RÉPUBLIQUE DU CAMEROUN
PAIX – TRAVAIL – PATRIE

COOPÉRATION CAMEROUN
BANQUE MONDIALE

PROJET D'APPUI AU DÉVELOPPEMENT DE L'ENSEIGNEMENT SECONDAIRE ET DES COMPÉTENCES POUR LA CROISSANCE ET L'EMPLOI

UNITÉ DE COORDINATION DU PROJET

COORDINATION TECHNIQUE DE LA COMPOSANTE II

REPUBLIC OF CAMEROON
PEACE – WORK – FATHERLAND

CAMEROON – WORLD BANK COOPERATION

SECONDARY EDUCATION AND SKILLS DEVELOPMENT PROJECT

PROJECT COORDINATION UNIT

TECHNICAL COORDINATION OF COMPONENT II

REFERENTIEL DE FORMATION PROFESSIONNELLE

SELON L'APPROCHE PAR COMPETENCES (APC)

GUIDE PÉDAGOGIQUE (GP)

SECTEUR : NUMERIQUE

METIER : PENTESTER

NIVEAU DE QUALIFICATION : TECHNICIEN SPECIALISE

EQUIPE DE REDACTION

N°	NOMS ET PRENOMS	STRUCTURES	QUALIFICATIONS
1	NDOUOH Sylvie	MINEFOP	Méthodologue
2	NGANSOP Henri Michel	DIGITECH	Ingénieur Informaticien
3	TAGNE Franck	INFO-SERVICES	Ingénieur Informaticien
4	YALONG OSSENG VICTOR	MINEFOP	PENTESTER

TABLE DES MATIÈRES

REMERCIEMENTS

Ce Guide Pédagogique a été élaboré et sera mis en œuvre 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 et la valorisation du métier de Pentester au Cameroun.

En outre, nous saluons et apprécions à sa juste valeur la collaboration avec les différents acteurs (Formateurs, Experts, Centres de formation et Entreprises) dans le cadre d'élaboration de ce Référentiel d'Evaluation.

Que ces Acteurs, Entreprises et Organisations Professionnelles consultés, dont les noms figurent sur les listes ci-dessous trouvent ici l'expression de nos remerciements pour leur disponibilité et leurs contributions significatives à la production d'un Référentiel d'Evaluation de qualité pour le métier de Pentester (niveau de qualification : Technicien Spécialisé).

ABRÉVIATIONS ET ACRONYMES

APC	Approche Par Compétences
AST	Analyse de la Situation de Travail
CFM	Centre de Formation aux Métiers
EPC	Équipements de Protection Collective
EPI	Équipements de Protection Individuelle
GP	Guide Pédagogique
GOPM	Guide d'Organisation Pédagogique et Matérielle
HSSE	Hygiène, Santé, Sécurité et Environnement
IGF	Inspection Générale des Formations
MINEFOP	Ministère de l'Emploi et de la Formation Professionnelle
OIF	Organisation internationale de la francophonie
REF	Référentiel de Formation
RMC	Référentiel Métier Compétences
VAE	Validation des Acquis et de l'Expérience

LISTE DES PERSONNES CONSULTÉES

- **Les professionnels**

N°	Noms et Prénoms	STRUCTUREE	QUALIFICATION
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	Formateur
5	ELOMBO ELOMBO Paul Patrick	IP_MAC	Formateur
6	DJEUMENI NGATCHOP Ulrich	GS_TVI	Professionnel

- **Les pédagogues**

N°	Nom et prénoms	STRUCTURE	QUALIFICATION
1	NGANSOP Henri Michel	DIGITECH	Formateur
2	ELOMBO ELOMBO Paul Patrick	IP_MAC	Formateur
3	TAGNE Franck	INFO-SERVICES	Formateur
4	NOKO Armel	Pentester	Formateur
5	NGIAMBA Christian	IUT Douala	Formateur

PREMIERE PARTIE : STRATEGIES DE FORMATION

I. 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.

II. 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.

III. 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. 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.

V. 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 1 : SYNTHÈSE DU PROGRAMME DE FORMATION

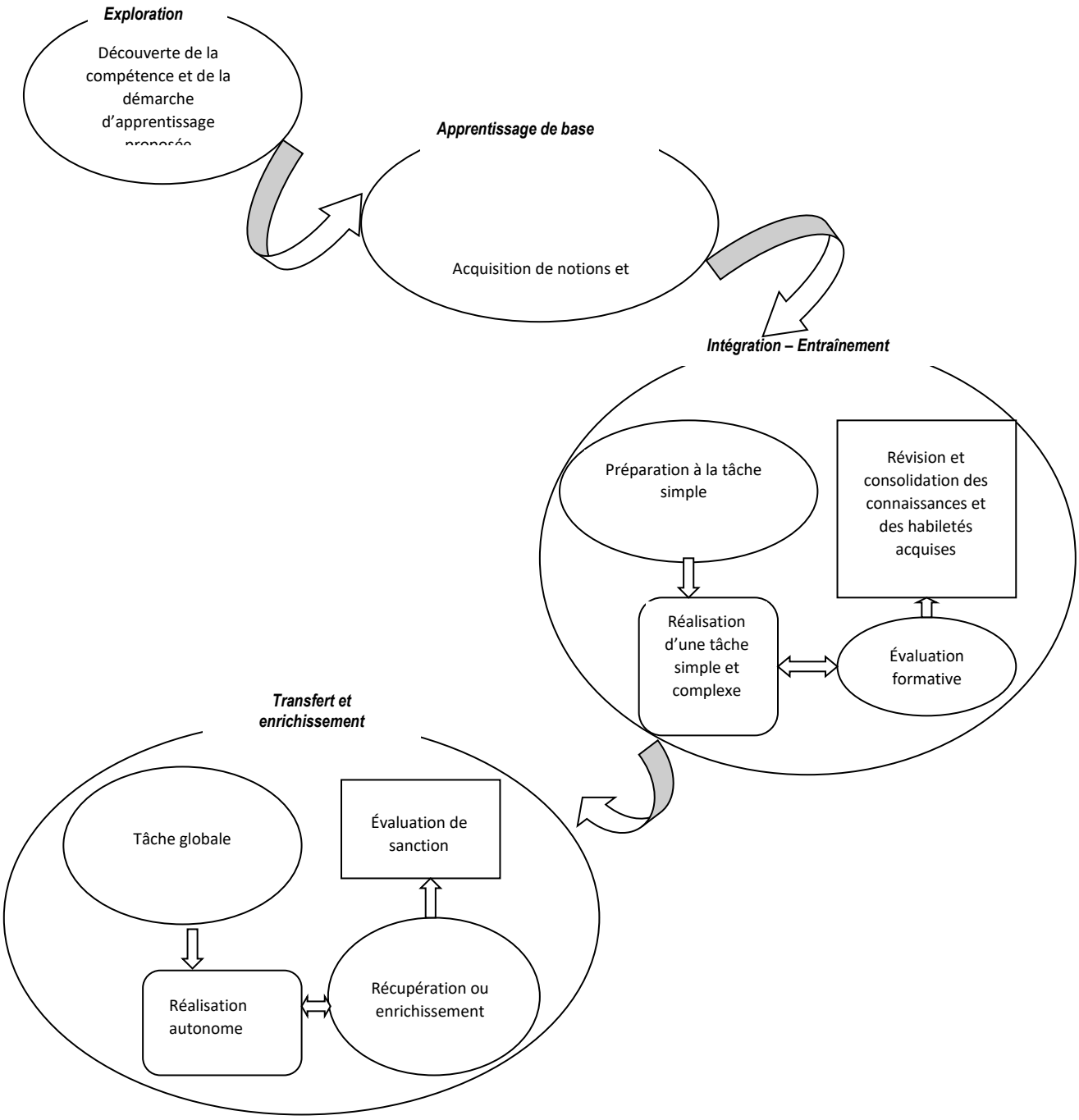
METIER : PENTESTER					**VOLUME HORAIRE : 1350 h**			
N°	**Énoncé de la compétence**	**Intitulé Module**	**Durée totale**	**Modalités**	**Stratégie d'évaluation**	**Durée de l'épreuve**	**Traduction**	**Types**
01	Se situer au regard du métier et de la formation	Métier et Formation	30	Orale	Ps Pr	2h	S	G
02	Communiquer en milieu professionnel	Communication en milieu professionnel	30	Écrite et orale	Ps Pr	2h	C	G
03	Appliquer le principe de la sécurité des comptes	Application du principe de la sécurité des comptes	60	Orale écrite, Pratique	Ps Pr	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	120	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	75	Pratique et écrite	Ps Pt	5h	C	P

12	Assurer la veille technologique en cyberattaque	Veille technologique en cyberattaque	75	Pratique et écrite	Ps Pt	5h	C	P
13	Rechercher un emploi	Entreprenariat	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			**1 350**					

VI. STRATEGIES PEDAGOGIQUES

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



VII. 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**	**75**	**75**	**315**	**30**	**30**	**60**	**60**	**60**	**120**	**45**	**1350**
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**	**125**	**150**	**120**	**75**	**75**	**315**	**30**	**30**	**60**	**60**	**60**	**115**	**45**	**1350**

DEUXIEME PARTIE : SUGGESTIONS PEDAGOGIQUES

VIII. 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.

COMPETENCE 01 **: Se situer au regard du métier et de la formation**		
NUMERO : 01	**DUREE D'APPRENTISSAGE/D'EVALUATION : 28 heures/02 heures**	
MODULE	**Métier et formation**	
FONCTION ET POSITION DE LA COMPETENCE Ce module est le tout premier par lequel l'apprenant amorcera sa formation en Pentester. Il vise à l'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 lui permettra de s'auto-évaluer en comparaison de sa personnalité, de son désir, de ses aptitudes en vue de confirmer sa participation au programme de formation		
DEMARCHE PARTICULIERE A LA COMPETENCE. Il est suggéré de répartir le temps d'apprentissage selon les proportions suivantes : 1. S'informer des réalités du métier et des perspectives professionnelles : 50% 2. S'informer sur le référentiel et la démarche de formation : 27% 3. Confirmer ou infirmer son orientation professionnelle : 16% Evaluation : 7%		
Savoirs liés à la compétence	**Balises**	**Activités d'enseignement et d'apprentissage**
1- S'informer des réalités du métier et des perspectives professionnelles		
1.1. Décrire des méthodes de repérage d'information	• Conditions de réceptivité : attention visuelle ; attention auditive ; climat favorable ; intérêt ; concentration ; bien-être physique et psychologique. • Connaissance au départ de ce que l'on cherche.	Par des exposés, à l'aide de documentation, de conférences, de visite de terrain ou de recherches personnelles, l'apprenant sera informé sur les différents types d'entreprises évoluant dans le secteur de la fabrication et maintenance des petits équipements et production d'énergie, sur les

COMPETENCE 01 **: Se situer au regard du métier et de la formation**		
NUMERO : 01	**DUREE D'APPRENTISSAGE/D'EVALUATION : 28 heures/02 heures**	
MODULE	**Métier et formation**	
	• Préparation pour discerner les points importants.	conditions d'exercice du métier, les exigences du marché et les possibilités d'évolution.
1.2. Distinguer une tâche d'une activité.	• Définitions des termes tels que tâche, Activité	
1.3. Décrire les particularités du marché du travail	• Délimitation du métier. • Catégories d'employeurs.	
1.4. Indiquer les exigences du métier	• Conditions de travail. • Possibilités d'avancement. • Égalité des sexes. Salaires	
2- S'informer sur le référentiel et la démarche de formation		
2.1 Énoncer les principes généraux de l'approche par compétences.	• Pédagogie de la réussite. • Approche active centrée sur l'élève. • Approche curriculaire, intégrée, multidimensionnelle et critériée.	par des exposés, à l'aide de documentation, de conférences, l'apprenant sera informé de la pertinence du programme de formation, des conditions de réussite et du mode d'évaluation. - Motiver les apprenants à entreprendre les activités proposées.
2.2 Lister les composantes du programme de formation.	• Modules du programme. • Stages en entreprise.	

COMPETENCE 01 **: Se situer au regard du métier et de la formation**		
NUMERO : 01	**DUREE D'APPRENTISSAGE/D'EVALUATION : 28 heures/02 heures**	
MODULE	**Métier et formation**	
2.3 Distinguer les habiletés, les aptitudes et les connaissances nécessaires pour exercer le métier.	• Définitions des termes tels que l'habileté, Aptitude…	
3**- Confirmer ou infirmer son orientation professionnelle**		
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 : Communication en milieu professionnel

COMPETENCE 02 : Communiquer en milieu professionnel.	
NUMERO : 02	**DUREE D'APPRENTISSAGE/EVALUATION** : 30 heures
MODULE ASSOCIE	**Communication en milieu professionnel**

FONCTION ET POSITION DE LA COMPETENCE

La mise en œuvre de cet 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. Traiter les informations : 30 %
2. Produire les messages indispensables à la vie professionnelle et sociale : 24 %
3. Communiquer oralement : 20%
4. Rendre compte de son activité : 20%
Evaluation :06%
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. Exploiter les ressources des langues officielles		
1.1 s'approprier les termes et expressions relatifs au métier en	•Vocabulaire spécifique au métier •Instructions, consignes et les communications •Glossaire ou un lexique bilingue	Lors de la planification des activités d'apprentissage et d'enseignement, assurez-vous de fournir aux apprenants des occasions de

français et en anglais		pratiquer et d'appliquer les compétences linguistiques dans des contextes réels et pertinents pour le métier. Encouragez l'utilisation de ressources bilingues, de supports audiovisuels et de mises en situation pratiques pour faciliter l'apprentissage et la compréhension des termes techniques et des compétences linguistiques requises. Assurez-vous également de créer un environnement d'apprentissage inclusif où les apprenants peuvent échanger, poser des questions et recevoir des commentaires constructifs pour améliorer leurs compétences linguistiques dans le contexte professionnel spécifique.
1.2 Utiliser le français	• Registres de langues •Clarté du langage •Normes de communication écrite •Normes de communication orale	
1.2 To make use of english language	•Types of documents • Level of Vocabulary •Level of langages	
1. 4 Exploiter un texte et des ressources documentaires	•Textes techniques •Manuels d'instruction •Ressources documentaires •Outils de recherche	
1.3 To exploit documentary resources	• •Technicals documents •Types of Dictionnaries •Encyclopedias •Types books •Informations	When planifying teaching and learning activities make provision for the trainees to practice and apply linguistic competences in the real and pertinent contexte of the trade. Insure an inclusive learning environnment where the trainees can exchange ; ask questions and receive constructive comments in the order to ameliorate their linguistic competences in the specific professional contexte concerned.
2. Interagir avec les membres de l'équipe et la hiérarchie		
2.1 Identifier les attitudes à adopter dans un contexte professionnel.	•Importance des attitudes professionnelles •Attitudes professionnelles •Processus d'adaptation en contexte professionnel	Lors de la planification des activités d'apprentissage et d'enseignement, encouragez les apprenants à réfléchir de manière critique

	•Types de contexte professionnel.	sur leurs propres attitudes, comportements et compétences en matière de communication professionnelle. Mettez l'accent sur l'importance de l'éthique, de l'intégrité et de la responsabilité dans le métier concerné. Encouragez les apprenants à partager leurs expériences, leurs défis et leurs succès dans l'interaction avec les membres de l'équipe et la hiérarchie. La compétence "Interagir avec les membres de l'équipe et la hiérarchie est importante.
2.2 Utiliser les comportements éthiques, d'intégrité et de conduite responsable	•Principes éthiques •Valeurs professionnelles •Comportements intègres •Règles et les réglementations	
2.3 To use of means of communication	• Communication process • ommunication styles •Communication tools	
3. Produire des écrits généraux et professionnels		
3.1 To analyse the Subjet	•Types de reasoning • Text interpretation méthods •Compétence in critical reasoning • Tools and elements of resolution	When planifying teaching and learning activities make provision for the trainees to practice and apply linguistic competences in the real and pertinent contexte of the trade. Insure an inclusive learning environnment where the trainees can exchange ; ask questions and receive constructive comments in the order to ameliorate their linguistic competences in the specific professional contexte concerned.
3.2 Rédiger une production dans la langue recommandée.	•Ecrits clairs, cohérent •Styles d'écriture •Outils et des ressources appropriés	textes, des scénarios, des Il est important d'adapter ces activités en fonction du niveau et des besoins des apprenants, ainsi que des ressources disponibles. Les activités peuvent être réalisées en classe, en ligne ou en combinant les deux approches, en utilisant des supports variés tels que des études de cas, des
3.3 Utiliser les ouvrages relatifs à la qualité de la langue	•Ouvrages de référence •Règles grammaticales et orthographiques appropriées pour produire des écrits corrects et de qualité. •Erreurs de langue dans les productions écrites.	

3.4 Rédiger les messages et des rapports	•Types de messages professionnels •Techniques d'organisation des informations •Langage professionnel	exercices pratiques, etc.
3.5 Vérifier l'efficacité et la qualité de la communication écrite	•Normes de qualité •Outils de vérification •Importances de la vérification •Processus de vérification	
4. Établir une relation conseil		
4.1 To Détermine needs	•Types of needs •Types of result •Catégorisation of needs •Specific eigencies, logistic constaints	When planifying teaching and learning activities make provision for the trainees to practice and apply linguistic competences in the real and pertinent contexte of the trade. •Insure an inclusive learning environnment where the trainees can exchange ; ask questions and receive constructive comments in the order to ameliorate their linguistic competences in the services et options, procédures administratives and exigences réglementaires.
4.2 Utiliser les moyens d'intervention	•Services et options •Procédures administratives •Exigences réglementaires	
4.3 Vérifier l'atteinte des objectifs	•Satisfaction des clients •Retours d'information •Indicateurs de performance	L'utilisation de simulations, de mises en situation pratiques et de discussions en groupe peut également être bénéfique pour favoriser l'apprentissage et l'échange d'expériences entre les apprenants. N'oubliez pas de fournir des retours d'information réguliers aux apprenants pour les aider à progresser dans le développement de cette compétence.
5. Encadrer une équipe de travail		

5.1 Établir un bilan de compétence	•Types de compétences et besoins •Forces et les faiblesses •Actions de développement	Il est important d'encourager la participation active des apprenants, en favorisant les échanges, les réflexions et les débats. Les activités pratiques, telles que les mises en situation réelle ou les projets d'équipe, peuvent également renforcer l'apprentissage et la compréhension des concepts liés à l'encadrement d'une équipe de travail.
5.2 Appliquer les techniques d'encadrement	•Types de communication •Objectifs clairs et mesurables •Techniques de coordination des activités	
5.3 to write a report	•Pertinent information •Catégorisation of information •Résultats • Proposition of actions	When planifying teaching and learning activities make provision for the trainees to practice and apply linguistic competences in the real and pertinent contexte of the trade. Insure an inclusive learning environnment where the trainees can exchange ; ask questions and receive constructive comments in the pertinent information, catégorisation of information, résultats and proposition of actions.

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% ;
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.	
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 ;	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

	• Authentification à deux facteurs (2FA) ; • Notification de compromission des mots de passe	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 • 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

5.2. Analyser le trafic réseau	• Trafic réseau ; • Protocoles réseau ; • Méthodes d'analyse : • Détection d'anomalies, • Patterns • Corrélation des événements Etc	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
5.3. 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 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.
6.2 Vérifier les logs	• Définition des logs ; • Types de logs ; • Sources de logs ; • Contenu des logs ; • Format des logs ; • Analyse des logs ; • Détection des anomalies	
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 groupe et discussions en classe, simulations d'audits et de processus de certification
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	
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	

<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 colspan="2">DUREE D’APPRENTISSAGE/D’EVALUATION 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 colspan="3">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.</td></tr>
<tr><td colspan="3">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%</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 composants des systèmes informatiques</td></tr>
<tr><td>1.1 Interpréter les traitements applicatifs</td><td>• Traitements applicatifs ;
• Flux de données ;
• Fonctionnalités ;
• Dépendances
• Modélisation des processus
• Documentation des traitements</td><td>Après avoir fait des démonstrations sur l’identification des composants des systèmes, par l’interprétation des</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**	
1.2. Optimiser les ressources systèmes	• Ressources systèmes ; • Goulets d'étranglement ; • Optimisation du CPU ; • Optimisation de la mémoire • Virtualisation et conteneurisation • Automatisation des opérations :	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.
1.3. Choisir les logiciels	• Besoins ; • Fonctionnalités ; • Évaluation des options ; • Compatibilité et intégration ; • Personnalisation et extensibilité • Évolutivité et croissance ; • Fournisseurs	
2. **Utiliser l'architecture système et applicative**		
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

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**	
2.2. 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	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.
2.3 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 ; • Mesure de la latence ; • Causes de latence ; • Optimisation de la latence ; • Priorisation du trafic • Gestion des incidents.	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
3.2 Contrôler la fiabilité des transmissions	• Mécanismes de contrôle de la fiabilité ; • Gestion des erreurs ; • Protocoles de transport fiables ;	

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**	
	• Contrôle de flux ; • Pertes de paquets ;	confidentialité des échanges Seul ou en groupe, l'apprenant effectuera des recherches et présentera devant ses pairs le résultat de ses travaux.
3.3.. Vérification de la Sécurité et de la confidentialité des échanges	• Enjeux de sécurité • Cryptographie • Protocoles sécurisés • Identités et accès • Protection contre les attaques • Certificats • Sécurisation des réseaux sans fil	
4**. Appliquer les protocoles de communication**		
4.1. Choisir les types de protocole	• Modèles de communication et leurs protocoles • Types de protocoles • Protocoles haut niveau • Choix des protocoles	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,
4.2. Contrôler la charge réseau	• Charge actuelle ; • Prévision de la charge future ; • Équilibrage de charge • Trafic de pointe.	

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**	
4.3. Vérifier la Robustesse et la résistance aux aléas	• 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	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

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**
1. Effectuer l'administration système		

<table>
<tr><td colspan="3">COMPETENCE 05 : Configurer les systèmes d’exploitation</td></tr>
<tr><td>NUMERO : 5</td><td colspan="2">DUREE D’APPRENTISSAGE/D’EVALUATION : 56 heures/04heures</td></tr>
<tr><td>MODULE</td><td colspan="2">Configuration des systèmes d’exploitation</td></tr>
<tr><td>1.1. Organiser l’administration système</td><td>• Définition des processus ;
• Élaboration de politiques ;
• Planification des ressources
• Documentation ;
• Collaboration interfonctionnelle ;
• Surveillance et évaluation ;
• Amélioration continue</td><td rowspan="2">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.</td></tr>
<tr><td>1.2. Respecter les procédures d'administration système</td><td>• Formation et sensibilisation ;
• Application cohérente ;
• Gestion des changements ;
• Suivi des performances ;
• Rétroaction et amélioration continue ;
• Conformité réglementaire</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**	
		Le formateur encadre les activités des apprenants afin d'assurer l'intégration des apprentissages.
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 ;	le formateur prépare les apprenants à être proactifs dans la gestion de la sécurité des systèmes d'exploitation, en les dotant des

<table>
<tr><td colspan="3">COMPETENCE 05 : Configurer les systèmes d’exploitation</td></tr>
<tr><td>NUMERO : 5</td><td colspan="2">DUREE D’APPRENTISSAGE/D’EVALUATION : 56 heures/04heures</td></tr>
<tr><td>MODULE</td><td colspan="2">Configuration des systèmes d’exploitation</td></tr>
<tr><td></td><td>• Planification des mises à jour ;
• Sensibilisation ;</td><td rowspan="2">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.
.
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.</td></tr>
<tr><td>3.2. Détecter les compromissions</td><td>• Activités réseau ;
• Journaux de sécurité ;
• Outils de détection d'intrusion ;
• Incidents de sécurité.</td></tr>
<tr><td colspan="3">4. Gérer la sécurité OS :</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**	
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 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.
4.2. Détecter les menaces avancées	• Menaces avancées ; • Vulnérabilités OS ; • Logiciels malveillants OS • Réponses aux incidents OS ; • Veille technologique.	
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.	
4.4. Détecter l'incident à courte durée	• Incidents à courte durée ; • Signaux d'alertes ; • Outils de détection ; • Surveillance en temps réel :	

COMPETENCE 05 **: Configurer les systèmes d'exploitation**		
NUMERO : 5	**DUREE D'APPRENTISSAGE/D'EVALUATION** : 56 **heures/04heures**	
MODULE	**Configuration des systèmes d'exploitation**	
	• Incidents rapides ; • Formation pratique.	OS, 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.
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 ; • Gestion des Mises à jour ; • Dépannage et résolution des problèmes.	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. L'apprenant, par le biais d'exercices développe sa capacité de mieux gérer les périphériques. Le formateur encadre les activités des
5.2. Vérifier l'Intégrité des données échangées	• Méthodes de vérification ; • Hachage ;	

COMPETENCE 05 **: Configurer les systèmes d'exploitation**		
NUMERO : 5	**DUREE D'APPRENTISSAGE/D'EVALUATION** : 56 **heures/04heures**	
MODULE	**Configuration des systèmes d'exploitation**	
	• Redondance cyclique (CRC) :; • Codes de vérification d'erreur (ECC) ; • Gestion des erreurs ;	apprenants afin d'assurer l'intégration des apprentissages. .
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** : 112 **heures/08 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.
En ce qui concerne le temps alloué à l'apprentissage, il est suggéré de le répartir selon les proportions suivantes :

<table>
<tr><td colspan="3">COMPETENCE 06 : Utiliser les langages de programmation</td></tr>
<tr><td>NUMERO : 6</td><td colspan="2">DUREE D’APPRENTISSAGE/D’EVALUATION : 112 heures/08 heures</td></tr>
<tr><td>MODULE</td><td colspan="2">Utilisation des langages de programmation</td></tr>
<tr><td colspan="3">• 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.</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 le langage de programmation généralistes</td></tr>
<tr><td>○ 1.1. Identifier les caractéristiques et spécificités</td><td>• Concepts de base ;
• Syntaxe du langage ;
• Design Pattern ;
• Gestion de la mémoire ;
• Erreurs et exceptions ;
• Frameworks ;</td><td rowspan="2">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.</td></tr>
<tr><td>1.2 Comparer les langages.</td><td>• Syntaxe et structure ;
• Gestion de la mémoire et des ressources ;</td></tr>
</table>

COMPETENCE 06 **: Utiliser les langages de programmation**		
NUMERO : 6	**DUREE D'APPRENTISSAGE/D'EVALUATION** : 112 **heures/08 heures**	
MODULE	**Utilisation des langages de programmation**	
	• 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
2.2. Elaborer le développement défensif	• Principes de sécurité des applications ; • Bonnes pratiques de codage sécurisé ; • Autorisations et des privilèges ; • Attaques et menaces courantes ;	
2.3. Gérer les vulnérabilités	• Vulnérabilités potentielles dans les applications web • Risques associés à chaque vulnérabilité identifiée	

COMPETENCE 06 **: Utiliser les langages de programmation**		
NUMERO : 6	**DUREE D'APPRENTISSAGE/D'EVALUATION** : 112 **heures/08 heures**	
MODULE	**Utilisation des langages de programmation**	
	• Développement de correctifs	apporte des 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.
2.4. 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 ;	
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

COMPETENCE 06 **: Utiliser les langages de programmation**		
NUMERO : 6	**DUREE D'APPRENTISSAGE/D'EVALUATION** : 112 **heures/08 heures**	
MODULE	**Utilisation des langages de programmation**	
3.2. Analyser et optimiser l'algorithmes	• Analyse d'algorithmes ; • Notions de complexité ; • Analyse asymptotique ; • Types de problèmes ; • Méthodes d'optimisation ; • Analyse empirique ; • Cas d'utilisation ; • Évolution des algorithmes ; • Évaluation et comparaison ;	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.
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,
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** : 112 **heures/08 heures**	
MODULE	**Utilisation des langages de programmation**	
	• Programmation ; • Débogage et tests	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.
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,
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 ; • Cryptographie et gestion des identités ; • Tests de sécurité et analyse statique du code	

COMPETENCE 06 **: Utiliser les langages de programmation**		
NUMERO : 6	**DUREE D'APPRENTISSAGE/D'EVALUATION** : 112 **heures/08 heures**	
MODULE	**Utilisation des langages de programmation**	
5.4. Gérer les vulnérabilités	• Vulnérabilités potentielles dans le code source • Risques • Tests de sécurité ; • Développement de correctifs ;	échange avec d'autres apprenants, présente la production du groupe, participe à la mise en commun en plénière, participe aux synthèses, note la synthèse.
5.5. 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 : 70 heures/ 05h</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 ;</td></tr>
</table>

	• Partage de l'information	
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 ; • Impact des failles de sécurité identifiées ; • Formulation de recommandations.	Par des exposés en group, le formateur amènera les apprenants à identifier les techniques d'attaques, 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**		
5.1 Identification 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**
1. 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 les consignes, prend des notes, échange avec
1.2. Choisir les outils en fonction des tests	• Différents types de tests	

	• Sélection des outils • Mise en pratique • Bonnes pratiques et recommandations	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. 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	
3. 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	

4. 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	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.

	• Présentation des Constatations :	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	Cours Magistraux et Présentations Démonstrations Pratiques et Exercices Études de Cas et Discussions en Groupe Projets Pratiques sur des Techniques Réelles

	• 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	
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	• Vulnérabilités	

réseaux/applications	• Outils de détection ; • Résultats ; • Correctifs	
2. Tester l'efficacité du réseau et des applications		
2.1. 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.
2.2. Utiliser les préconisations	• Meilleures pratiques et normes de sécurité ; • Conformité des réseaux et des applications • Implications ; • Actions spécifiques ;	
2.3. Identifier des failles	• Outils d'analyse ; • Données de test ; • Résultats ;	
3. Tester les systèmes d'exploitation		
3.1. Décrire les configurations et services testés	• Configurations critiques ; • Services activés sur les OS • Sécurité du système d'exploitation ; • Autorisations d'accès • Services vulnérables ; • Documentation des résultats ;	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 recommander des mesures correctives appropriées pour renforcer la sécurité et la résilience du système. Le formateur formera des groupes, donnera des
3.2. Effectuer le scanne de vulnérabilité	• Outils de scan de vulnérabilité ; • Installation et configuration • Scans de vulnérabilité ; • Rapport détaillé des résultats.	

3.3. Recommander les correctifs et mesures	• Vulnérabilités ; • Priorisation des correctifs ; • Stratégies de déploiement ; • Mesures compensatoires ; • Correctifs déployés ;	exercices de cas pratique aux apprenants et s'attardera sur les méthodes et recommandation produites par les apprenants.

COMPETENCE 10 **: Proposer les stratégies d'atténuation**		
NUMERO : 10	**DUREE D'APPRENTISSAGE/D'EVALUATION : 140 heures/ 10h**	
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 : • Recommandations d'Amélioration • Présentation des Constatations :	Par l'entremise d'exposés et/ou d'études de cas, le formateur présente aux apprenants à utiliser les modèles de compromission. 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 microsegmentation • Gestion de la microsegmentation du réseau. • Efficacité de la microsegmentation • 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 microsegmentation 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

5.2 Utiliser les bonnes pratiques et référentiels reconnus ;	• Standards de Sécurité • Risques • Authentification Multifacteur (AMF) • Cryptage des Données • Mises à Jour Régulières • Sécurité	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.
5.3 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	Cours Magistraux et Présentations Démonstrations Pratiques et Exercices Études de Cas et Discussions en Groupe Projets Pratiques

	• Gestion et Maintenance de l'Architecture de Sécurité	
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 • Scénarios de Tests dans les Projets Réels	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 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 :70 heures/ 5h**	
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 % 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.		
Savoirs liés à la compétence	Balises	Activités d'enseignement et d'apprentissage
1. Configurer les pare-feux et des IDS/IPS		

1.1. Validation **des tests**	• Objectifs des tests ; • Scénarios de test ; • Plan de test ; • Sélection des outils ; • Configuration des tests ; • Exécution des tests ; • Résultats ; • Normes ; • Anomalies • Validation finale	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.
1.2. Documentation des techniques produites	• Types de documentation ; • Description des techniques ; • Procédures pas à pas ; • Normes de documentation ; • Formats de documentation ; • Versionnage ;	
2. Implémenter une politique de filtrage et de détection		
2.1. Utilisation des bonnes pratiques de sécurité ;	• Principe du moindre privilège ; • Segmentation du réseau ; • 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
2.2. Déploiement sur l'infrastructure cible ;	• Infrastructure existante ; • Objectifs de sécurité ; • Solutions de sécurité ;	

	• Architecture de sécurité ; • Planification du déploiement ; • Equipements de sécurité	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.
2.3. 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	
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		
3.2 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
3.4. Collecte des logs et métriques	• Sources de logs ; • Evénements à collecter ; • Agents de collecte ; • Traitement des logs ; • Métriques	
3.4 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 : 70heures/ 5h**	
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.
1.2. Analyser les tendances et	• Collecte de données ;	

évolutions ;	• Tendances émergentes ; • Evolutions futurs ; • Bonnes pratiques	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.
1.3. 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.	

COMPETENCE 13 **: rechercher l'emploi**		
NUMERO : 13	**DUREE D'APPRENTISSAGE** : 42 h /3h	
MODULE	**Entrepreneuriat**	
FONCTION ET POSITION DE LA COMPETENCE		
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.		
DEMARCHE PARTICULIERE A LA COMPETENCE		
La répartition du temps d'apprentissage est suggérée selon les proportions suivantes : 1. S'initier à la connaissance de l'entreprise et des éléments comptables, à l'économie, à des notions juridiques et sociales : 22% 2. S'approprier les techniques de recherche d'emploi : 36% ; 3. s'approprier les techniques de base de montage d'un projet de création d'entreprise (entrepreneuriat) : 36% 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. S'initier à la connaissance de l'entreprise et des éléments comptables, à l'économie, à des notions juridiques et sociales.		
1.1 S'approprier la notion d'entreprise	• Rôles • Diversité d'entreprises • Classements selon la taille • Découpage en fonction des services	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.
1.2 Déterminer les opérations commerciales	• Besoins du consommateur • Le marché • Flux et documents commerciaux	

COMPETENCE 13 **: rechercher l'emploi**		
1.3 Déterminer les éléments comptables	• Le bilan • Notions de charge, de produits, de valeurs ajoutées, de résultats • Taxe à la valeur ajoutée (TVA) • Eléments de comptabilité matière • Notion d'amortissement à partir d'exemple • Analyse et calcul de coûts	
1.4 Décrire l'entreprise et son environnement	• Environnement économique • Relation avec les principaux agents de la vie économique • Environnement social et politique	
1.5 S'approprier les notions de base en économie	• Les entreprises et la production • Les échanges économiques • Les impôts et les prélèvements • Les problèmes économiques	

COMPETENCE 13 : RECHERCHER L'EMPLOI		
NUMERO : 13	**DUREE D'APPRENTISSAGE** : 42 h /3h	
MODULE	**ENTREPRENARIAT**	
FONCTION ET POSITION DE LA COMPETENCE		
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.		
DEMARCHE PARTICULIERE A LA COMPETENCE		
La répartition du temps d'apprentissage est suggérée selon les proportions suivantes : 1. S'initier à la connaissance de l'entreprise et des éléments comptables, à l'économie, à des notions juridiques et sociales : 25% 2. S'approprier les techniques de recherche d'emploi : 35% 3. s'approprier les techniques de base de montage d'un projet de création d'entreprise (entrepreneuriat) : 35% Évaluation : 5% 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'initier à la connaissance de l'entreprise et des éléments comptables, à l'économie, à des notions juridiques et sociales.		
1.1 Appliquer les notions d'entreprise, d'économie et de droit des affaires	• Diversité d'entreprises • Classements selon la taille • Découpage en fonction des services • Entreprises et production • Echanges économiques • Impôts et prélèvements • Problèmes économiques	Le formateur présente des cours théoriques sur les concepts et les principes de base de l'entreprise, de l'économie et du droit des affaires. Il soumet les apprenants aux études de cas d'entreprises réelles pour comprendre comment ces notions sont appliquées

COMPETENCE 13 : RECHERCHER L'EMPLOI		
	• Concepts et principes de base du droit des affaires.	dans des situations concrètes. Les apprenants effectuent des recherches individuelles ou en groupe sur des sujets spécifiques liés à l'entreprise, à l'économie et au droit des affaires. Ils participent à des débats et des discussions en classe pour approfondir leur compréhension et développer leur capacité de critique. Les apprenants participent à des stages en entreprise pour observer directement comment ces notions sont mises en pratique dans un environnement professionnel.
1.2 Réaliser les opérations commerciales et les éléments comptables	• Vente, achat et gestion des stocks • Logiciels de comptabilité • Enregistrement des transactions commerciales • Relevés financiers • Performances financières d'une entreprise. • Bilans comptables, comptes de résultat et budgets	Le formateur organise des ateliers pratiques où les apprenants réalisent des opérations commerciales telles que la vente, l'achat, la gestion des stocks, etc. Ils utilisent des logiciels de comptabilité pour enregistrer les transactions commerciales, produire des relevés financiers et analyser les performances financières d'une entreprise. Les apprenants effectuent des tâches pratiques telles que la préparation et l'interprétation de bilans comptables, de

COMPETENCE 13 : RECHERCHER L'EMPLOI		
		comptes de résultat et de budgets. I Ils travaillent sur des projets de groupe où ils doivent créer et gérer une entreprise fictive, en effectuant toutes les opérations commerciales et comptables nécessaires.
2.S'approprier les techniques de recherche d'emploi		
2.1 Monter un CV	• Principes de base de la rédaction d'un CV, • Structure, contenu et mise en forme d'un CV • Méthodologie de rédaction de CV	Le formateur présente les principes de base de la rédaction d'un CV, y compris la structure, le contenu et la mise en forme. Les apprenants étudient des exemples de CV pour comprendre les bonnes pratiques et les erreurs à éviter. Ils participent à des ateliers où ils doivent recevoir des conseils personnalisés sur la rédaction de CV. Les apprenants participent également à des simulations d'entretiens d'embauche où ils pourront discuter et affiner des CV en fonction des besoins du marché du travail.
2.2Appliquer les procédures de recherche d'emploi	• Méthodes de recherche d'emploi (recherche en ligne, réseaux professionnels et salons de l'emploi) • Rédaction de lettres de motivation, • Préparation d'entretiens d'embauche • Stratégies de recherche d'emploi	Les apprenants apprennent les différentes méthodes de recherche d'emploi, telles que la recherche en ligne, les réseaux professionnels et les salons de l'emploi. Ils participent à des ateliers sur la rédaction de lettres de motivation, la

COMPETENCE 13 : RECHERCHER L'EMPLOI		
		préparation d'entretiens d'embauche et le développement de compétences en communication. Sous le regard du formateur, ils effectuent des exercices pratiques de recherche d'emploi, tels que la rédaction de lettres de motivation adaptées à des offres d'emploi spécifiques. Ils reçoivent des conseils et des retours d'experts en carrière sur les stratégies de recherche d'emploi efficaces. Ils participent également à des entretiens simulés pour se préparer aux entretiens réels.
3. S'approprier les techniques de base de montage d'un projet de création d'entreprise (entrepreneuriat)		
3.1 Examiner les conditions de réussite d'un projet de création ou d'auto emploi	• Facteurs clés de réussite • Expériences des sucesss story • Viabilité d'un projet de création d'entreprise • Aspects financiers, juridiques, marketing et opérationnels. • Tendances du marché et opportunités d'entrepreneuriat. • Défis, risques et stratégies de réussite liés à la création d'entreprise ou à l'auto-emploi.	Le formateur organise des études des cas d'entrepreneurs à succès et analyser les facteurs clés qui ont contribué à leur réussite. Le formateur fait participer les apprenants à des séminaires et à des conférences animées par des entrepreneurs expérimentés qui partageront leurs expériences et leurs conseils. Les apprenants travaillent sur des projets de groupe où ils doivent évaluer la

COMPETENCE 13 : RECHERCHER L'EMPLOI		
		viabilité d'un projet de création d'entreprise, en déterminants les aspects financiers, juridiques, marketing et opérationnels. Ils effectuent des recherches individuelles sur des secteurs d'activité spécifiques pour comprendre les tendances du marché et les opportunités d'entrepreneuriat. Enfin, les apprenants participent à des discussions en classe sur les défis, les risques et les stratégies de réussite liés à la création d'entreprise ou à l'auto-emploi.
3.2 Présenter un plan d'affaires	• Principes de base de la rédaction d'un plan d'affaires • Structure, sections clés et contenu nécessaire d'un plan d'affaires • Elaboration d'un plan d'affaires •	Le formateur expose sur les principes de base de la rédaction d'un plan d'affaires, y compris la structure, les sections clés et le contenu nécessaire. Les apprenants étudient des exemples de plans d'affaires pour comprendre les bonnes pratiques et les éléments essentiels. Ils participent à des ateliers où ils seront guidés dans l'élaboration d'un plan d'affaires pour un projet spécifique. Les apprenants reçoivent des conseils et des retours d'experts en entrepreneuriat

COMPETENCE 13 : RECHERCHER L'EMPLOI		
		sur la façon d'améliorer leur plan d'affaires. Ils présentent leur plan d'affaires devant un auditoire et reçoivent des commentaires et des suggestions pour l'améliorer.

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

EQUIPE DE VALIDATION

N°	Noms et Prénoms	STRUCTURE	QUALIFICATIONS
1	NDOUOH Sylvie	MINEFOP	Méthodologue
2	NGANSOP Henri Michel	DIGITECH	Ingénieur Informaticien
3	TAGNE Franck	INFO-SERVICE	Ingénieur Informaticien
4	NGANKAM NIEGUE FABO Perry	CANAL+	Professionnel
5	NGIAMBA Christian	IUT DOUALA	formateur