • Détection des vulnérabilités des réseaux/applications.
4	Tester l'efficacité du réseau et des applications :	• Analyse judicieuse des résultats de tests ; • Application efficace des préconisations. • Détection correcte de failles dans les APIs, services web

5	Tester les systèmes d'exploitation :	• Gestion efficace des configurations et services testés ; • Précision correcte du diagnostic de vulnérabilité ; • Recommandation pertinente des correctifs et mesures

MODULE N°10 : Proposition des stratégies d'atténuation	**Code : PSA10**	**Durée : 120 h**
Enoncé de la compétence traduite en comportement : *Proposer les stratégies d'atténuation*		

CONTEXTE DE REALISATION

- A l'intérieur, dans un bureau
- Travail effectué individuellement ou en équipe ou sous supervision.

À partir :

- De réels ou simulés
- De consignes et d'instructions
- De situations propres à une intrusion

À l'aide :

- d'un ordinateur, .

CRITÈRES GÉNÉRAUX DE PERFORMANCE :

- Qualité de l'analyse de risque effectuée en amont ;
- Pertinence des mesures d'atténuation proposées au regard des vulnérabilités identifiées ;
- Prise en compte du niveau de maturité de la cible et de ses contraintes techniques/métiers ;
- Exhaustivité du périmètre couvert par les mesures (actifs, données, processus...) ;
- Priorisation des mesures en fonction du niveau de criticité des risques ;
- Équilibre entre sécurité, performance et facilité de déploiement ;
- Adéquation des mesures avec les bonnes pratiques et référentiels en vigueur ;
- Détail technique des préconisations et de leur mise en œuvre ;
- Indications de coûts et de délais de déploiement ;
- Pertinence du suivi et de l'évaluation proposés pour s'assurer de l'efficacité des mesures ;
- Qualité rédactionnelle et pédagogie du document de recommandations.

Éléments de compétence	***Critères particuliers de performance***

1	Évaluer la propagation latérale de l'attaquant	• Utilisation parfaite des modèles de compromission ; • Simulation efficace des scénarios de propagation ; • Calcul correct des métriques de propagation.
2	Concevoir des scénarios de segmentation réseau	• Elaboration correcte d'un microsegmentation du réseau ; • Gestion efficace des scénarios ; • documentation pertinente de la technique proposée.
3	Analyser les risques et menaces	• Analyse efficace des menaces et vulnérabilités ; • Exploitation correcte du contexte organisationnel et règlementaire ; • Analyse efficace des mises à jour.
4	Réaliser des conseils sur l'architecture sécurité	• Rapprochement pertinent entre les objectifs métiers et niveaux de services attendus ; • Proposition appropriée d'une architecture de sécurité robuste ; • Évolution correcte de la solution en fonction des besoins futurs
5	Élaborer une politique de sécurité	• Production efficace d'une documentation présentant la politique de sécurité ; • Utilisation correcte des bonnes pratiques et référentiels reconnus ; • Elaboration correcte d'un plan d'action de suivi et d'audit.
6	Préconiser des mesures techniques	• Proposition pertinente des solutions exhaustives ; • Déploiement et administration correctes d'une politique de sécurité ; • Reduction efficace des risques.
7	Valider la mise en œuvre	• Validation efficace des tests effectués ; • Utilisation correcte des scénarios de tests ; • Contrôle efficace du respect des spécifications définies.

MODULE Nº 11 : Configuration des pares-feux et des systèmes de détection d'intrusions	**Code : CPSD 11**	**Durée : 120 h**

Enoncé de la compétence traduite en comportement : *Configurer les pares-feux et des systèmes de détection d'intrusions*

CONTEXTE DE REALISATION

- A l'intérieur, dans un bureau
- Travail effectué individuellement ou en équipe ou sous supervision.

À partir :

- de problèmes réels ou simulés
- de consignes et d'instructions
- de situations propres à une intrusion

À l'aide :

- d'un ordinateur,
- .Pare-feu

CRITERES GENERAUX DE PERFORMANCE :

- Maîtrise technique des équipements (pare-feu, IDS/IPS...) et de leur configuration ;
- Qualité et exhaustivité de l'analyse des besoins et des risques en amont ;
- Pertinence des règles/signatures définies au regard des menaces et vulnérabilités ;
- Prise en compte des contraintes métiers et techniques de l'environnement cible ;
- Équilibre entre niveau de sécurité et performance des équipements ;
- Respect des bonnes pratiques de configuration (segmentation, filtrage applicatif...) ;
- Facilité d'administration et de supervision des équipements ;
- Qualité des tests de validation et de la documentation technique produite ;
- Formation et accompagnement des équipes opérationnelles ;
- Capacité à faire évoluer les configurations dans le temps ;

Éléments de compétence		***Critères particuliers de performance***
1	Configurer les pare-feux et des IDS/IPS	• Définition Précise des règles/signatures ; • Validation correcte des tests effectués ; • Documentation correcte des techniques produites
2	Implémenter une politique de filtrage et de détection	• Utilisation correcte des bonnes pratiques de sécurité ; • Déploiement approprié sur l'infrastructure cible ; • Mesure efficace de la politique de filtrage et de détection

3	Gérer les règles, les signatures et les listes blanches/noires	• Réactivité appropriée aux nouvelles menaces ; • Contrôle efficace d'impact des modifications ; • Exploitation correcte de la supervision des configurations.
4	Superviser les événements de sécurité générés	• Exploitation rationnelle des corrélations et alertes remontées ; • Collecte exhaustive des logs et métriques ; • Analyse correcte de reporting des incidents

MODULE N°12 : Veille technologique en cyberattaque	**Code : VTC12**	**Durée : 90 h**
Enoncé de la compétence traduite en comportement : *assurer la veille technologique en cyberattaque*		

CONTEXTE DE REALISATION

- A l'intérieur, dans un bureau
- Travail effectué individuellement ou en équipe ou sous supervision.

À partir :

- de problèmes réels ou simulés
- de consignes et d'instructions
- de situations propres à une intrusion

À l'aide :

- d'un ordinateur,
- Connexion internet

CRITÈRES GÉNÉRAUX DE PERFORMANCE :

- Exhaustivité des sources de veille exploitées (bases de vulnérabilités, rapports de CERT, médias spécialisés, forums techniques, etc.) ;
- Pertinence du filtrage et de la sélection des informations selon leur criticité potentielle ;
- Rapidité de diffusion des alertes sur les nouvelles menaces ou vulnérabilités détectées ;
- Qualité de l'analyse des tendances et de l'évolution des techniques d'attaque ;
- Capacité à anticiper l'émergence de nouveaux vecteurs d'attaque ;
- Pertinence des préconisations pour renforcer la sécurité face aux nouvelles menaces ;
- Mise à jour régulière des procédures de veille et des outils utilisés.

Éléments de compétence		*Critères particuliers de performance*
1	Assurer la veille technologique et sécuritaire -	• diffusion Rapide des alertes sur les nouvelles menaces ; • analyse pertinente des tendances et évolutions ; • Collecte efficace de la documentation des informations.
2	Analyser les nouvelles techniques d'attaques	• Identification précise des vecteurs et failles exploités ; • Évaluation réaliste de la criticité et de l'impact potentiel ; • Exploitation efficace des mises à jour de l'analyse en fonction des retours.
3	Évaluer l'impact sur l'architecture existante	• Analyse correcte des risques encourus ; • Utilisation correcte des scénarios de tests ; • Exploitation Précise de la documentation des résultats
4	Préconiser des mesures correctives	• Rapprochement correct entre les objectifs de sécurité et le niveau de risque ; • Implémentation et pertinence correcte des solutions ; • Exploitation correcte du rapport coût/bénéfice et des contraintes ; • Adaptation correcte du délai de mise en œuvre à la criticité.
5	Valider la réponse apportée	• validation correcte des tests de effectués ; • Production exacte d'une documentation des résultats ; • Vérification correcte du respect des spécifications définies.

Module 13 : Entrepreneuriat	Code : ENT13	Durée : 45 heures

ENONCE DE LA COMPETENCE TRADUITE EN SITAUTION : Rechercher un emploi

CONTEXTE DE REALISATION

A Individuellement ou en équipe

À partir de

- Signalement ou saisie d'opportunités
- Besoins du marché
- Plan d'affaire
- Initiatives personnelles

A l'aide de

- Outils informatiques
- Modèles courants de plans d'affaire

ELEMENTS DE COMPETENCE	MISE EN ŒUVRE DE LA COMPETENCE	CRITERES D'ENGAGEMENT DANS LA DEMARCHE
1. Identifier les conditions de réussite d'un projet de création d'entreprise ou d'auto emploi	1.1 Interpréter l'environnement économique 1.2 Étudier le marché de l'emploi 1.3 Adopter des stratégies individuelles pour une gamme de produits ou de services	• Interprétation succincte de l'environnement économique • Interprétation succincte du marché • Positionnement stratégique dans une gamme de produits ou de services
2. Monter un projet d'installation	2.1. S'approprier les procédures de base de montage d'un projet 2.2. Etudier le milieu 2.3. Collecter les informations 2.4. Identifier le projet 2.5. Rédiger le projet	• Maitrise des procédures de montage de projet • Choix judicieux du milieu • Collectes judicieuses des informations • Identification correcte du projet • Rédaction correcte du projet
3. Rechercher un financement	3.1 Identifier les sources de financement 3.2 Soumettre une demande de financement	• Recherche judicieuse des sources de financement • Montage correct d'un dossier de financement

	3.3 Défendre le projet	• Défendre méticuleux d'un projet
4. Exécuter un projet	4.1 Conduire les opérations du projet 4.2 Mobiliser les ressources humaines et matérielles 4.3 Mettre en œuvre les activités 4.4 Evaluer la mise en œuvre du plan d'affaires 4.5 Suivre son installation 4.6 Evaluer le projet	• Mise en œuvre judicieux du plan • Mobilisation judicieuse des ressources • Mise en œuvre judicieuse des activités • Suivi judicieux du projet • Evaluation correcte du projet
5. S'approprier les techniques de recherche d'emploi	5.1 Répondre à une interview, à une offre d'emploi 5.2 Rédiger un CV 5.3 Rédiger une demande d'emploi/ lettre de motivation.	• Réponse pertinente à une interview, à une offre d'emploi • Rédaction correcte d'un CV • Rédaction judicieuse d'une demande d'emploi, de la lettre de motivation. • Élaboration conforme d'un plan de rédaction.

Module 14 : Stage professionnel	**Code : STG14**	**Durée :315 heures**
Enonce de la compétence traduite en situation : s'intégrer en milieu professionnel		
CONTEXTE DE REALISATION Dans un milieu professionnel En présence de l'encadreur de stage ou tuteur En présence des responsables de l'entreprise. A partir de l'exécution des tâches professionnelles A l'aide de la collaboration étroite entre l'école et l'entreprise.		
ELEMENTS DE COMPETENCE	**MISE EN ŒUVRE DE LA COMPETENCE**	**CRITERES D'ENGAGEMENT DANS LA DEMARCHE**

1- Préparer son séjour en milieu de travail	1.1 Prendre connaissance des modalités et des renseignements relatifs au stage 1.2 S'informer sur l'organisation de l'entreprise 1.3 Se situer dans l'organisation de l'entreprise par rapport à la tâche et à la place occupée dans la structure.	• Recueil des données pertinentes relatives au stage et à l'organisation de l'entreprise • Description exhaustive des tâches prévues pour son stage • Choix judicieux des entreprises susceptibles d'accueillir le stagiaire • Élaboration conforme du dossier de stage.
2- Respecter les principes de discipline et de déontologie	2.1 Présenter les qualités personnelles et professionnelles 2.2 S'informer des consignes des supérieurs, de sécurité, des règlements de l'entreprise et des normes environnementales.	• Respect méticuleux des consignes, des règlements, de la hiérarchie et des normes environnementales • Démonstration correcte des qualités personnelles et professionnelles.
3- Exécuter les activités en milieu de travail	3.1 Observer le contexte du travail 3.2 Effectuer diverses tâches professionnelles 3.3 Vérifier la satisfaction de l'encadreur par rapport aux activités effectuées 3.4 Relater ses observations sur le contexte de travail et sur les tâches exercées dans l'entreprise	• Exécution appropriée des tâches • Assimilation parfaite et démonstration des opérations liées au métier • Développement judicieux des attitudes professionnelles • Utilisation adéquate des matériels de l'entreprise.
4- Comparer ses perceptions aux réalités du métier	4.1 Relater sa perception du métier avant et après le stage 4.2 Évaluer l'influence de l'expérience vécue sur le choix d'un futur emploi.	• Résumé succinct de l'expérience de stage • Démonstration correcte de l'influence du stage sur le choix d'un futur emploi
5- Rédiger le rapport de stage	5.1 S'informer sur le plan de rédaction et du contenu d'un rapport de stage 5.2 Utiliser une expression soutenue dans la rédaction du rapport de stage.	• Respect judicieux des principes de la langue utilisée • Pertinence du contenu du rapport • Rédaction soignée et concise du rapport de stage.

RÉFÉRENCES 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

REFERENTIEL D'EVALUATION ET DE CERTIFICATION(REC)

III.1. PRESENTATION D'UN REFERENTIEL D'EVALUATION

a) Nature

Le Référentiel d'Evaluation (REV) repose sur les compétences issues du Référentiel de Métier-Compétences (RMC) et de celles propres au projet de formation. Il est un guide proposant des orientations en matière d'évaluation des compétences : compétences traduites en comportement et compétences traduites en situation. Différents acteurs évoluant au sein du système de formation professionnelle, ils peuvent définir de manière différente l'expression : évaluation des apprentissages. C'est ainsi que l'apprenant, le formateur, les autres personnes qui travaillent dans la Structure de formation, les responsables de la gestion centrale de la formation, sont amenés à dégager divers points de vue sur la notion d'évaluation, selon qu'ils ont à l'intégrer dans leur apprentissage, à la mettre en application ou à la gérer. Prenant en compte tous ces cas de figure, on peut considérer que l'évaluation se situe au cœur des processus d'apprentissage, de formation et de gestion de la formation professionnelle.
Souvent, l'on a perçu ou retenu de la notion d'évaluation des apprentissages, l'aspect qui consiste à porter un jugement sur la maîtrise des compétences et sur la performance des apprenants qui souhaitent obtenir une qualification. Cette perception limite la place que devrait occuper l'évaluation au sein d'un processus de formation et d'apprentissage. En formation professionnelle, la fonction « évaluation" présente certaines caractéristiques et se déploie en s'appuyant sur des valeurs et des orientations de base. Tous ces éléments constituent un cadre de référence à partir duquel l'évaluation des apprentissages est structurée et mise en œuvre.

b) Structure

Le Référentiel d'Evaluation se présente comme suit :

- une présentation des concepts et des principales définitions ;
- une description synthèse du Référentiel de Formation ;
- une présentation des outils d'évaluation.

c) Finalités

L'évaluation des apprentissages constitue l'un des fondements du système de formation professionnelle. La transparence doit apparaître dans sa mise en place et sa réalisation, car la valeur et la reconnaissance de la qualification en dépendent. Pour être réalisé dans les normes, l'on doit s'appuyer sur une politique nationale d'évaluation des apprentissages.
Le volet le plus connu de l'évaluation est l'évaluation sommative ou de sanction. Les résultats de cette évaluation doivent être exprimés sous forme de « succès » ou d'« échec ». En effet, toute pédagogie de la réussite sur laquelle repose l'APC nécessite une étroite association entre formation, apprentissage et évaluation. L'évaluation doit non seulement être intégrée aux différentes phases d'acquisition des compétences, mais elle doit également constituer l'un des piliers de la démarche d'apprentissage de l'apprenant. L'acquisition d'une compétence ne peut se faire sans que l'apprenant ait développé sa capacité de juger des résultats atteints et de la performance réalisée. Cet aspect de l'évaluation est appelé « évaluation formative », c'est-à-dire un soutien à l'apprentissage par la mesure et l'évaluation de sa progression. Dans la perspective d'une formation qualifiant l'apprenant pour l'exercice d'un métier, on vise un niveau d'acquisition des compétences énoncées dans le programme (REF) qui correspond à celui qui est attendu au seuil d'entrée sur le marché du travail.

d) Modalités d'évaluation des compétences

Il faut relever qu'évaluer une compétence implique des choix afin de ne pas surévaluer. Il faut, en effet, éviter d'évaluer un élément déjà pris en compte plusieurs fois et se concentrer sur les aspects importants de la compétence. Le modèle d'évaluation utilisé en APC impose une façon de faire dans l'élaboration des tableaux de spécifications au regard du nombre de points à distribuer et de la détermination du seuil de réussite. Les tableaux de spécifications regroupent, entre autres, les indicateurs et les critères d'évaluation relatifs aux éléments retenus de la compétence, dans le référentiel de formation, afin de reconnaître chaque compétence et de la sanctionner, en plus de déterminer un seuil de réussite.

e) Eléments prescriptifs

Les compétences issues du Référentiel de Métier-Compétences (RMC) et celles propres au projet de formation constituent l'essence même de cette formation. Leur apprentissage n'est pas facultatif ou optionnel. Les principaux éléments qui seront considérés comme obligatoires ou prescriptifs sont les suivants dans le cadre de la présente formation :

- La durée totale de formation, incluant le temps consacré à l'évaluation. Toutefois, la durée de la formation reliée à chaque compétence est facultative pour accorder une certaine souplesse aux Structures de formation ;
- Les Tableaux de spécifications et leurs différentes composantes :
  - éléments de la compétence et situations de mise en œuvre de la compétence ;
  - stratégies retenues ;
  - indicateurs et critères d'évaluation ;
  - points attribués aux critères d'évaluation ou critères cochés en relation avec le seuil de réussite ;
  - seuil de réussite ;
  - règle de verdict, le cas échéant

III.2. PRÉSENTATION DES CONCEPTS ET DES PRINCIPALES DÉFINITIONS

a) Concepts

La compétence en formation professionnelle se définit comme « le pouvoir d'agir, de réussir et de progresser, qui permet de réaliser adéquatement des tâches ou des activités de travail et qui se fonde sur un ensemble organisé de savoirs (ce qui implique certaines connaissances, habiletés dans divers domaines, perceptions, attitudes, etc.) ». Puisque la compétence se définit de façon multidimensionnelle, son évaluation se doit de l'être également ; toutes les dimensions importantes d'une compétence sont donc considérées au moment d'en évaluer l'acquisition. Ainsi, l'évaluation porte sur les connaissances, les habiletés, les perceptions et les attitudes sur lesquelles se fonde la compétence. Tous les critères de performance d'un programme doivent obligatoirement être atteints et évalués en cours de formation ou aux fins de la sanction.

Le mode d'évaluation privilégiée en formation professionnelle est celui de type « critériel ». Ce type d'évaluation permet d'établir si une personne a atteint le niveau requis, en matière de performance ou de participation, au regard d'une tâche ou d'une activité, et ce, en fonction de critères précis. Il s'agit donc de vérifier dans quelle mesure un apprenant a atteint une compétence déterminée dans le programme de formation, selon les critères de performance du programme et selon les critères définis pour l'évaluation aux fins de la sanction, en évitant de le situer par rapport à ses pairs ou à un groupe.

b) Principales définitions

Activités d'apprentissage.
Actions diverses proposées par le formateur dans le but de favoriser l'atteinte d'un objectif d'apprentissage.

Appréciation.
Démarche de la pensée aboutissant à un jugement de valeur.

Banque d'épreuves.
Réserve d'épreuves couvrant les modules d'un programme de formation. La banque peut être informatisée ou sur papier.

Critère.
Élément auquel se réfère une personne pour juger, apprécier ou définir quelque chose.

Éléments critères.
Caractéristique d'une performance ou d'un produit. On se réfère à cette caractéristique pour mesurer ou donner une appréciation.

Épreuve.
Exercice donné sous forme écrite ou orale que subit un apprenant en classe ou lors d'un examen afin d'être jugé selon ses capacités.

Évaluation.
Action de juger et d'apprécier la valeur d'une chose, d'une technique, d'une méthode ou d'une personne.

Évaluation critériée.
Évaluation de la performance d'une personne lors de l'accomplissement d'une tâche et jugée par rapport à un seuil ou à un critère de réussite.

Évaluation formative.
Démarche d'évaluation qui consiste à vérifier la progression d'un apprenant au regard des objectifs, atteints ou non, à informer l'apprenant et le formateur sur les difficultés rencontrées afin de lui suggérer ou de lui faire découvrir des moyens de renforcer, améliorer ou/et corriger les acquis.

Évaluation multidimensionnelle.
Évaluation dont les différents aspects d'une compétence : savoirs, savoir être et savoir-faire sont pris en compte.

Évaluation de sanction ou certificative.
Évaluation effectuée à la fin d'un module ou d'une formation pour attester de l'acquisition ou non de la compétence ou des compétences.

Fidélité d'un instrument d'évaluation.
Capacité d'un instrument de mesurer avec la même exactitude chaque fois qu'il est utilisé.

Jugement.
Démarche intellectuelle par laquelle une personne se forme une opinion et l'émet.

Règle de verdict.
Élément d'évaluation qui doit être obligatoirement réussi.

Reprise.
Synonyme du passage d'une nouvelle épreuve dans le cadre du même module après constat d'échec ou d'abandon. Le droit à la reprise est acquis lorsque l'apprenant n'a pas atteint le seuil de réussite d'un module.

Seuil de réussite.
Niveau de qualité à partir duquel on considère une performance comme réussie. Il peut s'agir d'une note ou d'une description qualitative se basant sur des critères.
Test d'une épreuve.
Essai d'une épreuve auprès d'un groupe restreint d'apprenants afin de vérifier la faisabilité et la validité de l'épreuve.
Tolérance.
Marge d'inexactitude ou d'erreur admise lors d'une épreuve de connaissances pratiques ou d'activités d'apprentissage pratique
Univoque.
Se dit d'une interprétation unique
Validité d'un instrument d'évaluation.
Capacité d'un instrument de mesurer réellement ce qu'il prétend évaluer.
Versions d'une épreuve.
Différentes épreuves évaluant la même compétence soit par une mise en situation différente, ou par la production d'un produit différent ou par la prestation d'un service différent mais dont les éléments critères sont identiques et de difficulté de même niveau.

III.3. DESCRIPTION SYNTHÈSE DU RÉFÉRENTIEL DE FORMATION

Le scénario de formation se trouve au cœur du référentiel de formation. Il consiste à présenter les choix qui ont résulté de la définition des compétences issues du référentiel métier-compétences (elles même découlant de l'AST). Ces compétences sont traduites en actions observables et en résultats mesurables, éléments sur lesquels reposent l'acquisition par l'apprenant et leur évaluation.

En plus de mettre en évidence la liste des compétences requises pour exercer un métier, le référentiel de formation les décrit de manière exhaustive et pose des balises qui déterminent une démarche d'acquisition desdites compétences. En conséquence, selon les modalités de réalisation de la compétence, le référentiel de formation s'appuie sur deux techniques différentes pour décrire les compétences : la traduction en comportement et la traduction en situation.

Ainsi, le référentiel de formation pour le métier de Pentester traduit les orientations particulières en matière de formation. Il prépare donc la personne à devenir un travailleur du secteur du numérique pouvant mener des activités d'évaluation de la sécurité d'un système d'information à travers différents angles d'attaques seul, en équipe ou sous supervision, pour le compte d'une entreprise ou à son compte personnel.
De plus, le référentiel de formation vise à rendre apte le Pentester à réaliser la simulation des attaques malveillantes pour identification puis exploitation des vulnérabilités au sein du Système Informatique, 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.

Dans l'exercice de son métier, le Pentester doit 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 etc….

Étant donné que le Pentester travaille souvent seul, en équipe ou sous supervision, il doit démontrer de bonnes attitudes relationnelles en milieu de travail ou même dans la société.

a) Tableau synthèse du référentiel de formation

De ce point de vue, les compétences ci-après pour le métier Pentester correspondant aux attitudes, habiletés et comportements attendus de la personne qui exerce ce métier ont été retenues.

N°	Énoncé de la compétence	Durée	CS	CG	Unités	Types d'objets	Types de compétences	Titre du Module	Code
1	Se situer au regard du métier et de la formation	30	0	30	2	S	G	Métier et Formation	**MEF01**
2	Communiquer en milieu professionnel	45	0	45	3	S	G	Communication en milieu professionnel	**COM02**
3	Appliquer le principe de la sécurité des comptes	60	0	60	4	S	G	Application du Principe de la sécurité des comptes	**APS03**
4	Exploiter l'architecture des systèmes informatiques des réseaux et des protocoles	60	0	60	8	C	G	Exploitation de l'architecture des systèmes informatiques des réseaux et des protocoles	**EAS04**
5	Configurer les systèmes d'exploitation	60	0	60	4	C	G	Configuration des systèmes d'exploitation	**CSE05**
6	Utiliser les langages de programmation	60	0	60	4	C	G	Utilisation des langages de programmation	**ULP06**
7	Identifier les vulnérabilités potentielles dans les Systèmes informatiques	90	90	0	6	C	P	Identification des vulnérabilités potentielles dans les Systèmes informatiques	**IVP07**
8	Configurer les outils de test de pénétration des systèmes d'exploitation	120	120	0	8	C	P	Configuration des outils de test de pénétration des systèmes d'exploitation	**COP09**
9	Tester la vulnérabilité sur les Réseaux, les applications, site web et les systèmes d'exploitation	150	150	0	10	C	P	Tests de vulnérabilité sur les Réseaux, les applications, site web et les systèmes d'exploitation	**RVA08**
10	Proposer les stratégies d'atténuation	120	120	0	8	C	P	Proposition des stratégies d'atténuation	**PSA10**

11	Configurer les pares-feux et des systèmes de détection d'intrusions	120	120	0	8	C	P	Configuration des pares-feux et des systèmes de détection d'intrusions	**CPF11**
12	Assurer la veille technologique en cyberattaque	90	90	0	6	C	P	Veille technologique en cyberattaque	**VTC12**
13	Rechercher un emploi	45	0	45	3	S	G	Entreprenariat	**ENT13**
14	S'intégrer en milieu professionnel	315	315	/	21	S	P	Stage	**STG14**
	Total	**1360**	**1005**	**360**	**94**				
			73,62 %	**26,38 %**					

Une unité = 15 heures

L’analyse globale du référentiel de formation est présentée sous forme de tableaux établis avant la rédaction du référentiel d’évaluation. Il s’agit du tableau d’analyse des compétences générales et du processus de travail ainsi que du tableau d’analyse des critères généraux de performance. Ces tableaux, produits à partir de la matrice des objets de formation, permettent de mettre en évidence les liens entre les compétences particulières et le processus de travail ou entre les compétences particulières et les compétences générales, liens qui seront retenus dans la stratégie d’évaluation. Ils permettent également de faire ressortir les critères principaux qui pourront être utilisés dans l’élaboration des outils d’évaluation. Finalement, ils permettent d’éviter la surévaluation qui consisterait à évaluer à de multiples reprises la même compétence ou le même élément de compétence. Ce sont des outils essentiels à l’élaboration des tableaux de spécifications.

b) Tableau d'analyse des compétences générales et du processus de travail

Pentester Compétences particulières	Numéro de la compétence	Type d' objectif	Compétences générales							Processus de travail				
			Se situer au regard du métier et de la formation	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	Rechercher un emploi	Planifier le travail à réaliser	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			1	2	3	4	5	6	13					**7**
Type d'objectif			S	S	S	C	C	C	**S**					
COMPÉTENCES PARTICULIÈRES														
Identifier les vulnérabilités potentielles dans les Systèmes informatiques	7	C	☐	●	●	●	●	●	☐	●	●	●	⊗	
Configurer les outils de test de pénétration des systèmes d'exploitation	8	C	☐	●	●	●	●	●	☐	●	●	●	●	
Tester la vulnérabilité sur les Réseaux, les applications, site web et les systèmes d'exploitation	9	C	☐	●	●	●	●	●	☐	●	●	●	●	
Proposer les stratégies d'atténuation	10	C	☐	●	●	●	●	●	☐	●	●	●	●	
Configurer les pares-feux et des systèmes de détection d'intrusions	11	C	☐	●	●	●	●	●	☐	●	●	●	●	
Assurer la veille technologique en cyberattaque	12	C	☐	●	●	●	●	●	☐	●	●	●	●	
S'intégrer en milieu professionnel	14	S	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	
Nombre de compétences	**7**													**14**

●Réinvestissement au niveau de l'évaluation ⊗ Liens fonctionnels non retenus pour les fins d'évaluation ☐ Aucune application dans le référentiel de formation

c) Table d'analyse des critères généraux de performance

Pentester ***(Compétences traduites en comportement)***	**Numéro de la compétence**	**COMPETENCES TRADUITES EN COMPORTEMENT**	**Durée (h)**	**CRITERES GENERAUX DE PERFORMANCE**								
				Respect des bonnes pratiques de configuration	Disponibilité des services et capacité à assurer la continuité d'activité	Faculté d'évolution et d'adaptation aux changements	Niveau de robustesse contre les attaques et protection des informations	Performance des paramètres systèmes pour maximiser les ressources et accélérer les traitements	Description technique experte des résultats pour qualifier les vulnérabilités	Gestion avancée des vulnérabilités identifiées (classification, priorisation, remédiation) ;	Respect de la méthodologie des principes et processus de développement	Veille technologique sur les mises à jour des outils de test
Communiquer en milieu professionnel	2	C	30	☐	☐	☐	☐	☐	☐	☐	☐	☐
Appliquer les principes de la sécurité des comptes	3	C	60	△	△	△	○	○	○	○	○	○
Exploiter l'architecture des systèmes informatiques des réseaux et des protocoles	4	C	60	△	☐	△	○	○	○	○	○	△
Configurer les systèmes d'exploitation	5	C	60	△	△	△	△	△	△	△	△	○
Utiliser les langages de programmation	6	C	60	△	△	△	△	△	△	△	△	△
Identifier les vulnérabilités potentielles dans les Systèmes informatiques	7	C	90	△	△	△	△	△	△	△	△	△
Configurer les outils de test de pénétration des systèmes d'exploitation	8	C	120	△	△	△	△	△	△	△	△	△
Tester la vulnérabilité sur les Réseaux, les applications, site web et les systèmes d'exploitation	9	C	150	△	△	△	△	△	△	△	△	△
Proposer les stratégies d'atténuation	10	C	120	△	△	△	△	△	△	△	△	△
Configurer les pares-feux et des systèmes de détection d'intrusions	11	C	120	△	△	△	△	△	△	△	△	△
Assurer la veille technologique en cyberattaque	12	C	90	△	△	△	△	△	△	△	△	△

☐ Aucune relation dans le programme de formation △ Retenu au niveau de l'évaluation ○ Critères non retenus pour les fins d'évaluation de sanction.

III.4. PRESENTATION DES OUTILS

Les outils pour l'évaluation de chacune des compétences retenues pour le métier de **''Pentester''** donnent une présentation qui répond bien aux exigences de l'évaluation.
Ces outils comprennent :

- Les tableaux de spécifications ;
- La description de l'épreuve ;
- La fiche d'évaluation ou de la participation.

a) Tableau de spécifications

Le tableau de spécifications pour l'évaluation d'une compétence traduite en comportement ou en situation présente les indicateurs et les critères d'évaluation relatifs aux éléments et aux situations du programme de formation retenus pour l'évaluation aux fins de la sanction. Pour chaque situation ou élément, on formule un ou des indicateurs de performance, qui présentent un aspect à évaluer ou qui précisent sous quel angle on compte évaluer un élément de compétence. Les indicateurs sont accompagnés de critères d'évaluation sur lesquels on se base pour juger si la performance évaluée est satisfaisante.
Pour un objectif pédagogique traduit en comportement, la pondération (ou le poids relatif) accordée à chaque critère est indiquée, ainsi que le seuil de réussite attendu. Les éléments d'évaluation reposent sur des comportements relatifs aux tâches ou aux productions particulières du métier. Pour l'évaluer, on dispose des stratégies d'évaluation suivantes :

- L'évaluation du produit de travail ;
- L'évaluation du processus de travail ;
- Une combinaison des stratégies précédentes.

Pour un objectif pédagogique traduit en situation, on retrouve les critères dont le formateur se sert pour juger (inférer) si la compétence est acquise au-delà de la participation de l'apprenant aux activités.

b) Description de l'épreuve

La description de l'épreuve, élaborée à partir du tableau de spécifications, vise à uniformiser le niveau de complexité des différentes épreuves assorties aux compétences du programme de formation et à soutenir l'élaboration des épreuves administrées dans les centres de formation. Elle est présentée à titre de suggestion et tourne autour de quatre éléments suivants :

- Les renseignements généraux ;
- Le déroulement de l'épreuve ;
- Le matériel ;
- Les consignes particulières.

c) Fiche d'évaluation

La fiche d'évaluation reprend les indicateurs et les critères d'évaluation adoptés pour l'évaluation aux fins de la sanction (tableaux de spécifications) et les précise davantage, le cas échéant, sous forme d'éléments d'observations. Ces fiches peuvent aussi faire mention des marges de tolérance acceptées. Elle fait état de la pondération associée aux critères d'évaluation. Elle présente aussi le seuil de réussite fixé dans le tableau de spécifications. La fiche d'évaluation guide les centres de formation et les formateurs dans la description des épreuves au moment de la réalisation des activités d'évaluation et, comme les descriptions d'épreuve ou de participation, elle est fournie à titre de suggestion.

Lorsque la stratégie d'évaluation correspond à un processus de travail, les épreuves mixtes (connaissances pratiques et activités d'apprentissage pratique) sont recommandées.
Cependant, lorsque la stratégie d'évaluation correspond à un produit, une épreuve conduisant au développement des activités d'apprentissage pratique est recommandée.

III.5. ÉVALUATION DES COMPÉTENCES

a) Modalités d'évaluation formative

Il faut relever qu'évaluer une compétence implique des choix afin de ne pas surévaluer. Il faut, en effet, éviter d'évaluer un élément déjà pris en compte plusieurs fois et se concentrer sur les aspects importants de la compétence. Le modèle d'évaluation utilisé en APC impose une façon de faire dans l'élaboration des tableaux de spécifications au regard du nombre de points à distribuer et de la détermination du seuil de réussite. Les tableaux de spécifications regroupent, entre autres, les indicateurs et les critères d'évaluation relatifs aux éléments retenus de la compétence, dans le référentiel de formation, afin de reconnaître chaque compétence et de la sanctionner, en plus de déterminer un seuil de réussite.

b) Éléments d'évaluation

Type de compétence	Éléments
Compétence traduite en situation	• Tableau de spécifications • Description de l'engagement • Fiche d'évaluation
Compétence traduite en comportement	• Tableau de spécifications • Description de l'épreuve • Fiche d'évaluation

Dans le cas de la compétence traduite en comportement, les éléments de l'évaluation reposent sur des comportements relatifs aux tâches ou aux productions particulières du métier.
Dans le cas des compétences traduites en situation, l'évaluation est orientée sur l'engagement de l'apprenant dans la démarche qui lui est proposée durant la formation.

c) Évaluation sommative

Deux types d'épreuves constituent l'évaluation sommative au MINEFOP. Il s'agit :

- L'Épreuve Professionnelle de Synthèse : c'est une épreuve d'ordre procédurale qui consiste à évaluer les connaissances et savoirs être du candidat sur l'ensemble des compétences acquises durant sa formation. Sa note éliminatoire est de « inférieure à 8/20 ».
- L'Épreuve de mise en situation professionnelle : c'est une épreuve d'ordre pratique qui l'apprenant en situation de travail. Il permet d'évaluer les savoirs faire de l'apprenant relevant du cœur du métier. Sa note éliminatoire est de « inférieure à 14/20 ».

Les contenus type desdites épreuves sont définis ainsi qu'il suit :

Tableau 1 : Synthèse du programme de formation

N°	Énoncé de la compétence	Durée	CP	CG	Unités	Types d'objets	Types de compétences	Titre du Module
1	Se situer au regard du métier et de la formation	30	0	30	2	S	G	Métier et Formation
2	Communiquer en milieu professionnel	45	0	45	3	S	G	Communication en milieu professionnel
3	Appliquer le principe de la sécurité des comptes	60	0	60	4	S	G	Application du principe de sécurité des comptes
4	Exploiter l'architecture des systèmes informatiques des réseaux et des protocoles	60	0	60	4	C	G	Exploitation de l'architecture des systèmes informatiques des réseaux et des protocoles
5	Configurer les systèmes d'exploitation	60	0	60	4	C	G	Configuration des systèmes d'exploitation
6	Utiliser les langages de programmation	60	0	60	4	C	G	Utilisation des langages de programmation
7	Identifier les vulnérabilités potentielles dans les Systèmes informatiques	90	90	0	6	C	P	Identification des vulnérabilités potentielles dans les Systèmes informatiques
8	Configurer les outils de test de pénétration des systèmes d'exploitation	120	120	0	8	C	P	Configuration des outils de test de pénétration des systèmes d'exploitation
9	Tester la vulnérabilité sur les Réseaux, les applications, site web et les systèmes d'exploitation	150	150	0	10	C	P	Tests de la vulnérabilité, sur les Réseaux, les applications, site web et les systèmes d'exploitation
10	Proposer les stratégies d'atténuation	120	120	0	8	C	P	Proposition des stratégies d'atténuation
11	Configurer les pares-feux et des systèmes de détection d'intrusions	120	120	0	8	C	P	Configuration des pares-feux et des systèmes de détection d'intrusions

12	Assurer la veille technologique en cyberattaque	90	90	0	6	C	P	Veille technologique en cyberattaque
13	Rechercher un emploi	45	0	45	3	S	G	Entreprenariat
14	S'intégrer en milieu professionnel	315	315	/	21	S	P	Stage
	Total	**1365**	**1005**	**360**	**94**			
			73,62%	**26,38%**				

Le tableau de synthèse ci-dessus présente l'énoncé des 14 compétences du métier Pentester**,** faisant objet d'évaluation certificative dans le Référentiel d'évaluation. Il décrit pour chaque compétence, les modalités d'évaluation privilégiées (épreuve de connaissance pratique ou épreuve pratique) et les stratégies (processus, produit, propos) retenues par l'équipe d'élaboration du référentiel pour certifier chaque compétence. Il précise la durée totale de chaque épreuve de certification et le seuil de réussite. Concernant le matériel indispensable lors de l'administration des épreuves, le tableau ramène à la fiche descriptive de chaque épreuve.

Renseignements complémentaires

Certaines épreuves comportent deux parties : une partie relative aux connaissances pratiques et une partie pratique. Pour ces épreuves, la partie relative aux connaissances pratiques est individuelle alors que la partie pratique peut être traitée en équipe de maximum cinq (5) candidats, mais chaque candidat est évalué sur sa participation au travail d'équipe.

Pour les épreuves de 5 h et plus, elles sont élaborées de façon à être administrées en deux temps si possible sur deux jours.

Grille de rétroaction

La grille de rétroaction en annexe est destinée à assurer l'amélioration continue des épreuves. Elle comporte des questionnaires destinés aux évaluateurs. Elle est renseignée par ces derniers puis acheminée à la direction chargée des examens et concours qui fait la synthèse.

COMPÉTENCES TRADUITES EN SITUATIONS

TABLEAU DE SPÉCIFICATIONS			
Métier	**PENTESTER**	**Code : MEFO 01**	
Compétence 01: Se situer au regard du métier et de la formation		**Durée d'apprentissage :**	**30 h**
Éléments de la compétence	**Indicateurs**	**Critères d'évaluation**	
S'informer sur le métier	1. Recueil de données sur la nature et sur les exigences du métier	1.1 Description judicieuse de la nature et des exigences de l'emploi	☐
	2. Recueil de données sur les caractéristiques du marché du travail	2.1 Résumé succinct des principales caractéristiques du travail	☐
S'informer sur le programme de formation et engagement de la démarche	3. Collecte d'informations sur le programme, la démarche de formation et d'évaluation	3.1 Description des compétences à acquérir	☐
		3.2 Description correcte des modes d'évaluation	■
	4. Participation à une rencontre de groupe	4.1 Expression correcte de la perception du programme de formation	☐
		4.2 Comparaison correcte de sa perception du programme de formation avec le marché du travail	☐
Évaluer et confirmer son engagement	5. Présentation d'un bilan personnel	5.1 Précision correcte de goûts, aptitudes, champs d'intérêt et qualités personnelles	■
		5.2 synthèse correcte des différents aspects du métier	☐
	6. Décision définitive de poursuite de programme	6.1 choix final de poursuite ou non du programme de formation	■
Seuil de réussite : 6 des 9 critères d'évaluation, dont les critères noircis, pour que l'on considère la compétence acquise			

DESCRIPTION DE L'ENGAGEMENT	**Code : MEFO 01**

Compétence 1 : Se situer au regard du métier et de la formation

Renseignements généraux

L'évaluation de la participation de l'apprenant à des activités vise à assurer l'acquisition de la compétence : « Se situer au regard du métier et de la démarche de formation ».

L'évaluation de la participation est faite tout au long du module par le formateur, à l'aide d'une grille. Elle porte sur la participation de l'apprenant aux différentes activités individuelles, en groupe et en sous-groupe, et non sur les résultats obtenus.

L'épreuve comprend trois parties. Chacune des parties est accompagnée de consignes particulières.

Déroulement

- *S'informer sur le métier*

Cette partie recueille des données sur la majorité des sujets à traiter et exprime convenablement la perception du métier au moment d'une rencontre de groupe en faisant le lien avec l'information recueillie.

Dans leur recherche, les apprenants auront à préciser :

- deux types d'entreprises et leurs produits ou services offerts;
- des perspectives d'emploi et l'échelle de salaires dans ce milieu de travail;
- des tâches associées au métier;
- les principales conditions de travail ;
- les conditions d'entrée sur le marché de travail ;
- des habiletés et des comportements qui sont propres au métier.
- *S'informer sur le programme de formation et engagement de la démarche*

L'évaluation de cette partie porte sur la participation de l'apprenant aux discussions de groupe, sur les exigences auxquelles il faut satisfaire pour pratiquer le métier et la perception qu'ont les apprenants de la formation.

Au cours de la discussion, l'apprenant aura :

- à présenter au moins trois avantages et trois inconvénients à pratiquer le métier;
- à commenter quelques règles de l'éthique professionnelle ;
- à échanger des points de vue sur l'approche par compétences et son influence sur les apprentissages et les modes d'évaluation ;
- à commenter les modules indiqués au tableau synthèse du programme.
- *Evaluer et confirmer son engagement*

L'évaluation de cette partie porte sur la qualité du rapport rédigé expliquant principalement le choix de l'orientation professionnelle de l'apprenant.

Dans le rapport, l'apprenant aura :

- à démontrer, par quelques exemples, comment son choix d'orientation par rapport à la profession de Pentester d'élevage est en conformité ou non avec ses goûts, ses aptitudes et ses champs d'intérêt;
- à donner des exemples quant aux possibilités d'exercer le métier et de progresser dans ce métier.

FICHE D'EVALUATION		Code : MEFO 01	
N° et énoncé de la compétence	**1. Se situer au regard du métier et de la formation**		
Module 1 : Métier et formation			
Nom de l'apprenant : Structure de formation : Date de l'évaluation : Signature du formateur :		**Résultat** **SUCCES** ☐	**ECHEC** ☐
ELEMENTS D'OBSERVATION		**Jugement** **OUI**	**NON**
1. Recueil de données sur la nature et sur les exigences du métier 1. Recueil de données sur la nature et sur les exigences du métier		☐	☐
2. Recueil de données sur les caractéristiques du marché du travail 2.1 Résume les principales caractéristiques du travail		☐	☐
2. Recueil de données sur les caractéristiques du marché du travail 2.1 Résumé succinct des principales caractéristiques du travail		☐	☐
3. Collecte d'informations sur le programme, la démarche de formation et d'évaluation 3.1 Description des compétences à acquérir 3.2 Description correcte des modes d'évaluation		☐ ☐	☐ ☐
4. Participation à une rencontre de groupe 4.1 Expression correcte de la perception du programme de formation 4.2 Comparaison correcte de sa perception du programme de formation avec le marché du travail		☐ ☐	☐ ☐
5. Présentation d'un bilan personnel 5.1 Précision correcte de goûts, aptitudes, champs d'intérêt et qualités personnelles 5.2 synthèse correcte des différents aspects du métier		☐ ☐	☐ ☐
6. Décision définitive de poursuite de programme 6.1 choix final de poursuite ou non du programme de formation		☐	☐
TOTAL :		**/9**	
Seuil de réussite : 6 oui sur une possibilité de 9 (dont la satisfaction aux exigences des critères d'évaluation 3.2, 5.1 et 5.2.			
Remarque :			

TABLEAU DE SPÉCIFICATIONS				
METIER :	**Pentester**		**Code : COM 02**	
Compétence 02 : Communiquer en milieu professionnel			**Durée d'apprentissage**	**45h**
Éléments de la compétence	**Stratégie**	**Indicateurs**	**Critères d'évaluation**	**Points**
Exploiter les ressources des langues officielles	Produit	1. Appropriation des termes et expressions relatifs au métier en français et en anglais	1.1 Utilisation appropriée de formules et des termes relatifs au métier en français et en anglais	05
		2. Utilisation du français	2.1 Application appropriée du code grammatical du français	05
		3. Making use of English language	3.1 Appropriated use of English language rules	05
		4. Exploitation d'un texte et des ressources documentaires	4.1 Détermination des éléments pertinents d'un texte	05
		5. Exploitation of documentary resources	5.1 Détermination of pertinent éléments of a document	05
Interagir avec les membres de l'équipe et la hiérarchie	Produit	6. Identification des attitudes à adopter dans un contexte professionnel.	6.1 Reconnaissance des attitudes à adopter dans un contexte professionnel.	05
		7. Utilisation des comportements éthiques, d'intégrité et de conduite responsable	7.1 Démonstration de comportements éthiques, d'intégrité et de conduite responsable.	05
		8. Use of means of communication	Use of appropriate means of communication	05
Produire des écrits généraux et professionnels		9. Subjet analysis	15.1 Réponse correcte aux questions portant sur un texte.	05
			15.2 Pertinent analysis of the subjet	05
		10. Rédaction d'une production dans la langue recommandée.	2.1 Rédaction correcte d'une production dans la langue recommandée.	05
		11. Utilisation des ouvrages relatifs à la qualité de la langue	○ Utilisation efficace des ouvrages relatifs à la qualité de la langue	05

		12. Rédaction des messages et des rapports	○ Rédaction claire et concise de messages.	05
			○ Production de rapports clairs et concis.	
		13. Vérification de l'efficacité et de la qualité de la communication écrite	13.1 Vérification judicieuse de l'efficacité et de la qualité de la communication écrite.	05
Établir une relation conseil	Produit	14. Détermination of needs	14.1 Precise détermination of needs	05
		15. Utilisation des moyens d'intervention	12.1Détermination des moyens d'intervention appropriés.	
			12.2Mise en œuvre adéquate des moyens d'intervention.	05
		16. Vérification de l'atteinte des objectifs	○ Communication appropriée de l'information pertinente.	
			16.2 Vérification objective de l'atteinte des objectifs.	05
Encadrer une équipe de travail	Produit	17. Établissement d'un bilan de compétence	○ Établissement judicieuse d'un bilan de compétence	05
		18. Application des techniques d'encadrement	18.1 Identification des aspects favorables à la conduite de réunions.	
			18.2Application judicieuse des techniques d'encadrement	05
		19. Writing of report	19.1 Judicious writing of report	05

DESCRIPTION DE L'ÉPREUVE		CODE : COM 02
N° 02 et Enoncé de la compétence	**Communiquer en milieu professionnel**	
Renseignements généraux		
L'épreuve a pour but d'évaluer la compétence relative à « Communiquer en milieu professionnel ». Il s'agit d'une épreuve d'évaluation qui prend en considération une portion d'évaluation des connaissances théoriques et une portion de type pratique. L'évaluation de type pratique pourrait être administrée individuellement ou en groupe en fonction de l'élément de compétence et du matériel disponible. L'évaluation des connaissances théoriques pourrait être réalisée avec l'ensemble des apprenants. L'environnement de réalisation de l'épreuve de type pratique pourrait s'inspirer d'une situation en milieu de travail. La durée cumulée de l'ensemble des épreuves pourrait être d'environ 2 heures, et inclure la portion pratique combinée à celle de l'évaluation des connaissances théoriques pour les différents éléments de compétence soit 01 heure pour chaque type d'évaluation.		
Contenu de l'épreuve A partir d'un texte en rapport une situation de travail ou le domaine d'activité, le formateur amènera les apprenants à faire ressortir l'idée principale du texte et à répondre à des questions dont le but est de juger leur capacité d'exploitation de documents et de production des écrits, tout en respectant les règles grammaticales usuelles dans les deux langues. Par ailleurs, l'apprenant pourra être mis en situation de communiquer oralement dans les deux langues dans le cadre de la portion pratique de l'épreuve.		
Matériel (Pour un groupe de 25 apprenants) • *01 micro-ordinateur* • *Dictionnaires* • *livres* • *01 vidéoprojecteur* • *Etc.*		
Consigne particulière ➢ L'épreuve pourrait être administrée après le temps d'apprentissage des compétences 3. ➢ L'observation pourrait être faite en simulation. ➢ En cas d'échec, l'épreuve devrait être reprise dans son ensemble. Si un seul élément est très faible comparativement aux autres pour lesquels les performances de l'apprenant seraient excellentes, seul cet élément pourrait être repris.		

FICHE D'ÉVALUATION			CODE : COM02
N° 02 et Énoncé de la compétence	**Communiquer en milieu professionnel**		**Durée 2 h**
Nom de l'apprenant : Structure de formation : Date de l'évaluation : Signature du formateur :			Résultat SUCCÈS ☐ ÉCHEC ☐
ÉLÉMENTS D'OBSERVATION	OUI	NON	RÉSULTATS
1. APPROPRIATION DES TERMES ET EXPRESSIONS RELATIFS AU MÉTIER EN FRANÇAIS ET EN ANGLAIS 1.1 Utilisation appropriée de formules et des termes relatifs au métier en français et en anglais			0 ou 5
2. UTILISATION DU FRANÇAIS 2.1 Application appropriée du code grammatical du français			0 ou 5
3. MAKING USE OF ENGLISH LANGUAGE 3.1 Appropriated use of English language rules			0 ou 5
4. EXPLOITATION D'UN TEXTE ET DES RESSOURCES DOCUMENTAIRES 4.1 Détermination des éléments pertinents d''un texte			0 ou 5
5. EXPLOITATION OF DOCUMENTARY RESOURCES 5.1 Détermination of pertinent éléments of a document			0 ou 5
6. IDENTIFICATION DES ATTITUDES À ADOPTER DANS UN CONTEXTE PROFESSIONNEL 6.1 Reconnaissance des attitudes à adopter dans un contexte professionnel.			0 ou 5
7. UTILISATION DES COMPORTEMENTS ÉTHIQUES, D'INTÉGRITÉ ET DE CONDUITE RESPONSABLE 7.1 Démonstration de comportements éthiques, d'intégrité et de conduite responsable.			0 ou 5
8. Use of means of communication 8.1 Use of appropriate means of communication			0 ou 5
9. RÉSOLUTION DES QUESTIONS PORTANT SUR UN TEXTE. 9.1 Réponse correcte aux questions portant sur un texte. 9.2 Analyse pertinente d'un sujet.			0 ou 5 0 ou 5
10. RÉDACTION D'UNE PRODUCTION DANS LA LANGUE RECOMMANDÉE. 10.1 Rédaction correcte d'une production dans la langue recommandée.			

FICHE D'ÉVALUATION			CODE : COM02
N° 02 et Énoncé de la compétence	**Communiquer en milieu professionnel**		**Durée 2 h**
			0 ou 5
11. UTILISATION DES OUVRAGES RELATIFS À LA QUALITÉ DE LA LANGUE 11.1 Utilisation efficace des ouvrages relatifs à la qualité de la langue			0 ou 5
12. RÉDACTION DES MESSAGES ET DES RAPPORTS 12.1 Rédaction claire et concise de messages. 12.2 Production de rapports clairs et concis.			0 ou 5
13. VÉRIFICATION DE L'EFFICACITÉ ET DE LA QUALITÉ DE LA COMMUNICATION ÉCRITE 13.1 Vérification judicieuse de l'efficacité et de la qualité de la communication écrite.			0 ou 5
14. Détermination of needs 14.1 Precise détermination of needs			0 ou 5
15. UTILISATION DES MOYENS D'INTERVENTION 15.1 Détermination des moyens d'intervention appropriés. 15.2 Mise en œuvre adéquate des moyens d'intervention.			0 ou 5
16. VÉRIFICATION DE L'ATTEINTE DES OBJECTIFS 16.1 Communication appropriée de l'information pertinente. 16.2 Vérification objective de l'atteinte des objectifs.			0 ou 5
17. ÉTABLISSEMENT D'UN BILAN DE COMPÉTENCE 17.1 Établissement judicieuse d'un bilan de compétence			0 ou 5
18. APPLICATION DES TECHNIQUES D'ENCADREMENT 18.1 Identification des aspects favorables à la conduite de réunions. 18.2 Application judicieuse des techniques d'encadrement			0 ou 5
19. Writing of report 19.1 Judicious writing of report			0 ou 5
		TOTAL :	/100
Seuil de réussite : 70%			
Règle de verdict : Le formateur devra s'assurer qu'en dehors de la maîtrise des opérations, l'apprenant adopte des attitudes respectant les règles de sécurité et de préservation de l'environnement pour lesquelles il aura été évalué à la compétence 3.	Oui ☐	Non ☐	
Remarque :			

TABLEAU DE SPÉCIFICATIONS				
Métier	**PENTESTER**		**Code : ENTR 13**	
N° et Énoncé de la Compétence	**Rechercher un emploi**		**Durée d'apprentissage**	45heures
Éléments de la compétence	**Stratégie**	Indicateurs	**Critères d'évaluation**	**Points**
S'initier à la connaissance de l'entreprise et des éléments comptables, à l'économie, à des notions juridiques et sociales.	Processus	1. Notion d'entreprise, notions en économie, notions de base en droit des affaires,	1.1 Mise en pratique conforme des notions de base	20
		2. Réalisation judicieuse des opérations commerciales et des éléments comptables	2.1 Réalisation judicieuse des opérations commerciales et des éléments comptables	10
S'approprier les techniques de recherche d'emploi	Produit	3. Montage des CV	3.1 montage judicieuse des CV	10
	Processus	4. Application des procédures de recherche d'emploi	4.1 Application judicieuse des procédures de recherche d'emploi	25
S'approprier les techniques de base de montage d'un projet de création d'entreprise (entrepreneuriat).	Processus	5. Examination des conditions de réussite d'un projet de création ou d'auto emploi	5.1Examination judicieuse des conditions de réussite d'un projet de création ou d'auto emploi	10
		6. Présentation d'un plan d'affaires	6.1Redaction correcte d'un plan d'affaires	25

DESCRIPTION DE L'EPREUVE	**Code : ENT13**
N° et Énoncé de la Compétence	**13 Rechercher un emploi**

Renseignements généraux

L'épreuve a pour but d'évaluer la compétence relative à « Rechercher un emploi ».
Il s'agit d'une épreuve qui prend en considération une portion d'évaluation des connaissances pratiques et celle d'activités d'apprentissage pratique.
L'épreuve d'activités d'apprentissage pratique pourrait être administrée individuellement ou en groupe.
L'évaluation des connaissances pratiques pourrait être réalisée avec l'ensemble des apprenants.
L'épreuve pourrait être d'une durée de 3 heures, ce qui inclut la phase pratique et celle de l'évaluation des connaissances pratiques.

Déroulement de l'épreuve

On pourra demander à l'apprenant de jouer le rôle d'un candidat soumis à une interview pour un emploi.

Matériel

- 01 table ;
- 03 chaises pour le jury ;
- 01 chaise pour l'apprenant ;
- Questionnaires ;
- Papier et stylos.

Consignes particulières

L'épreuve pourrait être administrée durant le temps d'apprentissage d'une compétence subséquente (compétence 13) ou d'une compétence évaluée en parallèle, (compétences 12) ;
L'observation pourrait être faite en simulation pour le premier cas d'évaluation.
En cas d'échec, l'épreuve pourrait être reprise dans son ensemble. Si un seul élément est très faible comparativement aux autres pour lesquels les performances de l'apprenant seraient excellentes, seul cet élément pourrait être repris.

FICHE D'EVALUATION			**Code : ENT13**
N° et Énoncé de la Compétence	**13 Rechercher un emploi**		**Durée : 45h**
Nom de l'apprenant : Structure de formation : Date de l'évaluation : Signature du formateur :			**Résultat** **SUCCES** ☐ **ECHEC** ☐
ELEMENTS D'OBSERVATION	**OUI**	**NON**	**RESULTATS**
1. NOTION D'ENTREPRISE, NOTIONS EN ECONOMIE, NOTIONS DE BASE EN DROIT DES AFFAIRES 1.1 Mise en pratique conforme des notions de base			0 ou 20
2. REALISATION JUDICIEUSE DES OPERATIONS COMMERCIALES ET DES ELEMENTS COMPTABLES 2.1 Réalisation judicieuse des opérations commerciales et des éléments comptables			0 ou 10
3. MONTAGE DES CV 3.1 Montage judicieuse des CV			0 ou 10
4. APPLICATION DES PROCEDURES DE RECHERCHE D'EMPLOI 4.1 Application judicieuse des procédures de recherche d'emploi			0 ou 25
5. EXAMINATION DES CONDITIONS DE REUSSITE D'UN PROJET DE CREATION OU D'AUTO EMPLOI 5.1Examination judicieuse des conditions de réussite d'un projet de création ou d'auto emploi			0 ou 10
6. PRESENTATION D'UN PLAN D'AFFAIRES 6.1Redaction correcte d'un plan d'affaires			0 ou 25
TOTAL			**/100**
Seuil de réussite : 70%			
Remarque :			

TABLEAU DE SPECIFICATIONS			
Métier	**PENTESTER**	**Code :**	**STG14**
N° 14 et Énoncé de la Compétence	**S'intégrer au milieu professionnel**	**Durée d'apprentissage**	**315 heures**
Eléments de la compétence	**Indicateurs**	**Critères d'évaluation**	
Préparer son séjour en milieu de travail	1. Recueil des données pertinentes pour le stage	1.1 Recueil correct des données pertinentes pour le stage	☐
		1.2 Description exhaustive des tâches prévues pour son stage	
	2.1 Choix des stages	2.1 Choix judicieux des entreprises pour le stage	☐
		2.2 Élaboration conforme du dossier de stage	
Respecter les principes de discipline et de déontologie	3. Distinction des règles de conduite	3.1Respect des consignes, des règlements, de la hiérarchie et des normes environnementales	■
	4. Application des règles de conduite de l'entreprise	4.1Démonstration des qualités personnelles et professionnelles	
Exécuter les activités en milieu de travail	5. Utilisation des équipements	5.1 Exécution appropriée des tâches	■
		5.2 Assimilation parfaite et démonstration des opérations liées au métier	
	6. Exécution ou participation aux tâches	6.1 Développement des attitudes professionnelles	
		6.2 Choix et utilisation adéquats des matériels de l'entreprise	
Comparer ses perceptions aux réalités du métier	7. Participation à des échanges sur le stage	7.1 Résumé de l'expérience de stage	☐
	8. Relation entre la formation et les exigences du milieu de travail	8.1 Démonstration de l'influence du stage sur le choix d'un futur emploi	
Rédiger le rapport de stage	9. Respect du canevas de rédaction du rapport de stage	9.1 Respect des principes de la langue utilisée	☐
		9.2 Pertinence du contenu du rapport	☐
	10. Rédaction du rapport de stage	10.1 Rédaction soignée et concise	
Seuil de réussite : 3 des 5 critères d'évaluation, dont les critères noircis, pour que l'on considère la compétence acquise			

DESCRIPTION DE L'ENGAGEMENT	Code : STG14
N° et Énoncé de la Compétence	14 S'intégrer en milieu professionnel

Renseignements généraux

L'épreuve a pour but d'évaluer l'engagement de l'apprenant dans la démarche qui vise à assurer l'acquisition de la compétence « S'intégrer en milieu professionnel ».

L'évaluation de l'apprenant est faite tout au long de la durée de stage par le maître de stage et par un jury après le retour de stage.

Déroulement de l'épreuve

- Préparer son séjour en milieu de travail

L'évaluation de l'apprenant s'effectuerait à l'occasion d'une rencontre de groupe qui porte sur la recherche et la prospection des entreprises du domaine du numérique.

Durant cette rencontre, l'apprenant devrait établir au moins deux liens entre son métier et les entreprises de production d'aliments des animaux d'élevage.

Une telle rencontre devrait être dirigée de manière à ce que tous les apprenants aient l'occasion de s'exprimer.

L'évaluation de l'apprenant s'effectuerait également à l'occasion d'une production écrite où l'apprenant présentera les démarches à entreprendre pour obtenir une place de stage.

- Respecter les principes de discipline et de déontologie

L'évaluation de l'apprenant s'effectuerait à l'occasion d'une rencontre de groupe qui présente le règlement et le code de conduite de l'entreprise. Durant cette rencontre, l'apprenant devrait déterminer au moins deux principes et deux obligations à suivre dans l'entreprise.

Une telle rencontre devrait être dirigée de manière à ce que tous les apprenants aient l'occasion de s'exprimer.

- Exécuter les activités en milieu de travail

Pendant toute la durée du stage, l'apprenant devrait être évalué à hauteur de 50% par le maitre de stage pour ses connaissances, attitudes, habiletés manifestées au cours de son travail.

- Comparer ses perceptions aux réalités du métier

L'évaluation s'effectuerait à l'occasion d'une rencontre de groupe qui porte sur l'auto évaluation de l'apprenant. L'apprenant devrait présenter sa perception du métier et les conséquences du stage sur le développement personnel vis-à-vis du métier.

Une telle rencontre devrait être dirigée de manière à ce que tous les apprenants aient l'occasion de s'exprimer

- Rédiger le rapport de stage

L'évaluation s'effectuerait à l'occasion d'une présentation d'un rapport de stage, à hauteur de 50% devant un jury mis en place par la structure de formation. Un groupe restreint d'apprenants pourrait présenter le même rapport si ceux-ci ont suivi le stage dans une même entreprise, et par conséquence évaluer après présentation de ce rapport.

Les réponses aux questions du jury portent pour 50% de la partie de l'évaluation réservée audit jury.

FICHE D'EVALUATION	Code : STG14
N° et Énoncé de la Compétence	**14. S'intégrer au milieu professionnel**

Nom de l'apprenant :
Structure de formation :
Date de l'évaluation :

Signature du formateur :

Résultat	
SUCCES	**ECHEC**
☐	☐

ELEMENTS D'OBSERVATION	**Jugement**	
	OUI	**NON**
1. RECUEIL DES DONNEES PERTINENTES POUR LE STAGE 1.1 Recueil correct des données pertinentes pour le stage 1.2 Description exhaustive des tâches prévues pour son stage	☐	☐
2.1 CHOIX DES STAGES 2.1 Choix judicieux des entreprises pour le stage 2.2 Élaboration conforme du dossier de stage	☐	☐
3. DISTINCTION DES REGLES DE CONDUITE 3.1Respect des consignes, des règlements, de la hiérarchie et des normes environnementales	☐	☐
4. APPLICATION DES REGLES DE CONDUITE DE L'ENTREPRISE 4.1Démonstration des qualités personnelles et professionnelles	☐	☐
5. UTILISATION DES EQUIPEMENTS 5.1 Exécution appropriée des tâches 5.2 Assimilation parfaite et démonstration des opérations liées au métier	☐	☐
6. EXECUTION OU PARTICIPATION AUX TACHES 6.1 Développement des attitudes professionnelles 6.2 Choix et utilisation adéquats des matériels de l'entreprise	☐	☐
7. PARTICIPATION A DES ECHANGES SUR LE STAGE	☐	☐

7.1 Résumé de l'expérience de stage		
8. RELATION ENTRE LA FORMATION ET LES EXIGENCES DU MILIEU DE TRAVAIL 8.1 Démonstration de l'influence du stage sur le choix d'un futur emploi	☐	☐
9. RESPECT DU CANEVAS DE REDACTION DU RAPPORT DE STAGE 9.1 Respect des principes de la langue utilisée 9.2 Pertinence du contenu du rapport	☐	☐
10. REDACTION DU RAPPORT DE STAGE 10.1 Rédaction soignée et concise	☐	☐
TOTAL :	**/10**	
Seuil de réussite : 4 des 7 critères d'évaluation dont la satisfaction aux exigences des critères 3.1 et 6.1		

COMPÉTENCES TRADUITES EN COMPORTEMENT

TABLEAU DE SPÉCIFICATIONS				
METIER :	**PENTESTER**		**Code**	**APS03**
N° et libellé de la compétence	**3. Appliquer les principes de la sécurité des comptes**		Durée d'apprentissage	60 heures
Éléments de la compétence	**Stratégie**	**Indicateurs**	**Critères d'évaluation**	**Points**
S'informer des lois et des règlements sur la santé et la sécurité au travail	Processus	1. Identification du corpus et du dispositif juridique	1.1 Interprétation juste de la législation du travail	**05**
			1.2 Relevé approprié des normes et des procédures de santé et de sécurité au travail	**05**
		2. Repérage de l'information dans les documents et les pictogrammes	2.1. Repérage adéquat de l'information dans les documents et les pictogrammes	**05**
Gérer les identités	Processus	3. Techniques et règles de gestion des identités	3.1. Respect judicieux du nombre d'identités	**05**
			3.2. Respect judicieux du délai de provisioning d'une nouvelle identité	**05**
		4. Renouvellement des mots de passe	4.1 Renouvellement approprié des mots de passe	**05**
Contrôler les mots de passe	Processus	5. Utilisation des mesures de sécurité des mots de passe	5.1. Sécurisation correcte des mots de passe ;	**05**
			5.2. Respect de la complexité des mots de passe ;	**05**
		6. Respect du délai de réinitialisation d'un mot de passe oublié/compromis	6.1. Respect du délai de réinitialisation d'un mot de passe oublié/compromis	**05**
Contrôler les accès	Processus	7.Identification des accès	7.1. Authentification correcte des accès	**05**
			7.2. Respect strict du délai d'approbation d'une demande d'accès	**05**

		8.Découverte du nombre de violations	8.1. Détection correcte du Nombre de violations	**05**
Détecter les activités anormales	Processus	9. Respect du temps moyen de détection des incidents	9.1. Respect strict du délai entre la survenue et détection d'un incident	**05**
		10. Génération des alertes	10.1. Génération efficace des alertes	**05**
		11Analyse approfondie du trafic réseau.	11.1. Analyse approfondie du trafic réseau.	**05**
Élaborer la Journalisation et traçabilité	Processus	12. Gestion des logs et du temps moyen d'agrégation	12.1. Gestion efficace du délai d'agrégation des logs dans l'outil de SIEM	**05**
		13. vérification des logs	12.1. Vérification efficace des logs	**05**
		14Contrôle de la traçabilité	13.1. Contrôle efficace de la traçabilité	**05**
Gérer les incidents	Processus	15. Détection et de résolution des compromissions	15.1. Détections et résolution efficace des compromissions	**05**
		16. Identification des taux de réussite d'activités testées	16.1. Détermination correcte du taux de réussite des plans de reprise d'activité testés	**05**
		17.Evaluation correcte de la maturité par des audits et la certification ;	17.1Evaluation correcte de la maturité par des audits et la certification ;	**05**

DESCRIPTION DE L'ÉPREUVE		Code : APS03
METIER :	**PENTESTER**	
N° et énoncé de la compétence	**3. Appliquer les principes de la sécurité des comptes**	**Durée :4h**

Renseignements généraux

L'épreuve a pour but d'évaluer la compétence relative à « *Appliquer les principes de la sécurité des comptes* Il s'agit d'une épreuve d'évaluation qui prend en considération une portion d'évaluation des connaissances théoriques et une portion de type pratique. Cependant, dans l'impossibilité de produire une épreuve mixte, l'évaluation des connaissances théoriques devrait être priorisée.

L'évaluation de type pratique pourrait être administrée à un groupe restreint d'apprenants en raison de la disponibilité du matériel et de la capacité du formateur à observer plusieurs personnes à la fois. L'évaluation des connaissances théoriques pourrait être réalisée avec l'ensemble des participants. L'environnement de réalisation de l'épreuve de type pratique devrait s'inspirer le plus possible d'une situation en milieu de travail.

L'épreuve pourrait être d'une durée d'environ 3 heures, ce qui inclut la portion pratique combinée à celle de l'évaluation des connaissances théoriques.

Déroulement de l'épreuve

Par l'entremise d'une épreuve de connaissances théoriques, on pourrait demander à l'apprenant de Gérer les identités, de sécuriser les mots de passe, de contrôler les accès et de détecter les activités anormales.

On pourrait également demander à l'apprenant, dans le cadre d'une évaluation pratique, d'effectuer quelques techniques de sécurisation des mots de passe en respectant la complexité des mots de passe ou de présenter les techniques à réaliser pour respecter le délai de réinitialisation d'un mot de passe oublié/compromis.

La mise en situation (texte définissant le contexte de la campagne ou étude de cas) pourrait être utilisée à titre d'évaluation des connaissances théoriques pour l'ensemble des éléments de la compétence.

L'épreuve pourrait donc être mixte et impliquer des activités en sous-groupe pour vérifier le travail d'équipe.

Matériel *(Pour un groupe de 25 apprenants)*

- Ordinateurs et serveurs
- Logiciels de gestion des comptes
- Outils de test de vulnérabilité
- Environnement de test sécurisé
- Documentation et rapports

Consigne particulière

- L'épreuve pourrait être administrée durant le temps d'apprentissage d'une compétence subséquente (compétences (5,6 et 7), ou d'une compétence évaluée en parallèle);
- En cas d'échec, l'épreuve devrait être reprise dans son ensemble. Si un seul élément est très faible comparativement aux autres pour lesquels les performances de l'apprenant seraient excellentes, seul cet élément pourrait être repris.

FICHE D'ÉVALUATION		Code : APS03
Métier	**PENTESTER**	
N° et énoncé de la compétence	**3. Appliquer les principes de la sécurité des comptes**	

Nom de l'apprenant : Structure de formation : Date de l'évaluation : Signature du formateur :	**Résultat**	
	SUCCÈS	**ÉCHEC**
	☐	☐

ÉLÉMENTS D'OBSERVATION	**OUI**	**NON**	**RÉSULTATS**
1. Identification du corpus et du dispositif juridique 1.1 Interprétation juste de la législation du travail 1.2 Relevé approprié des normes et des procédures de santé et de sécurité au travail			 0 ou 05 0 ou 05
2. Repérage de l'information dans les documents et les pictogrammes 2.1 Repérage adéquat de l'information dans les documents et les pictogrammes			 0 ou 05
3. Techniques et règles de gestion des identités 3.1. Respect judicieux du nombre d'identités 3.2. Respect judicieux du délai de provisioning d'une nouvelle identité			0 ou 05 0 ou 10
4. Renouvellement des mots de passe 4.1. Renouvellement approprié des mots de passe			 0 ou 05
5. Application des mesures de sécurité des mots de passe 5.1. Sécurisation correcte des mots de passe 5.2. Respect de la complexité des mots de passe ;			 0 ou 05 0 ou 05
6. Respect du délai de réinitialisation d'un mot de passe oublié/compromis 6.1. Respect du délai de réinitialisation d'un mot de passe oublié/compromis			 0 ou 05
7.Identification des accès 7.1. Respect strict du délai d'approbation d'une demande d'accès			 0 ou 05
8. Détection correcte du Nombre de violations 8.1. Détection du Nombre de violations			0 ou 05
9.Respect du temps moyen de détection des incidents			

9.1. Respect strict du délai entre la survenue et détection d'un incident			0 ou 05
10. Analyse du trafic réseau 10.1. Analyse approfondie du trafic réseau			0 ou 05
11. Génération efficace des alertes 11. 1. Génération des alertes			0 ou 05
12. Gestion des logs et du temps moyen d'agrégation 12.1. Gestion efficace du délai d'agrégation des logs dans l'outil de SIEM			0 ou 05
13. Vérification efficace des logs 13.1. Vérification correcte des logs			0 ou 05
14.Contrôle de la traçabilité 14.1. Contrôle efficace de la traçabilité			
15. le temps moyen de détection et de résolution des compromissions 15.1. Détections et résolution efficace des compromissions			0 ou 05
16. Identification des taux de réussite d'activités testées 16.1. Détermination correcte du taux de réussite des plans de reprise d'activité testés			0 ou 05
17.Evaluation de la maturité par des audits et la certification ; 17.1 Evaluation correcte de la maturité par des audits et la certification ;			0 ou 05
		TOTAL :	**/100**
Seuil de réussite : 70 % et obligation de satisfaire aux exigences des critères 3.1, 4.1 et 6.2.			
Règle de verdict : Le formateur devra s'assurer qu'en dehors de la maîtrise des opérations, l'apprenant adopte des attitudes respectant les règles de sécurité pour lesquelles il aura été évalué à la compétence 3.	**Oui** ☐	**Non** ☐	

TABLEAU DE SPÉCIFICATIONS			
METIER :	**PENTESTER**	**Code**	**EAS04**
No et libellé de la compétence	**4. Exploiter l'architecture des systèmes informatiques des réseaux et des protocoles**	**Durée d'apprentissage**	**60h**

Éléments de la compétence	Stratégie	Indicateurs	Critères d'évaluation	Points
Identifier les composants des systèmes informatiques	Processus	1.Interpretation des traitements applicatifs	1.1 Choix exact du matériel ;	10
		2.Optimisation des ressources systèmes	2.1. Identification correcte des données ;	10
		3. Choix des logiciels	3.1 Identification correcte des logiciels	10
Utiliser l'architecture système et applicative	Processus	4.Utilisation de l'architecture système et applicative	4.1. Utilisation correcte l'architecture système et applicative	10
		5.Suivi de l'architecture système et applicative	5.1. Suivi correcte de l'architecture système et applicative	05
		6. Isolation/Sécurisation correcte des applications	6.1 Isolation/Sécurisation correcte des applications.	05
Utiliser les réseaux	Processus	7. Contrôle des latences des communications	7.1. Contrôle efficace des latences des communications	10
		8.Gestion de la fiabilité des transmissions	8.1. Gestion appropriée de la fiabilité des transmissions	10
		9.Assurer la Sécurité et confidentialité des échanges	9.1. Sécurité et confidentialité correctes des échanges	05
Appliquer les protocoles de communication	Processus	10. Choix des types de protocole	10.1. Identification judicieuse des types de protocole	05
		11. Contrôle de la charge réseau	11.1. Contrôle correcte de la charge réseau	10
		12. Vérification de la Robustesse et résistance aux aléas	12.1. Vérification correcte de la Robustesse et résistance aux aléas.	10

DESCRIPTION DE L'ÉPREUVE		Code : EAS04
N° 4	**Énoncé de la compétence : Exploiter l'architecture des systèmes informatiques des réseaux et des protocoles**	

Renseignements généraux

L'épreuve a pour but d'évaluer l'engagement de l'apprenant dans une démarche qui vise à assurer l'acquisition de la compétence relative à « Exploiter l'architecture des systèmes informatiques des réseaux et des protocoles Il s'agit d'une épreuve d'évaluation qui prend en considération l'évaluation des connaissances théoriques et pratiques et elle pourrait être administrée individuellement à l'écrit.

L'évaluation des connaissances théoriques pourrait être réalisée avec l'ensemble des apprenants et l'évaluation des connaissances pratiques pourrait être administrée par groupes en fonction du nombre de postes informatiques disponibles pour les dessins assistés par ordinateur.

L'évaluation portera sur les points suivants :

- Identifier les composants des systèmes informatiques ;
- Utiliser l'architecture système et applicative ;
- Utiliser les réseaux ;
- Appliquer les protocoles de communication

La durée de l'épreuve pourrait être d'environ 04 heures, pour l'évaluation des connaissances théoriques et pratiques en fonction des différents éléments de compétence, dans une salle informatique ou dans une salle d'ordinateurs munis de logiciels de la cybersécurité.

Liens avec les autres compétences

Cette compétence est en relation avec les compétences générales «3, 5 et toutes les compétences particulières du Référentiel de Formation.

Contenu de l'épreuve

Cette épreuve comporte trois à quatre exercices de connaissances théoriques et pratiques qui s'appuient sur des situations authentiques du métier de Pentester et couvrent l'ensemble des aspects cités plus haut.

- A partir d'une mise en situation, l'apprenant pourrait être amené à résoudre des problèmes d'Identification des composants des systèmes informatiques liés à la cybersécurité, sur les aspects de la Gestion efficace des Performance des traitements applicatifs, de l'Optimisation correcte des ressources systèmes et de l'Identification correcte des logiciels ; etc…

Matériel *(Pour un groupe de 25 apprenants)*

Pour la composition de l'épreuve, le matériel requis par apprenant est composé :

- Ordinateurs et serveurs
- Logiciels de simulation
- Outils de test de sécurité
- Matériel de réseau
- Documentation et rapports
- Stylo à bille, crayons de dessin ;

Consigne particulière

- L’épreuve pourrait être administrée après le temps d’apprentissage des compétences 3 .
- En cas d'échec, l'épreuve pourrait être reprise dans son ensemble. Si un seul élément est très faible comparativement aux autres pour lesquels les performances de l'apprenant seraient excellentes, seul cet élément pourrait être repris.
- Les résultats seront arrondis à 10 près, sauf indication contraire du formateur.

FICHE D'ÉVALUATION			Code : EAS04
Énoncé de la compétence :	4. **Exploiter l'architecture des systèmes informatiques des réseaux et des protocoles**		**Durée : 4 h**
Nom de l'apprenant :		**Résultat**	
Établissement d'enseignement :		**SUCCÈS**	**ÉCHEC**
Date de l'évaluation :			
Signature du formateur :			

ÉLÉMENTS D'OBSERVATION	OUI	NON	RÉSULTATS
1. Interprétation des traitements applicatifs et des ressources systèmes 1.1 Gestion efficace des Performance des traitements applicatifs ;			0 ou 10
2.Optimisation des ressources systèmes 2.1. Optimisation correcte des ressources systèmes			0 ou 10
3.Choix des logiciels 3.1 Identification correcte des logiciels			0 ou 10
4. Utilisation de l'architecture système et applicative			0 ou 10
4.1. Utilisation correcte l'architecture système et applicative			0 ou 05
5. Suivi de l'architecture système et applicative.			
5.1. Suivi correcte de l'architecture système et applicative			0 ou 05
6.Isolation/Sécurisation des applications 6.1 Isolation/Sécurisation correcte des applications			0 ou 05
7. Contrôle des latences des communications 7.1. Contrôle efficace des latences des communications			0 ou 05
8.Gestion de la fiabilité des transmissions 8.1. Gestion appropriée de la fiabilité des transmissions			0 ou 10
9. Sécurité et confidentialité des échanges 9.1. Sécurité et confidentialité correctes des échanges			0 ou 05
10.Choix des types de protocole 10.1. Identification judicieuse des types de protocole			0 ou 05

11.Gestion de la charge réseau 11.1. Gestion correcte de la charge réseau			0 ou 10
12. Robustesse et résistance aux aléas 12.1. Robustesse et résistance efficace aux aléas			0 ou 05
		TOTAL :	**/100**
Seuil de réussite : 70%			
Règle de verdict : Néant			
Remarque :			

TABLEAU DE SPÉCIFICATIONS				
METIER	**PENTESTER**		**Code**	**CSE05**
N° et énoncé de la compétence	**5. Configurer les systèmes d'exploitation.**		**Durée d'apprentissage**	**60 h**
Éléments de la compétence	**Stratégie**	**Indicateurs**	**Critères d'évaluation**	**Points**
Effectuer l'administration système	Processus	1.Organisation de l'administration système	1.1. Gestion efficace de l'administration système	10
			1.2 Suivi correcte des actions d'administration système.	5
		2. Respect des procédures d'administration système	2.1. Respect des procédures d'administration système	5
Organiser les utilisateurs et les droits	Processus	3. Supervision de l'Intégrité des comptes utilisateurs	3.1 Supervision efficace des mécanismes d'authentification	5
			3.2. Supervision efficace de l'Intégrité des comptes utilisateurs	10
		4. Suivi des actions sur les comptes	4.1. Suivi correcte des actions sur les comptes	5
Appliquer la sécurité des systèmes d'exploitation	Processus	5. Identification des taux de correction des vulnérabilités	5.1 Gestion efficace de protection contre les vulnérabilités	5
			5.2. Résistance efficace aux attaques ciblées	5
		6.Détection des compromissions	6.1. Détection correcte des compromissions	5
Contrôler la sécurité OS:	Processus	7. Description des mécanismes de défense	7.1 Gestion efficace des mécanismes de défense	10
		8. Découverte des menaces avancées	8.1 Détection correcte des menaces avancées	5
		9. identification et analyses des événements de sécurité	9.1. Détermination correcte du Journal des événements de sécurité	5
		10.Détection d'incident à courte durée	10.1. Réponse efficace aux incidents.	5
Gérer les périphériques	Processus	11. Échanges des données avec les périphériques	11.1. Échanges efficaces avec les périphériques	5
			11.2. Échange minutieuse des données	5
		12. Vérification de l'Intégrité des données échangées	12.1. Vérification correcte de l'Intégrité des données échangées	5
		Suivi des actions sur les périphériques.	Suivi correcte des actions sur les périphériques.	5

DESCRIPTION DE L'ÉPREUVE	Code : CSE05
N° et énoncé de la compétence	**5. Configurer les systèmes d'exploitation.**

Renseignements généraux

L'épreuve a pour but d'évaluer l'engagement de l'apprenant dans une démarche qui vise à assurer l'acquisition de la compétence relative à « Configurer les systèmes d'exploitation ».

Il s'agit d'une épreuve d'évaluation qui prend en considération l'évaluation des connaissances théoriques et pratiques et elle pourrait être administrée individuellement à l'écrit.

L'évaluation des connaissances théoriques pourrait être réalisée avec l'ensemble des apprenants et l'évaluation des connaissances pratiques pourrait être administrée par groupes en fonction du nombre de postes disponibles.

L'évaluation portera sur les points suivants :

- Effectuer l'administration système
- Gérer les utilisateurs et les droits
- Gérer la sécurité des systèmes d'exploitation
- Gérer la sécurité OS:

La durée de l'épreuve pourrait être d'environ 04 heures, pour l'évaluation des connaissances théoriques et pratiques en fonction des différents éléments de compétence.

Liens avec les autres compétences

Cette compétence est en relation avec les compétences générales 6, 7 etc. et toutes les compétences particulières du Référentiel de Formation.

Contenu de l'épreuve

Cette épreuve comporte trois à quatre exercices de connaissances théoriques et pratiques qui s'appuient sur des situations authentiques du métier de Technicien – Pentester et couvrent l'ensemble des aspects cités plus haut.

- A partir d'une mise en situation, l'apprenant pourrait être amené à résoudre des problèmes de Gestion des utilisateurs et des droits liés à la cybersécurité, sur les aspects de la Gestion efficace des mécanismes d'authentification, de la Gestion efficace de l'Intégrité des comptes utilisateurs et de la Traçabilité correcte des actions sur les comptes etc.

Matériel *(Pour un groupe de 25 apprenants)*

Pour la composition de l'épreuve, le matériel requis par apprenant est composé :

- Ordinateurs complet avec des caractéristiques requises
- Supports d'installation
- Connexion Internet.
- Documentation et guides

Consigne particulière

- L'épreuve pourrait être administrée après la compétence relative à l'exploitation *de l'architecture des systèmes informatiques des réseaux et des protocoles.*
- En cas d'échec, l'épreuve pourrait être reprise dans son ensemble. Si un seul élément est très faible comparativement aux autres pour lesquels les performances de l'apprenant seraient excellentes, seul cet élément pourrait être repris.

FICHE D'ÉVALUATION		Code : CSE05		
N° et énoncé de la compétence	**5. Configurer les systèmes d'exploitation**			**Durée : 4h**
Nom de l'apprenant :			**Résultat**	
Établissement d'enseignement :			**SUCCÈS**	**ÉCHEC**
Date de l'évaluation :				
Signature du formateur :				

ÉLÉMENTS D'OBSERVATION	OUI	NON	RÉSULTATS
1.Description de l'administration système 1.1. Gestion efficace de l'administration système 1.2 Suivi correcte des actions d'administration système.			0 ou 10 0 ou 05
2. Respect des procédures d'administration système 2.1 Respect des procédures d'administration système			0 ou 05
3 Supervision de l'Intégrité des comptes utilisateurs 3.1 Supervision efficace des mécanismes d'authentification ; 3.2. Supervision efficace de l'Intégrité des comptes utilisateurs			0 ou 05 0 ou 10
4. Suivi des actions sur les comptes 4.1. Suivi correcte des actions sur les comptes			0 ou 05
5. Identification des taux de correction des vulnérabilités 5.1 Gestion efficace de protection contre les vulnérabilités 5.2. Résistance efficace aux attaques ciblées			0 ou 05 0 ou 05
6.Détection des compromissions 6.1. Détection correcte des compromissions			0 ou 05
7. Description des mécanismes de défense 7.1 Gestion efficace des mécanismes de défense			0 ou 10
8. Découverte des menaces avancées 8.1 Détection correcte des menaces avancées			0 ou 05
9. identification et analyses des événements de sécurité 9.1. Détermination correcte du Journal des événements de sécurité			0 ou 05
10.Détection d'incident à courte durée 10.1. Réponse efficace aux incidents			0 ou 05
11.Échanges des données avec les périphériques 11.1. Échanges efficaces avec les périphériques ; 11.2. Échange minutieuse des données			0 ou 05 0 ou 05

12. Vérification de Intégrité des données échangées 12.1. Vérification correcte de l'Intégrité des données échangées			0 ou 05
13.Suivi des actions sur les périphériques 13.1. Suivi correcte des actions sur les périphériques.			0 ou 05
		TOTAL :	**/100**
Seuil de réussite : 70%			
Règle de verdict : Néant			
Remarque :			

TABLEAU DE SPÉCIFICATIONS				
METIER	**PENTESTER**		**Code**	**UASI04**
N° et énoncé de la compétence	**6. Utilisation des langages de programmation**		**Durée d'apprentissage**	**120h**
Éléments de la compétence	**Stratégie**	**Indicateurs**	**Critères d'évaluation**	**Points**
Identifier le langage de programmation généralistes :	Processus	1. Identification des caractéristiques et spécificités	1.1. Identification correcte des caractéristiques et spécificités	10
		2. Comparaison des langages	2.1. Comparaison minutieuse des langages entre eux ;	05
		3. Acquisition des nouveaux langages	3.1. Gestion efficace sur les évolutions et nouveaux langages	05
Acquérir les notions en Développement web, applicatif et bases de données	Processus	4.Identification des types de langage	4.1. Acquisition correcte du HTML/CSS, frameworks front-end comme React, Angular, PHP, Node.js, langage de base de données	05
		5.Elaboration du développement défensif	5.1. Acquisition correcte du développement défensif	05
		6.Gestion des vulnérabilités	6.1. Gestion correcte des vulnérabilités	05
		7.Description de la Cryptographie	7.1. Acquisition correcte de la Cryptographie	05
		8.Utilisation des identités	8.1. Gestion correcte des identités	05
Acquérir les notions d'algorithmie et structures de données	Produit	9.Acquisition de la Gestion, de l'Implémentation et de l'Optimisation des algorithmes "	9.1. Gestion efficace de la complexité des algorithmes ;	05
			9.2. Implémentation correcte d'algorithmes courants ;	05
		10. Analyse et optimisation d'algorithmes	10.1. Analyse et optimisation efficace d'algorithmes	**05**
Utiliser la programmation système	Processus	11.Utilisation de la mémoire et threads	11.1. Utilisation appropriée de la mémoire et threads	**05**
		12.Utilisation des Langages de bas niveau comme C, assemblage	12.1 Utilisation correcte des Langages de bas niveau comme C, assemblage	05
		13.Utilisation du Développement embarqué/temps réel	13.1. Utilisation appropriée du Développement embarqué/temps réel.	05

Sécuriser le code source	Processus	14.Exécution des tests de vulnérabilités	14.1. Exécution correcte des tests de vulnérabilités	05
		15.Attribution des droits et permissions	15.1. Attribution appropriée des droits et permissions	05
		16.Utilisation du développement défensif	16.1. Utilisation correcte du développement défensif	05
		17.Gestion des vulnérabilités	17.1Gestion efficace des vulnérabilités	05
	Processus.	18.Utilisation judicieuse de la Cryptographie	18.1. Utilisation judicieuse de la Cryptographie	05

DESCRIPTION DE L'ÉPREUVE	Code : UASI04

Compétence 6 : **Utilisation des langages de programmation**

Renseignements généraux

L'épreuve a pour but d'évaluer l'engagement de l'apprenant dans une démarche qui vise à assurer l'acquisition de la compétence relative à « Utilisation *des langages de programmation* ».

Il s'agit d'une épreuve d'évaluation qui prend en considération l'évaluation des connaissances théoriques et pratiques et elle pourrait être administrée individuellement à l'écrit.

L'évaluation des connaissances théoriques pourrait être réalisée avec l'ensemble des apprenants et l'évaluation des connaissances pratiques pourrait être administrée par groupes en fonction du nombre de postes informatiques disponibles pour les dessins assistés par ordinateur.

L'évaluation portera sur les points suivants :

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.

La durée de l'épreuve pourrait être d'environ 08 heures, pour l'évaluation des connaissances théoriques et pratiques en fonction des différents éléments de compétence, dans un atelier équipé des ordinateurs et d'équipements informatiques.

Liens avec les autres compétences

Cette compétence est en relation avec les compétences générales 7, 8 et 9 du Référentiel de Formation.

Contenu de l'épreuve

Cette épreuve comporte deux exercices de connaissances théoriques et pratiques qui s'appuient sur des situations authentiques du métier de Technicien spécialiste en Pentester et couvrent l'ensemble des aspects cités plus haut.

A partir d'une mise en situation, l'apprenant pourrait être amené à résoudre des problèmes d'Acquisition des notions en Développement web et applicatif par l'utilisation des différentes techniques d'acquisition correcte du HTML/CSS, frameworks front-end comme React, Angular, PHP, Node.js, d'acquisition correcte du développement défensif, de la gestion correcte des vulnérabilités, d'acquisition correcte de la cryptographie et de la Gestion correcte des identités.

Matériel *(Pour un groupe de 25 apprenants)*

- Mobilier.
- Ordinateurs :
- Éditeurs de code
- Environnements de développement intégrés (IDE) :
- Documentation et ressources en ligne
- Connexion Internet :
- Blocs notes

Consigne particulière L'épreuve pourrait être administrée dès la fin du temps d'apprentissage de la compétence. En cas d'échec, l'épreuve devrait être reprise dans son ensemble. Si un seul élément est très faible comparativement aux autres pour lesquels les performances de l'apprenant seraient excellentes, seul cet élément pourrait être repris.

FICHE D'ÉVALUATION			**Code : ULP06**
Compétence 6: Utilisation des langages de programmation			**Durée :4h**
Nom de l'apprenant : Structure de formation : Date de l'évaluation : Signature du formateur :			**Résultat** **SUCCÈS** ☐ **ÉCHEC** ☐
ÉLÉMENTS D'OBSERVATION	**OUI**	**NON**	**RÉSULTATS**
1. **Identification des caractéristiques et spécificités** 1.1. Identification correcte des caractéristiques et spécificités			0 ou 05
2. **Comparaison des langages** 2.1. Comparaison minutieuse des langages entre eux			0 ou 05
3. **Acquisition des nouveaux langages** 3.1. Gestion efficace sur les évolutions et nouveaux langages			0 ou 05
4.**Identification des types de langage** 4.1. Acquisition correcte du HTML/CSS, frameworks front-end comme React, Angular, PHP, Node.js.			0 ou 05
5.**Elaboration du développement défensif** 5.1. Acquisition correcte du développement défensif			0 ou 05
6.**Gestion des vulnérabilités** 6.1. Gestion correcte des vulnérabilités			0 ou 05
7.**Description de la Cryptographie** 7.1. Acquisition correcte de la Cryptographie			0 ou 05

8.**Utilisation des identités** 8.1. Gestion correcte des identités			0 ou 05
9.**Acquisition de la Gestion, de l'Implémentation et de l'Optimisation des algorithmes** 9.1. Gestion efficace de la complexité des algorithmes			0 ou 05
9.2. Implémentation correcte d'algorithmes courants			0 ou 05
10 **Analyse et optimisation d'algorithmes** 10.1. Analyse et optimisation efficace d'algorithmes			0 ou 05
11.Utilisation de la mémoire et threads 11.1. Utilisation appropriée de la mémoire et threads			0 ou 05
12.Utilisation des Langages de bas niveau comme C, assemblage 12.1 Utilisation correcte des Langages de bas niveau comme C, assemblage			0 ou 05
13.Utilisation du Développement embarqué/temps réel 13.1. Utilisation appropriée du Développement embarqué/temps réel			0 ou 10
14.Exécution des tests de vulnérabilités 14.1. Exécution correcte des tests de vulnérabilités			0 ou 05
15.Attribution des droits et permissions 15.1. Attribution appropriée des droits et permissions			0 ou 05
16.Utilisation du développement défensif 16.1. Utilisation correcte du développement défensif			0 ou 05
17.Gestion des vulnérabilités 17.1Gestion efficace des vulnérabilités			0 ou 05
18.Utilisation judicieuse de la Cryptographie 18.1. Utilisation judicieuse de la Cryptographie			0 ou 05
		TOTAL :	**/100**
Seuil de réussite : 70 % et obligation de satisfaire aux exigences des critères 1.1; 5.1; 4.1			
Règle de verdict : Le formateur devra s'assurer qu'en dehors de la maîtrise des opérations, l'apprenant adopte des attitudes respectant les règles de sécurité pour lesquelles il aura été évalué.	**Oui** ☐	**Non** ☐	
Remarque :			

TABLEAU DE SPÉCIFICATIONS				
Métier	**PENTESTER**		Code	**IVP07**
N° et libellé de la compétence	**7 Identifier les vulnérabilités potentielles dans les Systèmes informatiques**		Durée d'apprentissage/d'évaluation	**90h**
Éléments de la compétence	Stratégie	Indicateurs	Critères d'évaluation	Points
Acquérir les connaissances approfondies en sécurité informatique	Processus	1. transmission des connaissances de référence	1. 1. Acquisition parfaite des concepts, modèles et normes de référence	05
			1.2. Transmission correcte des connaissances	05
		2. détection des nouvelles menaces.	2.1 Identification correcte des nouvelles menaces.	05
		3. identification des nouvelles avancées dans le domaine	3.1 Contrôle exact de l'évolution des connaissances.	05
Décrire un audit de configuration	Processus	4. Vérification du périmètre couvert et des tests réalisés	4.1 Vérification correcte du périmètre couvert	10
			4.2 Vérification correcte des tests réalisé ;	10
		5.Élaboration du rapport d'audit	5.1 Précision -pertinente du rapport d'audit produit	05
Effectuer une analyse statique et dynamique de code source	Processus	6. Identification des vulnérabilités	6.1. Détection correcte des vulnérabilités	10
		7.Acquisition des résultats et des recommandations	7.1 Précision pertinente des résultats produits	05
			7.2. Détermination Pertinente des recommandation	05
Effectuer les tests d'intrusion ("penetration esting")	Processus	8.Analyse des failles de sécurité	8.1 Exploitation correcte des vulnérabilités	10
		9. précision des prévisions	9.1 Détermination correcte des résultats	10
Veiller sur les vulnérabilités	Processus	10. anticipation des tendances émergentes à partir des sources identifiées	10.1. Identification judicieuse des sources de veille	05
		11. Exploitation des alertes sur les vulnérabilités	11.1 Exploitation correcte des alertes sur les vulnérabilités	05
		12. Contextualisation du Niveau de Précision de la sécurité	12.1 Contextualisation efficace par rapport au système audité	05

DESCRIPTION DE L'ÉPREUVE	Code : IVP07
Métier	**PENTESTER**
N° et énoncé de la compétence	7**. Identifier les vulnérabilités potentielles dans les Systèmes informatiques**

Renseignements généraux

L'épreuve a pour but d'évaluer la compétence relative à « *: Identifier les vulnérabilités potentielles dans les Systèmes informatiques* ». Il s'agit d'une épreuve d'évaluation qui prend en considération une portion d'évaluation des connaissances théoriques et une portion de type pratique.
L'évaluation de type pratique pourrait être administrée individuellement.
L'évaluation des connaissances théoriques pourrait être réalisée avec l'ensemble des apprenants. L'environnement de réalisation de l'épreuve de type pratique devrait s'inspirer le plus possible d'une situation en milieu de travail.
La durée cumulée de l'ensemble des épreuves pourrait être d'environ 4 heures, et inclure la portion pratique combinée à celle de l'évaluation des connaissances théoriques pour les différents éléments de compétence.

Déroulement de l'épreuve

- Par l'entremise d'une épreuve de connaissances théoriques, on pourrait demander à l'apprenant de décrire un processus d'acquisition des connaissances approfondies en sécurité informatique, d'un audit de configuration, d'une analyse statique et dynamique de code source, des tests d'intrusion ("penetration testing») et de Veille sur les vulnérabilités.

Matériel (Pour un effectif de 25 apprenants)

- Ordinateurs portables puissants,
- Logiciels de détection de vulnérabilités.
- Outils d'analyse de sécurité
- Connexion Internet :
- etc

Consignes particulières

- L'épreuve pourrait être administrée durant le temps d'apprentissage d'une compétence subséquente ou d'une compétence évaluée en parallèle.
- En cas d'échec, l'épreuve devrait être reprise dans son ensemble. Si un seul élément est très faible comparativement aux autres pour lesquels les performances de l'apprenant seraient excellentes, seul cet élément pourrait être repris.

FICHE D'ÉVALUATION			Code : IVP07
N° et énoncé de la compétence	**7. Identifier les vulnérabilités potentielles dans les Systèmes informatiques**		**Durée :6h**
Nom de l'apprenant : Structure de formation : Date de l'évaluation : Signature du formateur :			**Résultat** **SUCCÈS** ☐ **ÉCHEC** ☐
ÉLÉMENTS D'OBSERVATION	**OUI**	**NON**	**RÉSULTATS**
1. transmission des connaissances de référence 1. 1. Acquisition parfaite des concepts, modèles et normes de référence ;			0 ou 05
1.2. Transmission correcte des connaissances			0 ou 05
2. détection des nouvelles menaces. 2.1 Identification correcte des nouvelles menaces ;			0 ou 05
3. identification des nouvelles avancées dans le domaine 3.1 Contrôle exact de l'évolution des connaissances			0 ou 05
4. Vérification du périmètre couvert et des tests réalisés 4.1 Vérification correcte du périmètre couvert			0 ou 10
4.2 Vérification correcte des tests réalisé ;			0 ou 10
5.Élaboration du rapport d'audit 5.1 Précision -pertinente du rapport d'audit produit			0 ou 05
6. Identification des vulnérabilités 6.1. Détection correcte des vulnérabilités			0 ou 10
7.Acquisition des résultats et des recommandations 7.1 Exploitation correcte des vulnérabilités			0 ou 05
8. précision des prévisions 8.1 Détermination correcte des résultats			0 ou 10
9. anticipation des tendances émergentes à partir des sources identifiées			0 ou 05

9.1. Identification judicieuse des sources de veille			
10. anticipation des tendances émergentes à partir des sources identifiées 10.1. Identification judicieuse des sources de veille			0 ou 10
11. Exploitation des alertes sur les vulnérabilités 11.1 Exploitation correcte des alertes sur les vulnérabilités			0 ou 05
12. Contextualisation du Niveau de Précision de la sécurité 12.1 Contextualisation efficace par rapport au système audité			0 ou 010
		TOTAL :	**/100**
Seuil de réussite : 70 % et obligation de satisfaire aux exigences des critères 2.1;3.1;4.1;6.1;11.1			
Règle de verdict : Le formateur devra s'assurer qu'en dehors de la maîtrise des opérations, l'apprenant adopte des attitudes respectant les règles de sécurité pour lesquelles il aura été évalué.	**Oui** ☐	**Non** ☐	
Remarque :			

TABLEAU DE SPÉCIFICATIONS				
Métier	**PENTESTER**		**Code**	**COP08**
N° et Énoncé de la compétence	8. **Configurer les outils de test de pénétration des systèmes d'exploitation**		**Durée d'apprentissage**	**120h**
Éléments de la compétence	**Stratégie**	**Indicateurs**	**Critères d'évaluation**	**Points**
Utiliser des outils de tests de pénétration d'intrusion	Processus	1. Exploitation des fonctionnalités des outils	1.1 Exploitation efficace des fonctionnalités des outils	
		2**.** Identification des outils en fonction des tests	2.1. Choix pertinent des outils en fonction des tests	10
	Processus	3. Documentation des résultats	3.1 Documentation pertinente des résultats	
Configurer les outils	Processus	4. Réalisation des paramétrages	4. **1.** Réalisation correcte des paramétrages	10
	Produit	5. Choix des options/modules	5.1. Sélection pertinente des options/modules	10
	Processus	6. Exécution des tâches de configuration	6.1. Exécution appropriée des tâches de configuration	10
		7. protection des configurations déployées	7.1. Sécurisation correcte des configurations déployées	10
Configurer les systèmes d'exploitation cibles	Processus	8. Spécification des OS ciblés	8.1 Spécification efficace des OS ciblés	10
		9.. Documentation des services et ports testés	9.1. Documentation pertinente des services et ports testé	
	Processus	10. Utilisation des mises à jour des configurations	10.1 Exploitation efficace des mises à jour des configurations	10
Elaborer les Scripts	Processus	11.Exploitation des codes langage	11.1. Utilisation correcte du code /langage	10
	Processus	12. Utilisation des fonctionnalités	12.1. Gestion Pertinente des fonctionnalités	10
	Produit	13 Vérification de l'efficacité des scripts	13.1 Vérification correcte de l'efficacité des scripts	10
	Processus	14 Documentation pertinente des techniques des scripts	14.1 Documentation pertinente des techniques des scripts	

DESCRIPTION DE L'ÉPREUVE		Code : COP08
N° et énoncé de la compétence	**8. Configurer les outils de test de pénétration des systèmes d'exploitation**	
Renseignements généraux		
L'épreuve a pour but d'évaluer la compétence relative à « *Configurer les outils de test de pénétration des systèmes d'exploitation* ». Il s'agit d'une épreuve d'évaluation qui prend en considération une portion d'évaluation des connaissances théoriques et une portion de type pratique. L'évaluation de type pratique pourrait être administrée individuellement. L'évaluation des connaissances théoriques pourrait être réalisée avec l'ensemble des apprenants. L'environnement de réalisation de l'épreuve de type pratique devrait s'inspirer le plus possible d'une situation en milieu de travail. La durée cumulée de l'ensemble des épreuves pourrait être d'environ 10 heures, et inclure la portion pratique combinée à celle de l'évaluation des connaissances théoriques pour les différents éléments de compétence.		
Déroulement de l'épreuve Par l'entremise d'une épreuve de connaissances théoriques, on pourrait demander à l'apprenant d'Utiliser des outils de tests de pénétration d'intrusion, de Configurer les outils, les systèmes d'exploitation cibles et d'Elaborer les Scripts intelligents.		
Matériel (Pour un effectif de 25 apprenants) • Matériel informatique • Outils de test d'intrusion • Environnement de test • Matériel de réseau : • Outils de capture de trafic • Stylo à bille, crayons de dessin ;		
Consignes particulières • L'épreuve pourrait être administrée durant le temps d'apprentissage d'une compétence subséquente ou d'une compétence évaluée en parallèle. • En cas d'échec, l'épreuve devrait être reprise dans son ensemble. Si un seul élément est très faible comparativement aux autres pour lesquels les performances de l'apprenant seraient excellentes, seul cet élément pourrait être repris.		

FICHE D'ÉVALUATION		Code : COP08
N° et libellé de la compétence	**8. Configurer les outils de test de pénétration des systèmes d'exploitation**	**Durée :8h**

Nom de l'apprenant : Établissement d'enseignement : Date de l'évaluation : Signature du formateur :	**Résultat**	
	H	**ÉCHEC**
	☐	☐

ÉLÉMENTS D'OBSERVATION	**OUI**	**NON**	**RÉSULTATS**
1. Exploitation des fonctionnalités des outils 1.1. Exploitation efficace des fonctionnalités des outils			
2. Identification des outils en fonction des tests 2.1. Choix pertinent des outils en fonction des tests			0 ou 010
3. Documentation des résultats 3.1 Documentation pertinente des résultats			
4. Réalisation des paramétrages 4. **1.** Réalisation correcte des paramétrages			0 ou 10
5. **Choix** des options/modules 5.1. Sélection pertinente des options/modules			0 ou 10
6. Exécution appropriée des tâches de configuration 6.1. Exécution appropriée des tâches de configuration			0 ou 10
7. protection des configurations déployées 7.1. Sécurisation correcte des configurations déployées			0 ou 10
8. Spécification des OS ciblés 8.1 Spécification efficace des OS ciblés			0 ou 10
9.. Documentation des services et ports testés 9.1. Documentation pertinente des services et ports testés			

FICHE D'ÉVALUATION		Code : COP08	
N° et libellé de la compétence	**8. Configurer les outils de test de pénétration des systèmes d'exploitation**	**Durée :8h**	
10. **Utilisation** des mises à jour des configurations 10.1 Exploitation efficace des mises à jour des configurations			0 ou 10
11.Exploitation des codes langage 11.1. Utilisation correcte du code /langage			0 ou 10
12. Utilisation des fonctionnalités 12.1. Gestion Pertinente des fonctionnalités			0 ou 10
13. Vérification de l'efficacité des scripts 13.1 Vérification correcte de l'efficacité des scripts			0 ou 10
14 Documentation pertinente des techniques des scripts 14.1 Documentation pertinente des techniques des scripts			
EXIGENCES L'évaluation des connaissances pratiques pourrait être utilisée au cas où une observation (évaluation pratique) ne pourrait pas être réalisée. Si tel est le cas, l'apprenant devra répondre adéquatement à 80 % des questions qui lui sont posées afin d'obtenir la totalité des points associés au critère d'évaluation			
		TOTAL :	**/100**
Seuil de réussite : 70 points			
Règle de verdict : Le formateur devra s'assurer qu'en dehors de la maîtrise des opérations, l'apprenant adopte des attitudes respectant les règles de sécurité.	**Oui** ☐	**Non** ☐	
Remarque			

TABLEAU DE SPÉCIFICATIONS				
Métier : PENTESTER			**Code**	**RVA09**
N° et Énoncé de la compétence	**9. Tester la vulnérabilité sur les réseaux, les applications, site web et les systèmes d'exploitation**		**Durée d'apprentissage/d'évaluation**	**150h**
Éléments de la compétence	**Stratégie**	**Indicateurs**	**Critères d'évaluation**	**Points**
Analyser la topologie et les flux réseau	Produit	1. Production des informations	1.1.Production correcte des informations	**05**
		2. Réalisation de la cartographie réseaux	2.1..Réalisation correcte de la cartographie réseau	**05**
	Processus	3.Gestion des flux	3.1.Gestion efficace des flux	**05**
		4.Evaluation des métriques réseau	4.1.Evaluation correcte des métriques réseau	**05**
Identifier les vecteurs d'intrusion réseau	Processus	5.Identification des techniques d'attaque réseau	5.1. Identification correcte des techniques d'attaque réseau ;	**05**
		6. Analyse appropriée des logs et alertes	6.1. Analyse appropriée des logs et alertes	**05**
		7. Collecte minutieuse des vecteurs potentiels couverts	7.1. Collecte minutieuse des vecteurs potentiels couverts.	**05**
Décrire les outils de tests de vulnérabilités	Processus	**8.** Acquisition des outils de test d'intrusion des réseaux /applications	8.1 Présentation correcte des outils de tests d'intrusion/pentesting	10
			8.2 Description parfaite des fonctionnalités	05
		9. Détection des vulnérabilités des réseaux/applications	9.1. Détection correcte des vulnérabilités des réseaux/applications	05
Tester l'efficacité du réseau et des applications :	Processus	10.Description des résultats de tests	10.1. Analyse judicieuse des résultats de tests	10
		11.Utilisation des préconisations	11.1. Application efficace des préconisations	05
		12.Identification des failles	12.1. Détection correcte de failles dans les APIs, services web	05
Tester les systèmes d'exploitation :	Processus	13. Description des configurations et services testés	13.1. Gestion efficace des configurations et services testés ;	05
		14.Scanne des vulnérabilités	14.1Précision correcte du diagnostic de vulnérabilité	05
	Produit	15. Recommandation des correctifs et mesures	15. 1. Recommandation des correctifs et mesures	10

DESCRIPTION DE L'ÉPREUVE		Code : RVA09
N° et énoncé de la compétence	*9.* **Tester la vulnérabilité sur les Réseaux, les applications, site web et les systèmes d'exploitation**	

Renseignements généraux

L'épreuve a pour but d'évaluer la compétence relative à « *Effectuer les tests de vulnérabilité, sur les Réseaux, les applications, site web et les systèmes d'exploitation* ». Il s'agit d'une épreuve d'évaluation qui prend en considération une portion d'évaluation des connaissances théoriques et une portion de type pratique.

L'évaluation de type pratique pourrait être administrée individuellement.

L'évaluation des connaissances théoriques pourrait être réalisée avec l'ensemble des apprenants. L'environnement de réalisation de l'épreuve de type pratique devrait s'inspirer le plus possible d'une situation en milieu de travail.

La durée cumulée de l'ensemble des épreuves pourrait être d'environ 10 heures, et inclure la portion pratique combinée à celle de l'évaluation des connaissances théoriques pour les différents éléments de compétence.

Déroulement de l'épreuve

Par l'entremise d'une épreuve de connaissances théoriques, on pourrait demander à l'apprenant d'Analyser la topologie et les flux réseau, d' Analyser les risques et menaces, de Décrire les outils de tests de vulnérabilités, de Tester l'efficacité du réseau, des applications, du système d'exploitation, et de présenter un rapport des résultats.

On pourrait également demander à l'apprenant, dans le cadre d'une évaluation pratique, de Tester l'efficacité d'un serveur web à partir des outils de test de son choix.

Matériel (Pour un effectif de 25 apprenants)

- Ordinateurs portables puissants,
- Outils de test d'intrusion
- Environnement de test
- Matériel de réseau :
- Outils de capture de trafic

Consignes particulières

- L'épreuve pourrait être administrée durant le temps d'apprentissage d'une compétence subséquente ou d'une compétence évaluée en parallèle.
- En cas d'échec, l'épreuve devrait être reprise dans son ensemble. Si un seul élément est très faible comparativement aux autres pour lesquels les performances de l'apprenant seraient excellentes, seul cet élément pourrait être repris.

FICHE D'ÉVALUATION		Code : RVAP09
N° et énoncé de la compétence	9. **Tester la vulnérabilité sur les Réseaux des applications, site web et les systèmes d'exploitation**	**Durée : 10 h**

Nom de l'apprenant : Structure de formation : Date de l'évaluation : Signature du formateur :	**Résultat**	
	SUCCÈS	**ÉCHEC**
	☐	☐

ÉLÉMENTS D'OBSERVATION	**OUI**	**NON**	**RÉSULTATS**
1.Production des informations 1.1.Production correcte des informations			0 ou 10
2.Réalisation de la cartographie réseaux 2.1..Réalisation correcte de la cartographie réseau			0 ou 05
3.Evaluation des métriques réseau 3.1. Evaluation correcte des métriques réseau			0 ou 05
4.Identification des techniques d'attaque réseau 4.1.Identification correcte des techniques d'attaque réseau			0 ou 05
5.Gestion des logs et alertes 5.1. Gestion efficace des logs et alertes			0 ou 05
6.Utilisation des modèles de compromission 6.1.Utilisation parfaite des modèles de compromission			0 ou 05
7.Calcul des métriques de propagation 7.1. Calcul correct des métriques de propagation			0 ou 05
8**.** Acquisition des outils de test d'intrusion des réseaux /applications			0 ou 10
8.1 Présentation correcte des outils de tests d'intrusion/pentesting 8.2 Description parfaite des fonctionnalités			0 ou 05
9. Détection des vulnérabilités des réseaux ou applications 9.1 Détection des vulnérabilités des réseaux ou applications			0 ou 05
10.Description des résultats de tests			0 ou 10

FICHE D'ÉVALUATION			Code : RVAP09
N° et énoncé de la compétence	9. **Tester la vulnérabilité sur les Réseaux des applications, site web et les systèmes d'exploitation**		**Durée : 10 h**
10.1. Analyse judicieuse des résultats de tests			
11.Utilisation des préconisations 11.1. Application efficace des préconisations			0 ou 05
12.Identification des failles 12.1. Détection correcte de failles dans les APIs, services web			0 ou 05
13. Description des configurations et services testés 13.1. Gestion efficace des configurations et services testés.			0 ou 05
14.Scanne des vulnérabilités 14.1Précision correcte du diagnostic de vulnérabilité			0 ou 05
15. Recommandation des correctifs et mesures 15.1 Conduite rigoureuse des tests, mesures et contrôles permettant de valider ou non les hypothèses			0 ou 10
EXIGENCES L'évaluation des connaissances pratiques pourrait être utilisée au cas où une observation (évaluation pratique) ne pourrait pas être réalisée. Si tel est le cas, l'apprenant devra répondre adéquatement à 70 % des questions qui lui sont posées afin d'obtenir la totalité des points associés au critère d'évaluation			
		TOTAL :	**/100**
Seuil de réussite: 70 points			
Règle de verdict.	**Oui** ☐	**Non** ☐	
Remarque			

TABLEAU DE SPÉCIFICATIONS				
Métier	**PENTESTER**		**Code**	**PSA10**
N° et libellé de la compétence	**10. Proposition des stratégies d'atténuation**		**Durée d'apprentissage**	**120h**
Éléments de la compétence	Stratégie	**Indicateurs**	**Critères d'évaluation**	**Points**
Évaluer la propagation latérale de l'attaquant	Processus	1.Utilisation des modèles de compromission	1.1.Utilisation parfaite des modèles de compromission ;	**05**
		2.Simulation des scénarios de propagation	2.2.Simulation efficace des scénarios de propagation	05
	Produit	**3.** Calcul des métriques de propagation	3.1.Calcul correct des métriques de propagation	**05**
Concevoir des scénarios de segmentation réseau	Processus	4.Elaboration d'un microsegmentation du réseau ;	4.1.Elaboration correcte d'un microsegmentation du réseau ;	**05**
	Processus	5.Gestion des scénarios	5.1.Gestion efficace des scénarios	**05**
	Produit	6.documentation de la technique proposée	6.1.documentation pertinente de la technique proposée	**05**
Analyser les risques et menaces	Processus	7.Analyse des menaces et vulnérabilités ;	7.1Analyse efficace des menaces et vulnérabilités ;	**05**
	Processus	8Exploitation du contexte organisationnel et règlementaire ;	8.1.Exploitation correcte du contexte organisationnel et règlementaire ;	**05**
	Processus	9.Analyse efficace des mises à jour	91.Analyse efficace des mises à jour	**05**
Réaliser des conseils sur l'architecture sécurité	Produit	10. Elaboration d'une microsegmentation du réseau	10.1.Elaboration correcte d'une microsegmentation du réseau	**05**
	Processus	11. Gestion des scénarios	11.1 Gestion efficace des scénarios	**05**
		12. Documentation de la technique proposée	12.1Documentation correcte de la technique proposée	**05**
Élaborer une politique de sécurité	Processus	13.Gestion des bonnes pratiques et référentiels reconnus	13.1Production efficace d'une documentation présentant la politique de sécurité	**05**

			13.2. Utilisation correcte des bonnes pratiques et référentiels reconnus ;	
	Produit	14.Elaboration d'un plan d'action de suivi et d'audit	14.1. Elaboration correcte d'un plan d'action de suivi et d'audit	**05**
Préconiser des mesures techniques	Processus	15.Proposition des solutions exhaustives ;	15.1.Proposition pertinente des solutions exhaustives ;	**05**
		16. Déploiement et administration correctes d'une politique de sécurité ;	16.1.Déploiement et administration correctes d'une politique de sécurité ;	**05**
		17.Reduction efficace des risques	17.1.Reduction efficace des risques	**05**
Valider la mise en œuvre	Processus	18. Validation des tests	18.1.Utilisation correcte des scénarios de tests	**05**
			17.2Gestion efficace des tests effectués	**05**
		19. .Contrôle du respect des spécifications définies	18.1Contrôle efficace du respect des spécifications définies	**05**

DESCRIPTION DE L'ÉPREUVE		Code : PSA10
N° et énoncé de la compétence	**10. Proposition des stratégies d'atténuation**	

Renseignements généraux

L'épreuve a pour but d'évaluer la compétence relative à **«** *Proposition des stratégies d'atténuation* ».

Il s'agit d'une épreuve d'évaluation qui prend en considération l'évaluation des connaissances théoriques et de type pratique. Cependant, dans l'impossibilité de produire une épreuve mixte, l'évaluation des connaissances pratiques devrait être priorisée.

L'évaluation de type pratique pourrait être administrée à un groupe restreint d'apprenants en raison de la disponibilité du matériel, de la matière d'œuvre et de la capacité du formateur à observer plusieurs personnes à la fois. L'évaluation des connaissances théoriques pourrait être réalisée avec l'ensemble des participants. L'environnement de réalisation de l'épreuve de type pratique devrait s'inspirer le plus possible d'une situation en milieu de travail.

L'épreuve pourrait être d'une durée d'environ 10 heures, ce qui inclut la portion combinée à celle de l'évaluation des connaissances théoriques et pratique.

Déroulement de l'épreuve

Par l'entremise d'une épreuve de connaissances pratique, on pourrait demander à l'apprenant à simuler une situation d'attaque ou d'intrusion dans un environnement donné, mettre en place des mesures de sécurité supplémentaires, et proposer des mesures d'amélioration.

Matériel et équipements (Pour un groupe de 25 apprenants)

- Matériel informatique
- Outils de test d'intrusion
- Environnement de test
- Matériel de réseau :
- Outils de capture de trafic
- Les blocs notes

Les Bics et crayons

Consigne particulière

- L'épreuve pourrait être administrée durant le temps d'apprentissage d'une compétence subséquente, ou d'une compétence évaluée en parallèle (compétences 12 et 14);
- En cas d'échec, l'épreuve devrait être reprise dans son ensemble. Si un seul élément est très faible comparativement aux autres pour lesquels les performances de l'apprenant seraient excellentes, seul cet élément pourrait être repris.

FICHE D'ÉVALUATION			Code : PSA10
N° et énoncé de la compétence	**10. Proposition des stratégies d'atténuation**		**Durée :8h**
Nom de l'apprenant : Structure de formation : Date de l'évaluation : Signature du formateur :			**Résultat** **SUCCÈS** ☐ **ÉCHEC** ☐
ÉLÉMENTS D'OBSERVATION	**OUI**	**NON**	**RÉSULTATS**
1.Utilisation des modèles de compromission 1.1.Utilisation parfaite des modèles de compromission ;			0 ou 05
2.Simulation des scénarios de propagation 2.2.Simulation efficace des scénarios de propagation			0 ou 05
3.Calcul des métriques de propagation 3.1.Calcul correct des métriques de propagation			0 ou 05
4.Elaboration d'un microsegmentation du réseau 4.1.Elaboration correcte d'un microsegmentation du réseau			0 ou 05
5.Gestion des scénarios 5.1.Gestion efficace des scénarios			0 ou 05
6.documentation de la technique proposée 6.1.documentation pertinente de la technique proposée			0 ou 05
7.Exploitation du contexte organisationnel et règlementaire 7.1.Exploitation correcte du contexte organisationnel et règlementaire ;			0 ou 05
8.Analyse efficace des mises à jour 8.1.Analyse efficace des mises à jour			0 ou 05
9.Elaboration d'une microsegmentation du réseau 9.1.Elaboration correcte d'une microsegmentation du réseau			0 ou 05
10.Gestion des scénarios 10.1.Gestion efficace des scénarios			0 ou 05

11.Documentation de la technique proposée 11.1.Documentation correcte de la technique proposée			0 ou 05
12.Gestion des bonnes pratiques et référentiels reconnus 12.1.Production efficace d'une documentation présentant la politique de sécurité 12.2. Utilisation correcte des bonnes pratiques et référentiels reconnus ;			**0 ou 05** 0 ou 05
13.Elaboration d'un plan d'action de suivi et d'audit 13.1.Elaboration correcte d'un plan d'action de suivi et d'audit			0 ou 05
14.Proposition des solutions exhaustives ; 14.1.Proposition pertinente des solutions exhaustives			0 ou 05
15.Déploiement et administration correctes d'une politique de sécurité 15.1.Déploiement et administration correctes d'une politique de sécurité ;			0 ou 05
16.Reduction efficace des risques 16.1.Reduction efficace des risques			0 ou 05
17.Validation des tests 17.1.Utilisation correcte des scénarios de tests 17.2.Gestion efficace des tests effectués			0 ou 05 0 ou 05
18. .Contrôle du respect des spécifications définies 18.1Contrôle efficace du respect des spécifications définies			0 ou 05
		TOTAL :	**/100**
Seuil de réussite : 70 % et obligation de satisfaire aux exigences des critères 1.1;5.1 ,7.1, 13.2			
Règle de verdict : Le formateur devra s'assurer qu'en dehors de la maîtrise des opérations, l'apprenant adopte des attitudes respectant les règles de sécurité pour lesquelles il aura été évalué à la compétence 03.	**Oui** ☐	**Non** ☐	
Remarque :			

TABLEAU DE SPÉCIFICATIONS				
Métier	**PENTESTER**		**Code : CPF11**	**CPF11**
N° et énoncé de la compétence	**11. Configurer les pares-feux et des systèmes de détection d'intrusions**		**Durée d'apprentissage**	**120h**
Éléments de la compétence	**Stratégie**	**Indicateurs**	**Critères d'évaluation**	**Points**
Configurer les pares-feux et des IDS/IPS		1 Validation **des tests**	1.1. Définition Précise des règles/signatures	**5**
			1.2. Validation correcte des tests effectués	**5**
	Produit	2 Documentation des techniques produites	2.1. Documentation correcte des techniques produites	**10**
Implémenter une politique de filtrage et de détection	Processus	3 Utilisation des bonnes pratiques de sécurité ;	3.1. Utilisation correcte des bonnes pratiques de sécurité ;	**10**
		4 Déploiement sur l'infrastructure cible ;	4.1. Déploiement approprié sur l'infrastructure cible ;	**10**
		5 Mesure de la politique de filtrage et de détection	5.1. Mesure efficace de la politique de filtrage et de détection	**10**
Gérer les règles, les signatures et les listes blanches/noires	Processus	6 Réactivité aux nouvelles menaces ;	6.1. Réactivité appropriée aux nouvelles menaces ;	**10**
		7 Gestion des configurations	7.1. Contrôle efficace d'impact des modifications ;	**5**
			7.2. Exploitation correcte de la supervision des configurations.	**5**
Superviser les événements de sécurité générés	Processus	8 Exploitation des corrélations et alertes remontées ;	8.1. Exploitation rationnelle des corrélations et alertes remontées ;	**10**
	Produit	9 Collecte des logs et métriques	9.1. Collecte Exhaustive des logs et métriques	**10**
	Processus	10 Description de reporting des incidents	10.1. Description correcte de reporting des incidents	**10**

DESCRIPTION DE L'ÉPREUVE	Code : CPF11
N° et énoncé de la compétence	**11. Configurer les pares-feux et des systèmes de détection d'intrusions**

Renseignements généraux

L'épreuve a pour but d'évaluer la compétence relative à « **Configurer les pares-feux et des systèmes de détection d'intrusions** ».
Il s'agit d'une épreuve d'évaluation qui prend en considération l'évaluation des connaissances théoriques et petite portion de type pratique.
L'évaluation de type pratique pourrait être administrée à un groupe restreint d'apprenants en raison de la disponibilité du matériel, de la matière d'œuvre et de la capacité du formateur à observer plusieurs personnes à la fois. L'évaluation des connaissances théoriques pourrait être réalisée avec l'ensemble des participants. L'environnement de réalisation de l'épreuve de type pratique devrait s'inspirer le plus possible d'une situation en milieu de travail.
L'épreuve pourrait être d'une durée d'environ 5 heures, ce qui inclut la portion combinée à celle de l'évaluation des connaissances théoriques (1h) et pratique(4h).

Déroulement de l'épreuve

Par l'entremise d'une épreuve de connaissances pratique, à partir de la sélection des outils de test, la création d'un environnement de test isolé et la configuration des systèmes de pare-feu et de détection d'intrusions. On pourrait demander l'exécution des scénarios d'attaque, de faire des Analyse des résultats, une Améliorations et ajustements

Matériel et équipements (Pour un groupe de 25 apprenants)

- Ordinateurs
- Internet
- Systèmes de Détection d'Intrusion (IDS.
- Systèmes de Prévention d'Intrusion (IPS) .
- Pare-feux (Firewalls) .
- Logiciels de Gestion des Alertes :
- Outils de Surveillance du Trafic
- Les blocs notes
- Les Bics et crayons

Consigne particulière

- L'épreuve pourrait être administrée durant le temps d'apprentissage d'une compétence subséquente, ou d'une compétence évaluée en parallèle (compétences 13 et 14);
- En cas d'échec, l'épreuve devrait être reprise dans son ensemble. Si un seul élément est très faible comparativement aux autres pour lesquels les performances de l'apprenant seraient excellentes, seul cet élément pourrait être repris.

FICHE D'ÉVALUATION		**Code : CPF11**
N° et énoncé de la compétence	**11. Configurer les pares-feux et des systèmes de détection d'intrusions**	**Durée : 8h**

Nom de l'apprenant : Structure de formation : Date de l'évaluation : Signature du formateur :	**Résultat**	
	SUCCÈS	**ÉCHEC**
	☐	☐

ÉLÉMENTS D'OBSERVATION	**OUI**	**NON**	**RÉSULTATS**
1.Validation des tests 1.1. Définition Précise des règles/signatures ;			0 ou 05
1.2.Validation correcte des tests effectués ;			0 ou 05
2.Production des documents techniques 2.1. Documentation correcte des techniques produites			0 ou 10
3.Utilisation des bonnes pratiques de sécurité ; 3.1 Utilisation correcte des bonnes pratiques de sécurité ;			0 ou 10
4.Déploiement sur l'infrastructure cible 4.1 Déploiement approprié sur l'infrastructure cible			0 ou 10
5.Mesure de la politique de filtrage et de détection 5.1. Mesure efficace de la politique de filtrage et de détection			0 ou 10
6.Réactivité aux nouvelles menaces ; 6.1. Réactivité appropriée aux nouvelles menaces ;			0 ou 10
7.Gestion des configurations 7.1 Contrôle efficace d'impact des modifications ;			0 ou 05
7.2 Exploitation correcte de la supervision des configurations.			0 ou 05
8.Exploitation des corrélations et alertes remontées ; 8.1. Exploitation rationnelle des corrélations et alertes remontées ;			0 ou 10
9.Collecte des logs et métriques			0 ou 10

9.1. Collecte Exhaustive des logs et métriques			
10.Description de reporting des incidents 10.1 Description correcte de reporting des incidents			0 ou 10
		TOTAL:	**/100**
Seuil de réussite : 70 %			
Règle de verdict : Le formateur devra s'assurer qu'en dehors de la maîtrise des opérations, l'apprenant adopte des attitudes respectant les règles de sécurité pour lesquelles il aura été évalué à la compétence 03.	**Oui** ☐	**Non** ☐	
Remarque :			

TABLEAU DE SPÉCIFICATIONS				
Métier	**PENTESTER**		**Code : VTC12**	**VTC12**
N° et énoncé de la compétence	**12. Assurer la veille technologique en cyberattaque**		**Durée d'apprentissage**	**90h**
Éléments de la compétence	**Stratégie**	**Indicateurs**	**Critères d'évaluation**	**Points**
Assurer la veille technologique et sécuritaire	Processus	1. diffusion des alertes sur les nouvelles menaces ;	1.1.diffusion correcte des alertes sur les nouvelles menaces ;	**05**
		2. analyse des tendances et évolutions ;	2.1 analyse pertinente des tendances et évolutions ;	**10**
	Produit	3. Collecte de la documentation	3.1 Collecte efficace de la documentation des informations	**05**
Analyser les nouvelles techniques d'attaques	Processus	4. Identification des vecteurs et failles exploités ;	4.1. Identification précise des vecteurs et failles exploités ;	**05**
		5. Évaluation de la criticité et de l'impact potentiel	5.1 Évaluation correcte de la criticité et de l'impact potentiel	**10**
		6. Exploitation des mises à jour	6.1 Exploitation efficace des mises à jour de l'analyse en fonction des retours	**05**
Évaluer l'impact sur l'architecture existante	Processus	7. Analyse des risques encourus ;	7.1. Analyse correcte des risques encourus ;	**10**
		8. Gestion des scénarios de test	8.1 Utilisation correcte des scénarios de tests ;	**05**
			8.2 Exploitation Précise de la documentation des résultats	**05**
Préconiser des mesures correctives	Processus	9. Gestion des risques	9.1. Rapprochement correcte entre les objectifs de sécurité et le niveau de risque ;	**05**
			9.2. Implémentation et pertinence correcte des solutions ;	**05**
		10. Exploitation du rapport coût/bénéfice et des contraintes	10.1 Exploitation correcte du rapport coût/bénéfice et des contraintes	**05**
		11. Adaptation du délai de mise en œuvre à la criticité.	11.1 Adaptation correcte du délai de mise en œuvre à la criticité.	**05**
				05
Valider la réponse apportée	Processus	12. Exécution des tests	12.1 exécution correcte des tests;	**05**
		13. Production d'une documentation des résultats	13.1 Production exacte d'une documentation des résultats ;	**05**
		14. Respect des spécifications définies	14.1 Respect correct des spécifications définies.	**05**

DESCRIPTION DE L'ÉPREUVE	**Code : VTC12**
N° et énoncé de la compétence	**12.. Assurer la veille technologique en cyberattaque**

Renseignements généraux

L'épreuve a pour but d'évaluer la compétence relative à « Assurer la veille technologique en cyberattaque ».
Il s'agit d'une épreuve d'évaluation qui prend en considération l'évaluation des connaissances théoriques et petite portion de type pratique.
L'évaluation de type pratique pourrait être administrée à un groupe restreint d'apprenants en raison de la disponibilité du matériel, de la matière d'œuvre et de la capacité du formateur à observer plusieurs personnes à la fois.
L'évaluation des connaissances théoriques pourrait être réalisée avec l'ensemble des participants. L'environnement de réalisation de l'épreuve de type pratique devrait s'inspirer le plus possible d'une situation en milieu de travail
L'épreuve pourrait être d'une durée d'environ (5 heures), ce qui inclut la portion combinée à celle de l'évaluation des connaissances théoriques et pratique.

Déroulement de l'épreuve

Par l'entremise d'une épreuve de connaissances pratique, on pourrait demander à l'apprenant d'assurer la veille sur les menaces, sur les technologique., sur la réglementation, sur la concurrence et sur l'écosystème

Matériel et équipements (Pour un groupe de 25 apprenants)

- Ordinateurs
- Internet ;
- Les logiciels

Consigne particulière

- L'épreuve pourrait être administrée durant le temps d'apprentissage d'une compétence subséquente, ou d'une compétence évaluée en parallèle (compétences 13 et 14);
- En cas d'échec, l'épreuve devrait être reprise dans son ensemble. Si un seul élément est très faible comparativement aux autres pour lesquels les performances de l'apprenant seraient excellentes, seul cet élément pourrait être repris.

FICHE D'ÉVALUATION	Code : VTC12	
N° et énoncé de la compétence	**12.. Assurer la veille technologique en cyberattaque**	**Durée :6h**

Nom de l'apprenant : Structure de formation : Date de l'évaluation : Signature du formateur :	Résultat	
	SUCCÈS	**ÉCHEC**
	☐	☐

ÉLÉMENTS D'OBSERVATION	**OUI**	**NON**	**RÉSULTATS**
1. Diffusion des alertes sur les nouvelles menaces 1.1. Diffusion correcte des alertes sur les nouvelles menaces			0 ou 05
2. Analyse des tendances et évolutions ; 2.1. Analyse pertinente des tendances et évolutions ;			0 ou 10
3. Collecte de la documentation 3.1. Collecte efficace de la documentation des informations			0 ou 05
4. Identification des vecteurs et failles exploités ; 4.1. Identification précise des vecteurs et failles exploités ;			0 ou 10
5. Évaluation de la criticité et de l'impact potentiel 5.1 Évaluation correcte de la criticité et de l'impact potentiel			0 ou 10
6. Exploitation des mises à jour 6.1 Exploitation efficace des mises à jour de l'analyse en fonction des retours			0 ou 05
7. Analyse des risques encourus ; 7.1. Analyse correcte des risques encourus ;			0 ou 10
8. Gestion des scénarios de test 8.1 Utilisation correcte des scénarios de tests ; 8.2 Exploitation Précise de la documentation des résultats			0 ou 05
9. Gestion des risques 9.1. Rapprochement correcte entre les objectifs de sécurité et le niveau de risque ; 9.2. Implémentation et pertinence correcte des solutions ;			0 ou 10

10. Exploitation du rapport coût/bénéfice et des contraintes 10.1 Exploitation correcte du rapport coût/bénéfice et des contraintes			0 ou 05
11. Adaptation du délai de mise en œuvre à la criticité. 11.1 Adaptation correcte du délai de mise en œuvre à la criticité.			0 ou 05
12. Exécution des tests 12.1 exécution correcte des tests ;			0 ou 05
13. Production d'une documentation des résultats 13.1 Production exacte d'une documentation des résultats ;			0 ou10
14. Respect des spécifications définies 14.1 Respect correct des spécifications définies.			0 ou 05
		TOTAL :	**/100**
Seuil de réussite : 70 %			
Règle de verdict : Le formateur devra s'assurer qu'en dehors de la maîtrise des opérations, l'apprenant adopte des attitudes respectant les règles de sécurité pour lesquelles il aura été évalué à la compétence 03.	**Oui** ☐	**Non** ☐	
Remarque :			

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

GUIDE PEDAGOGIQUE(GP)

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

PREMIERE PARTIE : STRATEGIES DE FORMATION

IV.1. PRÉSENTATION GENERALE DU GUIDE

1. Nature

L'objectif principal d'un guide pédagogique est d'appuyer les formateurs et l'équipe pédagogique responsables de la mise en œuvre de la formation dans chaque établissement. Le milieu, les types de formations offertes, le profil des apprenants, les caractéristiques du personnel enseignant, les ressources physiques et matérielles mises à disposition ainsi que la nature des partenariats accessibles font de chaque structure de formation un lieu unique. Dans un tel contexte, il ne saurait être question d'instaurer des modes d'intervention et des stratégies éducatives uniformes.

Au contraire, il faut laisser à chaque structure de formation toute la marge de manœuvre possible pour adapter le scénario de formation élaboré lors de la production du référentiel de formation tout en s'assurant du respect des rubriques prescrites, dont les standards de performance retenus pour les compétences. Le guide pédagogique doit donc allier latitude et souplesse en vue de la réalisation de la formation.

Le guide pédagogique présente dans un premier temps les principes pédagogiques recommandés pour soutenir la livraison de la formation en respect de l'Approche Par Compétences. Il présente aussi le projet pédagogique et les intentions qui soutiennent celui-ci. Il permet de renforcer les liens spécifiques entre le référentiel de formation et la traduction des intentions pédagogiques exprimées par l'équipe de production. Il définit deux outils pédagogiques (chronogramme suggéré et fiches de suggestions pédagogiques) destinés à aider le formateur, l'équipe pédagogique ainsi que les gestionnaires de la structure de formation à effectuer la planification et l'organisation de la formation. Dans un second temps, y sont présentées des fiches contenant des suggestions pédagogiques pour chacune des compétences identifiées dans le référentiel de formation. Ces fiches constituent l'essence du guide pédagogique.

2. Buts

Bien que le guide pédagogique soit un instrument facultatif, contrairement au référentiel de formation qui est prescriptif, sa mise à la disposition des formateurs et des équipes pédagogiques permet d'atteindre divers buts :

- Contribuer fortement à diffuser les valeurs de base qui devraient présider à la réalisation de la formation ;
- Consolider les diverses approches pédagogiques et les modalités de collaboration entre les équipes de formateurs et d'agents ou conseillers pédagogiques des structures de formation ;
- Proposer diverses approches susceptibles de mieux répondre aux besoins des apprenants en formation et de favoriser leur insertion et leur cheminement dans la vie active ;
- Prendre en compte, dans le projet éducatif, l'acquisition de compétences transversales qui relèvent du développement global de la personne et s'alignent avec les objectifs de la formation générale de base ;
- Proposer une démarche de planification pédagogique destinée à faciliter le travail initial du formateur.

IV.2. PRINCIPES PÉDAGOGIQUES

Lorsqu'une équipe de pédagogues aborde l'élaboration d'un guide pédagogique, elle doit généralement avoir en tête un modèle théorique pour mettre en évidence les valeurs qui sous-tendent ses actions et adopter un cadre de référence pour étayer son projet. En rappel, l'Approche Par Compétences (APC) place l'apprenant au centre de la démarche de formation et le reconnaît comme premier acteur responsable de ses apprentissages. Le modèle constructiviste et socioconstructiviste d'apprentissage s'inscrit bien dans cette perspective.

Selon cette approche, les nouveaux savoirs se développent progressivement, à la manière d'une véritable construction, c'est-à-dire en retenant les connaissances antérieures comme assises, et en établissant des réseaux de liens entre les diverses réalités avec lesquelles on entre en contact. Le socioconstructivisme, issu du constructivisme, ajoute la dimension des relations humaines, des interactions et des questionnements mutuels dans la construction des savoirs et le développement des compétences.

Ces principes découlent directement des bases conceptuelles, des valeurs et du cadre de référence qui ont présidé à la mise en place de l'APC. Ils constituent des lignes directrices devant être suivies dans le choix des stratégies d'enseignement et d'apprentissage pour permettre aux apprenants d'atteindre les buts du référentiel de formation.

Voici quelques principes généraux qui s'appliquent également dans le cadre du référentiel de formation du menuisier-ébéniste :

- Faire participer activement les apprenants et les rendre responsables de leurs apprentissages ;
- Tenir compte du rythme et de la façon d'apprendre de chacun ;
- Prendre en compte et réinvestir les acquis scolaires ou expérientiels des apprenants ;
- Considérer que la possibilité ou la capacité d'apprendre est fortement liée aux stratégies et aux moyens utilisés pour acquérir les compétences ;
- Favoriser le renforcement et l'intégration des apprentissages ;
- Privilégier des activités pratiques d'apprentissage et des projets adaptés à la réalité du marché du travail ;
- Communiquer avec les apprenants dans un langage correct et en utilisant les termes techniques appropriés ;
- Rechercher le plus possible la collaboration du milieu du travail ;
- Faire découvrir aux apprenants que la formation professionnelle constitue une voie importante d'intégration sociale et de développement personnel.

IV.3. PROJET DE FORMATION ET INTENTIONS PÉDAGOGIQUES

Le projet est structuré à partir des finalités, des orientations et des buts généraux de la formation professionnelle. Il s'inspire des valeurs et des principes pédagogiques qui ont présidé à l'élaboration du référentiel de formation. Chaque structure de formation est appelée à établir ou à actualiser son projet éducatif lors de l'implantation d'un référentiel de formation, et ce avant sa mise en œuvre.
L'élaboration d'un projet de formation implique également une prise en considération des spécificités de la formation offerte par la structure de formation, des caractéristiques des ressources

humaines mobilisées, des ressources physiques et matérielles disponibles, de la nature du partenariat avec le milieu du travail et du contexte général.

Le projet définit les intentions pédagogiques et les stratégies d'apprentissages à mettre en place pour l'ensemble de la formation professionnelle, plus spécifiquement pour chaque filière de formation offerte dans la structure de formation.
Les intentions pédagogiques sont des visées éducatives qui découlent du projet de formation et qui servent de guides pour les interventions auprès de l'apprenant. Elles touchent généralement des dimensions significatives du développement professionnel et personnel des apprenants qui n'ont pas fait l'objet de formulations explicites dans les buts du référentiel ou les compétences retenues. Elles incitent le personnel formateur à intervenir dans une direction donnée, chaque fois qu'une situation s'y prête.
Voici donc quelques intentions éducatives d'ordre général qui sont insérées dans le projet éducatif de la mise en œuvre du programme de formation de PENTESTER :

- Développer chez les apprenants, le sens des responsabilités et du respect de la personne ;
- Accroître, chez les apprenants, l'autonomie, l'initiative et l'esprit d'entreprise ;
- Développer chez les apprenants, la pratique de l'autoévaluation ;
- Développer chez les apprenants, une discipline personnelle et une méthode de travail ;
- Augmenter chez les apprenants, le souci de protéger l'environnement ;
- Développer chez les apprenants, la préoccupation du travail bien fait ;
- Développer chez les apprenants, le sens de l'économie du temps et des ressources ;
- Développer chez les apprenants, la préoccupation d'utiliser avec soin les différents équipements.

IV.4. PRÉSENTATION GÉNÉRALE DU RÉFÉRENTIEL DE FORMATION

Le scénario de formation se trouve au cœur du référentiel de formation. Il consiste à présenter les choix qui ont résulté de la définition des compétences issues du référentiel métier-compétences (elles même découlant de l'AST). Ces compétences sont traduites en actions observables et en résultats mesurables, éléments sur lesquels reposent l'acquisition par l'apprenant et leur évaluation. En plus de mettre en évidence la liste des compétences requises pour exercer un métier, le référentiel de formation les décrit de manière exhaustive et pose des balises qui déterminent une démarche d'acquisition desdites compétences. En conséquence, selon les modalités de réalisation de la compétence, le référentiel de formation mise sur deux techniques différentes pour décrire les compétences : la traduction en comportement et la traduction en situation.
En conséquence, le référentiel de formation pour le métier Pentester traduit les orientations particulières en matière de formation. Il prépare donc la personne à devenir un travailleur de la Cybersécurité selon les règles de sécurité et la réglementation.

Le référentiel de formation vise à rendre apte les lauréats de la cybersécurité à évaluer la sécurité d'un système d'information à travers différents angles d'attaques, mais toujours de manière cadrée. Les buts du référentiel traduisent les orientations particulières en matière de formation. Il prépare donc la personne à devenir un travailleur du secteur du numérique pouvant mener des activités de la cybersécurité seul, en équipe ou sous supervision, pour le compte d'une entreprise ou à son compte personnel.

De plus, le référentiel de formation vise à rendre apte le Pentester à réaliser la simulation 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 PENTESTER.
Dans l'exercice de son métier, le Pentester doit maîtriser l' Application des principes de la sécurité des comptes, d'Utilisation de l'architecture des systèmes informatiques des réseaux et des protocoles, de la Configuration des systèmes d'exploitation d'utilisation des langages de programmation, d' Identification des vulnérabilités potentielles dans les Systèmes informatiques, utilisation 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 ….
Étant donné que le Pentester travaille souvent seul, en équipe ou sous supervision, il doit démontrer de bonnes attitudes relationnelles en milieu de travail ou même dans la société.

IV.5. LISTE DES COMPÉTENCES

Le tableau suivant est conçu à partir de l'information contenue dans le référentiel de formation. Cette synthèse présente les compétences ordonnancées ainsi que les durées de formation qui s'y rapportent. Le tableau résume en fait la logique de formation présentée dans la matrice des objets de formation et dans le logigramme d'acquisition des compétences. Il prépare donc l'utilisateur du guide pédagogique à mieux comprendre la portée du programme de Pentester, tout en lui donnant déjà des pistes sur l'organisation du chronogramme de formation.

Synthèse du référentiel de formation

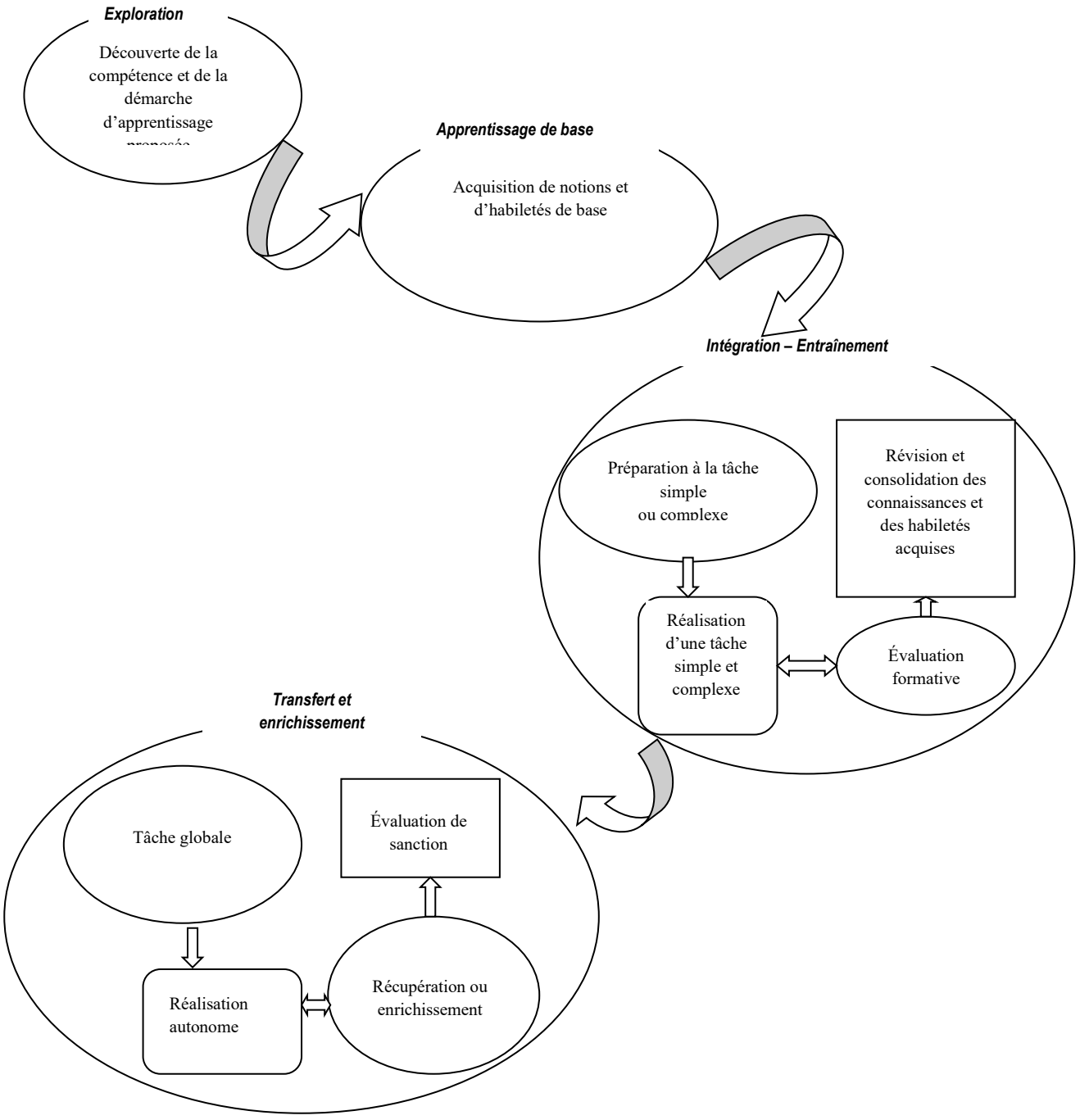
TABLEAU 2 : SYNTHÈSE DU PROGRAMME DE FORMATION

METIER : PENTESTER					**VOLUME HORAIRE : 1350 h**			
N°	**Énoncé de la compétence**	**Intitulé Module**	**Durée totale**	**Modalités**	**Stratégie d'évaluation**	**Durée de l'épreuve**	**Traduction**	**Types**
01	Se situer au regard du métier et de la formation	Métier et Formation	30	Orale	Ps Pt	2h	S	G
02	Communiquer en milieu professionnel	Communication en milieu professionnel	45	Écrite et orale	Ps Pt	3h	S	G
03	Appliquer le principe de la sécurité des comptes	Application du principe de la sécurité des comptes	60	Orale écrite, Pratique	Ps Pt	4h	C	G
04	Exploiter l'architecture des systèmes informatiques des réseaux et des protocoles	Exploitation de l'architecture des systèmes informatiques des réseaux et des protocoles	60	Écrite	Ps Pt	8h	C	G
05	Configurer les systèmes d'exploitation	Configuration des systèmes d'exploitation	60	Écrite	Ps Pt	4h	C	G
06	Utiliser les langages de programmation	Utilisation des langages de programmation	60	Pratique et écrite	Ps	4h	C	G
07	Identifier les vulnérabilités potentielles dans les Systèmes informatiques	Identification des vulnérabilités potentielles dans les Systèmes informatiques	90	Pratique Écrite	Ps Pt	6h	C	P
08	Configurer les outils de test de pénétration des systèmes d'exploitation	Configuration des outils de test de pénétration des systèmes d'exploitation	120	Pratique Écrite	Ps Pt	8h	C	P
09	Tester la vulnérabilité sur les Réseaux des applications, des site web et les systèmes d'exploitation	Tests de vulnérabilité sur les Réseaux des applications, site web et les systèmes d'exploitation	150	Pratique Écrite	Ps Pt	10h	C	P
10	Proposer les stratégies d'atténuation	Proposition des stratégies d'atténuation	120	Pratique Écrite	Ps Pt	8h	C	P

11	Configurer les pares-feux et des systèmes de détection d'intrusions	Configuration des pares-feux et des systèmes de détection d'intrusions	120	Pratique et écrite	Ps Pt	8h	C	P
12	Assurer la veille technologique en cyberattaque	Veille technologique en cyberattaque	90	Pratique et écrite	Ps Pt	6h	C	P
13	Rechercher un emploi	Entrepreneuriat	45	Pratique et écrite	Ps Pt	3h	S	G
14	S'intégrer en milieu professionnel	Intégration en milieu professionnel	315	Pratique	Ps Pt	21h	S	P
Total			**1 365**					

IV.6. STRATEGIES PEDAGOGIQUES

Selon le cas, le processus d'acquisition de compétences est illustré par les schémas ci-dessous.



IV.7. PRÉSENTATION DU CHRONOGRAMME

Le chronogramme de réalisation de la formation est une représentation schématique de l'ordre selon lequel les compétences devraient être acquises et de la répartition dans le temps des activités d'enseignement, d'apprentissage et d'évaluation. Il assure une planification globale de l'ensemble du référentiel de formation et permet de voir l'articulation qui existe entre les compétences. Ce type de planification vise à assurer une certaine cohérence et une progression des apprentissages.

Le chronogramme s'inspire du logigramme de la séquence d'acquisition des compétences présenté dans le référentiel de formation. À cette étape, il est réalisé dans le but de donner une idée globale du déroulement de la formation. Le chronogramme devient en quelque sorte une seconde version plus détaillée du logigramme.

Le chronogramme permet de décrire en détail le déroulement de la formation et de préciser les modalités selon lesquelles des thèmes autres que la formation reliée au métier (la formation générale par exemple) peuvent être intégrés à la formation. C'est à l'aide du chronogramme que les personnes travaillant à la planification pédagogique (responsables pédagogiques, formateurs de la spécialité, etc.) pourront tenir compte, pour une compétence donnée, des apprentissages déjà effectués, de ceux qui se déroulent en parallèle et de ceux à venir. La position retenue aura une incidence déterminante sur l'ensemble des choix pédagogiques ultérieurs.

Le chronogramme sert également à établir une base de répartition dans le temps des activités d'enseignement et d'apprentissage. Cette répartition implique la prise en considération de la nature et des contraintes associées à la réalisation des activités d'enseignement, d'apprentissage et d'évaluation. En conséquence, le chronogramme ici présenté repose sur une situation type et devra être ajusté en fonction de la situation réelle de chaque structure de formation, voire de chaque période de l'année, et en fonction des contraintes locales.

	Compétences particulières							Compétences générales							
Numéro	**7**	**8**	**9**	**10**	**11**	**12**	**14**	**1**	**2**	**3**	**4**	**5**	**6**	**13**	**T**
Durée (H)	**90**	**120**	**150**	**120**	**120**	**90**	**315**	**30**	**45**	**60**	**60**	**60**	**60**	**45**	**1365**
Semaine															
1								30							30
2									10	10	10	5			35
3									10	10	10	5			35
4									10	10	10	5			35
5										10	10	10	5		35
6										10	10	10	5		35
7										10	10	10	5		35
8	10	5										10	10		35
9	10	10										5	10		35
10	10	10	5										10		35
11	10	10	5										5		30
12	10	10	5										5		30
13	10	10	5										5		30
14	10	10	5												35
15	10	10	5												35
16	10	10	15												35
17		10	15	10											35
18		10	10	10	5										35
19		10		10	15										35
20		10	10	10	5										35
21			10	10	10	5									35

22			10	10	10	5									35
23			10	10	10	5									35
24			10	10	10	5									35
25			10	10		15									35
26			10	10		15									35
27			10	10		15									35
28				10		10								15	35
29							5							30	35
32							40								40
33							40								40
34							40								40
35							40								40
36							40								40
37							40								40
38							40								40
39							30								30
TOTAL	**90**	**120**	**150**	**120**	**120**	**90**	**315**	**30**	**45**	**60**	**60**	**60**	**60**	**45**	**1365**

DEUXIEME PARTIE : SUGGESTIONS PEDAGOGIQUES

IV.8. PRESENTATION DES FICHES DE SUGGESTION PEDAGOGIQUES

Les suggestions pédagogiques pour le métier de Pentester, présentées sous forme de fiches, reprennent l'énoncé de la compétence, lequel est accompagné d'informations complémentaires telles que le numéro de la compétence et la durée allouée pour son acquisition.
Les fiches de suggestions pédagogiques renseignent sur la position, le rôle et la démarche particulière de chaque compétence. Elles fournissent ensuite une liste des savoirs liés à chaque compétence ainsi que leurs balises, lesquelles renseignent sur l'étendue ou sur les limites des savoirs en cause. Enfin, elles contiennent des suggestions d'activités d'enseignement et d'apprentissage de façon à couvrir l'ensemble des savoirs liés à la compétence et des éléments qui s'y rapportent.

<table>
<tr><td colspan="3">COMPETENCE N°1 : Se situer au regard du métier et de la formation</td></tr>
<tr><td>NUMERO : 1</td><td colspan="2">DUREE D’APPRENTISSAGE : 30heures</td></tr>
<tr><td>MODULE ASSOCIE</td><td>Métier et formation</td><td></td></tr>
<tr><td colspan="3">FONCTION ET POSITION DE LA COMPETENCE</td></tr>
<tr><td colspan="3">Ce module est le tout premier par lequel l’apprenant amorcera sa formation en production d’aliments des animaux d’élevage. Il vise à informer sur les différents aspects de ce métier au regard du marché de l’emploi et sur la démarche de formation. L’obtention de ces informations permettra à l’apprenant de s’autoévaluer en comparaison de sa personnalité, de son désir, de ses aptitudes en vue de confirmer sa participation au programme de formation.</td></tr>
<tr><td colspan="3">DEMARCHE PARTICULIERE A LA COMPETENCE
Il est suggéré de répartir le temps d’apprentissage selon les proportions suivantes :
1. S’informer sur le métier : 40 %
2. S’informer sur le programme de formation et engagement de la démarche : 40 %
3. Evaluer et confirmer son engagement : 20 %
Il est suggéré de respecter l’ordre des éléments, tel que décrit dans le référentiel de formation.</td></tr>
<tr><td>Savoirs liés à la compétence</td><td>Balises</td><td>Activités d’enseignement et d’apprentissage</td></tr>
<tr><td colspan="3">1. S’informer sur le métier</td></tr>
<tr><td>1.1 Recueillir les données sur la nature et sur les exigences du métier</td><td>• Nature du métier
• Exigences du métier</td><td rowspan="3">Par des exposés, à l’aide de la documentation, de conférences, l’apprenant sera informé sur le métier.</td></tr>
<tr><td>1.2 Inventorier les habiletés, aptitudes, attitudes nécessaires pour pratiquer le métier</td><td>• Habiletés
• Aptitudes
• Attitudes</td></tr>
<tr><td>1.3 Identifier les particularités du milieu professionnel</td><td>• Éléments de compétence
• Conditions de réussite
• Critères de participation
• Conditions d’encadrement</td></tr>
<tr><td colspan="3">2. S’informer sur le programme de formation et engagement de la démarche</td></tr>
</table>

COMPETENCE N°1 : Se situer au regard du métier et de la formation		
NUMERO : 1	**DUREE D'APPRENTISSAGE :**	**30heures**
MODULE ASSOCIE	**Métier et formation**	
2.1 Collecter les informations sur le programme, la démarche de formation et d'évaluation	• Compétences • Tâches • Aptitudes • Connaissances • Habiletés • Démarche de formation • Stratégie d'évaluation	Par des exposés, à l'aide de la documentation, de conférences, l'apprenant sera informé de la pertinence du programme de formation, des conditions de réussite et du mode d'évaluation. Ils seront également motivés à entreprendre les activités proposées.
2.2 Apprécier la formation	• Points forts • Limites de la formation	
3- Evaluer et confirmer son engagement.		
3.1 Distinguer les aptitudes des champs d'intérêt.	• Différence entre ce que l'on aime et la possibilité que l'on a de le réaliser.	Le formateur à travers des exposés doit permettre aux apprenants d'avoir une vision juste du métier et de la formation Il doit fournir aux apprenants les moyens d'évaluer avec honnêteté et objectivité leur orientation professionnelle.
3.2 Décrire les raisons de son choix de poursuite de la formation.	• Autoévaluation. • Raisons motivant la décision.	
3.3 Décrire les principaux éléments d'un rapport confirmant un choix d'orientation professionnelle.	• Résumé de ses goûts, ses aptitudes et de ses champs d'intérêt. • Résumé des exigences relatives à l'exercice du métier • Parallèle entre les deux aspects qui précèdent • Brève conclusion sur son choix d'orientation.	

COMPETENCE 02 : Communiquer en milieu professionnel		
NUMERO : 02	**DUREE D'APPRENTISSAGE** : 45 h	
MODULE ASSOCIE	**Communication en milieu professionnel**	
FONCTION ET POSITION DE LA COMPETENCE		
La mise en œuvre de cette partie d'apprentissage vise à faire acquérir et à renforcer le potentiel nécessaire à tout acte de communication. Les contenus d'enseignement se définissent aussi bien en termes de connaissances transmises qu'en termes de supports et d'activités pédagogiques puisées dans les activités menées dans l'entreprise. Ils visent à constituer pour l'apprenant un capital de savoirs et de méthodes auxquels il puisse se référer.		
DEMARCHE PARTICULIERE A LA COMPETENCE		
La répartition du temps d'apprentissage est suggérée selon les proportions suivantes : 1.S'approprier les termes et expressions indispensables pour la communication en milieu de travail :15% 2.Traiter les informations : 20% 3. Produire les messages indispensables à la vie professionnelle et sociale : 25% 4. Communiquer oralement : 20% 5. Rendre compte de son activité : 20%. Il est suggéré de respecter l'ordre des éléments, tel que décrit dans le référentiel de formation.		
Savoirs liés à la compétence	**Balises**	**Activités d'enseignement et d'apprentissage**
1.S'approprier les termes et expressions indispensables pour la communication en milieu de travail		
1.1 Utiliser la langue française de manière appropriée	• Définition des termes • Grammaire • Vocabulaire • Formulation des phrases donnant lieu à une instruction, une description de procédés, une	Par des activités pratiques écrites et orales, le formateur permet à l'apprenant d'appliquer les consignes sur les règles de grammaire et de vocabulaire dans l'usage du français et de

COMPETENCE 02 : Communiquer en milieu professionnel		
	demande ou information, une suggestion, un conseil, ect.	l'anglais comme outils de communication en milieu professionnel.
1.2 To adequately make use of the english language	• Words meaning • Grammar • Vocabulary • Sentence formulation for instructions, process description, informations, application, advice, suggestions.	
2. Traiter les informations		
2.1 Elargir son vocabulaire technique	• Explication du sens des mots dans leurs contextes • Choix parmi plusieurs définitions • Usages des outils lexicaux courants	A partir d'une information orale, d'un texte ou d'une situation professionnelle donnée, l'enseignant développe la stratégie de lecture silencieuse de texte ou d'extraits, d'écoute de documents sonore, d'observation des documents audiovisuels, de commentaires des documents graphiques. Suivant cette approche, l'apprenant parvient à exploiter les informations, déterminer le sens et les idées essentielles d'un message, classer des principales manifestations thématiques.
2.2 Comprendre une situation de communication simple	• Schéma élémentaire de la communication • Différentes situations de communication • Repérage d'interlocuteurs, de message et de support de communication	
2.3 Saisir le sens global d'un texte lu	• Réponses à des questions précises sur le contenu du texte • Reformulation de tout ou d'une partie du texte	
2.4 Saisir le sens d'une information de source non écrite et en retenir le contenu	• Réponses à des questions précises de l'information • Reformulation des messages	
3.Produire les messages indispensables à la vie professionnelle et sociale		
3.1 Utiliser différents outils et supports de communication	• Exploitation des outils de communication • Utilisation du vocabulaire technique du métier	

COMPETENCE 02 : Communiquer en milieu professionnel		
	• Construction raisonnée de phrases de structure simple	L'enseignant donne un sens à l'apprentissage de la communication couplé avec l'apprentissage de la discipline professionnelle, dans la pratique quotidienne des activités de l'apprenant. Cela donne l'occasion aux apprenants d'agir en communiquant par écrit.
3.2 Restituer à l'écrit une information issue de la vie courante	• Formulation d'exemples ou d'arguments par écrit, pour justifier ou contredire une affirmation • Exploitation d'un message et production des informations écrites	
3.4 Exprimer une opinion ou une appréciation à l'écrit	• Formulation de message écrit, pour partager un avis ou un sentiment par rapport à une situation donnée	
4. Communiquer oralement		
4.1 Restituer à l'oral une information issue de la vie courante	• Allocution formulée d'exemples ou d'arguments, pour justifier ou contredire une affirmation	L'enseignant donne un sens à l'apprentissage de la communication couplé avec l'apprentissage de la discipline professionnelle, dans la pratique quotidienne des activités de l'apprenant. Cela donne l'occasion aux apprenants d'agir en communiquant oralement.
4.2 Exprimer une opinion ou une appréciation à l'oral	• Formulation de message oral, pour partager un avis ou un sentiment par rapport à une situation donnée	
5. **Rendre compte de son activité**		
5.1 Rendre compte par écrit ou oral des opérations effectuées	• Collecte des informations • Restitution des données • Difficultés rencontrées • Incidents de service, des dysfonctionnements • Solutions correctives • Justification du travail effectué.	A l'aide des activités pratiques, le formateur réitère les indications et consignes de prise de note et de rédaction du compte rendu. L'apprenant renforce ainsi sa compétence dans la communication avec ses coéquipiers, sa hiérarchie et le public.

COMPETENCE 02 : Communiquer en milieu professionnel		
5.2 Rédiger des rapports	• Utilisation du vocabulaire technique et des règles de grammaire • Documents techniques. • Règles techniques de rédaction ou de formulation	
COMPETENCE 03 : Appliquer le principe de la sécurité des comptes		
NUMERO : 03	**DUREE D'APPRENTISSAGE/D'EVALUATION : 56 heures/ 4 h**	
MODULE ASSOCIE	Application du principe de la sécurité des comptes	

FONCTION ET POSITION DE LA COMPETENCE

Cette compétence est réinvestie dans les différentes compétences particulières du programme de formation. Cela signifie que l'apprenant qui, à la fin de sa formation, intègre le marché du travail aura à mettre en application cette compétence dans toutes les tâches qu'il aura à accomplir sur le marché du travail. Cela se comprend étant donné que l'aspect santé et sécurité des comptes et au travail rentre dans toutes les tâches pratiques à accomplir.
Cette compétence de formation va, en permettant à l'apprenant de distinguer les risques inhérents au travail de technicien spécialisé Pentester, vise essentiellement l'acquisition d'une préoccupation constante pour l'application stricte des règles de santé et de sécurité des comptes, de l'hygiène et de l'environnement dans l'exercice des tâches.

DEMARCHE PARTICULIERE A LA COMPETENCE

Compte tenu de l'importance des apprentissages de cette compétence, il est recommandé d'en renforcer les compétences par l'entremise des autres compétences qui y sont associées. En conséquence, des temps d'apprentissage réguliers et appliqués à chaque compétence sont davantage préconisés au cours d'une session intensive de formation. En misant sur cette approche, l'apprenant parviendra plus efficacement à adopter le comportement préventif souhaité
Il est suggéré de répartir le temps d'apprentissage selon les proportions suivantes :

1. S'informer des lois et des règlements sur la santé et la sécurité au travail : 10%
2. Contrôler les identités : 10% ;
3. Contrôler les mots de passe : 15% ;
4. Contrôler les accès : 10% ;

COMPETENCE 02 : Communiquer en milieu professionnel		
5. Détecter les activités anormales : 13% ; 6. Élaborer la Journalisation et traçabilité : 15 % ; 7. Gérer les incidents : 20% Evaluation :07% Il est suggéré de respecter l'ordre des éléments, tel que décrit dans le référentiel de formation.		
Savoirs liés à la compétence	**Balises**	**Activités d'enseignement et d'apprentissage**
1. S'informer des lois et des règlements sur la santé et la sécurité au travail		
1.1 Identifier le corpus et le dispositif juridique 1.2 Repérer l'information dans les documents et les pictogrammes	• Documents juridiques • Lois • Ordonnances • Décrets • Arrêtés • Décisions • Revues scientifiques	Par des exposés, à l'aide de documentation, de conférences, l'apprenant sera informé du dispositif juridique relatif à la santé et à la sécurité liée à la cybersécurité. Le formateur motivera les apprenants à entreprendre les activités de recherche y afférentes.
2. Contrôler les identités		
2.1. Respecter les Techniques et règles de gestion des identités	• Généralités sur les Identités ; • Authentification et autorisation ; • La gouvernance des identités	Le formateur à travers des exposés doit permettre aux apprenants d'avoir une vision large sur les Techniques et règles de gestion des identités à l'exercice du métier de technicien Pentester etc. L'apprenant s'exercera à travers des activités de recherche et présente devant ses pairs le résultat de ses travaux.
2.2. Renouveler les mots de passe	• Renouvellement des mots de passe ; • Fréquence de renouvellement ; • Exigences de longueur.	

COMPETENCE 02 : Communiquer en milieu professionnel		
3**. Contrôler les mots de passe**		
3.1. Utiliser les mesures de sécurité des mots de passe	• Complexité des mots de passe • Longueur minimale des mots de passe ; • Politiques de renouvellement ; • Authentification à deux facteurs (2FA) ; • Notification de compromission des mots de passe	Par des exercices répétés, le formateur montrera aux apprenants comment utiliser des mesures de sécurité des mots de passe en respectant le délai de réinitialisation d'un mot de passe oublié ou compromis . L'apprenant s'exercera à travers des activités pratiques à utiliser les mesures de sécurité des mots de passe.
3.2. Respecter le délai de réinitialisation d'un mot de passe oublié/compromis	• Délai de réinitialisation ; • Politiques et procédures • Raisons de l'existence du délai ; • Sensibilisation des utilisateurs	
4.**Contrôler les accès**		
4.1. Identifier les accès	• Types d'accès ; • Identification des utilisateurs ; • Identification des dispositifs ; • Authentification unique (SSO); • Attributs d'identification • Gestion des sessions	Le formateur à travers des exposés permettra aux apprenants d'identifier **les accès** d'un système informatique L'apprenant développera des attitudes, aptitudes et présente la maîtrise de l'élément de compétence à travers des exercices pratiques.
4.2. Découvrir le nombre de violations	• Violations ; • Outils de détection ; • Violations internes et externes • Risques	

COMPETENCE 02 : Communiquer en milieu professionnel		
	• Rapports d'incidents	
4.**Détecter les activités anormales**		
5.1 Respecter le temps moyen de détection des incidents	• Activités anormales ; • Indicateurs d'activité anormale ; • Détection des anomalies internes **;** • Détection des menaces externes	Après avoir fait des démonstrations de détection des activités anormales par le respect du temps moyen de détection des incidents, l'analyse du trafic réseau et la génération efficace des alertes r, le formateur s'assurera que les apprenants, par le biais d'exercices répétés, maîtrisent l'exécution de ces opérations
5.2. Analyser le trafic réseau	• Trafic réseau ; • Protocoles réseau ; • Méthodes d'analyse : • Détection d'anomalies, • Patterns • Corrélation des événements Etc	
5.3. Générer les alertes	• Alertes ; • Critères de déclenchement ; • Niveaux de priorité, • Format des alertes Etc	
6.Élaborer la Journalisation et traçabilité		
6.1. Gérer le temps moyen d'agrégation	• Mesure et d'Analyse du MTTA • Facteurs Influents sur le MTTA • Amélioration Continue du MTTA	Le formateur à travers des exposés permettra aux apprenants d'élaborer la Journalisation et la traçabilité des logs à travers la gestion
6.2 Vérifier les logs	• Définition des logs ; • Types de logs ; • Sources de logs ; • Contenu des logs ;	

COMPETENCE 02 : Communiquer en milieu professionnel		
	• Format des logs ; • Analyse des logs ; • Détection des anomalies	du temps moyen d'agrégation, la vérification des logs et le contrôle de la traçabilité L'apprenant développera des attitudes, aptitudes et présente la maîtrise de l'élément de compétence à travers des exercices pratiques.
6.3 Contrôler la traçabilité	• Traçabilité ; • Objectifs du contrôle de la traçabilité ; • Sources de traçabilité ; • Contenu de la traçabilité ; • Normes et exigences ; • Politiques de traçabilité ; • Technologies de traçabilité	
7.Gérer les incidents		
7.1. Détecter et résoudre les compromissions	• Définition du temps moyen de détection (MTTD); • Définition du temps moyen de résolution (MTTR); • Importance du MTTD et du MTTR; • Facteurs influençant le MTTD et le MTTR • Méthodes de réduction du MTTD. • Post-incident	Par des exposés, à l'aide de documentation, de conférences, l'apprenant sera informé sur le temps moyen de détection et de résolution des compromissions, sur l'Identification des taux de réussite d'activités testées etc. Motiver les apprenants à entreprendre les activités de recherche y afférentes, Études de cas et analyses de cas pratiques, travaux de

COMPETENCE 02 : Communiquer en milieu professionnel		
7.2. Identifier les taux de réussite d'activités testées	• Taux de réussite ; • Types d'activités testées ; • Indicateurs de réussite ; • Amélioration continue. • Méthodes d'évaluation	groupe et discussions en classe, simulations d'audits et de processus de certification
7.3 Evaluer la maturité par des audits et la certification	• Évaluation de la Maturité • Audit de Maturité • Normes et Référentiels pour l'Audit et la Certification • Préparation à la Certification • Bonnes Pratiques	

COMPETENCE 04 Exploiter l'architecture des systèmes informatiques des réseaux et des protocoles		
NUMERO : 04	**DUREE D'APPRENTISSAGE/D'EVALUATION**	**56/04h**
MODULE	**Exploitation de l'architecture des systèmes informatiques des réseaux et des protocoles**	
FONCTION ET POSITION DE LA COMPETENCE Cette compétence générale permet à l'apprenant d'**Exploiter l'architecture des systèmes informatiques des réseaux et des protocoles.** Elle est acquise un peu après le début du programme de formation, pour permettre aux apprenants d'acquérir des notions sur l'identification des composants des systèmes informatiques, l'utilisation de l'architecture système et applicative et l'utilisation des réseaux.		
DEMARCHE PARTICULIERE A LA COMPETENCE. Etant donné que la maîtrise de cette compétence a un rôle important dans la maitrise du programme, Il est suggéré de répartir le temps d'apprentissage selon les proportions suivantes : 1.Identifier les composants des systèmes informatiques 23% 2. Utiliser l'architecture système et applicative : 35% 3. Utiliser les réseaux : 35% Evaluation :07%		
Savoirs liés à la compétence	**Balises**	**Activités d'enseignement et d'apprentissage**
1.Identifier les composants des systèmes informatiques		
1.1 Interpréter les traitements applicatifs	• Traitements applicatifs ; • Flux de données ; • Fonctionnalités ; • Dépendances • Modélisation des processus	Après avoir fait des démonstrations sur l'identification des composants des systèmes, par l'interprétation des

<table>
<tr><td colspan="3">COMPETENCE 04 Exploiter l’architecture des systèmes informatiques des réseaux et des protocoles</td></tr>
<tr><td>NUMERO : 04</td><td>DUREE D’APPRENTISSAGE/D’EVALUATION</td><td>56/04h</td></tr>
<tr><td>MODULE</td><td colspan="2">Exploitation de l’architecture des systèmes informatiques des réseaux et des protocoles</td></tr>
<tr><td></td><td>• Documentation des traitements</td><td rowspan="3">traitements applicatifs, l’Optimisation des ressources systèmes, le Choix des logiciels, d’un système informatique, le formateur s’assurera que les apprenants, par le biais d’exercices répétés, maîtrisent l’exécution de ces opérations.</td></tr>
<tr><td>1.2. Optimiser les ressources systèmes</td><td>• Ressources systèmes ;
• Goulets d'étranglement ;
• Optimisation du CPU ;
• Optimisation de la mémoire
• Virtualisation et conteneurisation
• Automatisation des opérations :</td></tr>
<tr><td>1.3. Choisir les logiciels</td><td>• Besoins ;
• Fonctionnalités ;
• Évaluation des options ;
• Compatibilité et intégration ;
• Personnalisation et extensibilité
• Évolutivité et croissance ;
• Fournisseurs</td></tr>
<tr><td colspan="3">2. Utiliser l’architecture système et applicative</td></tr>
</table>

COMPETENCE 04 Exploiter l'architecture des systèmes informatiques des réseaux et des protocoles		
NUMERO : 04	**DUREE D'APPRENTISSAGE/D'EVALUATION**	**56/04h**
MODULE	**Exploitation de l'architecture des systèmes informatiques des réseaux et des protocoles**	
2.1 Manipuler l'architecture système et applicative	• Concepts d'architecture ; • Besoins métier ; • Principes architecturaux ; • Planification stratégique ; • Conception de l'architecture ; • Gestion des changements ;	Par un exposé, le formateur doit présenter aux apprenants les techniques d'utilisation de l'architecture système et applicative en mettant un accent sur la manipulation de l'architecture système et applicative, sur le Suivi de l'architecture système et applicative et sur l'Isolation/Sécurisation correcte des applications tout en leur expliquant comment fonctionne un système informatique Le formateur encadre les activités des apprenants afin d'assurer l'intégration des apprentissages.
2.2. Suivre l'architecture système et applicative	• Indicateurs de performance • Collecte de données ; • Rapports et tableaux de bord • Réponse aux incidents ; • Optimisation des performances ; • Formation et sensibilisation	
2.3 Isoler/Sécuriser les applications	• Principes de sécurité ; • Isolation des environnements ; • Chiffrement des données ; • Protection contre les attaques ; • Sécurité du code	
3. **Utiliser les réseaux**		
3.1. Contrôler les latences des communications	• Types de latences ;	

<table>
<tr><td colspan="3">COMPETENCE 04 Exploiter l’architecture des systèmes informatiques des réseaux et des protocoles</td></tr>
<tr><td>NUMERO : 04</td><td>DUREE D’APPRENTISSAGE/D’EVALUATION</td><td>56/04h</td></tr>
<tr><td>MODULE</td><td colspan="2">Exploitation de l’architecture des systèmes informatiques des réseaux et des protocoles</td></tr>
<tr><td></td><td>• Mesure de latence ;
• Causes de latence ;
• Optimisation de latence ;
• Priorisation du trafic
• Gestion des incidents.</td><td rowspan="3">Par des exposés, à l’aide de documentation, de conférences, de visite d’entreprise, ou de recherches personnelles, l’apprenant sera informé sur l’utilisation des réseaux et particulièrement sur le Contrôle des latences des communications, sur le Contrôle de la fiabilité des transmissions et sur la Sécurité et confidentialité des échanges
Seul ou en groupe, l’apprenant effectuera des recherches et présentera devant ses pairs le résultat de ses travaux.</td></tr>
<tr><td>3.2 Contrôler la fiabilité des transmissions</td><td>• Mécanismes de contrôle de la fiabilité ;
• Gestion des erreurs ;
• Protocoles de transport fiables ;
• Contrôle de flux ;
• Pertes de paquets ;</td></tr>
<tr><td>3.3.. Vérification de la Sécurité et de la confidentialité des échanges</td><td>• Enjeux de sécurité
• Cryptographie
• Protocoles sécurisés
• Identités et accès
• Protection contre les attaques
• Certificats
• Sécurisation des réseaux sans fil</td></tr>
<tr><td colspan="3">4. Appliquer les protocoles de communication</td></tr>
</table>

<table>
<tr><td colspan="3">COMPETENCE 04 Exploiter l’architecture des systèmes informatiques des réseaux et des protocoles</td></tr>
<tr><td>NUMERO : 04</td><td>DUREE D’APPRENTISSAGE/D’EVALUATION</td><td>56/04h</td></tr>
<tr><td>MODULE</td><td colspan="2">Exploitation de l’architecture des systèmes informatiques des réseaux et des protocoles</td></tr>
<tr><td>4.1. Choisir les types de protocole</td><td>• Modèles de communication et leurs protocoles
• Types de protocoles
• Protocoles haut niveau
• Choix des protocoles</td><td rowspan="3">Par l'entremise d’exposés et/ou d'études de cas, le formateur présente aux apprenants les techniques d’application des protocoles de communication en s’appuyant le choix des types de protocole, sur le contrôle de la charge réseau et sur la. Robustesse et résistance aux aléas
L’apprenant, par le biais d’exercices, développe sa capacité de recherche et d’exploitation d’informations pertinentes sur un système d’information étudié, et présenté expose le résultat de ses travaux d’apprentissage.
Le formateur encadre les activités des apprenants afin d'assurer l'intégration des apprentissages</td></tr>
<tr><td>4.2. Contrôler la charge réseau</td><td>• Charge actuelle ;
• Prévision de la charge future ;
• Équilibrage de charge
• Trafic de pointe.</td></tr>
<tr><td>4.3. Vérifier la Robustesse et la résistance aux aléas</td><td>• Robustesse et résilience ;
• Points de défaillance ;
• Conception de la redondance ;
• Tolérance aux pannes
• Test de résilience ;
• Sécurisation des communications
• Sauvegarde et récupération
• Gestion des incidents</td></tr>
</table>

COMPETENCE 05 : Configurer les systèmes d'exploitation		
NUMERO : 5	**DUREE D'APPRENTISSAGE/D'EVALUATION** : 56 **heures/04heures**	
MODULE	**Configuration des systèmes d'exploitation**	
FONCTION ET POSITION DE LA COMPETENCE Cette compétence générale permet à l'apprenant d'acquérir les habilités nécessaires pour **Configurer les systèmes d'exploitation d'un système Informatique**. Elle vise aussi à doter l'apprenant de savoirs et savoir-faire lui permettant de comprendre le fonctionnement de l'administration système, la gestion des utilisateurs et les droits, la gestion de la sécurité des systèmes d'exploitation, et la gestion de la sécurité des OS, toutes choses préalables à la pratique du métier Technicien Spécialisé Pentester. Elle est acquise à mi-parcours du programme de formation, pour permettre aux apprenants d'acquérir des notions devant être utilisées lors de l'acquisition des compétences particulières. Les connaissances et habiletés acquises dans ce module seront réinvesties et mises à contribution à divers degrés lors de la réalisation des activités d'apprentissage des modules relatifs à :« Utilisation de l'architecture des systèmes informatiques des réseaux et des protocoles **», et «** Utilisation des langages de programmation »**,**		
DEMARCHE PARTICULIERE A LA COMPETENCE. Etant donné que la maîtrise de cette compétence générale joue un rôle important dans la maîtrise du programme, Il est suggéré de répartir le temps d'apprentissage selon les proportions suivantes : 1. Effectuer l'administration système :22% 2. Organiser les utilisateurs et les droits :21% 3. Appliquer la sécurité des systèmes d'exploitation :25% ; 4. Contrôler la sécurité OS : 25% Evaluation : 7%		
Savoirs liés à la compétence	**Balises**	**Activités d'enseignement et d'apprentissage**

COMPETENCE 05 : Configurer les systèmes d'exploitation		
NUMERO : 5	**DUREE D'APPRENTISSAGE/D'EVALUATION** : 56 **heures/04heures**	
MODULE	**Configuration des systèmes d'exploitation**	
1. Effectuer l'administration système		
1.1. Organiser l'administration système	• Définition des processus ; • Élaboration de politiques ; • Planification des ressources • Documentation ; • Collaboration interfonctionnelle ; • Surveillance et évaluation ; • Amélioration continue	En administration système, Le formateur devra développer chez ses apprenants des compétences essentielles telles que la planification des tâches, la gestion des utilisateurs et des groupes, la sécurisation du système, la sauvegarde des données, la gestion des mises à jour et des correctifs, ainsi que la surveillance et le diagnostic du système. Il insistera également sur l'importance des rapports complets pour assurer la traçabilité des activités au sein d'une organisation. L'apprenant devra s'engager activement à mettre en pratique les compétences acquises, respecter les procédures établies, documenter son travail et collaborer avec son équipe pour atteindre les objectifs fixés par le formateur. Le formateur encadre les activités des apprenants afin d'assurer l'intégration des apprentissages.
1.2. Respecter les procédures d'administration système	• Formation et sensibilisation ; • Application cohérente ; • Gestion des changements ; • Suivi des performances ; • Rétroaction et amélioration continue ; • Conformité réglementaire	

COMPETENCE 05 : Configurer les systèmes d'exploitation		
NUMERO : 5	**DUREE D'APPRENTISSAGE/D'EVALUATION** : 56 **heures/04heures**	
MODULE	**Configuration des systèmes d'exploitation**	
2.Organiser les utilisateurs et leurs droits		
2.1. Gérer l'intégrité des comptes utilisateurs	• Politiques de mot de passe robustes ; • Activités des comptes ; • Comptes et privilèges ; • Authentification multi-facteurs.	Par l'entremise d'exposés et/ou d'études de cas, le formateur présente aux apprenants les techniques permettant de Gérer les utilisateurs et leurs droits. L'apprenant, par le biais de recherche et de question posées développe sa capacité à gérer l'intégrité des comptes utilisateurs et d'assurer la traçabilité des actions sur les comptes devant ses pairs, présenter les résultats de ses travaux. Le formateur encadre les activités des apprenants afin d'assurer l'intégration des apprentissages.
2.2. Assurer la traçabilité des actions sur les comptes	• Journaux d'activité ; • Intégration des journaux : • Surveillance des connexions ; • Autorisations ;	
3**.Gérer la sécurité des systèmes d'exploitation**		
3.1. Identifier les taux de correction des vulnérabilités	• Vulnérabilités ; • Correctifs ; • Planification des mises à jour ; • Sensibilisation ;	le formateur prépare les apprenants à être proactifs dans la gestion de la sécurité des systèmes d'exploitation, en les dotant des compétences nécessaires pour identifier et remédier aux vulnérabilités avant qu'elles ne soient exploitées, tout en étant capables de détecter rapidement les compromissions et de prendre des mesures correctives appropriées pour protéger les systèmes et les données.
3.2. Détecter les compromissions	• Activités réseau ; • Journaux de sécurité ; • Outils de détection d'intrusion ; • Incidents de sécurité.	

COMPETENCE 05 : Configurer les systèmes d'exploitation		
NUMERO : 5	**DUREE D'APPRENTISSAGE/D'EVALUATION** : 56 **heures/04heures**	
MODULE	**Configuration des systèmes d'exploitation**	
		L'apprenant doit développer des compétences pratiques pour identifier les vulnérabilités, appliquer les correctifs et détecter les compromissions. Il doit surveiller activement les mises à jour de sécurité, développer un sens de la détection des anomalies et agir de manière proactive pour réduire les risques et protéger les systèmes. Le formateur encadre les activités des apprenants afin d'assurer l'intégration des apprentissages.
4. Gérer la sécurité OS (opérating system) :		
4.1. Décrire les mécanismes de défense dans la sécurité des OS	• Contrôle d'accès ; • Gestion des droits ; • Surveillance des activités ; • Logiciels malveillants ; • Mises à jour et correctifs Etc.	Le formateur prépare les apprenants à être proactifs dans la gestion de la sécurité des OS, en leur fournissant les connaissances et les compétences nécessaires pour détecter, analyser et répondre efficacement aux menaces et aux incidents de sécurité. L'apprenant doit acquérir des connaissances approfondies et développer des compétences pratiques en matière de sécurité des systèmes d'exploitation, notamment en comprenant les mécanismes de défense, en détectant les menaces avancées, en identifiant et
4.2. Détecter les menaces avancées	• Menaces avancées ; • Vulnérabilités OS ; • Logiciels malveillants OS • Réponses aux incidents OS ; • Veille technologique.	

COMPETENCE 05 : Configurer les systèmes d'exploitation		
NUMERO : 5	**DUREE D'APPRENTISSAGE/D'EVALUATION** : 56 **heures/04heures**	
MODULE	**Configuration des systèmes d'exploitation**	
4.3. Identifier et analyser les événements de sécurité	• Sources de sécurité ; • Evénements de sécurité ; • Normalisation et nettoyage des données ; • Indicateurs de compromission • Rapport d'incidents.	analysant les événements de sécurité, ainsi qu'en détectant et répondant aux incidents à courte durée. Il doit exercer la vigilance, la réactivité, la collaboration et la communication, tout en restant continuellement informé des nouvelles menaces et des meilleures pratiques de sécurité. détecte et analyse les menaces et produit un rapport d'incident devant ses pairs Le formateur encadre les activités des apprenants afin d'assurer l'intégration des apprentissages.
4.4. Détecter l'incident à courte durée	• Incidents à courte durée ; • Signaux d'alertes ; • Outils de détection ; • Surveillance en temps réel : • Incidents rapides ; • Formation pratique.	
5.**Gérer les périphériques**		
5.1. Échanger les données avec les périphériques	• Types de périphériques ; • Configuration et installation ; • Gestion des pilotes ; • Surveillance et maintenance ; • Files d'attente d'impression • Sécurité des périphériques • Intégration avec le réseau ;	Par l'entremise d'exposés et/ou d'études de cas, le formateur présente aux apprenants les différentes stratégies de gestion des périphériques, permettant d'effectuer les échanges des données avec les périphériques, la vérification de l'intégrité des données échangées. etc.

COMPETENCE 05 : Configurer les systèmes d'exploitation		
NUMERO : 5	**DUREE D'APPRENTISSAGE/D'EVALUATION** : 56 **heures/04heures**	
MODULE	**Configuration des systèmes d'exploitation**	
	• Gestion des Mises à jour ; • Dépannage et résolution des problèmes.	L'apprenant, par le biais d'exercices développe sa capacité de mieux gérer les périphériques. Le formateur encadre les activités des apprenants afin d'assurer l'intégration des apprentissages. .
5.2. Vérifier l'Intégrité des données échangées	• Méthodes de vérification ; • Hachage ; • Redondance cyclique (CRC) ; • Codes de vérification d'erreur (ECC) ; • Gestion des erreurs	
5.3. Suivre les actions sur les périphériques	• Actions sur les périphériques ; • Types d'actions à suivre ; • Collecte des données ; • Paramètres à suivre • Notification des événements • Audit et conformité	

COMPETENCE 06 : Utiliser les langages de programmation	
NUMERO : 6	**DUREE D'APPRENTISSAGE/D'EVALUATION** : 56 **heures/04 heures**
MODULE	**Utilisation des langages de programmation**

FONCTION ET POSITION DE LA COMPETENCE

Cette compétence générale, permet à l'apprenant d'acquérir les habilités nécessaires à l'utilisation des langages de programmation. Par cette compétence, l'apprenant sera amené à utiliser le langage de programmation généralistes, à acquérir des notions en Développement web et applicatif, des notions d'algorithmique et structures de données, à l'utilisation de la programmation système et à la Sécurisation du code source.

La compétence en Utilisation des langages de programmation vise à rendre les apprenants capables de :

1. Identifier le langage de programmation généralistes : 15%
2. Acquérir les notions en Développement web et applicatif ; 23%
3. Acquérir les notions d'algorithmie et structures de données ;22%
4. Utiliser la programmation système 17%
5. Sécuriser le code source17%

Évaluation : 7%

Les connaissances et habiletés acquises dans ce module seront réinvesties et mises à contribution à divers degrés lors de la réalisation des activités d'apprentissage des modules relatifs à l'«Identification des vulnérabilités potentielles dans les Systèmes informatiques », à la «Réalisation des tests de vulnérabilité, sur des Réseaux, des applications, site web et les systèmes d'exploitation», à la «Configuration des outils de test de pénétration des systèmes d'exploitation », à la «Proposition des stratégies d'atténuation », à la «Configuration des pares-feux et des systèmes de détection d'intrusions », à la « veille technologique en cyberattaque et à «l'Intégration en milieu de travail».

Cette compétence s'acquiert avant d'entamer la mi-parcours de la formation.

DEMARCHE PARTICULIERE A LA COMPETENCE

Etant donné que la maîtrise de cette compétence a une incidence directe sur le développement de la capacité d'assurer une maintenance de qualité des véhicules automobiles, il est recommandé de s'appesantir sur les éléments énumérés ci-dessous.

COMPETENCE 06 : Utiliser les langages de programmation		
NUMERO : 6	**DUREE D'APPRENTISSAGE/D'EVALUATION** : 56 **heures/04 heures**	
MODULE	**Utilisation des langages de programmation**	
En ce qui concerne le temps alloué à l'apprentissage, il est suggéré de le répartir selon les proportions suivantes : • Identifier le langage de programmation généralistes :17% • Acquérir les notions en Développement web et applicatif :20% • Acquérir les notions d'algorithmie et structures de données :15h • Utiliser la programmation système :23% • Sécuriser le code source :18 % Evaluation : 7% Par ailleurs, ce qui a trait au déroulement des séquences d'apprentissage, bien qu'il soit suggéré de retenir l'ordre proposé dans le référentiel de formation pour le cinquième élément de compétence, les situations de mise en œuvre associées à chaque élément n'ont pas à être réalisées selon l'ordre exact présenté et de façon linéaire. Au contraire, le formateur doit considérer le déroulement qui lui semble le plus susceptible d'amener l'apprenant à développer les habiletés et attitudes visées.		
Savoirs liés à la compétence	Balises	**Activités d'enseignement et d'apprentissage**
1 **Identifier le langage de programmation généralistes**		
○ 1.1. Identifier les caractéristiques et spécificités	• Concepts de base ; • Syntaxe du langage ; • Design Pattern ; • Gestion de la mémoire ; • Erreurs et exceptions ; • Frameworks ;	Le formateur présente les objectifs de la séquence. Il présente des notions de programmation orientée objet, gestion de la mémoire et des ressources. Il fait constituer des groupes de travail, donne des consignes de travail portant sur la gestion de la mémoire et des ressources en programmation.

COMPETENCE 06 : Utiliser les langages de programmation		
NUMERO : 6	**DUREE D'APPRENTISSAGE/D'EVALUATION** : 56 **heures/04 heures**	
MODULE	**Utilisation des langages de programmation**	
1.2 Comparer les langages.	• Syntaxe et structure ; • Gestion de la mémoire et des ressources ; • Performance ; • Compatibilité et portabilité ; • Scénarios d'utilisation ; • Tendances et évolutions etc.	L'apprenant écoute, pose des questions, exécute les consignes, prend des notes, échange avec d'autres apprenants, présente la production du groupe, participe à la mise en commun en plénière, participe aux synthèses, note la synthèse.
1.3. Acquérir les nouveaux langages	• Besoins et objectifs ; • Recherche et sélection du langage approprié ;	
2. Acquérir les notions en Développement web et applicatif		
2.1. Identifier les types de langage	• Front-end • Back-end • Base de données ; • Script et de balisage ; • Développement d'applications mobiles, etc.	Le formateur présente les concepts des langages côté client (frontend), côté serveur (backend), de base de données, de script et de balisage, ainsi que des langages de développement d'applications mobiles. Il organise des démonstrations sur des systèmes réels ou simulés, fournit des exemples et de la documentation, et encourage les recherches individuelles. En formant des groupes de travail, il coordonne les travaux pratiques et les activités de groupe, organise les présentations des productions de groupes, et apporte des
2.2. Elaborer le développement défensif	• Principes de sécurité des applications ;	

COMPETENCE 06 : Utiliser les langages de programmation		
NUMERO : 6	**DUREE D'APPRENTISSAGE/D'EVALUATION** : 56 **heures/04 heures**	
MODULE	**Utilisation des langages de programmation**	
	• Bonnes pratiques de codage sécurisé ; • Autorisations et des privilèges ; • Attaques et menaces courantes ;	informations complémentaires. De plus, il supervise le processus de développement des correctifs suite à l'identification des vulnérabilités, ainsi que l'analyse des risques associés à chaque vulnérabilité identifiée. L'apprenant écoute, pose des questions, exécute les consignes, prend des notes, échange avec d'autres apprenants, présente la production du groupe, participe à la mise en commun en plénière, participe aux synthèses, note la synthèse.
2.3. Gérer les vulnérabilités	• Vulnérabilités potentielles dans les applications web • Risques associés à chaque vulnérabilité identifiée • Développement de correctifs	
2.4. Décrire la Cryptographie	• Fondements de la cryptographie ; • Types de chiffrement ; • Fonctionnement des algorithmes de hachage ; • Génération et gestion des clés ; • Cryptographie dans le développement web et applicatif ;	

COMPETENCE 06 : Utiliser les langages de programmation		
NUMERO : 6	**DUREE D'APPRENTISSAGE/D'EVALUATION** : 56 **heures/04 heures**	
MODULE	**Utilisation des langages de programmation**	
2.5. Utiliser les identités	• Identités utilisateur dans les applications web et applicatives ; • Autorisation des utilisateurs ; • Profils utilisateur dans les applications web et applicatives ;	
3. Acquérir les notions d'algorithmie et structures de données		
3.1. Implémenter les algorithmes courants	• Algorithmes ; • Choix et conception d'algorithmes appropriés ; • Algorithmes dans un langage de programmation spécifique • Optimisation des algorithmes, Etc.	Le formateur effectue des exercices pratiques réguliers pour renforcer les compétences acquises dans le nouveau langage de programmation, en résolvant des problèmes algorithmiques ou en participant à des compétitions de programmation. L'apprenant écoute, pose des questions, exécute les consignes, prend des notes, échange avec d'autres apprenants, présente la production du groupe, participe à la mise en commun en plénière, participe aux synthèses, note la synthèse.
3.2. Analyser et optimiser l'algorithmes	• Analyse d'algorithmes ; • Notions de complexité ; • Analyse asymptotique ; • Types de problèmes ; • Méthodes d'optimisation ;	

COMPETENCE 06 : Utiliser les langages de programmation		
NUMERO : 6	**DUREE D'APPRENTISSAGE/D'EVALUATION** : 56 **heures/04 heures**	
MODULE	**Utilisation des langages de programmation**	
	• Analyse empirique ; • Cas d'utilisation ; • Évolution des algorithmes ; • Évaluation et comparaison ;	
4. Utiliser la programmation système		
4.1. Utiliser la mémoire et threads	• Gestion de la mémoire ; • Utilisation des threads ; • Mémoire et threads ; • Problèmes liés à la mémoire et aux threads ;	Le formateur, ayant présenté les notions sur l'utilisation de la programmation système, s'assurera que les apprenants maîtrisent les compétences essentielles, notamment la gestion de la mémoire, l'utilisation des threads, l'optimisation de leur utilisation, la détection et la résolution des problèmes associés. Il veillera également à ce qu'ils comprennent les concepts de bas niveau tels que la gestion de la mémoire et les pointeurs, ainsi que la syntaxe et les structures de base, notamment dans le contexte de la programmation en C. En outre, le formateur garantira la compréhension des principes des systèmes embarqués et temps réel, de leur architecture et des langages de programmation couramment utilisés, ainsi que des techniques de débogage et de test adaptées à cet environnement.
4.2. Utiliser les Langages de bas niveau	• Concepts de bas niveau. • Syntaxe et structures de base ; • Concepts de base de la programmation système ;	
4.3. Utiliser le Développement embarqué/temps réel	• Systèmes embarqués et temps réel ; • Architecture des systèmes embarqués ; • Langages de programmation • Systèmes d'exploitation embarqués ;	

COMPETENCE 06 : Utiliser les langages de programmation		
NUMERO : 6	**DUREE D'APPRENTISSAGE/D'EVALUATION** : 56 **heures/04 heures**	
MODULE	**Utilisation des langages de programmation**	
	• Programmation ; • Débogage et tests	
5. Sécuriser le code source		
5.1. Exécuter les tests de vulnérabilités	• Tests de vulnérabilités ; • Outils de test de vulnérabilités • Planification des tests ; • Exécution des tests et analyse des résultats ; • Rapports et documentation	Le formateur présente les notions sur l'utilisation des langages de programmation. Il constitue des groupes de travail, donne des consignes sur la planification et l'exécution des tests de vulnérabilités, analyse les résultats, et production des rapports détaillés. il transmet aux apprenants les concepts de base de la cryptographie, aide à choix des algorithmes appropriés, et sécurisation des données et des logiciels. L'apprenant écoute, pose des questions, exécute les consignes, prend des notes, échange avec d'autres apprenants, présente la production du groupe, participe à la mise en commun en plénière, participe aux synthèses, note la synthèse.
5.2. Attribuer les droits et permissions	• Droits d'accès aux utilisateurs et aux groupes ; • Restriction des privilèges des utilisateurs • Contrôle d'accès aux ressources sensibles	
5.3. Utiliser le développement défensif	• Principes de développement défensif ; • Entrées utilisateur ; • Bibliothèques sécurisées ;	

COMPETENCE 06 : Utiliser les langages de programmation		
NUMERO : 6	**DUREE D'APPRENTISSAGE/D'EVALUATION** : 56 **heures/04 heures**	
MODULE	**Utilisation des langages de programmation**	
	• Cryptographie et gestion des identités ; • Tests de sécurité et analyse statique du code	
5.4. Gérer les vulnérabilités	• Vulnérabilités potentielles dans le code source • Risques • Tests de sécurité ; • Développement de correctifs ;	
5.5. Utiliser la Cryptographie	• Concepts de base ; • Choix des algorithmes de cryptographie appropriés • Chiffrement des données sensibles ; • Signature numérique ;	

<table>
<tr><td colspan="3">COMPETENCE 07 : Identifier les vulnérabilités potentielles dans les Systèmes informatiques</td></tr>
<tr><td>NUMERO : 7</td><td colspan="2">DUREE D’APPRENTISSAGE/D’EVALUATION : 84 heures/ 6h</td></tr>
<tr><td>MODULE</td><td colspan="2">Identification des vulnérabilités potentielles dans les systèmes informatiques</td></tr>
<tr><td colspan="3">FONCTION ET POSITION DE LA COMPETENCE</td></tr>
<tr><td colspan="3">Cette compétence est dispensée à mi-parcours de la formation. Elle permet à l’apprenant : (i) d’acquérir les connaissances approfondies en sécurité informatique ; (ii) de décrire un audit de configuration ; (iii) d’effectuer une analyse statique et dynamique de code source ; (iv) d’effectuer les tests d'intrusion ("pénétration testing») et de veiller sur les vulnérabilités.</td></tr>
<tr><td colspan="3">DEMARCHE PARTICULIERE A LA COMPETENCE</td></tr>
<tr><td colspan="3">Il est suggéré de répartir le temps d’apprentissage selon les proportions suivantes :
• Acquérir les connaissances approfondies en sécurité informatique : 15 % ;
• Décrire un audit de configuration :15 % ;
• Effectuer une analyse statique et dynamique de code source :20 % ;
• Effectuer les tests d'intrusion ("pénétration testing"). :30% ;
• Veiller sur les vulnérabilités :15%
Evaluation : 05% ;
Il est suggéré de respecter l’ordre des éléments, tel que décrit dans le référentiel de formation.</td></tr>
<tr><td>Savoirs liés à la compétence</td><td>Balises</td><td>Activités d’enseignement et d’apprentissage</td></tr>
<tr><td colspan="3">1.Acquérir les connaissances approfondies en sécurité informatique</td></tr>
<tr><td>1.1. Transmettre les connaissances de référence</td><td>• Sources de connaissances pertinentes et fiables ;
• Informations de manière structurée ;
• Documents en cybersécurité</td><td rowspan="2">Par des exemples et des illustrations, le formateur devra conduire les apprenants à développer une expertise approfondie en sécurité informatique, tout en se mettant à jour sur les dernières tendances et à être prêts à faire face aux défis de sécurité émergents</td></tr>
<tr><td>1.2. Détecter les nouvelles menaces</td><td>• Veille technologique ;
• Outils de détection ;
• Partage de l’information</td></tr>
</table>

1.3. Identifier les nouvelles avancées dans le domaine	• Publications sur la sécurité informatique ; • Participation à des communautés/forum ; • Veille technologique ;	
2- **Décrire un audit de configuration**		
2.1 Vérifier le périmètre couvert et les tests réalisés	• Définition du périmètre ; • Exigences de sécurité ; • Exécution des tests ; • Documentation des résultats.	Le formateur explique les objectifs de l'audit de configuration, guidant les apprenants dans la définition du périmètre de l'évaluation, la sélection des outils, l'élaboration d'un plan d'audit détaillé, et la documentation systématique des résultats. L'apprenant à travers des activités pratiques s'exerce à produire un rapport d'audit.de configuration.
2.2 Élaborer le rapport d'audit	• Organisation des résultats ; • Présentation des constats claires et concises ; • Recommandations d'amélioration ; • Priorisation des actions ; • Rapport d'audit ;	
3- Effectuer une analyse statique et dynamique de code source		
3.1. Identifier les vulnérabilités	• Outils d'analyse statique ; • Tests dynamiques ; • Résultats ; • Rapport des vulnérabilités ;	Le formateur à travers des exposés et à partir des exercices entrainera les apprenants à réaliser une analyse approfondie du code source tout en les amenant à utiliser à la fois des techniques d'analyse statique et dynamique.
3.2. Acquérir les résultats et des recommandations	• Outils d'analyse statique et dynamique du code source ; • Résultats ; • Recommandations ; • Priorisation des actions ;	
4- Effectuer les tests d'intrusion ("penetration testing")		
4.1. Analyser les failles de sécurité	• Vecteurs d'attaque ; • Outils d'analyse. ; • Résultats des tests d'intrusion ;	Par des exposés en group, le formateur amènera les apprenants à identifier les techniques d'attaques,

	• Impact des failles de sécurité identifiées ; • Formulation de recommandations.	l'élaboration des stratégies de sécurité, la mise en œuvre des correctifs et la rédaction d'un rapport lors des tests d'intrusion.
4.2. Préciser les prévisions	• Élaboration d'une stratégie ; • Cibles potentielles ; • Scénarios d'attaque ; • Risques.	
4.3. Exécuter le plan d'amélioration	• Correctifs • Surveillance continue ; • Plan d'amélioration en fonction des nouvelles menaces ; • Sensibilisation et formation des utilisateurs.	
5- **Veiller sur les vulnérabilités**		
5.1Identification des sources de veille	• Publications de rapports de sécurité ; • Bases de données de vulnérabilités ; • Listes de diffusion et forums de sécurité informatique ; • Rapports de recherche et des publications académiques.	A l'aide des exercices de cas pratiques, le formateur présentera aux apprenant l'importance d'assurer une la veille sur les vulnérabilités, les apprenants devront comprendre la nécessité de rester à jour sur les menaces de sécurité et d'adopter des pratiques proactives pour protéger les systèmes et les données.
5.2. Exploiter les alertes sur les vulnérabilités	• Impact potentiel des vulnérabilités signalées ; • Priorisation des correctifs ; • Déploiements de correctifs ; • Surveillance des correctifs déployés ; • Sensibilisation des utilisateurs.	
5.3. Contextualiser le Niveau de Précision de la sécurité	• Alertes ; • Informations ; • Pertinence ; • Adaptation des mesures de mitigation.	

COMPETENCE 08 : Configurer les outils de test de pénétration des systèmes d'exploitation		
NUMERO : 08	**DUREE D'APPRENTISSAGE/D'EVALUATION : 112 heures/8h**	
MODULE	**Configuration des outils de test de pénétration des systèmes d'exploitation**	
FONCTION ET POSITION DE LA COMPETENCE		
Cette compétence particulière permet à l'apprenant de comprendre le fonctionnement des systèmes d'exploitation et leurs spécificités, de découvrir les outils et les méthodologies pour les tests d'intrusion, et d'acquérir une méthode de test d'intrusion répétable et documentable Cette compétence, dans le processus de formation, arrive en huitième position sur les quatorze (14) compétences du référentiel de formation.		
DEMARCHE PARTICULIERE A LA COMPETENCE		
Étant donné que cette compétence est particulière et au cœur du métier, il est suggéré de repartir le temps d'apprentissage selon les proportions suivantes : 1. Utiliser des outils de tests de pénétration d'intrusion : 15% 2. Configurer les outils : 27% 3. Configurer les systèmes d'exploitation cibles : 32% 4. Élaborer les Scripts intelligents : 20% Evaluation : 6% Il est suggéré de respecter l'ordre des éléments, tel que décrit dans le référentiel de formation.		
Savoirs liés à la compétence	**Balises**	**Activités d'enseignement et d'apprentissage**
2.3 Utiliser des outils de tests de pénétration d'intrusion		
1.1 Exploiter les fonctionnalités des outils	• Fonctionnalités des outils • Exploitation des données • Avantages des fonctionnalités • Outils collaboratifs • Outils de marketing	A l'aide des exercices pratiques, le formateur présentera aux apprenant les différents outils Il leur parlera du choix des outils en fonctions des tests à réaliser. L'apprenant écoute, pose des questions, exécute

1.2. Choisir les outils en fonction des tests	• Différents types de tests • Sélection des outils • Mise en pratique • Bonnes pratiques et recommandations	les consignes, prend des notes, échange avec d'autres apprenants, présente la production du groupe, participe à la mise en commun en plénière, participe aux synthèses, note la synthèse.
1.3 Documenter les résultats	• Éléments clés de la documentation des résultats • Méthodes de documentation des résultats • Bonnes pratiques de documentation des résultats • Outils et ressources	
2.4 Configurer les outils		
2.1 Réaliser les paramétrages	• Notions Fondamentales • Outils et Environnement de Paramétrage • Paramétrage des Systèmes d'Exploitation • Réseaux et Sécurité • Gestion des Services et Applications • Optimisation et Dépannage	Par l'entremise d'exposés, cours théoriques avec supports visuels (diapositives, vidéos), études de cas et scénarios pratiques pour illustrer la réalisation des paramétrages, la sélections des modules, l'exécution des taches de configuration et leur configuration. L'apprenant, écoute, pose des questions, exécute les consignes, prend des notes, échange avec d'autres apprenants et pratique sous la supervision du formateur. Le formateur encadre les activités des apprenants afin d'assurer l'intégration des apprentissages par le biais des travaux pratiques en laboratoire pour mettre en pratique toutes les techniques.
2.2 Sélectionner les options/modules	• Installation et configuration • Bonnes pratiques de sélection des options/modules	
2.3 Exécuter les tâches de configuration	• Notions Fondamentales • Outils et Environnement de Configuration • Configuration des Systèmes d'Exploitation • Configuration Réseau • Configuration des Services et Applications • Automatisation des Tâches de Configuration	
2.4 Sécuriser les configurations déployées	• Configurations déployées	

	• Risques et des vulnérabilités • Bonnes pratiques de sécurisation des configurations déployées • Accès et autorisations • Sécurisation des communications • Tests de sécurité et audits • Incidents de sécurité	
2.5 Configurer les systèmes d'exploitation cibles		
3.1 Spécifier les OS ciblés	• Installation et configuration • Besoins et contraintes • Sélection des OS ciblés • Logiciels aux OS ciblés • Tests et validation sur les OS ciblés • Evolutions des OS • Bonnes pratiques de spécification des OS ciblés	Le formateur mettra les apprenants en situation, Seul ou en équipe. À partir de mises en situations et de logiciels appropriés fournis par le formateur. Il amènera les apprenants à installer et configurer les systèmes d'exploitation L'apprenant écoute, observe, pose des questions, exécute les consignes, prend des notes, échange avec d'autres apprenants et pratique sous la supervision du professeur les exercices. Le formateur encadre les activités des apprenants afin d'assurer l'intégration des apprentissages.
3.2 Documenter les services et ports testés	• Services et Ports Réseau • Test des Services et Ports • Modèles de Documentation • Techniques d'Analyse des Résultats • Rapports de Sécurité • Résultats	

3.3 Exploiter les mises à jour des configurations	• Planification des mises à jour • Gestion des mises à jour avec des outils spécifiques • Bonnes pratiques de déploiement des mises à jour • Sécurisation des mises à jour	
2.6 Élaborer les Scripts intelligents		
4.1 Utiliser le code /langage	• Environnement de Développement • Syntaxe de Base et Principes Fondamentaux • Fonctions et Modules • Manipulation de Données • Gestion des Erreurs • Interactions avec les Bases de Données (si applicable) • Développement d'Applications ou de Projets Simples	Le formateur fait un cours magistral interactif avec présentations des différents langages, invite les implémenter les fonctionnalités gérées. L'apprenant écoute, pose des questions, exécute les consignes, prend des notes, échange avec d'autres apprenants et pratique sous la supervision du professeur les exercices en atelier sous forme de projets.
4.2 Gérer les fonctionnalités	• Fonctionnalités existantes • Outils et Technologies • Déploiement et Gestion Avancée • Suivi et évaluation des fonctionnalités	
4.3 Elaborer les scripts	• Bases de la Programmation • Traitement de Fichiers et de Données • Interactions avec le Système d'Exploitation • Automatisation des Tâches • Gestion des Erreurs et Débogage • Sécurité et Bonnes Pratiques	Le formateur présente un cours interactif incluant des présentations, des démonstrations et des exercices pratiques. Les apprenants participent activement à travers des projets individuels et en groupe
4.4 Documenter les techniques des scripts	• Bonnes pratiques en documentation	

	• Outils de documentation • Documentation Interne dans les Scripts • Documentation Externe et Guides d'Utilisation • Bonnes Pratiques de Publication et de Partage	

COMPETENCE 09 : Tester la vulnérabilité sur les Réseaux des applications, site web et les systèmes d'exploitation	
NUMERO : 9	**DUREE D'APPRENTISSAGE/D'EVALUATION : 140 heures/ 10 h**
MODULE	Tests de vulnérabilité sur les Réseaux des applications, site web et les systèmes d'exploitation
FONCTION ET POSITION DE LA COMPETENCE	
Cette compétence particulière est dispensée vers la fin de l'année de formation. Elle permet à l'apprenant de : (i) de Décrire les outils de tests de vulnérabilités ; (ii) de Tester l'efficacité du réseau et des applications ; (iii) **de** Tester les systèmes d'exploitation	
DEMARCHE PARTICULIERE A LA COMPETENCE	
Il est suggéré de répartir le temps d'apprentissage selon les proportions suivantes : 1. Analyser la topologie et les flux réseau : 15% 2. Identifier les vecteurs d'intrusion réseau : 15% 3. Décrire les outils de tests de vulnérabilités :10% 4. Tester l'efficacité du réseau et des applications :30% 5. Tester les systèmes d'exploitation : 20% ; Evaluation :10% Il est suggéré de respecter l'ordre des éléments, tel que décrit dans le référentiel de formation.	

Savoirs liés à la compétence	Balises	Activités d'enseignement et d'apprentissage
1) Analyser la topologie et les flux réseau :		
1.1 Produire les informations	• Collecte des informations • Traitement et Organisation des informations • Rapports et Documentation : • Recommandations d'Amélioration • Présentation des Constatations :	Par l'entremise d'exposés et/ou d'études de cas, le formateur présente aux apprenants les techniques de production des informations. L'apprenant, par le biais d'exercices développe sa capacité à exécuter à produire l'information. Le formateur encadre les activités des apprenants afin d'assurer l'intégration des apprentissages.
1.2. Réaliser la cartographie réseau	• Cartographie Réseau • Méthodes de Cartographie Réseau • Outils de Cartographie Réseau • Outils de Découverte Automatisée • Bonnes Pratiques et Considérations	Cours Magistraux et Présentations Démonstrations Pratiques et Exercices Études de Cas et Discussions en Groupe Projets Pratiques sur des Techniques Réelles
1.3Gerer les flux	• Concepts Clés de la Gestion des Flux • Objectifs de la Gestion des Flux • Outils et Technologies de Gestion des Flux	
1.4 Evaluer les métriques réseau	• Métriques Réseau : • Principales Métriques Réseau à Évaluer : • Méthodes d'Évaluation des Métriques Réseau : • Interprétation des Résultats et Actions Correctives :	
2.**Identifier les vecteurs d'intrusion réseau**		

2.1 . Identifier les techniques d'attaque réseau	• Introduction aux Attaques Réseau • Ingénierie Sociale • Logiciels Malveillants (Malware) • Exploitation des Vulnérabilités • Attaques de Réseau • Accès Physique et Compromission des Identifiants • Attaques sans Fichier • Exploitation des Services Exposés	
2.2.Analyser les logs et les alertes	• Introduction aux Logs et Alertes • Collecte et Gestion des Logs • Analyse des Logs • Introduction aux SIEM (Security Information and Event Management) • Détection et Réponse aux Incidents	Cours Magistraux et Présentations Démonstrations Pratiques et Exercices Études de Cas et Discussions en Groupe Projets Pratiques sur des Techniques Réelles
2.3. Collecter les vecteurs potentiels couverts	• Introduction aux Vecteurs d'Intrusion • Vecteurs d'Intrusion Basés sur l'Ingénierie Sociale • Vecteurs d'Intrusion Basés sur les Logiciels Malveillants • Exploitation des Vulnérabilités • Vecteurs d'Intrusion Réseau • Accès Physique et Compromission des Identifiants • Attaques sans Fichier (Fileless Attacks) • Exploitation des Services Exposés	

	• Collecte et Analyse des Vecteurs d'Intrusion • Réponse aux Incidents et Remédiation	
1. **Décrire les outils de tests de vulnérabilités**		
1.1 Acquérir les outils de test d'intrusion des réseaux /applications	Mise à jour des outils Outils de tests d'intrusion Installation et configuration	Le formateur guide les apprenants dans l'utilisation des outils de test de vulnérabilité sur le réseau informatique et les applications, l'analyse des données, la mise en œuvre des correctifs et la production d'un rapport.
1.2 Détecter les vulnérabilités des réseaux/applications	• Vulnérabilités • Outils de détection ; • Résultats ; • Correctifs	
2. Tester l'efficacité du réseau et des applications		
1.1. Décrire les résultats de tests	• Données ; • Problèmes ; • Rapports détaillés ;	Le formateur organisera des groupes de travail de maximum 5 apprenants à qui il affectera des thèmes d'exposé portant sur le test de l'efficacité du réseau et des applications.
1.2. Utiliser les préconisations	• Meilleures pratiques et normes de sécurité ; • Conformité des réseaux et des applications • Implications ; • Actions spécifiques ;	
1.3. Identifier des failles	• Outils d'analyse ; • Données de test ; • Résultats ;	
2. Tester les systèmes d'exploitation		
2.1. Décrire les configurations et services testés	• Configurations critiques ; • Services activés sur les OS • Sécurité du système d'exploitation ; • Autorisations d'accès • Services vulnérables ;	A travers les exercices pratiques, le formateur amène les apprenants à acquérir les compétences nécessaires pour tester efficacement les systèmes d'exploitation, identifier les failles de sécurité et

	• Documentation des résultats ;	recommander des mesures correctives appropriées pour renforcer la sécurité et la résilience du système. Le formateur formera des groupes, donnera des exercices de cas pratique aux apprenants et s'attardera sur les méthodes et recommandation produites par les apprenants.
2.2. Effectuer le scanne de vulnérabilité	• Outils de scan de vulnérabilité ; • Installation et configuration • Scans de vulnérabilité ; • Rapport détaillé des résultats.	
2.3. Recommander les correctifs et mesures	• Vulnérabilités ; • Priorisation des correctifs ; • Stratégies de déploiement ; • Mesures compensatoires ; • Correctifs déployés ;	

COMPETENCE 10 : Proposer les stratégies d'atténuation		
NUMERO : 10	**DUREE D'APPRENTISSAGE/D'EVALUATION : 112 heures/ 8h**	
MODULE	**Proposition des stratégies d'atténuation**	
FONCTION ET POSITION DE LA COMPETENCE		
Cette compétence particulière, dans le processus de formation, arrive en dixième position sur les quatorze (14) compétences du référentiel de formation. Elle est mobilisée lors de la mise en œuvre des compétences (7, 8, 9, 11et 12). L'acquisition de cette compétence permet à l'apprenant de comprendre les stratégies d'atténuation et les mettre en œuvre de manière proactive et continue, pour renforcer la sécurité des système informatiques et réduire le risque d'intrusions et de compromissions.		
DEMARCHE PARTICULIERE A LA COMPETENCE		
Étant donné que cette compétence est particulière et au cœur du métier, il est suggéré de repartir le temps d'apprentissage selon les proportions suivantes : 1. Évaluer la propagation latérale de l'attaquant 2. Concevoir des scénarios de segmentation réseau 3. Analyser les risques et menaces 4. Réaliser des conseils sur l'architecture sécurité 5. Élaborer une politique de sécurité 6. Préconiser des mesures techniques 7. Valider la mise en œuvre :17% Évaluation : **7%** Il est suggéré de respecter l'ordre des éléments, tel que décrit dans le référentiel de formation.		
Savoirs liés à la compétence	Balises	Activités d'enseignement et d'apprentissage
1. Évaluer la propagation latérale de l'attaquant		
1.1 Utilisation parfaite des modèles de compromission ;	• Collecte des informations • Traitement et Organisation des informations • Rapports et Documentation :	Par l'entremise d'exposés et/ou d'études de cas, le formateur démontre aux apprenants comment utiliser les modèles de compromission.

	• Recommandations d'Amélioration • Présentation des Constatations :	L'apprenant, par le biais d'exercices développe sa capacité à exécuter à produire l'information. Le formateur encadre les activités des apprenants afin d'assurer l'intégration des apprentissages.
1.2 Simulation efficace des scénarios de propagation ;	• Cartographie Réseau • Méthodes de Cartographie Réseau • Outils de Cartographie Réseau • Outils de Découverte Automatisée • Bonnes Pratiques et Considérations	Le formateur initie les apprenants aux différentes techniques simulation de scenarios de propagation et calcul des métriques de propagation. L'apprenant écoute, pose des questions, exécute les consignes, prend des notes, échange avec d'autres apprenants, participe aux synthèses, note la synthèse.
1.3 Calcul correct des métriques de propagation	• Métriques Réseau : • Principales Métriques Réseau à Évaluer : • Méthodes d'Évaluation des Métriques Réseau : • Interprétation des Résultats et Actions Correctives :	
2. **Concevoir des scénarios de segmentation réseau**		
2.1 Elaborer la microsegmentation du réseau	• Introduction à la Microsegmentation • Concepts Fondamentaux de la Sécurité Réseau • Architectures et Technologies de Microsegmentation • Planification de la Microsegmentation • Implémentation de la Microsegmentation • Outils et Techniques d'Implémentation	Cours Magistraux et Présentations Démonstrations Pratiques et Exercices Études de Cas et Discussions en Groupe Projets Pratiques sur des Techniques Réelles
2.2 Gérer les scénarios	• Introduction à la Gestion des Scénarios • Méthodologies de Création de Scénarios • Collecte et Analyse des Données • Élaboration des Scénarios	

	• Application des Scénarios à la Prise de Décision • Outils et Technologies pour la Gestion des Scénarios • Surveillance et Mise à Jour des Scénarios	
2.3 documenter la technique proposée	• Introduction à la Documentation Technique • Préparation de la Documentation • Rédaction Technique • Outils et Logiciels de Documentation • Processus de Révision et d'Édition • Publication et Diffusion	
3. Analyser les risques et menaces		
3.1 Identifier les techniques d'attaque réseau	• Ingénierie Sociale • Attaques par Déni de Service • Injection de Code • Autres techniques • Protection contre les Attaques Réseau :	Par l'entremise d'exposés et/ou d'études de cas, le formateur présente aux apprenants les techniques d'attaques réseaux. L'apprenant, par le biais d'exercices développe sa capacité à exécuter à identifier les différentes techniques d'attaques et les modes d'infiltrations. Le formateur encadre les activités des apprenants afin d'assurer l'intégration des apprentissages.
3.2 Gérer les logs et alertes	• Gestion des Logs : • Gestion des Alertes : • Bonnes Pratiques de Gestion des Logs et des Alertes :	Le formateur à partir d'un exposé présente la gestion des logs et des alertes. L'apprenant écoute, pose des questions, exécute les consignes, prend des notes, échange avec d'autres apprenants et pratique sous la supervision du professeur les exercices. Le formateur encadre les activités des apprenants afin d'assurer l'intégration des apprentissages.

3.3 Utiliser les modèles de compromission	• Compromission (IOC) • Techniques de planification • Indicateurs de compromission • Méthodes d'utilisation des indicateurs de compromission	Le formateur mettra les apprenants en situation, Seul ou en équipe. À partir de mises en situations et de documents appropriés fournis par le formateur. il amènera les apprenants à utiliser les modèles de compromission.
3.4 Calculer les métriques de propagation	• Intrusion et compromission. • Détection et d'analyse des intrusions. • Métriques de propagation des intrusions et leur calcul. • Intrusions. • Outils et technologies utilisés. • Bonnes pratiques en matière de sécurité informatique. • Aspects juridiques et éthiques	Par l'entremise d'exposés et/ou d'études de cas, le formateur présente aux apprenants les techniques de calculer des métriques de propagation L'apprenant, par le biais d'exercices développe ses capacités aux calcul des métriques de propagation Le formateur encadre les activités des apprenants afin d'assurer l'intégration des apprentissages.
4. Réaliser des conseils sur l'architecture sécurité		
4.1 Elaborer une microsegmentation du réseau	• Microsegmentation du réseau. • Sécurité spécifique d'un réseau • Virtualisation du réseau utilisé. • Architecture de micro segmentations • Gestion de la micro segmentation du réseau. • Efficacité de la micro segmentation • Implications juridiques et éthiques	Par l'entremise d'exposés et/ou d'études de cas, le formateur présente aux apprenants les techniques d'élaborations des micro segmentations du réseau et la gestion des scénarios de tests. Pendant les explications, les apprenants prennent notes, posent des questions et appliquent les exercices et exemples données par le formateur Le formateur encadre les activités des apprenants afin d'assurer l'intégration des apprentissages.
4.2 Gérer les scénarios	• Concepts de base • Scénarios dans Microsoft Excel. • Gestionnaire de scénarios. • Conséquences et résultats	

	• Cellules variables et les cellules résultantes • Synthèse des scénarios • Utilisation des scénarios. • Prise de décision. • Utilisation des scénarios,	
4.3 Documenter la technique proposée	• Éléments Clés de la Documentation Technique • Processus de Documentation • Éléments Essentiels de la Documentation • Bonnes Pratiques et Conseils Additionnels	
5. Élaborer une politique de sécurité		
5.1 Produire une documentation présentant la politique de sécurité	• Politique de Sécurité • Principes Fondamentaux • Responsabilités des Employés • Procédures en Cas d'Incident	Par l'entremise d'exposés et/ou d'études de cas, le formateur présente aux apprenants les plans d'élaboration d'une politique de sécurité. L'apprenant, par le biais d'exercices développe sa capacité à Produire une documentation présentant la politique de sécurité, à utiliser les bonnes pratiques et référentiels reconnues, enfin élaborer un plan d'action de suivi et d'audit. Pendant les explications, les apprenants prennent notes, posent des questions et appliquent les exercices et exemples données par le formateur. Le formateur encadre les activités des apprenants afin d'assurer l'intégration des apprentissages.
5.2 Utiliser les bonnes pratiques et référentiels reconnus ;	• Standards de sécurité • Risques • Authentification Multifacteur (AMF) • Cryptage des données • Mises à jour régulières • Sécurité	
5.3 Elaborer un plan d'action de suivi et d'audit	• Critères et planification d'audit • Collecte des données • Rapports d'audit • Recommandations • Formation et sensibilisation • Outils et Méthodologies d'Audit • Révision et Évaluation Continue	

6. Préconiser des mesures techniques		
6.1 Proposer des solutions exhaustives ;	• Introduction aux objectifs métiers et aux niveaux de Services • Comprendre les Besoins Métier • Élaboration des SLAs Basés sur les Objectifs Métiers • Implémentation des SLAs • Gestion des Performances et des Incidents	Cours Magistraux et Présentations Démonstrations Pratiques et Exercices Études de Cas et Discussions en Groupe Projets Pratiques et Simulations
6.2.Déployer et administrer une politique de sécurité ;	• Fondements de la Sécurité Informatique • Évaluation des Besoins en Sécurité • Conception de l'Architecture de Sécurité • Proposition d'une Architecture de Sécurité • Implémentation de l'Architecture de Sécurité • Gestion et Maintenance de l'Architecture de Sécurité	Cours Magistraux et Présentations Démonstrations Pratiques et Exercices Études de Cas et Discussions en Groupe Projets Pratiques
6.3.Reduire les risques	Introduction à l'Évolution des Solutions Technologiques Analyse des Besoins et des Tendances Conception de Solutions Évolutives Gestion du Changement et de la Complexité Adaptation et Évolution Continue Sécurité et Fiabilité	
7. Valider la mise en œuvre		
7.1 Utiliser les scénarios de tests	• Types de Scénarios de Tests • Conception de Scénarios de Tests • Exécution et Automatisation des Scénarios de Tests • Évaluation et Reporting des Résultats	Par l'entremise d'exposés et/ou d'études de cas, le formateur présente aux apprenants les techniques d'utilisation des scénarios de tests. L'apprenant, par le biais d'exercices développe sa capacité à

	• Scénarios de Tests dans les Projets Réels	exécuter à exécuter les scénarios et contrôler le respect des spécifications définies. Pendant les explications, les apprenants prennent notes, posent des questions et appliquent les exercices et exemples données par le formateur Le formateur encadre les activités des apprenants afin d'assurer l'intégration des apprentissages.
7.2 Gerer les tests effectués	• Importance • Planification des Tests • Cas de Tests • Exécution des Tests • Risques liés aux Tests	
7.3 Contrôler le respect des spécifications définies	• Spécifications • Plan de Contrôle Qualité • Vérifications Régulières • Processus de Validation • Résultats • Actions Correctives • Traçabilité et Transparence • Audits Qualité	

COMPETENCE 11 : Configurer les pares-feux et des systèmes de détection d'intrusions	
NUMERO : 11	**DUREE D'APPRENTISSAGE/D'EVALUATION :112 heures/ 8h**
MODULE	Configuration des pares-feux et des systèmes de détection d'intrusions
FONCTION ET POSITION DE LA COMPETENCE	
Cette compétence est essentielle pour protéger les systèmes et les données contre les intrusions. Il est important de configurer ces dispositifs en fonction des besoins spécifiques de l'organisation et de les maintenir à jour pour une protection efficace. C'est pourquoi la maitrise de la configuration des pares feux et des systèmes de protection pour l'apprenant peut être placée au cœur du métier.	
DEMARCHE PARTICULIERE A LA COMPETENCE	
Étant donné que cette compétence est particulière, il est suggéré de repartir le temps d'apprentissage selon les proportions suivantes : 1. Configurer les pare-feux et des IDS/IPS : 23 %	

<table>
<tr><td colspan="3">2. Implémenter une politique de filtrage et de détection :20 %
3. Gérer les règles, les signatures et les listes blanches/noires :10 %
4. Superviser les événements de sécurité générés :10 %
Evaluation :07%
Il est suggéré de respecter l’ordre des éléments, tel que décrit dans le référentiel de formation.</td></tr>
<tr><td>Savoirs liés à la compétence</td><td>Balises</td><td>Activités d’enseignement et d’apprentissage</td></tr>
<tr><td colspan="3">2.6.1 Configurer les pare-feux et des IDS/IPS</td></tr>
<tr><td>1.1. Validation des tests</td><td>• Objectifs des tests ;
• Scénarios de test ;
• Plan de test ;
• Sélection des outils ;
• Configuration des tests ;
• Exécution des tests ;
• Résultats ;
• Normes ;
• Anomalies
• Validation finale</td><td rowspan="2">Le formateur après avoir exposé les éléments de théorie nécessaires, et quelques démonstrations, l’apprenant est invité de manière répétitive sur plusieurs cas de figures à élaborer un plan de test, configurer les outils de test avant de l’exécuter.
L’apprenant écoute, pose des questions, exécute les consignes, prend des notes, échange avec d’autres apprenants et pratique sous la supervision du professeur les exercices.

Le formateur encadre les activités des apprenants afin d'assurer l'intégration des apprentissages.</td></tr>
<tr><td>1.2. Documentation des techniques produites</td><td>• Types de documentation ;
• Description des techniques ;
• Procédures pas à pas ;
• Normes de documentation ;
• Formats de documentation ;
• Versionnage ;</td></tr>
<tr><td colspan="3">2.6.2 Implémenter une politique de filtrage et de détection</td></tr>
<tr><td>2.1. Utilisation des bonnes pratiques de sécurité ;</td><td>• Principe du moindre privilège ;
• Segmentation du réseau ;</td><td></td></tr>
</table>

	• Identités et des accès ; • Chiffrement des données ; • Incidents de sécurité ;	A l'aide d'une mise en situation, le formateur amènera les apprenants à utiliser les bonnes pratiques de sécurité, le déploiement sur l'infrastructure cible et de mesurer la politique de filtrage et de détection par des exposés et des projections. L'apprenant écoute, pose des questions, exécute les consignes, prend des notes, échange avec d'autres apprenants et pratique sous la supervision du professeur les exercices. Le formateur encadre les activités des apprenants afin d'assurer l'intégration des apprentissages.
2.2. Déploiement sur l'infrastructure cible ;	• Infrastructure existante ; • Objectifs de sécurité ; • Solutions de sécurité ; • Architecture de sécurité ; • Planification du déploiement ; • Equipements de sécurité	
2.3. Mesure de la politique de filtrage et de détection	• Règles de filtrage ; • Précision des alertes ; • Réactivité aux incidents ; • Meilleures pratiques ; • Feedback et amélioration continue ; • Révision et ajustement de la politique	
2.6.3 Gérer les règles, les signatures et les listes blanches/noires		
3.1 Réactivité aux nouvelles menaces	• Menaces ; • Vulnérabilités ; • Criticité ; • Actions ; • Règles et des signatures ; • Test et validation ; • Gestion des listes blanches et noires.	Le formateur mettra les apprenants en situation, Seul ou en équipe. À partir de mises en situations et de documents appropriés fournis par le formateur. il amènera les apprenants à Réagir promptement face aux nouvelles menaces avant de réajuster les configurations. L'apprenant écoute, pose des questions, exécute les consignes, prend des notes, échange avec d'autres apprenants et pratique sous la supervision du professeur les exercices. Le formateur encadre les activités des apprenants afin d'assurer l'intégration des apprentissages.
3.2 Gestion des configurations	• Configurations ; • Contrôle des versions :	

	• Validation des modifications ; • Gestion des changements	
Superviser les événements de sécurité générés		
3.1 Exploitation des corrélations et alertes remontées ;	• Corrélations ; • Sources d'événements ; • Alertes remontées ; • Corrélation des événements ; • Attaques complexes ; • Outils de SIEM : • Alertes ;	Après avoir exposé sur les éléments théoriques d'exploitation des corrélations et alertes remontés, d'organes de liaison ; le formateur amène les apprenants, non seulement à reconnaître les éléments constitutifs de la collecte des logs et métriques d'un système informatique, leur limite, leur rôle mais aussi à faire leur représentation. L'apprenant écoute, pose des questions, exécute les consignes, prend des notes, échange avec d'autres apprenants et pratique sous la supervision du professeur les exercices. Le formateur mettra les apprenants en situation, Seul ou en équipe. À partir de mises en situations et de documents appropriés fournis par le formateur. Il fera Contrôler la qualité de l'intervention
3.2 Collecte des logs et métriques	• Sources de logs ; • Evénements à collecter ; • Agents de collecte ; • Traitement des logs ; • Métriques	
3.3 Description de reporting des incidents	• Incidents ; • Gravité ; • Contextualisation ; • Causes ; • Actions correctives	A partir des exposés sur la Description de reporting des incidents et leur structure le formateur amène les apprenants à produire de manière efficace un document. L'apprenant écoute, pose des questions, exécute les consignes, prend des notes, échange avec d'autres apprenants et pratique sous la supervision du professeur les exercices. Le formateur encadre les activités des apprenants afin d'assurer l'intégration des apprentissages.

COMPÉTENCE 12 : Assurer la veille technologique en cyberattaque		
Numéro : 12	**DUREE D'APPRENTISSAGE/D'EVALUATION : 84heures/ 6h**	
MODULE	Veille technologique en cyberattaque	
Fonction et position de la compétence		
La compétence particulière « **assurer la veille technologique en cybersécurité** » est essentielle pour la formation de l'apprenant car dans une entreprise il sera capable de surveiller les menaces potentielles pesant sur les systèmes d'information et de prendre des mesures préventives pour limiter les risques d'incidents.		
Démarche particulière à la compétence		
Etant donné que la maîtrise de cette compétence a une incidence directe sur l'acquisition des autres compétences particulières du métier, Il est suggéré de répartir le temps d'apprentissage selon les proportions suivantes : 1. Assurer la veille technologique et sécuritaire : 20% ; 2. Analyser les nouvelles techniques d'attaques : 30 %. 3. Évaluer l'impact sur l'architecture existante : 20 % ; 4. Préconiser des mesures correctives : 20 % ; 5. Valider la réponse apportée : 05% ; Evaluation : 5%.		
Savoirs liés à la compétence	**Balises**	**Activités d'enseignement et d'apprentissage**
1. Assurer la veille technologique et sécuritaire		
1.1.Diffuser les alertes sur les nouvelles menaces ;	• Nouvelles menaces • Détection d'intrusion, • Système de sécurité des informations, • Classification des menaces • Diffusion des alertes	Le formateur vise à préparer les apprenants à protéger efficacement les systèmes informatiques contre les menaces émergentes en assurant une veille technologique et sécuritaire proactive. A travers des exposés, les travaux pratiques en atelier. L'apprenant écoute, pose des questions, exécute les consignes, prend des notes, échange avec d'autres apprenants et pratique sous la supervision du professeur les exercices. Le formateur encadre les activités des apprenants afin d'assurer l'intégration des apprentissages.
1.2.Analyser les tendances et évolutions ;	• Collecte de données ; • Tendances émergentes ; • Evolutions futurs ; • Bonnes pratiques	
1.3. Documenter les informations	• Informations pertinentes ; • Méthodes de documentation	

	• Mise à jour régulière ; • Sécurisation des informations ;	
2. Analyser les nouvelles techniques d'attaques		
2.1 les vecteurs et failles exploités	• Types de vecteurs • Types de failles • Audit de sécurité • Bonnes pratiques	Par l'entremise d'exposés et/ou d'études de cas, le formateur présente aux apprenants les différentes techniques d'attaques. L'apprenant, par le biais d'exercices pratiques développe sa capacité à faire des mises à jour Le formateur encadre les activités des apprenants afin d'assurer l'intégration des apprentissages.
2.2 Évaluer la criticité et de l'impact potentiel	• Risques • Critères de criticité • Outils utilisés • Méthodes d'évaluation de la criticité • Bonnes pratiques et recommandations	
2.3 Exploitation des mises à jour	• Importance des Mises à Jour • Stratégies de Maintenance • Installation et configuration Mises à Jour • Bonnes Pratiques et Précautions	
• 3. **Évaluer l'impact sur l'architecture existante**		
3.1 Analyser les risques encourus	• Fondements de la sécurité informatique • Méthodologies de tests d'intrusion • Contrôles préventifs • Détections adaptées • Bonnes pratiques et gestion des risques	Le formateur à partir d'un exposé et ou de la mise en situation présente les différents scénarios de test. L'apprenant écoute, pose des questions, exécute les consignes, prend des notes, échange avec d'autres apprenants et pratique sous la supervision du professeur les exercices. Le formateur encadre les activités des apprenants afin d'assurer l'intégration des apprentissages.
3.2 Gérer les scénarios de test	• Modèles d'architecture réseau • Rédaction des cas de test • Combinaison des étapes • Test des conditions et fonctionnalités • Types de Scénarios	

4. Préconiser des mesures correctives :		
4.1 Gestion des risques	• Vulnérabilités du réseau et des postes de travail • Détection des intrusions • Prévention et de protection • Conséquences légales et actions à entreprendre • Sensibilisation et formation :	A l'aide d'une mise en situation, le formateur amènera l'apprenant à gérer les risques d'intrusion dans un système informatique Pendant les exposé et explications, les apprenants prennent notes, posent des questions et appliquent les exercices et exemples données par le formateur.
4.2 Exploiter le rapport coût/bénéfice et des contraintes	• Méthodologie d'exploitation • Bon exploit ou bon outil • Configuration de l'exploit	
4.2 Adapter le délai de mise en œuvre à la criticité	• Criticité • Mesures de sécurité urgentes • Allocation des ressources • Planification et suivi	
5. Valider la réponse apportée		
5.1 Valider les tests	• Équipement et outils de tests • Tests d'intrusion • Collecte des informations. • Rapports de test.	A l'aide d'une mise en situation, le formateur amènera les apprenants seul ou en équipe à diagnostiquer ou détecter les intrusions. L'apprenant écoute, pose des questions, exécute les consignes, prend des notes, échange avec d'autres apprenants et pratique sous la supervision du professeur les exercices. Le formateur encadre les activités des apprenants afin d'assurer l'intégration des apprentissages.
5.2 Produire la documentation	• Plan de test logiciel • Cahier de recette • Rapports de test • Mesures correctives	
5.3 Respecter les spécifications définies	• Cas d'utilisation. • Complément avec d'autres • Comportement attendu et observé. • Détection des défauts.	

<table>
<tr><td colspan="3">COMPETENCE N°13 : Rechercher un emploi</td></tr>
<tr><td>NUMERO : 13</td><td colspan="2">DUREE D'APPRENTISSAGE : 45 h</td></tr>
<tr><td>MODULE ASSOCIE</td><td colspan="2">Entrepreneuriat</td></tr>
<tr><td colspan="3">FONCTION ET POSITION DE LA COMPETENCE</td></tr>
<tr><td colspan="3">Les enseignements de cette compétence assurent à l'apprenant une meilleure connaissance de l'entreprise et de son environnement. Ils lui donnent des informations utiles dans la recherche de l'emploi et le préparent à s'adapter dans l'avenir dans un milieu professionnel.il intervient vers la fin de la formation afin de donner à l'apprenant les armes nécessaires pour s'implanter sur le marché de l'emploi.</td></tr>
<tr><td colspan="3">DEMARCHE PARTICULIERE A LA COMPETENCE</td></tr>
<tr><td colspan="3">La répartition du temps d'apprentissage est suggérée selon les proportions suivantes :
• Identifier les conditions de réussite d'un projet de création d'entreprise ou d'auto emploi :20%
• Monter un projet d'installation :20%
• Rechercher un financement :20%
• Exécuter un projet :20%
• S'approprier les techniques de recherche d'emploi : 20%
Il est suggéré de respecter l'ordre des éléments, tel que décrit dans le référentiel de formation.</td></tr>
<tr><td>Savoirs liés à la compétence</td><td>Balises</td><td>Activités d'enseignement et d'apprentissage</td></tr>
<tr><td colspan="3">1. Identifier les conditions de réussite d'un projet de création d'entreprise ou d'auto emploi</td></tr>
<tr><td>1.1 Etudier le marché</td><td>• Analyse du marché
• Facteurs de réussite
• Potentiels clients</td><td rowspan="2">Le formateur réitère les éléments de base sur l'entreprise, son fonctionnement et son organisation. L'apprenant reçoit en plus de notions sur le fonctionnement juridique et social de l'entreprise.
L'apprenant prend note et parvient à s'approprier des notions reçues.</td></tr>
<tr><td>1.2 Se Positionner dans une gamme de produits ou de services</td><td>• Besoins du consommateur
• Différents produits et services
• Le marché
• Flux et documents commerciaux</td></tr>
<tr><td colspan="3">2. Monter un projet d'installation</td></tr>
<tr><td>2.1 Assimiler les Procédures de montage de projet</td><td>• Procédures de montage de dossier
• Points de vigilance</td><td rowspan="2">A travers des exposés et de mise en situation professionnelle, le formateur amènera les apprenants à monter un projet. Pendant les explications, les apprenants prennent notes, posent des questions et exécutent les activités d'apprentissage.</td></tr>
<tr><td>2.2 Effectuer le Montage de projet</td><td>• Définition des objectifs
• Etude de faisabilité
• Planification</td></tr>
</table>

COMPETENCE N°13 : **Rechercher un emploi**		
3. Rechercher le financement		
3.1 Prospecter les sources de financement	• Opportunités de financement existantes • Techniques de recherche de financement • Techniques de négociation d'un projet • Démarche et condition de création d'une entreprise au Cameroun	A travers des exposés et de mise en situation professionnelle, le formateur montrera aux apprenants les techniques et procédures de recherche de financement. Il listera également les potentiels bailleurs de fond Pendant les explications, les apprenants prennent notes, posent des questions et exécutent les activités d'apprentissage.
3.1 Négocier le financement	• Bailleurs de fond • Techniques de négociations • Cadre réglementaire	
4. Exécuter un projet		
4.1 Mettre en œuvre un plan	• Etapes de la mise en œuvre d'un plan • Conseils pour mise en œuvre	A travers des exposés et de mise en situation professionnelle, le formateur montrera aux apprenants les techniques et procédures de mise en œuvre d'un plan, de mobilisation des ressources, d'implantation d'un projet. Puis emmènera chaque apprenant à monter un projet. Pendant les explications, les apprenants prennent notes, posent des questions et exécutent les activités d'apprentissage.
4.2 Mobiliser les ressources	• Méthodes et outils • Secteurs d'application • Mise en place d'un plan de mobilisation des ressources	
4.3 Implanter un projet	• Nature du projet • Objectifs • Echelle • Contraintes • Suivi et évaluation	
5.S'approprier les techniques de recherche d'emploi		
5.1 Assimiler les Procédures de montage de projet	• Procédures de montage de dossier • Points de vigilance	A travers des exposés et de mise en situation professionnelle, le formateur amènera les apprenants à monter un projet. Pendant les explications, les apprenants prennent notes, posent des questions et exécutent les activités d'apprentissage.
5.2 Effectuer le Montage de projet	• Définition des objectifs • Etude de faisabilité • Planification	

COMPETENCE 14 : S'intégrer en milieu professionnel		
NUMERO : 14	**DUREE D'APPRENTISSAGE** : 315 h	
MODULE ASSOCIE	**Intégration en milieu professionnel**	
FONCTION ET POSITION DE LA COMPETENCE		
Cette compétence est la dernière du programme de formation. Elle arrive au moment où l'apprenant doit commencer son intégration en milieu de travail. A ce moment, l'apprenant devra mettre en pratique dans l'entreprise, les compétences acquises pendant la formation. Les apprentissages à la réalisation de l'intégration en milieu de travail sont complétés, puisque l'intégration en milieu de travail se réalise en entreprise. Cette compétence donne droit à la validation des divers apprentissages réalisés pendant la formation. Elle permet d'acquérir des connaissances et d'attitudes nécessaires pour s'intégrer facilement au milieu de travail, en tenant compte des précisions et en participant aux activités proposées selon le plan de mise en situation.		
DEMARCHE PARTICULIERE A LA COMPETENCE		
La répartition du temps d'apprentissage est suggérée selon les proportions suivantes : 1. Préparer son séjour en milieu de travail : 20% 2. Respecter les principes de discipline et de déontologie : 20% 3. Exécuter les activités en milieu de travail : 30% 4. Comparer ses perceptions aux réalités du métier : 10% 5. Rédiger le rapport de stage : 20% L'ordre des éléments, tel que présenté dans le référentiel de formation devrait rester inchangé.		
Savoirs liés à la compétence	**Balises**	**Activités d'enseignement et d'apprentissage**
1. Préparer son séjour en milieu de travail		
1.1 Prospecter les entreprises	1. Réseau professionnel 2. Choix des entreprises 3. Recherche et démarches pour obtenir un stage	Les éléments de base sur les techniques de recherche et de prospection sont réitérés à l'apprenant par le formateur. L'apprenant reçoit les connaissances sur la rédaction administrative et les restitue à travers les résultats de ses recherches dans le cadre des échanges en groupe.
1.2 préparer un dossier de stage	· Règles de rédaction · Modalités de présentation et de dépôt de la demande · Ressources	

COMPETENCE 14 : S'intégrer en milieu professionnel		
2. Respecter les principes de discipline et de déontologie		
2.1Prendre connaissance du règlement de l'entreprise	• Règlement de l'entreprise • Code de conduite • Code de déontologie • Personnes ressources • Comportement en formation et réalités de l'entreprise	Les éléments essentiels et règles de discipline en vigueur au sein de l'entreprise sont indiqués par le formateur. L'apprenant les reçoit et les intègre dans son comportement pour réussir son cheminement professionnel.
2.2 Présenter son professionnalisme en milieu de travail	• Respect du règlement de l'entreprise • Discipline personnelle • Image de l'entreprise	
3. Exécuter les activités en milieu de travail		
3.1 Observer le contexte de travail	• Produits et marché • Associations professionnelles • Conditions de travail • Relations interpersonnelles • Santé et sécurité	L'apprenant exécute les tâches qui lui sont confiées sous la conduite et la supervision de l'encadreur. Le degré d'acquisition de ses apprentissages est mesuré. L'exécution des tâches permet de consolider les acquis et de démontrer l'adaptabilité aux changements.
3.2 Effectuer diverses tâches professionnelles prescrites	• Méthode de travail • Tâches prescrites • Qualité du travail fait • Economie du temps et des ressources • Utilisation du matériel et des équipements	
3.3 S'adapter à des conditions nouvelles	• Adaptation à des travaux complexes • Nouvelles conditions de réalisation • Evolution technologique • Equipements	
3.4 Relater ses observations sur le contexte de travail et sur les tâches exercées dans l'entreprise	• Milieu de travail • Pratiques professionnelles	
4. Comparer ses perceptions aux réalités du métier		

COMPETENCE 14 : S'intégrer en milieu professionnel		
4.1 Poser un jugement professionnel sur ses actions	1. Perception du métier que l'on a avant le stage avec celle que l'on a après 2. Auto-évaluation • Actions à entreprendre pour combler les écarts	
4.2 Evaluer l'influence de l'expérience sur le choix d'un futur emploi	3. Conséquences du stage sur le choix d'un emploi	
5. Rédiger le rapport de stage		
5.1 Appliquer les techniques de rédaction administrative	• Techniques de rédaction administrative • Eléments de contenu • Informations présentées • Apprentissages réalisés et situations rencontrées en milieu professionnel	Sous la conduite et la supervision de l'encadreur, l'apprenant rédigera son rapport de stage. Il sera jugé sur la qualité du rapport produit et surtout sur le respect des règles de rédaction administrative et de la pertinence des éléments qu'il présente.
5.2 Rédiger le rapport de stage	• Parties importantes d'un rapport • Contenu • Langage à utiliser	

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

GUIDE D'ORGANISATION PEDAGOGIQUE ET MATERIELLE(GOPM)

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

V.1. INTRODUCTION ET PRÉSENTATION DU GUIDE D'ORGANISATION PÉDAGOGIQUE ET MATÉRIELLE

Le guide d'organisation pédagogique et matérielle est un document d'accompagnement à caractère indicatif. En ce sens, l'administration centrale peut prescrire des conditions minimales d'implantation ou des modes de financement communs pour assurer la conformité des dispositifs et des moyens de formation.

Le Guide d'Organisation Pédagogique et Matérielle est un document de soutien. Il est considéré comme le support privilégié pour la mise en application d'un programme de formation. On y trouve l'information visant à combler les différents besoins inhérents aux programmes en matière de modes d'organisation, de ressources humaines, de matériel, d'appareillage et d'outillage, de ressources matérielles et d'aménagement des lieux.

Tenant compte des difficultés que certaines structures de formation pourraient rencontrées, ce guide précise les conditions minimales de mise en place de la formation en fournissant des renseignements sur certains scénarios possibles d'organisation, des données de nature administrative, pédagogique, technique et financière, pouvant être déployés.

Il est conseillé de l'utiliser pour l'implantation des référentiels de formation et d'évaluation dans les structures de formation. Ce document vise les personnes suivantes : les responsables de la gestion centrale (gestionnaires des ressources humaines, financières, physiques et matérielles), les gestionnaires d'établissement et les équipes pédagogiques chargées de la mise en place des nouveaux référentiels et de la formation.

Le guide d'organisation pédagogique et matérielle varie selon le contexte, le type de formation et la nature des besoins de chaque établissement de formation. Il est en fait le scénario retenu faisant suite aux travaux d'élaboration des référentiels de formation et d'évaluation. Il tient compte des décisions pédagogiques et organisationnelles, prises lors de l'élaboration de ces documents.

L'organisation pédagogique repose sur une détermination des besoins, tant quantitatifs que qualitatifs, en matière des ressources humaines.

Le logigramme du référentiel de formation propose d'aborder chaque compétence selon un ordre séquentiel de formation qui conditionne la mobilisation et l'utilisation des diverses ressources requises.

Le chronogramme de formation quant à lui est mis à contribution pour établir le nombre de formateurs nécessaires pour exécuter diverses tâches, préciser les domaines d'intervention qui pourraient être répartis entre ces formateurs, préciser les profils types des formateurs, appropriés à la mise en œuvre d'une formation de qualité. Il met en évidence les besoins de perfectionnement du personnel en place et permet de relever certaines carences portant sur les difficultés à accéder à une expertise plus spécialisée.

Une formation professionnelle de qualité demande un minimum de moyens : ressources humaines, ressources physiques et financières. Dans le cas où les moyens sont limités, de solutions de rechange doivent être trouvées et des modes d'organisation donnant accès à des ressources extérieures ou conduisant à la production des biens et de services doivent être explorés, pour pouvoir atténuer les coûts de formation.

En se basant sur le scénario retenu pour la mise en œuvre de formation, l'équipe de production a défini et présenté les équipements, la matière d'œuvre, les locaux et les aménagements que le projet de

formation demande. Une attention particulière doit être portée à l'utilisation de ces ressources et à l'entretien des équipements, pour garantir leur durabilité.

V.2. BUTS DU RÉFÉRENTIEL DE FORMATION

Le référentiel de formation vise à rendre apte les lauréats de la cybersécurité à évaluer la sécurité d'un système d'information à travers différents angles d'attaques, mais toujours de manière cadrée. Les buts du référentiel traduisent les orientations particulières en matière de formation. Il prépare donc la personne à devenir un travailleur du secteur du numérique pouvant mener des activités de la cybersécurité seul, en équipe ou sous supervision, pour le compte d'une entreprise ou à son compte personnel.
De plus, le référentiel de formation vise à rendre apte le Pentester à réaliser la simulation des attaques malveillantes pour identifier puis exploiter des vulnérabilités au sein du système informatique (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 Pentester.
Dans l'exercice de son métier, le Pentester doit maîtriser l' application des principes de la sécurité des comptes, d'utilisation de l'architecture des systèmes informatiques des réseaux et des protocoles, la Configuration des systèmes d'exploitation, l'utilisation des langages de programmation, l' identification des vulnérabilités potentielles dans les Systèmes informatiques, l'utilisation 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.

Étant donné que le Pentester travaille souvent seul, en équipe ou sous supervision, il doit démontrer de bonnes attitudes relationnelles en milieu de travail ou même dans la société.

V.3. DESCRIPTION DU REFERENTIEL DE FORMATION

Le référentiel de formation de Pentester a été élaboré suivant l'approche par compétences (APC) qui exige, notamment, la participation de partenaires du milieu de travail et du milieu de la formation.
Il a pour objet de professionnaliser le parcours de l'apprenant, lequel construit progressivement les éléments de sa compétence à travers l'acquisition de savoirs et savoir-faire, attitudes et comportements.
Il est formulé par objectifs, conçu selon une approche globale qui tient compte à la fois de facteurs tels les besoins de formation, la situation de travail, les buts ainsi que les stratégies et les moyens pour atteindre les objectifs.
Le référentiel de formation énonce et structure les compétences minimales que l'apprenant doit acquérir au terme de sa formation. Ce référentiel doit servir de référence pour la planification de l'enseignement et de l'apprentissage ainsi que pour la préparation du matériel didactique et du matériel d'évaluation.
Le référentiel de formation de Pentester prévoit une durée de 1350 heures pour la formation dont, 945 heures consacrées aux compétences particulières et 405 heures aux compétences générales soit respectivement 70% et 30 %. Cette durée couvre le temps consacré à la formation, à l'évaluation des apprentissages aux fins de la sanction des études et à l'enseignement correctif.
Le référentiel de formation est composé de 14 modules formés de 7 compétences générales et 7 compétences particulières.

Les modules de formation sont en lien les uns avec les autres et contribuent à l'acquisition des compétences. L'ordre séquentiel de passage des modules est présenté dans le logigramme.
Les liens entre les diverses compétences d'une part et entre les compétences et le processus de travail d'autre part permettent de décrire les compétences et la nature des relations qui les unissent, rendant ainsi cohérent et applicable le référentiel de formation. Les compétences sont traduites en actions observables et en résultats mesurables.
La durée de formation par module va de 30 à 150 heures à l'établissement. Elle est de 315 heures en milieu professionnel.
Le référentiel oriente une formation structurée autour de l'étude de situations donnant aux apprenants l'occasion de :

- comprendre : l'apprenant acquiert les savoirs et savoir-faire nécessaires à la compréhension des situations ;
- agir : l'apprenant mobilise les savoirs et acquiert la capacité d'agir et d'évaluer son action ;
- transférer : l'apprenant conceptualise et acquiert la capacité de transposer ses acquis dans des situations nouvelles.

Les compétences qui y sont développées sont les suivantes :

Tableau synthèse du programme

N°	Énoncé de la compétence	Durée	CS	CG	Unités	Types d'objets	Types de compétences	Titre du Module	Code
1	Se situer au regard du métier et de la formation	30	0	30	2	S	G	Métier et Formation	**MEF01**
2	Communiquer en milieu professionnel	45	0	45	3	S	G	Communication en milieu professionnel	**COM02**
3	Appliquer le principe de la sécurité des comptes	60	0	60	4	S	G	Application du Principe de la sécurité des comptes	**APSCO03**
4	Exploiter l'architecture des systèmes informatiques des réseaux et des protocoles	60	0	60	4	C	G	Exploitation de l'architecture des systèmes informatiques des réseaux et des protocoles	**EAS04**
5	Configurer les systèmes d'exploitation	60	0	60	4	C	G	Configuration des systèmes d'exploitation	**CSE05**
6	Utiliser les langages de programmation	60	0	60	4	C	G	Utilisation des langages de programmation	**ULP06**
7	Identifier les vulnérabilités potentielles dans les Systèmes informatiques	90	90	0	6	C	P	Identification des vulnérabilités potentielles dans les Systèmes informatiques	**IVP07**
8	Tester la vulnérabilité, sur des Réseaux, des applications, site web et les systèmes d'exploitation	120	120	0	8	C	P	Tests de vulnérabilité, sur des Réseaux, des applications, site web et les systèmes d'exploitation	**TVA08**
9	Configurer les outils de test de pénétration des systèmes d'exploitation	150	150	0	10	C	P	Configuration des outils de test de pénétration des systèmes d'exploitation	**COP09**

10	Proposer les stratégies d'atténuation	120	120	0	8	C	P	Proposition des stratégies d'atténuation	**PSA10**
11	Configurer les pares-feux et des systèmes de détection d'intrusions	120	120	0	8	C	P	Configuration des pares-feux et des systèmes de détection d'intrusions	**CPF11**
12	Assurer la veille technologique en cyberattaque	90	90	0	6	C	P	Veille technologique en cyberattaque	**VTC12**
13	Rechercher un emploi	45	0	45	3	S	G	Entreprenariat	**ENT13**
14	S'intégrer en milieu professionnel	315	315	/	21	S	P	Intégration en milieu de travail	**STG14**
	Total	**1356**	**1005**	**360**	**94**				
			73.62%	**26.38%**					

V.4. ORGANISATION DE LA FORMATION

Le guide d'organisation est centré sur les outils et les moyens à mettre en œuvre pour offrir la formation. Il ne traite donc pas des contenus ou des stratégies pédagogiques présentées dans le référentiel de formation et dans le guide pédagogique.

Pour réaliser le volet organisation pédagogique du guide d'organisation, l'ensemble des contenus du référentiel de formation, du guide pédagogique et du référentiel d'évaluation sont pris en considération.

L'organisation de la formation exige une planification qui conduit à déterminer la séquence de mise en œuvre des compétences et leur répartition dans le temps. Pour appuyer ces travaux, il a fallu le logigramme, que l'on retrouve dans le référentiel de formation. Ainsi que le chronogramme figuré dans le guide pédagogique.

Pour compléter cette planification, un tableau proposant un scénario de mise en œuvre de la formation s'ajoute.

Ainsi, se présentent les compétences avec de précisions sur leur mise en œuvre et des contraintes liées auxdites compétences. Pour l'organisation de cette formation, il est aussi nécessaire de connaitre les conditions d'admission au centre de formation et de promouvoir cette formation.

1. Conditions d'admission

L'admission en formation se fait par voie de concours. Les candidats désirant suivre la formation de Pentester doivent avoir au moins le Baccalauréat scientifique ou en informatique/GCE A LEVEL ou tout diplôme équivalent.

Il serait avantageux que les postulants au métier de Pentester sachent lire l'anglais parce qu'ils doivent comprendre et interpréter la documentation technique, rédigée la plupart du temps dans cette langue.

Ils doivent en outre aimer l'Informatique, faire preuve d'un esprit logique et d'un jugement sûr, aimer la lecture et se tenir à date sur les nouvelles technologies. En effet, ce métier exige une capacité d'analyse approfondie pour être en mesure de trouver la bonne solution aux problèmes rencontrés.

Il serait souhaitable de vérifier certaines qualités professionnelles chez les candidats qui désirent être admis au programme :

- Une Éthique professionnelle ;
- Une capacité à travailler sous pression ;
- Une acuité visuelle parfaite ;
- Des gestes précis ;
- Le souci de la qualité du travail ;
- L'esprit d'équipe ;
- La perception artistique ;
- L'esprit d'initiative.

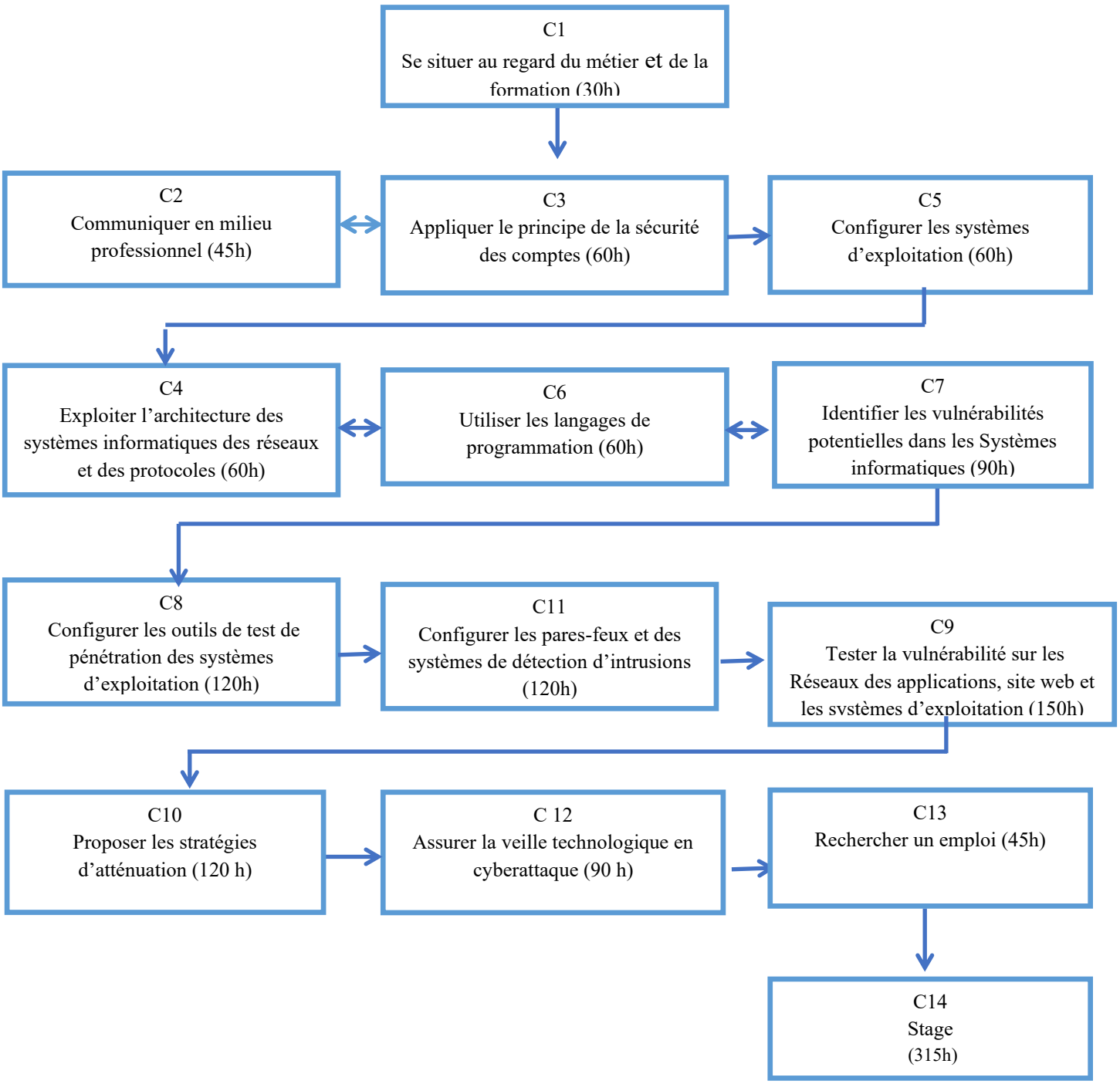
NB. Les diverses séquences de travail imposent le maintien prolongé en position debout

2. Présentation du logigramme

Le logigramme est une représentation schématique de l'ordre d'acquisition des compétences. C'est une séquence de mise en œuvre des compétences, et par conséquent de la mobilisation des ressources humaines, physiques et matériels nécessaires pour la formation. Le logigramme assure une planification du référentiel et présente l'articulation des compétences. Il vise à assurer la cohésion et la progression des apprentissages.

Le logigramme tient compte, pour une compétence donnée, des apprentissages déjà accomplis, de ceux qui se déroulent en parallèle et de ceux qui sont à venir. Son but est de donner une idée globale du déroulement de la formation.

Pour le métier de Pentester, le logigramme est proposé comme suit :


C1
Se situer au regard du métier et de la formation (30h)
C2
Communiquer en milieu professionnel (45h)
C3
Appliquer le principe de la sécurité des comptes (60h)
C5
Configurer les systèmes d'exploitation (60h)
C4
Exploiter l'architecture des systèmes informatiques des réseaux et des protocoles (60h)
C6
Utiliser les langages de programmation (60h)
C7
Identifier les vulnérabilités potentielles dans les Systèmes informatiques (90h)
C8
Configurer les outils de test de pénétration des systèmes d'exploitation (120h)
C11
Configurer les pares-feux et des systèmes de détection d'intrusions (120h)
C9
Tester la vulnérabilité sur les Réseaux des applications, site web et les systèmes d'exploitation (150h)
C10
Proposer les stratégies d'atténuation (120 h)
C 12
Assurer la veille technologique en cyberattaque (90 h)
C13
Rechercher un emploi (45h)
C14
Stage
(315h)

3. Présentation du chronogramme

Le chronogramme de réalisation de la formation est une représentation schématique présentant l'ordre selon lequel les compétences devraient être acquises et la répartition dans le temps, des activités d'enseignement, d'apprentissage et d'évaluation. Il assure une planification globale des compétences du référentiel et présente l'articulation qui existe entre les compétences. Cette planification vise à assurer une cohésion et une progression des apprentissages.

Le chronogramme respecte certaines contraintes organisationnelles à savoir :

- La durée totale du référentiel et celle attribuée à chaque compétence ;
- Le nombre d'heures d'apprentissage hebdomadaire, semestriel et annuel ;
- La logique de la matrice des objets de formation et du logigramme des compétences ;
- Les périodes durant lesquelles le milieu du travail se montre disponible pour organiser la tenue de stage.

Le chronogramme sert à résoudre les questions de définition des tâches du personnel, d'utilisation des locaux d'enseignement et des SCS de travaux pratiques. Il repose sur une situation type et devra être ajusté en fonction de la situation réelle de chaque structure de formation. Il peut également être modifié à chaque période de l'année, en fonction des contraintes locales.

Pour le métier de Pentester, le chronogramme est proposé comme suit :

CHRONOGRAMME

	Compétences particulières							Compétences générales							
Numéro	**7**	**8**	**9**	**10**	**11**	**12**	**14**	**1**	**2**	**3**	**4**	**5**	**6**	**13**	**T**
Durée (H)	**90**	**120**	**150**	**120**	**120**	**90**	**315**	**30**	**45**	**60**	**60**	**60**	**60**	**45**	**1365**
Semaine															
1								30							30
2									10	10	10	5			35
3									10	10	10	5			35
4									10	10	10	5			35
5										10	10	10	5		35
6										10	10	10	5		35
7										10	10	10	5		35
8	10	5										10	10		35
9	10	10										5	10		35
10	10	10	5										10		35
11	10	10	5										10		35
12	10	10	5										10		35
13	10	10	5										10		35
14	10	10	5										10		35
15	10	10	5										10		35
16	10	10	5										10		35
17		10	10	5									10		35
18		10	10	10	5										35
19		10	10	10	5										35
20		10	10	10	5										35
21			10	10	10	5									35

22			10	10	10	5									35
23			10	10	10	5									35
24			10	10	10	5									35
25			10	10	10	5									35
26			10	10	10	5									35
27			10	10		15									35
28			5	15		15									35
29						15								20	35
30														20	20
31														5	5
32							40								40
33							40								40
34							40								40
35							40								40
36							40								40
37							40								40
38							40								40
39							35								35
TOTAL	**90**	**120**	**150**	**120**	**120**	**90**	**315**	**30**	**45**	**60**	**60**	**60**	**60**	**45**	**1365**

4. Modes d’organisation à privilégier

Le mode d’organisation de la formation pourrait être compris à travers le tableau ci-dessous qui présente l’ensemble des compétences, la durée réservée à chaque compétence, la nature des activités, les installations physiques, les équipements spécialisés et le commentaire lié à chaque compétence.

Ce tableau précise les caractéristiques et les principales contraintes rattachées à la mise en œuvre des compétences.

La nature des compétences renseigne sur la répartition de temps pour la formation théorique et la formation pratique. Cette information est fournie à titre indicatif et peut être variée en fonction du contexte et des caractéristiques de l’environnement d’apprentissage.

Le tableau présente également les principales exigences en matière d’organisation physique et matérielle de la formation.

Les stages en entreprise et les autres activités sont mentionnés dans la colonne « commentaires ».

Le scénario de mise en œuvre de cette formation se présente comme suit :

N°	Titre du module	Compétences	Durée(h)	Nature des activités (T ou P)	Locaux ou installation physiques	Équipements spécialisés
1	Métier et Formation	Se situer au regard du métier et de la formation	30	100% T	En salle de classe ou en SCS	Non
2	Communication en milieu professionnel	Communiquer en milieu professionnel	45	70 % T, 30% P	En salle de classe, SCS	Ordinateur, vidéo projecteur
3	Application du Principe de la sécurité des comptes	Appliquer le principe de la sécurité des comptes	60	30 % T, 70% P	En salle de classe, SCS	Vidéo projecteur, ordinateur, connexion internet
4	Exploitation de l'architecture des systèmes informatiques des réseaux et des protocoles	Exploiter l'architecture des systèmes informatiques des réseaux et des protocoles	60	70 % T, 30% P	En salle de classe en SCS.	Vidéo projecteur, ordinateur, connexion internet
5	Configuration des systèmes d'exploitation	Configurer les systèmes d'exploitation	60	70 % T, 30% P	En salle de classe en SCS.	Vidéo projecteur, ordinateur, connexion internet, logiciels
6	Utilisation des langages de programmation	Utiliser les langages de programmation	60	70 % T, 30 % P	En salle de classe en SCS	Vidéo projecteur, ordinateur, connexion internet, logiciels.

N°	Titre du module	Compétences	Durée(h)	Nature des activités (T ou P)	Locaux ou installation physiques	Équipements spécialisés
7	Identification des vulnérabilités potentielles dans les Systèmes informatiques	Identifier les vulnérabilités potentielles dans les Systèmes informatiques	90	30 % T, 70 % P	En salle de classe en SCS	Vidéo projecteur, ordinateur, connexion internet, logiciels
8	Tests de vulnérabilité, sur des Réseaux, des applications, site web et les systèmes d'exploitation	Tester la vulnérabilité, sur les Réseaux, les applications, site web et les systèmes d'exploitation	120	30 % T, 70 % P	En salle de classe en SCS	Vidéo projecteur, ordinateurs, connexion internet, logiciels
9	Configuration des outils de test de pénétration des systèmes d'exploitation	Configurer les outils de test de pénétration des systèmes d'exploitation	120	30 % T, 70 % P	En salle de classe en SCS	Vidéo projecteur, ordinateurs, connexion internet, logiciels
10	Proposition des stratégies d'atténuation	Proposer les stratégies d'atténuation	150	30 % T, 70 % P	En salle de classe en SCS	Vidéo projecteur, ordinateurs, connexion internet, logiciels
11	Configuration des pares-feux et des systèmes de détection d'intrusions	Configurer les pares-feux et des systèmes de détection d'intrusions	120	30 % T, 70 % P	En salle de classe en SCS,	Vidéo projecteur, ordinateurs, connexion internet, logiciels

N°	Titre du module	Compétences	Durée(h)	Nature des activités (T ou P)	Locaux ou installation physiques	Équipements spécialisés
12	Veille technologique en cyberattaque	Assurer la veille technologique en cyberattaque	90	30 % T, 70 % P	En salle de classe en SCS	Vidéo projecteur, ordinateurs, connexion internet, logiciels
13	Entreprenariat	Rechercher un emploi	45	40 % T, 60 % P	En salle de classe en SCS	Vidéo projecteur, ordinateurs, connexion internet, logiciels.
14	Intégration en milieu professionnel	S'intégrer en milieu professionnel	315	100%P	En Entreprise	Ordinateur, connexion internet, logiciels

5. Promotion du programme

Il appartient aux établissements d'enseignement ou au ministère de la formation professionnelle de faire la promotion de leurs programmes de formation professionnelle auprès de la population en général, des apprenants potentiels et d'éventuels employeurs et, à cet égard, diverses pistes peuvent être exploitées. La promotion peut prendre différentes formes allant de journées portes ouvertes complétées par des visites guidées, jusqu'à la présence de stands à l'occasion de foires ou de salons thématiques.

Voici quelques éléments de promotion pouvant être mis en avant :

- Les perspectives d'emploi et les conditions de travail.
- La qualité de la formation assurée notamment par des formateurs expérimentés qui maîtrisent tous les aspects du métier de Pentester ;
- L'environnement scolaire dont le dispositif de formation et les exigences permettent de recréer le plus possible le contexte réel de travail ;
- L'approche de formation axée sur la pratique en relation étroite avec les compétences déterminées avec les partenaires du monde de travail ;
- La possibilité d'obtenir une qualification basée sur un ensemble de compétences retenues en relation avec l'exercice du métier ;
- Les conditions d'admissions à la formation.

V.5.RESSOURCES HUMAINES

Ce chapitre précise les besoins de formateurs / enseignants et de personnel de soutien. Il fournit les données pertinentes pour la sélection, la formation et le perfectionnement du personnel ou l'attribution des tâches aux employés. L'information fournie est à titre de suggestion.

Pour le choix du personnel et l'organisation du travail, on prend en compte les accords de travail et les conventions en vigueur. Ce chapitre détermine également les domaines dans lesquels il serait recommandé de proposer des activités de perfectionnement. Les formateurs sont des personnes ayant une bonne expérience en cybersécurité.

Même si la réussite de la mise en œuvre du programme dépend en grande partie de la compétence et de l'expérience professionnelle du personnel formateur en matière de pédagogie, de docimologie et d'andragogie, il sera peut-être souhaitable de recourir aux services de techniciens ou de spécialistes du métier.

La présente partie du Guide formule certaines suggestions à considérer au moment de choisir de nouveau personnel ou d'attribuer des tâches au personnel déjà en place.

1. Qualifications professionnelles

Pour former une équipe de formateurs efficace, la correspondance entre les caractéristiques des compétences du programme et l'expérience acquise dans la profession est prise en compte. De plus, l'affectation en priorité du personnel formateur dans son champ de compétence pourrait constituer un élément supplémentaire permettant d'assurer la qualité de l'enseignement.

Les formateurs du programme de Pentester sont appelés à faire état des savoirs et des compétences suivantes :

- Une capacité à enseigner et à communiquer ;
- Une formation en Administration Système et Réseaux Informatique ;
- Des habiletés en cybersécurité, développement d'application et serveur Web, protocole réseau et technologie de sécurité ;
- Des habiletés et aptitudes en illustrant de manière claire et pratique les techniques de tests d'intrusion, des propositions de correction et de production des rapports;
- Des habiletés en analyse des résultats des tests de vulnérabilité ;
- Capacité de créer et gérer des environnements de laboratoire virtuel ;
- Capacité à résoudre des problèmes de sécurité complexes de manière proactive ;
- Une éthique professionnelle et une compréhension approfondie des implications légales et éthiques liées au test d'intrusion ;
- Une veille technologique constante.

En outre, les qualités suivantes sont souhaitées :

- la capacité de s'exprimer clairement et de communiquer;
- la polyvalence;
- le sens de l'organisation et de la planification;
- la capacité de diriger une équipe de travail;
- la capacité de superviser des activités;
- la disponibilité;
- la capacité de se perfectionner;
- L'esprit d'équipe ;
- L'habilité manuelle et technique.

2. Besoins quantitatifs en matière de ressources humaines

Pour l'implantation du référentiel de formation professionnelle du métier de Pentester, le besoin exprimé en ressources humaines est le suivant :

Qualité	Nombre	Niveau académique	Formation professionnelle	Expérience professionnelle
Formateur spécialiste	2	Baccalauréat +3 ans	Spécialiste en Cybersécurité	Au moins 2 ans
	2	Baccalauréat +3 ans	Administrateur des systèmes et Réseaux	Au moins 2 ans
Technicien en Maintenance des Réseaux Informatiques	1	≥ BT	Souhaitée Ingénieur ou BTS en Maintenance des Réseaux Informatiques	Au moins 3 ans
Spécialiste en Génie logiciel	1	Baccalauréat +3 ans	≥licence ou équivalent	Au moins 3 ans
Spécialiste en droit des TIC	1	Baccalauréat +3 ans	≥licence ou équivalent	Au moins 3 ans

La répartition des tâches devrait tenir compte de l'organisation horaire proposée dans le chronogramme de formation ainsi que de l'organisation mise en œuvre par l'équipe pédagogique (chef d'unité, responsable des stages et insertion, professionnels divers).

3. Orientation du recrutement et compétences recherchées

Pour le recrutement de nouveaux formateurs, il est recommandé :

- les diplômés des grandes écoles de l'Enseignement Technique et professionnelle justifiant d'une expérience d'au moins deux ans (02) dans le domaine de compétence ;

- un baccalauréat auquel on aura associé au moins trois (03) années d'expériences avérées dans le domaine de compétence ;
- Une expérience de 10 ans au moins pour les titulaires d'un Bac Scientifique ou en TIC ou équivalent dans son domaine de compétence ;
- Une expérience de 15 ans au moins pour les non diplômés mais ayant acquis l'expérience sur le tas.

De plus, une formation en pédagogie (plus précisément selon l'Approche Par Compétences) est essentielle et devra être acquise au moment de l'embauche ou assurée le plus tôt possible après le recrutement.

4. Perfectionnement des formateurs

L'implantation du référentiel de formation demande le perfectionnement des formateurs. Pour cela, ils devraient demeurer en rapport avec l'entreprise pour être informer des nouvelles techniques et d'équipements nouveaux. À cet effet, le perfectionnement pourrait faire l'objet les domaines suivants :

Domaine technique

- Les systèmes d'exploitation
- les Logiciels de test d'intrusion ;
- les logiciels de sécurité;
- les logiciels de simulation;
- Les logiciels de traitement de texte :

Domaine pédagogique

Il est difficile de trouver un expert du métier ayant une formation pédagogique adéquate. Il est relativement facile de recruter des formateurs ayant une bonne maîtrise des compétences du métier visé. Pour cela, une formation de base s'impose pour la majorité des personnes recrutées pour la formation professionnelle. Il est en effet utile de réaliser un bilan de compétences de la personne recrutée afin de déterminer les besoins de perfectionnement, en tenant compte du personnel déjà en place et du personnel de soutien. Les besoins de perfectionnement peuvent concerner les volets de la planification et de la préparation des activités de formation et d'évaluation, les diverses méthodes à utiliser pour donner la formation, l'utilisation des équipements et de matériel pédagogiques et didactiques, etc. Les aspects plus distincts du référentiel de formation peuvent s'y ajouter. Pour ces activités, le guide pédagogique peut servir de référence de base.

Domaine de l'Approche par les Compétences

Il faut offrir aux formateurs, sans tenir compte de leur niveau de maîtrise du métier, une formation portant sur l'APC, approche utilisée pour élaborer le référentiel de formation et les guides d'accompagnement, pour apporter un soutien à l'implantation du référentiel de formation.

Pour cette formation, les thèmes abordés peuvent être par exemple l'appropriation du contenu du référentiel de formation, la lecture et l'interprétation de la matrice des objets de formation, l'utilisation des tableaux de spécification, etc.

L'APC implique une relation avec l'entreprise pour suivre l'évolution des nouveaux produits, des nouvelles technologies et des nouvelles techniques. A cet effet, les formateurs doivent participer aux colloques et aux journées d'information ou expositions organisées en collaboration avec les spécialistes du métier.

Des stages pratiques de courte durée en milieu professionnel peuvent aussi être une autre possibilité.

Domaine de la santé, l'hygiène, sécurité et environnement

Ce volet de perfectionnement implique la prise en charge de la prévention liée au mieux-être au travail. Ceci inclut les connaissances, les habilités et les attitudes pour préparer dans les bonnes conditions les personnes en emploi. Le souci de prévention doit être une préoccupation importante à intégrer dans l'apprentissage de tout métier ou de toute profession. Cette prévention doit s'appliquer dans l'exécution de toutes les tâches au cours des apprentissages et de l'évaluation.

Que ce soit sur le plan de la sécurité personnelle ou de protection de l'environnement, la démarche de prévention comporte trois étapes :

- Repérer les dangers et les facteurs de risque ;
- Corriger les situations à problèmes ;
- Prendre des dispositions pour éviter les problèmes.

Pour s'assurer que les formateurs maîtrisent les différents contours de la formation, un perfectionnement spécial devrait les accompagner.

V.6. ORGANISATION PHYSIQUE ET MATÉRIELLE

Pour déterminer les besoins en matière de ressources physique et matérielles, il faut une analyse systématique des informations liées à chaque compétence du référentiel de formation. Ces informations sont complétées par le contenu du référentiel d'évaluation. Les éléments de la compétence, le contexte de réalisation du référentiel de formation, les indicateurs et les critères d'évaluation fournissent la majorité des informations concernant les ressources physiques et matérielles.

Les fiches de suggestions pédagogiques fournissent les informations manquantes.

Une catégorisation des ressources physiques et matérielles nécessaires facilite le relevé des besoins et des conditions d'implantation des référentiels. La catégorisation regroupe les éléments ayant les caractéristiques communes et élabore des devis d'implantation ou de mise à niveau des dispositifs de formation. Une telle catégorisation aide à mettre en place ou à réviser les modalités de financement de la formation et d'entretien du parc d'équipements.

6.1.RESSOURCES MATERIELLES

Ce volet présente la liste des ressources matérielles nécessaires à la mise en œuvre du référentiel du métier Pentester

Les quantités proposées prennent en compte 25 apprenants et les ressources nécessaires pour le formateur.

Les tableaux ci-dessous présentent les ressources nécessaires classées par catégorie.

6.1.1. Machinerie, équipement et accessoires

Cette catégorie comprend les machines-outils. Ce sont des ensembles de mécanismes ou de pièces servant à exécuter un travail. Cette catégorie comprend aussi les accessoires, soit tout objet qui complète la machine ou un équipement. Elle inclut également les pièces de rechange, nécessaires à l'entretien et au bon fonctionnement des différentes machines-outils et équipements.

N°	Désignation	Description	Type de local	Compétence	Quantité
1	Desktop	Intel Core i7 2.5Ghz 10ième génération, Nvidia/AMD 4Go de dédié, 16Go de RAM DDR4, 1To SSD, Ecran 21 pouces, Claviers AZERTY/QWERTY Souris USB Windows 10/11 avec licence, Carte réseau GigaByte (sans fil), Lecteur CD/DVD	SCS	2,3,4,5,6,7,8,9,10,11,12	25
2	Laptop	Intel Core i7 2.5Ghz 10ième génération, Nvidia/AMD 2Go de dédié, 16Go de RAM DDR4, 5 12 SSD, Écrans 15.6 pouces, Windows 10/11 avec licence	Salle de classe et SCS	3,4, 5, 6, 7, 8, 9, 10, 11,12	26
3	Câblage connexion internet	• Type de connexion : Fibre optique • Bande Passante : 10Mbps dédiée • Latence : faible • Stable : Oui • Adresse IP : IPv4 (32 bits) et IPv6 (128 bits)	SCS	3, 4, 5, 6, 7, 8, 9, 10, 11,12	1

N°	Désignation	Description	Type de local	Compétence	Quantité
		Sécurité : Firewall, chiffrement			
4	Switch	Nombre de ports , 48 ports Type de port : RJ45, Il faut des switch manageables	SCS	3, 4, 5, 6, 7, 8, 9, 10, 11,12	1
5	Routeur	Routeur sans fil – commutateur 8 ports (intégré) Débit de transfert de données : 1 Gbits-s Protocole de liaison de données : Ethernet, Fast Ethernet, Gigabit Ethernet, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n Antenne : Détachable externe Nombre d'antennes : 2 Protection par firewall, DMZ port, compatible DHCP, prise en charge NAT, Prise en charge VPN, prise en charge PAT, prise en charge du réseau local (LAN) virtuel, filtrage de contenu, prise en charge d'IPv6, IPS (Intrusion Prevention System), filtrage de l'URL, possibilité d'évolution vers de nouveaux micrologiciels, IPSec Virtual Private Network (VPN), chiffrement WPA2, qualité de service (QDS), Dead Peer Detection (DPD), IPSec NAT-traversé (NAT-T), Wi-Fi Protected Setup (WPS), serveur DHCP, prise en charge SSID multiple, contrôle de la bande passante, technologie D-Link Green	SCS	3, 4, 5, 6, 7, 8, 9, 10, 11,12	1

N°	Désignation	Description	Type de local	Compétence	Quantité
6	Onduleurs	Système d'alimentation sans interruption Modele : SMC1500VA Marque : APC Puissance: 1500VA Technologie: Line interactive Tension D'entrée nominale : 230V	SCS	3, 4, 5, 6, 7, 8, 9, 10, 11,12	25
7	Groupe électrogène	Groupe électrogène triphasé Modèle : standard Carburant : diesel Vitesse : 1500 t/min Puissance continue : 10 KVA / 8000 W Puissance maximale : 11 KVA / 8800 W Puissance du moteur : 15 HP (ch) Tension : 400 V Capacité du réservoir : 60 L Consommation (à 75 %) : 2,5 L/h Autonomie à 75 % : 24 h Refroidissement par air Dimensions : 1600 x 700 x 1100 mm Poids : 350 kg Démarrage manuel ou automatique (au choix)	SCS	1,2;3,4,5,6,7,8,9,10,11,12,13	1
8	Serveur hôte	Processeur Intel Xeon E5-2690 v4 ou supérieur 128 Go de RAM ou plus 2 To de stockage SSD ou plus	SCS	3, 4, 5, 6, 7, 8, 9, 10, 11,12	1

6.1.2. Outils et instruments

Cette catégorie englobe une variété d'outils spécialisés utilisés par les pentesters pour explorer et identifier les vulnérabilités informatiques, effectuer des tests d'intrusion et exécuter des attaques simulées sur des systèmes cibles. Pour permettre aux apprenants de pratiquer en toute sécurité les techniques de test d'intrusion, des environnements de laboratoire virtuel équipés de ces outils les seront fourni par les formateurs.

N°	Désignation	Caractéristiques principales/Description	Type de local	Compétence	Quantité
1	Éditeur de code	Sublime Text	SCS et SC	3, 4, 5, 6, 7, 8, 9, 10, 11,12	1
		Atom			1
		Notepad			1
2	Analyseur de protocoles	Wireshark		3,4, 5, 6, 7, 8, 9, 10, 11,12	1
		Tcpdump			1
		Ethereal :			1
		Microsoft Network Monito			1
4	IDE outils de développent intégré	IntelliJ,	SCS et SC	3, 4, 5, 6, 7, 8, 9, 10, 11,12	1
		Eclipse,			1
		Visual Studio code			1
		NetBeans,			1
4	Outils de Test d'intrusion	Kali Linux	SCS et SC	3, 4, 5, 6, 7, 8, 9, 10, 11,12	1
		Burp Suite			1
		Metasploit			1
		OWASP ZAP			1
		Metasploit Framework			1
		Burp Suite			1
		Wireshark			1
		John the Ripper			1
		Aircrack-ng			1
		SQLMap, ,			1
		Netcat (nc),			1

N°	Désignation	Caractéristiques principales/Description	Type de local	Compétence	Quantité
		ZAP (Zed, Attack Proxy)			1
5	Logiciel client FTP	FlileZilla,	SCS et SC	3, 4, 5, 6, 7, 8, 9, 10, 11,12	1
		Jenkins,			1
		Ansible,			1
		Puppet,			1
		Kubernetes, etc.			1
6	Serveurs web	Apache,	SCS et SC	3, 4, 5, 6, 7, 8, 9, 10, 11,12	1
		Nginx,			1
		IIS (Internet Information Services)			1
		Lighttpd			1
7	Système de Gestion des Base de Données (SGBD)	Oracle	SCS et SC	3, 4, 5, 6, 7, 8, 9, 10, 11,12	1
		MySql,			1
		Microsoft SQL Serveur			1
		Postgres SQLetc.			1
8	Logiciel de modélisation de base de données	PowerAMC (pour modélisation merise)	SCS et SC	3, 4, 5, 6, 7, 8, 9, 10, 11,12	1
		Algo UML			1
		Windesign pour UML			1
9	Logiciel de gestion de projet	Gantt Projet,	SCS et SC	3, 4, 5, 6, 7, 8, 9, 10, 11,12	1
		Gira,			1
10	Logiciel de bureautique	Suite office 2019	SCS et SC	3, 4, 5, 6, 7, 8, 9, 10, 11,12	1
		Polaris office			1
11	Logiciel de Design	Figma	SCS et SC	3, 4, 5, 6, 7, 8, 9, 10, 11,12	1
		Adobe XD			1
		Origami Studio			1
12	Logiciel de documentation	Document 360	SCS et		1

N°	Désignation	Caractéristiques principales/Description	Type de local	Compétence	Quantité
		Google Chrome, ,	SC	3, 4, 5, 6, 7, 8, 9, 10, 11,12	1
13	Navigateurs	Mozillia FireFox,	SCS et SC	3, 4, 5, 6, 7, 8, 9, 10, 11,12	1
		Edge			1
		Google Chrome, ,			1
14	Lecteurs et éditeurs de PDF	Nitro	SCS et SC	3, 4, 5, 6, 7, 8, 9, 10, 11,12	1
		Adobe Reader			1
		Foxit Reader			1
15	Service cloud	Amazon Web Service,	SCS et SC	3, 4, 5, 6, 7, 8, 9, 10, 11,12	1
		Google Cloud			1
		Microsoft Azur			1
16	Clé USB	Capacité : 32Go	SCS, salle de formateur, SC	3, 4, 5, 6, 7, 8, 9, 10, 11,12	10
17	CD/DVD	Capacité : 02Go et 04Go	SCS, salle de formateur, SC	3, 4, 5, 6, 7, 8, 9, 10, 11,12	1 Paquets de 100
18	Disque Dur externe	Capacité : 1To	SCS, salle de formateur, SC	3, 4, 5, 6, 7, 8, 9, 10, 11,12	10

6.1.3. Matériels de sécurité

Cette partie concerne tout outil nécessaire à la sécurité au travail.

N°	Désignation	Caractéristiques principales/Description /Description	Type de local	Compétence	Quantité
20	**Logiciels de sécurité informatique**	**Fonctionnalités :** • Analyse en temps réel • Analyse à la demande • Mises à jour régulières • Quarantaine et suppression des menaces • Protection en temps réel des courriels et des navigateurs • Options de personnalisation • Licence et version : Abonnement annuel payant **Logiciels :** • Avast Antivirus • McAfee Antivirus • Norton Antivirus • Kaspersky Antivirus • Bitdefender Antivirus	SCS	3, 4, 5, 6, 7, 8, 9, 10, 11,12	28
		Pare-feu : pour surveiller et contrôler le trafic réseau entrant et sortant, et ainsi protéger contre les attaques provenant d'Internet.	SCS	3, 4, 5, 6, 7, 8, 9, 10, 11,12	-25
21	**VPN (Réseau Privé Virtuel)**	Permet au pentester de crypter son trafic Internet et de masquer son adresse IP	SCS	3, 4, 5, 6, 7, 8, 9, 10, 11,12	01

22	**Équipement de protection individuelle (EPI)**	**Lunettes de protection** : pour protéger les yeux lors de l'utilisation d'outils informatiques ou de matériel de test.	SCS	3, 4, 5, 6, 7, 8, 9, 10, 11,12	30
		Gants : pour protéger les mains lors de la manipulation de matériel potentiellement dangereux ou lors de tests physiques.	SCS	3, 4, 5, 6, 7, 8, 9, 10, 11,12	25
23	**Matériel de test spécialisé**	**Testeurs de tension et de continuité** : utilisés pour vérifier la sécurité électrique des installations.	SCS	3, 4, 5, 6, 7, 8, 9, 10, 11,12	25
		Détecteurs de gaz : pour identifier la présence de gaz toxiques ou inflammables dans l'environnement de travail.	SCS	3, 4, 5, 6, 7, 8, 9, 10, 11,12	2
24	**Dispositifs de sécurité physique**	**Serrures et badges d'accès** : pour limiter l'accès aux locaux sensibles où se déroulent les tests d'intrusion.	SCS	3, 4, 5, 6, 7, 8, 9, 10, 11,12	30
		• Alimentation : transformateur 52V 1,5A (fourni) • Sorties vidéo : 1 HDMI + 1 VGA • Résolution : 3MP • Type de connexion : POE (RJ45 cat. 6) • Nombre de canaux : 4 • Stockage : Sur disque dur SATA en option jusqu'à 10To • Port USB : 2 USB 2.0 • Température d'utilisation : -10°C--+55°C • Ajustement automatique de la luminosité • Vision nocturne	SCS	3, 4, 5, 6, 7, 8, 9, 10, 11,12	1

		• Flash lumineux lorsque la luminosité est faible • Détection de formes humaines • Caméra rotative pour une vision 360° • Mise au point longueur : 3.6mm • Distance de vision : 15m • Indice de protection : IP66 équipement étanche à la poussière et protégé contre les projections d'eau.			
25	Extincteur à poudre	Capacité : poudre de 5 kg. Type ABC avec supports murales et ancrages appropriés.	SCS	3, 4, 5, 6, 7, 8, 9, 10, 11,12	3
26	Trousse de premiers soins	Selon les normes exigées	SCS	3, 4, 5, 6, 7, 8, 9, 10, 11,12	2

6.1.4. Matière d'œuvre et matière première

Dans cette section, on précise la matière d'œuvre nécessaire à la prestation du programme à un groupe de 25 élèves.

N°	Désignation	Caractéristiques principales/Description	Type de local	Compétence	Quantité
1	Abonnement internet	Accès à internet par fibre optique, Bande passante : 20Mbt/s	SCS	3,4,5,6,7,8,9,10,11,12	1
2	Clé USB	Capacité : 32Go	SCS, salle de formateur, SC	3,4,5,6,7,8,9,10,11,12	10
3	CD/DVD	Capacité : 2Go et 04Go	SCS, salle de formateur, SC	3,4,5,6,7,8,9,10,11,12	1 paquet de 100
4	Disque dur externe	Capacité : 1To	SCS, salle de formateur, SC	3,4,5,6,7,8,9,10,11,12	05
5	Claviers	AZERTY / QXERTY	SCS	3,4,5,6,7,8,9,10,11,12	10
6	Souris	Souri USB	SCS	3,4,5,6,7,8,9,10,11,12	10
7	Cartouche d'encre	Compatibles à l'imprimante	SCS, salle de formateur, SC	3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14	10
8	Bloc note	Format A5 : 14,5 x 21 cm Grammage : 80 g/m² Quadrillage 5 x 5mm	SCS, salle de formateur, SC	3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14	25
9	Rame de Papier	Format A4 : 21 x 29,7 cm Grammage : 80 g/m²	SCS, salle de formateur, SC	3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14	5
	Câble réseau	Type : 4 paires torsadées blindé, Catégorie : 6, Norme : 10 bases T, Débit nominatif : 10-100Mb/s	SCS	3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14	
	Prise électrique	Nature : prise apparente, 16A ; 250V, proches : 3	SCS et SC	3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14	

	Clavier Destop	Identique à celui venu avec le Destop	SCS	3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14	
	Souris	Identique à celle venu avec la Destop	SCS	3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14	
	Goulotte	Type : PVC pour les murs et en bois pour le sol Épaisseur : en fonction de l'installation de la salle	SCS et SC	3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14	

6.1.5. Mobilier et équipement de bureau

Cette section précise les ameublements non fixés et non intégrés aux immeubles, par exemple des chaises, des pupitres des bureaux, des tables de travail, des fauteuils, etc.

N°	Désignation	Caractéristiques principales/Description	Type de local	Compétence	Quantité
1	Table formateur	1500x750X750 mm	SC	1à12	5
2	Tables des apprenants	Tables de 2 places avec casier	SC	1à12	13
3	Chaises	Chaise une place, avec mousse et confortable pour le dos	Salle spécialisée, SC, bureau du formateur	1à12	56
4	Tables 2 places d'ordinateurs	• 2 Tiroirs pour clavier • 2 Boxes pour Unité centrale • 160x80x76 cm	Salle spécialisée	1à12	13
5	Tableau blanc	1m40x1m40	SC, salle spécialisée	1à12	2
6	Imprimante Multifonction	• Imprimante	Bureau formateur	1à12	1
7	Armoire de rangement	En métal, 0,82mx1, 22mx0, 33m	Salle de maintenance	1à12	2
8	Bibliothèque	1220x1800x300mm en bois massif	Bureau formateur	1à12	1
9	Chaise pour personnel enseignant	Noire, ajustable (hauteur et dos) 5 roulettes	Bureau formateur	1à12	4

N°	Désignation	Caractéristiques principales/Description	Type de local	Compétence	Quantité
10	Classeur	Brand format, ouverture latérale (3 tiroirs), métal	Bureau formateur	1à12	2
11	Poubelle de bureau	Plastique 380x350x400mm	Bureau formateur, salle spécialisée, SC	1à12	3
12	Présentoir pour revues	4 tablettes réglables, métallique 200x1850mm	Bureau formateur	1à12	1

6.1.6. Matériel audiovisuel et informatique.

Cette section précise les appareils, équipements associés à l'informatique, par exemple, un ordinateur, un projecteur, une imprimante, un logiciel et un didacticiel, un film, une vidéocassette, un diaporama, etc.

N°	Désignation	Caractéristiques principales/Description	Type de local	Compétence	Quantité
1	Ecran de projection	Au mur ou mobile	Salle multimédia	2 à 12	2
2	Lecteur DVD et moniteur (TV) :	Avec support, TV, LCD de 100 mm	Salle multimédia	2 à 12	1
3	Vidéoprojecteur	2500 lumens avec deux lampes supplémentaires et tous les raccords pour l'ordinatrice alimentation de 220-1-50	Salle multimédia	2 à 12	1
6	Classeur latéral	A devants fixes, 4 tiroirs	Bureau formateur	2 à 12	3
8	Classeur de dessus de bureau	En plastique, trois niveaux pour format A4	Salle de classe	2 à 12	25
2	Photocopieur/scanneur	Pour multiplication des documents, canon IR 3035	Salle multimédia	2 à 12	2
6	Imprimante	Pour impression des documents, Hp laser couleur	Salle multimédia	2 à 12	3
7	Ordinateur Desktop	Disque dur 500 Go, Mémoire vive 8 Go processeur core i7 de 2 GHZ Lecteur-graveur CD-DVD carte graphique, cartes	Salle multimédia	2 à 12	25

N°	Désignation	Caractéristiques principales/Description	Type de local	Compétence	Quantité
		réseaux, 3 Ports USB, Clavier AZERTY, Souris USB, ports VGA ou HDMI pour les projecteurs, système d'exploitation Windows 10 ou 11			
8	Réseau Ethernet	Système pour 24 machines et tous les appareils informatiques et bureautiques en réseau	Salle multimédia	2 à 12	1
9	Réseau sans fil, WIFI	Système pour que l'ensemble des unités informatiques installées soient connectées dans le périmètre du centre de formation	Salle multimédia	2 à 12	1
10	Outil de rédaction des rapports	MS Word 2019	Salle multimédia	2 à 12	30
11	Outil de présentation	MS Powerpoint 2019	Salle multimédia	2 à 12	30

6.1.7. Matériel didactique

Cette section précise les livres, dictionnaires, manuels techniques et fascicules destinés aux apprenants, ouvrages de référence et revues, cartes, diagrammes, tableaux et graphiques, planches, etc.

N°	Désignation	Description	Type de local	Compétence	Quantité
1	Ouvrage de référence et revues	• Voir références à la fin du document • Ensemble des volumes de la bibliothèque du département de soudage.	SC	2 à 12	2
2	Cartes, chartes, tableaux, graphiques etc.	• Affiches de sécurité, documents descriptifs des machines de l'SCS et du laboratoire.	SC	2 à 12	1

N°	Désignation	Description	Type de local	Compétence	Quantité
3	Document information	• La santé et la sécurité dans les SCSs de formation	BF	2 à 12	10
5	The Legal Guide to Penetration Testing	• Auteur : Ben Halpert • Date de publication : 2016 • Maison d'édition : CreateSpace Independent Publishing Platform • Nombre de pages : Environ 200 pages	BF	2 à 12	10
6	"Professional Penetration Testing: Creating and Learning in a Hacking Lab	• Auteur : Thomas Wilhelm • Date de publication : 2013 • Maison d'édition : Syngress • Nombre de pages : Environ 400 page	BF	2 à 12	
	The Hacker Playbook: Practical Guide to Penetration Testing"	• Auteur : Peter Kim • Date de publication : 2014 • Maison d'édition : CreateSpace Independent Publishing Platform • Nombre de pages : Environ 360 pages	BF	2 à 12	28
	Cybersecurity Law"	• Auteur : Jeff Kosseff • Date de publication : 2018 • Maison d'édition : Wiley • Nombre de pages : Environ 528 pages	BF	2 à 12	28
10	Introduction au Pentesting	• Auteur : Vlad & JP ; • Date de publication :2021; • Maison d'édition :Campus du Libre,	SC	2 à 12	28

N°	Désignation	Description	Type de local	Compétence	Quantité
		• , Nombre de pages :, 35 pages			
	Hacking: The Art of Exploitation"	• Auteur : Jon Erickson □ • Date de publication : 2003 • Maison d'édition : No Starch Press • Nombre de pages : Environ 488 pages	BF	2 à 12	28
11	**Hacker's Guide: Sécurité informatique et pentests**	• Auteur : Eric Charton, Marc Dacier, Nicolas Ruff, • Date de publication :1 janvier 2017, • Maison d'édition : ENI, • Nombre de page :552 P	SC	2 à 12	28
12	**Le Guide Complet de l'Hacker Éthique**	• Auteur: Kim Nilsson, • Date de publication:23 October 2020 • Maison d'édition: independently • published, • Nombre de page :, 409 pages.	SC	2 à 12	28

6.2. RESSOURCES PHYSIQUES

Les ressources physiques du guide d'organisation présentent ici les renseignements portant sur les aménagements qu'exige la mise en œuvre d'un référentiel de formation pour le métier Pentester. Pour la construction d'une nouvelle structure de formation, ces informations sont essentielles. Que ce soit les classes, les SCS ou les espaces de travail, les informations présentées permettent de mettre en évidence les besoins de création, d'adaptation et de modification des locaux et des installations existantes.

6.2.1. Types d'aménagement physique à considérer

Tout aménagement est dépendant de son contexte d'apprentissage. Il est donc important de mettre en relation les aménagements et les activités d'apprentissage. Vu dans ce sens, à l'occasion de l'implantation d'un nouveau référentiel conçu selon l'APC, si la situation et les moyens le permettent, il faut procéder à la mise à niveau de l'ensemble des dispositifs de formation.

Des plans d'aménagements des locaux et des équipements devant répondre aux exigences de la formation doivent donc être suggérés. Les espaces délimités doivent être bien calculés en tenant compte du nombre d'apprenants et du poste de travail, du nombre d'appareils et du type d'équipement utilisé dans les SCSs et les autres locaux.

La mise en place de certaines installations exige le respect des normes et de règlements.

6.2.2. SCENARIO DE RECHANGE

La formation professionnelle développe les compétences rattachées directement à l'exercice d'un métier. Dans les milieux où les ressources humaines et financières sont limitées, cette formation représente un défi à relever. Pour y parvenir, trois conditions doivent être réunies, à savoir :

- disposer des ordinateurs performants et de qualité ;
- avoir accès à des personnes de qualité ;
- disposer des outils de tests d'intrusion et d'un environnement virtualiser pour simuler les attaques à temps réel.

Pour remplir la première condition, la documentation dans le cadre de la démarche d'ingénierie pédagogique, le matériel didactique et d'évaluation ont été produits.

La réponse appropriée à la deuxième condition est la sélection rigoureuse des nouveaux formateurs, la formation et le perfectionnement du personnel en place.

Une formation de qualité exige un minimum d'équipements et de matières d'œuvre. Étant donné la rareté des ressources financières, il est crucial de rechercher systématiquement le partenariat avec les entreprises pour stimuler l'extension des structures de formation et rendre plus accessible l'accès aux ressources professionnelles.

Les principales pistes à explorer sont les suivantes :

- la promotion des services ;
- la formation en entreprise ;

- le partage d'équipements avec les entreprises (locaux, outils) ;
- la collaboration à l'entretien des équipements de la structure de formation ;
- L'organisation des services aux entreprises comme la formation et le perfectionnement du personnel.

La production et la commercialisation des services

La formation professionnelle exige que les apprenants soient placés en situation de production des services à travers l'exercice de l'apprentissage du métier. Cette production pendant la formation donne lieu à une prestation de service. Il est donc possible d'exploiter ce potentiel pour contribuer à une partie du coût de financement d'une structure de formation. Cependant, il faudra développer un cadre rigoureux qui vise à assurer aux apprenants une bonne formation au détriment de la production et d'autofinancement.

Pour les activités de commercialisation, il faudrait envisager une révision des lois et des règlements qui régissent la gestion des structures de formation, accordant à celle-ci une certaine autonomie et une autorisation de disposer une partie des profits réalisés.

Ces activités de commercialisation nécessitent une révision des modes de gestion des structures de formation afin d'assurer une transparence de gestion, un processus rigoureux de compte rendu et de vérification.

Ces activités de commercialisation nécessitent également une sensibilisation de la communauté pour éviter de considérer les apprenants comme des personnels disponibles à bon marché. Ces activités, considérées comme une concurrence déloyale pour certains, pourraient nuire à la mission de la structure de formation et à son rayonnement.

La formation en entreprise

Dans un contexte où l'accès aux équipements spécialisés est limité, il est avantageux d'établir un partenariat avec les entreprises. Pour cela, il est proposé une approche selon laquelle, l'exploration et l'apprentissage de base se réalisent à la structure de formation et par la suite, le stage en entreprise pourrait compléter la formation, développer la dextérité et approfondir certaines notions ou compétences en relation avec l'environnement de l'entreprise.

Le partage d'équipements avec les entreprises

Dans certains domaines, il est possible que la structure de formation fasse l'achat d'équipement, seul ou avec les entreprises. Cet équipement sera mis partiellement à sa disposition, selon des modalités précises. Cette forme de collaboration permet à la structure de formation de réduire les coûts de d'implantation et de réaliser la formation tout en permettant aussi aux entreprises du milieu d'avoir accès à certains équipements qu'elle ne pourrait pas normalement se procurer.

La collaboration à l'entretien des équipements de la structure de formation

Il est possible d'obtenir la collaboration des entreprises du milieu pour l'entretien ou le renouvellement d'une partie d'équipements, puisqu'il est de l'intérêt des deux parties que ce parc informatique demeure disponible et fonctionnel.

L'organisation des services aux entreprises comme la formation et le perfectionnement du personnel

Par la voie d'échanges, la structure de formation peut offrir aux entreprises des places pour la formation de son personnel en contrepartie de leur contribution à l'appui pour la formation (matériel, équipement, entretien, stage en entreprise, etc.).

Ce type de scénario ne peut être généralisé et uniformisé, mais peut être adapté au contexte du milieu d'implantation de chaque structure de formation.

Les bâtiments de l'administration, la bibliothèque, le centre multimédia, la salle de classe et l'SCS seront chacun dotés d'une centrale solaire, 10h de fonctionnement par jour, 3 jours d'autonomie. Le scenario d'alimentation du réseau d'éclairage de chaque bâtiment est comme suit :

- Centrale solaire en bon état de fonctionnement=Alimentation électrique par l'énergie solaire ;
- Centrale solaire en panne=Alimentation électrique par ENEO ou par groupe électrogène.

Les puissances des kits solaires sont les suivantes :

- Administration : 8 KVA
- Salle de classe : 8 KVA
- SCS: 8 KVA
- Bibliothèque : 8 KVA
- Salle multimédia : 20 KVA

Le branchement de chaque bâtiment aura pour origine de branchement le tableau General basse tension situé dans le bloc technique à l'entrée du centre.

L'éclairage public du pourtour de la plateforme sera assuré par Candélabre solaire 1x84w.

Alimentation téléphonique et en réseau internet

La connexion aux différents réseaux sera assurée par la fibre optique situé dans la salle multimédia. La liaison du local informatique vers les bâtiments sera réalisée par des câbles réseaux et le WIFI.

Les systèmes d'alarme et de détection

Les aires de sports

Le parking

RÉFÉRENCES BIBLIOGRAPHIQUES

1. Samurçay R. et Pastré, P. (2004), Stratégie de la formation professionnelle, République du Cameroun, Toulouse : Octarès, 187 pages.
2. 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.
3. 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.
4. 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.
5. 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.
6. 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.
7. Yassine Maleh, 2023, Guide pratique pour devenir un Pentester Professionnel », Eyrolles, Vol.1, 512 pages
8. 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.
9. Nir Yehoshua, Uriel Kosayev, 2021, «Learn practical techniques and tactics to combat, bypass, and evade antivirus software», Packt Publishing, 100 pages.
10. 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
11. Anne Lupfer, 1er septembre 2010, « Gestion des risques en sécurité de l'information », Eyrolles ,1re édition, 230 pages.
12. Géorgie Weidman, 2014, « Tests de pénétration », Presse à amidon, 1ere Édition, 766 pages.
13. Bruno Favre, Pierre-Alain Goupille, 1er octobre 2005, « Guide pratique de sécurité informatique » DUNOD, 1re édition, 254 pages.
14. 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)
15. 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.

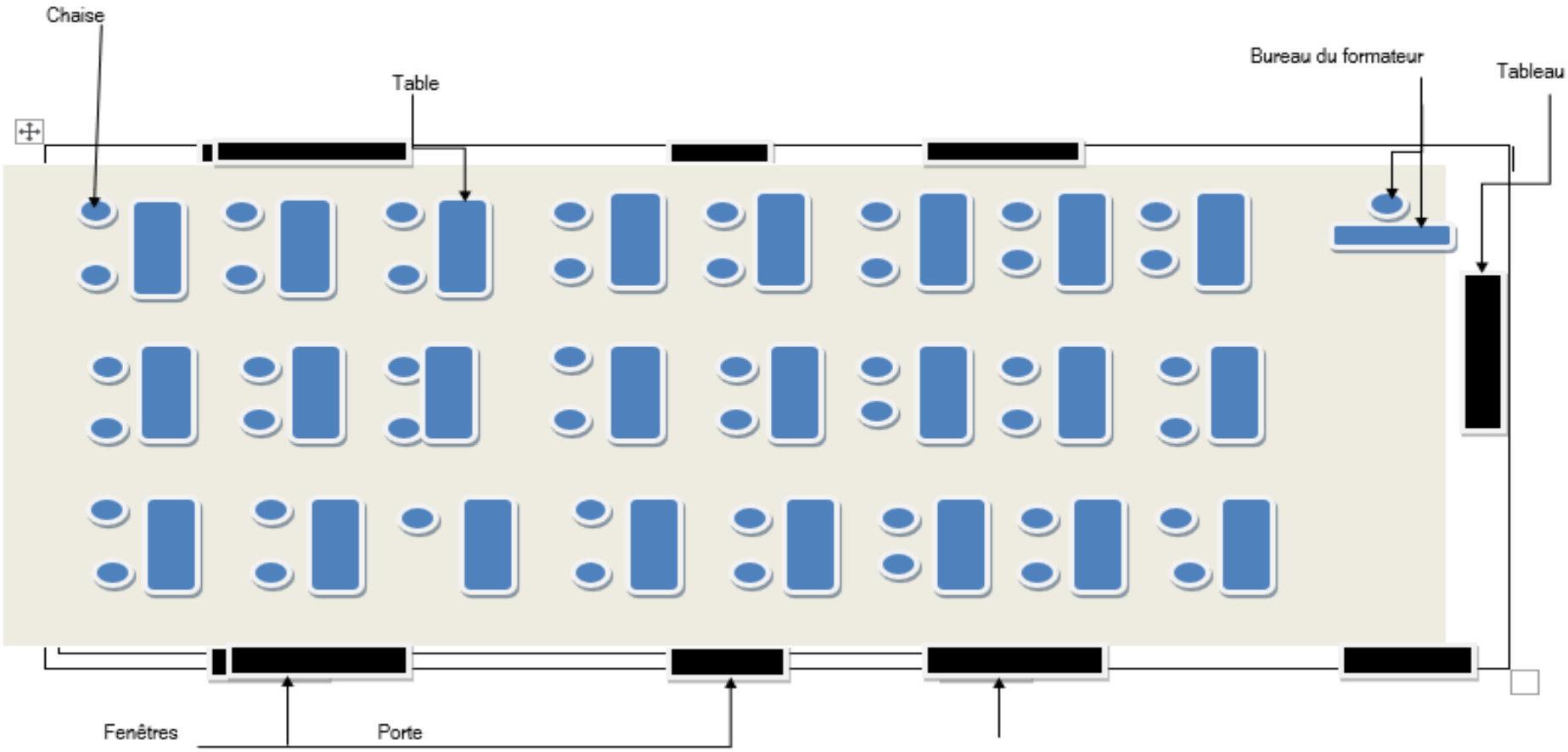
WEBOGRAPHIE

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

ANNEXES

A- PLAN D'AMENAGEMENT (PROPOSITION) D'UNE SALLE DE CLASSE



B-EXEMPLE DE PLAN DE MASSE D'UNE STRUCTURE DE FORMATION



Légende	
Code	Désignation
P1	Parking Visiteur/Service
P2	Parking Personnel
P3	Parking des Cadres
1-1	Guérite 1
1-2	Locaux techniques
2	Administration
3	CDI
4	Auditorium
5	Bloc Pédagogique
6	Restauration

Extension

1-3	Guérite 2
7	Logement Formateurs
8	Logement Apprenants
9	Logement d'Astreinte
	Voie véhicule extension

VRD

Circulation Véhicule
Trottoir
Plateforme
Circulation Piétonne
Parking

C-EXEMPLE DE PLAN D'OCCUPATION D'SCS, DU METIER PENTESTER

