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 Compétences (APC)

REFERENTIEL D'EVALUATION (REV)

SECTEUR : NUMERIQUE
METIER : PENTESTER
NIVEAU DE QUALIFICATION : TECHNICIEN SPECIALISE

EQUIPE DE REDACTION

N°°°	NOMS ET PRENOMS	STRUCTURE	QUALIFICATIONS
1	NDOUOH Sylvie	MINEFOP	METHODOLOGUE
2	NGANSOP Henri Michel	DIGITECH	INGENIEUR INFORMATICIEN
3	TAGNE Franck	INFO-SERVICES	INGENIEUR INFORMATICIEN

TABLE DES MATIÈRES

REMERCIEMENTS

Ce Référentiel d'Evaluation 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 de la formation et la valorisation de la filière Pentester au Cameroun

En outre, nous saluons et apprécions à sa juste valeur la collaboration avec les différents acteurs (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
RF	Référentiel de Formation
RMC	Référentiel Métier Compétences
GP	Guide Pédagogique
GPM	Guide d'Organisation Pédagogique et Matérielle
EPC	Équipements de Protection Collective
EPI	Équipements de Protection Individuelle
MINEFOP	Ministère de l'Emploi et de la Formation Professionnelle
FPT	Formation Professionnelle et Technique
IGF	Inspection Générale des Formations
DFOP	Direction de la Formation et de l'Orientation Professionnelles
OIF	Organisation internationale de la francophonie
REV	Référentiel d'Évaluation

LISTES 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

I. PRESENTATION D'UN REFERENTIEL D'EVALUATION

a). Nature

Le Référentiel d'Evaluation (REV) repose sur les compétences issues du Référentiel de Métier-Compétences (RMC) et de celles propres au projet de formation. Il est un guide proposant des orientations en matière d'évaluation des compétences : compétences traduites en comportement et compétences traduites en situation. Différents acteurs évoluant au sein du système de formation professionnelle, ils peuvent définir de manière différente l'expression : évaluation des apprentissages. C'est ainsi que l'apprenant, le formateur, les autres personnes qui travaillent dans la Structure de formation, les responsables de la gestion centrale de la formation, sont amenés à dégager divers points de vue sur la notion d'évaluation, selon qu'ils ont à l'intégrer dans leur apprentissage, à la mettre en application ou à la gérer. Prenant en compte tous ces cas de figure, on peut considérer que l'évaluation se situe au cœur des processus d'apprentissage, de formation et de gestion de la formation professionnelle.

Souvent, l'on a perçu ou retenu de la notion d'évaluation des apprentissages, l'aspect qui consiste à porter un jugement sur la maîtrise des compétences et sur la performance des apprenants qui souhaitent obtenir une qualification. Cette perception limite la place que devrait occuper l'évaluation au sein d'un processus de formation et d'apprentissage. En formation professionnelle, la fonction « évaluation" présente certaines caractéristiques et se déploie en s'appuyant sur des valeurs et des orientations de base. Tous ces éléments constituent un cadre de référence à partir duquel l'évaluation des apprentissages est structurée et mise en œuvre.

b) Structure

Le Référentiel d'Evaluation se présente comme suit :

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

c) Finalités

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

d) Modalités d'évaluation des compétences

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

référentiel de formation, afin de reconnaître chaque compétence et de la sanctionner, en plus de déterminer un seuil de réussite.

e) Eléments prescriptifs

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

- La durée totale de formation, incluant le temps consacré à l'évaluation. Toutefois, la durée de la formation reliée à chaque compétence est facultative pour accorder une certaine souplesse aux Structures de formation ;
- Les Tableaux de spécifications et leurs différentes composantes :

    - éléments de la compétence et situations de mise en œuvre de la compétence ;
    - stratégies retenues ;
    - indicateurs et critères d'évaluation ;
    - points attribués aux critères d'évaluation ou critères cochés en relation avec le seuil de réussite ;
    - seuil de réussite ;
    - règle de verdict, le cas échéant

II. PRÉSENTATION DES CONCEPTS ET DES PRINCIPALES DÉFINITIONS

a) Concepts

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

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

b) Principales définitions

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Seuil de réussite.

Niveau de qualité à partir duquel on considère une performance comme réussie. Il peut s'agir d'une note ou d'une description qualitative se basant sur des critères.

Test d'une épreuve.

Essai d'une épreuve auprès d'un groupe restreint d'apprenants afin de vérifier la faisabilité et la validité de l'épreuve.

Tolérance.

Marge d'inexactitude ou d'erreur admise lors d'une épreuve de connaissances pratiques ou d'activités d'apprentissage pratique

Univoque.

Se dit d'une interprétation unique

Validité d'un instrument d'évaluation.

Capacité d'un instrument de mesurer réellement ce qu'il prétend évaluer.

Versions d'une épreuve.

Différentes épreuves évaluant la même compétence soit par une mise en situation différente, ou par la production d'un produit différent ou par la prestation d'un service différent mais dont les éléments critères sont identiques et de difficulté de même niveau.

III. DESCRIPTION SYNTHÈSE DU RÉFÉRENTIEL DE FORMATION

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

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

Ainsi, le référentiel de formation pour le métier de Pentester traduit les orientations particulières en matière de formation. Il prépare donc la personne à devenir un travailleur du secteur du numérique pouvant mener des activités d'évaluation de la sécurité d'un système d'information à travers différents angles d'attaques seul, en équipe ou sous supervision, pour le compte d'une entreprise ou à son compte personnel.

De plus, le référentiel de formation vise à rendre apte le Pentester à réaliser la simulation des attaques malveillantes pour identification puis exploitation des vulnérabilités au sein du Système Informatique, Évaluer la sécurité des systèmes afin d'identifier les vulnérabilités potentielles qui pourraient être exploitées par des attaquants malveillants, Réaliser les tests d'intrusion en simulant des attaques ciblées pour mettre à l'épreuve la résistance des systèmes de l'organisation, Analyse des résultats et fournir des recommandations détaillées pour améliorer la sécurité, Rédiger les rapports, Sensibiliser à la sécurité afin de réduire les risques d'attaques informatiques.

Dans l’exercice de son métier, le Pentester doit Appliquer les principes de la sécurité des comptes, Exploiter l’architecture des systèmes informatiques des réseaux et des protocoles, Configurer les systèmes d’exploitation, Utiliser les langages de programmation etc….
Étant donné que le Pentester travaille souvent seul, en équipe ou sous supervision, il doit démontrer de bonnes attitudes relationnelles en milieu de travail ou même dans la société.

a) Tableau synthèse du référentiel de formation

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

N°	Énoncé de la compétence	Durée	CS	CG	Unités	Types d'objets	Types de compétences	Titre du Module	Code
1	Se situer au regard du métier et de la formation	30	0	30	2	S	G	Métier et Formation	**MEF01**
2	Communiquer en milieu professionnel	30	0	30	2	C	G	Communication en milieu professionnel	**COM02**
3	Appliquer le principe de la sécurité des comptes	60	0	60	4	S	G	Application du Principe de la sécurité des comptes	**APSC03**
4	Exploiter l'architecture des systèmes informatiques des réseaux et des protocoles	60	0	60	8	C	G	Exploitation de l'architecture des systèmes informatiques des réseaux et des protocoles	**EASI04**
5	Configurer les systèmes d'exploitation	60	0	60	4	C	G	Configuration des systèmes d'exploitation	**CSEP05**
6	Utiliser les langages de programmation	120	0	120	4	C	G	Utilisation des langages de programmation	**ULPR06**
7	Identifier les vulnérabilités potentielles dans les Systèmes informatiques	90	90	0	6	C	P	Identification des vulnérabilités potentielles dans les Systèmes informatiques	**IVPS07**
8	Configurer les outils de test de pénétration des systèmes d'exploitation	120	120	0	8	C	P	Configuration des outils de test de pénétration des systèmes d'exploitation	**COPS09**
9	Tester la vulnérabilité sur les Réseaux, les applications, site web et les systèmes d'exploitation	150	150	0	10	C	P	Tests de vulnérabilité sur les Réseaux, les applications, site web et les systèmes d'exploitation	**RVAP08**
10	Proposer les stratégies d'atténuation	120	120	0	8	C	P	Proposition des stratégies	**PSAT10**

								d’atténuation	
11	Configurer les pares-feux et des systèmes de détection d’intrusions	75	75	0	5	C	P	Configuration des pares-feux et des systèmes de détection d’intrusions	**CPFDI11**
12	Assurer la veille technologique en cyberattaque	75	75	0	5	C	P	Veille technologique en cyberattaque	**VTCY12**
13	Rechercher un emploi	45	0	45	3	S	G	Entreprenariat	**ENTR13**
14	S’intégrer en milieu professionnel	315	315	/	21	S	P	Intégration en milieu de travail	**STG14**
	Total	**1350**	**945**	**405**	**90**				
			70 %	**30%**					

Une unité = 15 heures

Pentester Compétences particulières	Numéro de la compétence	Type d'objectif	Compétences générales							Processus de trava			
			Se situer au regard du métier et de la formation	Communiquer en milieu professionnel	Appliquer les principes de la sécurité des comptes	Exploiter l'architecture des systèmes informatiques des	Configurer les systèmes	Utiliser les langages de	Rechercher un emploi		Exécuter le travail en adoptant	Contrôler la qualité du travail	Consigner et transmettre l'information
Numéro de la compétence			1	2	3	4	5	6	13				
Type d'objectif			S	C	C	C	C	C	**S**				
COMPÉTENCES PARTICULIÈRES													
Identifier les vulnérabilités potentielles dans les Systèmes informatiques	7	C	▭	●	●	●	●	●	▭	●	●	●	▯
Configurer les outils de test de pénétration des systèmes d'exploitation	8	C	▭	●	●	●	●	●	▭	●	●	●	●
Tester la vulnérabilité sur les Réseaux, les applications, site web et les systèmes d'exploitation	9	C	▭	●	●	●	●	●	▭	●	●	●	●
Proposer les stratégies d'atténuation	10	C	▭	●	●	●	●	●	▭	●	●	●	●
Configurer les pares-feux et des systèmes de détection d'intrusions	11	C	▭	●	●	●	●	●	▭	●	●	●	●
Assurer la veille technologique en cyberattaque	12	C	▭	●	●	●	●	●	▭	●	●	●	●
S'intégrer en milieu professionnel	14	S	▯	▯	▯	▯	▯	▯	▯	▯	▯	▯	▯
Nombre de compétences	**7**												

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

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

●

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

c) Table d'analyse des critères généraux de performance

Pentester (Compétences traduites en comportement)	Numéro de la compétence	COMPETENCES TRADUITES	Durée (h)	CRITERES GENERAUX DE PERFORMANCE								
				Respect des bonnes pratiques de configuration	Disponibilité des services et capacité à assurer la continuité	Faculté d'évolution et d'adaptation aux changements	Niveau de robustesse contre les attaques et protection des informations	Performance des paramètres systèmes pour maximiser les	Description technique experte des résultats pour qualifier les	Gestion avancée des vulnérabilités identifiées (classification, priorisation,	Respect de la méthodologie des principes et processus de	Veille technologique sur les mises à jour des outils de test
Communiquer en milieu professionnel	2	C	30	□	□	□	□	□	□	□	□	□
Appliquer les principes de la sécurité des comptes	3	C	60	△	△	△	O	O	O	O	O	O
Exploiter l'architecture des systèmes informatiques des réseaux et des protocoles	4	C	60	△	□	△	O	O	O	O	O	△
Configurer les systèmes d'exploitation	5	C	45	△	△	△	△	△	△	△	△	O
Utiliser les langages de programmation	6	C	120	△	△	△	△	△	△	△	△	△
Identifier les vulnérabilités potentielles dans les Systèmes informatiques	7	C	90	△	△	△	△	△	△	△	△	△
Configurer les outils de test de pénétration des systèmes d'exploitation	9	C	120	△	△	△	△	△	△	△	△	△
Tester la vulnérabilité sur les Réseaux, les applications, site web et les systèmes d'exploitation	8	C	120	△	△	△	△	△	△	△	△	△
Proposer les stratégies d'atténuation	10	C	150	△	△	△	△	△	△	△	△	△
Configurer les pares-feux et des systèmes de détection d'intrusions	11	C	120	△	△	△	△	△	△	△	△	△
Assurer la veille technologique en cyberattaque	12	C	90	△	△	△	△	△	△	△	△	△

□ Aucune relation dans le programme de formation

△ Retenu au niveau de l'évaluation

O Critères non retenus pour les fins d'évaluation de sanction.

IV. PRESENTATION DES OUTILS

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

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

a) Tableau de spécifications

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

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

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

b) Description de l'épreuve

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

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

c) Fiche d'évaluation

La fiche d'évaluation reprend les indicateurs et les critères d'évaluation adoptés pour l'évaluation aux fins de la sanction (tableaux de spécifications) et les précise davantage, le cas échéant, sous forme d'éléments d'observations. Ces fiches peuvent aussi faire mention des marges de tolérance acceptées. Elle fait état de la pondération associée aux critères d'évaluation. Elle présente aussi le seuil de réussite fixé dans le tableau de spécifications. La fiche d'évaluation

guide les centres de formation et les formateurs dans la description des épreuves au moment de la réalisation des activités d'évaluation et, comme les descriptions d'épreuve ou de participation, elle est fournie à titre de suggestion.
Lorsque la stratégie d'évaluation correspond à un processus de travail, les épreuves mixtes (connaissances pratiques et activités d'apprentissage pratique) sont recommandées.
Par contre, lorsque la stratégie d'évaluation correspond à un produit, une épreuve conduisant au développement des activités d'apprentissage pratique est recommandée.

V. ÉVALUATION DES COMPÉTENCES

a) Modalités d'évaluation formative

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

b) Éléments d'évaluation

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

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

c) Évaluation sommative

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

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

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

Tableau 1 : Synthèse du programme de formation

METIER : Pentester					**VOLUME HORAIRE : 1 350h**				
N°	**Énoncé de la compétence**	**Intitulé Module**	**Durée totale**	**Modalités**	**Stratégie d'évaluation**	**Durée de l'épreuve**	**Traduction**	**Types**	**Seuil de réussite**
01	Se situer au regard du métier et de la formation	Métier et Formation	30	Orale	Ps Pr	2	S	G	70%
02	Communiquer en milieu professionnel	Communication en milieu professionnel	30	Écrite et orale	Ps Pr	2	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	4	S	G	
04	Exploiter l'architecture des systèmes informatiques des réseaux et des protocoles	Exploitation de l'architecture des systèmes informatiques des réseaux et des protocoles	60	Pratique et écrite	Ps Pt	4	C	G	
05	Configurer les systèmes d'exploitation	Configuration des systèmes d'exploitation	60	Pratique et écrite	Ps Pt	4	C	G	
06	Utiliser les langages de programmation	Utilisation des langages de programmation	120	Pratique et écrite	Ps	8	C	G	
07	Identifier les vulnérabilités potentielles dans les Systèmes informatiques	Identification des vulnérabilités potentielles dans les Systèmes informatiques	90	Pratique Écrite	Ps Pt	6	C	G	

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	8	C	P	
09	Tester la vulnérabilité sur les Réseaux, les applications, site web et les systèmes d'exploitation	Tests de vulnérabilité sur les Réseaux, les applications, site web et les systèmes d'exploitation	150	Pratique Écrite	Ps Pt	10	C	P	
10	Proposer les stratégies d'atténuation	Proposition des stratégies d'atténuation	120	Pratique Écrite	Ps Pt	8	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	5	C	P	
12	Assurer la veille technologique en cyberattaque	Veille technologique en cyberattaque	75	Pratique et écrite	Ps Pt	5	C	P	
13	Rechercher un emploi	Entreprenariat	45	Pratique et écrite	Ps Pt	3	C	P	
14	S'intégrer en milieu professionnel	Intégration en milieu de travail	315	Pratique et écrite	Ps Pt	21	C	P	
Total			**1 350**						

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

Renseignements complémentaires

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

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

Grille de rétroaction

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

COMPÉTENCES TRADUITES EN SITUATIONS

TABLEAU DE SPÉCIFICATIONS			
Métier	**PENTESTER**	**Code : MEFO 01**	
Nº et énoncé de la compétence :	**1 – se situer au regard du métier et de la formation**	**Durée d'apprentissage :**	**30 h**
Éléments de la compétence	**Indicateurs**	**Critères d'évaluation**	
S'informer sur le métier	1. Recueil de données sur la nature et sur les exigences du métier	1.1 Description judicieuse de la nature et des exigences de l'emploi	☐
	2. Recueil de données sur les caractéristiques du marché du travail	2.1 Résumé succinct des principales caractéristiques du travail	☐
S'informer sur le programme de formation et engagement de la démarche	3. Collecte d'informations sur le programme, la démarche de formation et d'évaluation	3.1 Description des compétences à acquérir	☐
		3.2 Description correcte des modes d'évaluation	■
	4. Participation à une rencontre de groupe	4.1 Expression correcte de la perception du programme de formation	☐
		4.2 Comparaison correcte de sa perception du programme de formation avec le marché du travail	☐
Évaluer et confirmer son engagement	5. Présentation d'un bilan personnel	5.1 Précision correcte de goûts, aptitudes, champs d'intérêt et qualités personnelles	■
		5.2 synthèse correcte des différents aspects du métier	☐
	6. Décision définitive de poursuite de programme	6.1 choix final de poursuite ou non du programme de formation	■
Seuil de réussite : 6 des 9 critères d'évaluation, dont les critères noircis, pour que l'on considère la compétence acquise			

DESCRIPTION DE L'ENGAGEMENT	Code : MEFO 01

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

Renseignements généraux

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

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

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

Déroulement

- *S'informer sur le métier*

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

Dans leur recherche, les apprenants auront à préciser :

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

- *S'informer sur le programme de formation et engagement de la démarche*

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

Au cours de la discussion, l'apprenant aura :

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

- *Evaluer et confirmer son engagement*

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

Dans le rapport, l'apprenant aura :

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

FICHE D'EVALUATION		Code : MEFO 01	
N° et énoncé de la compétence	**1. Se situer au regard du métier et de la formation**		
Module 1 : Métier et formation			
Nom de l'apprenant : Structure de formation : Date de l'évaluation : _____ Signature du formateur :		**Résultat** **SUCCES** ☐ **ECHEC** ☐	
ELEMENTS D'OBSERVATION		**Jugement**	
		OUI	**NON**
1. Recueil de données sur la nature et sur les exigences du métier 1. Recueil de données sur la nature et sur les exigences du métier		☐	☐
2. Recueil de données sur les caractéristiques du marché du travail 2.1 Résume les principales caractéristiques du travail		☐	☐
2. Recueil de données sur les caractéristiques du marché du travail 2.1 Résumé succinct des principales caractéristiques du travail		☐	☐
3. Collecte d'informations sur le programme, la démarche de formation et d'évaluation 3.1 Description des compétences à acquérir 3.2 Description correcte des modes d'évaluation		☐ ☐	☐ ☐
4. Participation à une rencontre de groupe 4.1 Expression correcte de la perception du programme de formation 4.2 Comparaison correcte de sa perception du programme de formation avec le marché du travail		☐ ☐	☐ ☐
5. Présentation d'un bilan personnel 5.1 Précision correcte de goûts, aptitudes, champs d'intérêt et qualités personnelles 5.2 synthèse correcte des différents aspects du métier		☐ ☐	☐ ☐
6. Décision définitive de poursuite de programme 6.1 choix final de poursuite ou non du programme de formation		☐	☐
TOTAL :		**/9**	
Seuil de réussite : 6 oui sur une possibilité de 9 (dont la satisfaction aux exigences des critères d'évaluation 3.2, 5.1 et 5.3.			
Remarque :			

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

DESCRIPTION DE L'EPREUVE	Code : ENTR13….
N° et Énoncé de la Compétence	**13 Rechercher un emploi**

Renseignements généraux

L'épreuve a pour but d'évaluer la compétence relative à « Rechercher un emploi ».

Il s'agit d'une épreuve qui prend en considération une portion d'évaluation des connaissances pratiques et celle d'activités d'apprentissage pratique.

L'épreuve d'activités d'apprentissage pratique pourrait être administrée individuellement ou en groupe.

L'évaluation des connaissances pratiques pourrait être réalisée avec l'ensemble des apprenants.

L'épreuve pourrait être d'une durée de 3 heures, ce qui inclut la phase pratique et celle de l'évaluation des connaissances pratiques.

Déroulement de l'épreuve

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

Matériel

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

Consignes particulières

L'épreuve pourrait être administrée durant le temps d'apprentissage d'une compétence subséquente (compétence 13) ou d'une compétence évaluée en parallèle, (compétences 12) ;

L'observation pourrait être faite en simulation pour le premier cas d'évaluation.

En cas d'échec, l'épreuve pourrait être reprise dans son ensemble. Si un seul élément est très faible comparativement aux autres pour lesquels les performances de l'apprenant seraient excellentes, seul cet élément pourrait être repris.

FICHE D'EVALUATION		Code : ENTP13
N° et Énoncé de la Compétence	13 Rechercher un emploi	Durée : 315h

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

_____

Signature du formateur :

Résultat	
SUCCES	ECHEC
☐	☐

ELEMENTS D'OBSERVATION	OUI	NON	RESULTATS
1. NOTION D'ENTREPRISE, NOTIONS EN ECONOMIE, NOTIONS DE BASE EN DROIT DES AFFAIRES 1.1 Mise en pratique conforme des notions de base			0 ou 20
2. REALISATION JUDICIEUSE DES OPERATIONS COMMERCIALES ET DES ELEMENTS COMPTABLES 2.1 Réalisation judicieuse des opérations commerciales et des éléments comptables			0 ou 10
3. MONTAGE DES CV 3.1 Montage judicieuse des CV			0 ou 10
4. APPLICATION DES PROCEDURES DE RECHERCHE D'EMPLOI 4.1 Application judicieuse des procédures de recherche d'emploi			0 ou 25
5. EXAMINATION DES CONDITIONS DE REUSSITE D'UN PROJET DE CREATION OU D'AUTO EMPLOI 5.1Examination judicieuse des conditions de réussite d'un projet de création ou d'auto emploi			0 ou 10
6. PRESENTATION D'UN PLAN D'AFFAIRES 6.1Redaction correcte d'un plan d'affaires			0 ou 25
TOTAL			**/100**
Seuil de réussite : 70%			
Remarque :			

TABLEAU DE SPECIFICATIONS			
Métier	**PENTESTER**	**Code :**	**STAG14….**
N° 14 et Énoncé de la Compétence	**S'intégrer au milieu professionnel**	**Durée d'apprentissage**	**315 heures**
Eléments de la compétence	**Indicateurs**	**Critères d'évaluation**	
Préparer son séjour en milieu de travail	1. Recueil des données pertinentes pour le stage	1.1 Recueil correct des données pertinentes pour le stage	☐
		1.2 Description exhaustive des tâches prévues pour son stage	
	2.1 Choix des stages	2.1 Choix judicieux des entreprises pour le stage	☐
		2.2 Élaboration conforme du dossier de stage	
Respecter les principes de discipline et de déontologie	3. Distinction des règles de conduite	3.1Respect des consignes, des règlements, de la hiérarchie et des normes environnementales	■
	4. Application des règles de conduite de l'entreprise	4.1Démonstration des qualités personnelles et professionnelles	
Exécuter les activités en milieu de travail	5. Utilisation des équipements	5.1 Exécution appropriée des tâches	■
		5.2 Assimilation parfaite et démonstration des opérations liées au métier	
	6. Exécution ou participation aux tâches	6.1 Développement des attitudes professionnelles	
		6.2 Choix et utilisation adéquats des matériels de l'entreprise	
Comparer ses perceptions aux	7. Participation à des échanges sur le stage	7.1 Résumé de l'expérience de stage	☐

réalités du métier	8. Relation entre la formation et les exigences du milieu de travail	8.1 Démonstration de l'influence du stage sur le choix d'un futur emploi	
Rédiger le rapport de stage	9. Respect du canevas de rédaction du rapport de stage	9.1 Respect des principes de la langue utilisée	☐
		9.2 Pertinence du contenu du rapport	☐
	10. Rédaction du rapport de stage	10.1 Rédaction soignée et concise	
Seuil de réussite : 3 des 5 critères d'évaluation, dont les critères noircis, pour que l'on considère la compétence acquise			

DESCRIPTION DE L'ENGAGEMENT	Code : STAG14….
N° et Énoncé de la Compétence	**14 S'intégrer au milieu professionnel**

Renseignements généraux

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

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

Déroulement de l'épreuve

18 Préparer son séjour en milieu de travail

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

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

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

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

19 Respecter les principes de discipline et de déontologie

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

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

20 Exécuter les activités en milieu de travail

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

21 Comparer ses perceptions aux réalités du métier

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

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

22 Rédiger le rapport de stage

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

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

FICHE D'EVALUATION	Code : STAG14
N° et Énoncé de la Compétence	**14 S'intégrer au milieu professionnel**

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

_____
Signature du formateur :

Résultat	
SUCCES	**ECHEC**
☐	☐

ELEMENTS D'OBSERVATION	**Jugement**	
	OUI	**NON**
1. RECUEIL DES DONNEES PERTINENTES POUR LE STAGE 1.1 Recueil correct des données pertinentes pour le stage 1.2 Description exhaustive des tâches prévues pour son stage	☐	☐
2.1 CHOIX DES STAGES 2.1 Choix judicieux des entreprises pour le stage 2.2 Élaboration conforme du dossier de stage	☐	☐
3. DISTINCTION DES REGLES DE CONDUITE 3.1Respect des consignes, des règlements, de la hiérarchie et des normes environnementales	☐	☐
4. APPLICATION DES REGLES DE CONDUITE DE L'ENTREPRISE 4.1Démonstration des qualités personnelles et professionnelles	☐	☐
5. UTILISATION DES EQUIPEMENTS 5.1 Exécution appropriée des tâches 5.2 Assimilation parfaite et démonstration des opérations liées au métier	☐	☐
6. EXECUTION OU PARTICIPATION AUX TACHES 6.1 Développement des attitudes professionnelles 6.2 Choix et utilisation adéquats des matériels de l'entreprise	☐	☐
7. PARTICIPATION A DES ECHANGES SUR LE STAGE 7.1 Résumé de l'expérience de stage	☐	☐
8. RELATION ENTRE LA FORMATION ET LES EXIGENCES DU MILIEU DE TRAVAIL 8.1 Démonstration de l'influence du stage sur le choix d'un futur emploi	☐	☐
9. RESPECT DU CANEVAS DE REDACTION DU RAPPORT DE STAGE 9.1 Respect des principes de la langue utilisée 9.2 Pertinence du contenu du rapport	☐	☐
10. REDACTION DU RAPPORT DE STAGE 10.1 Rédaction soignée et concise	☐	☐
TOTAL :	**/7**	

Seuil de réussite : 4 des 7 critères d'évaluation dont la satisfaction aux exigences des critères 3.1 et 6.1

COMPÉTENCES TRADUITES EN COMPORTEMENT

TABLEAU DE SPÉCIFICATIONS				
METIER :	**Électricien Bâtiment**		**Code : COM 02**	
N° 02 et libellé de la compétence	**Communiquer en milieu professionnel**		**Durée d'apprentissage**	**30h**
Éléments de la compétence	**Stratégie**	**Indicateurs**	**Critères d'évaluation**	**Points**
Exploiter les ressources des langues officielles	Produit	1. Appropriation des termes et expressions relatifs au métier en français et en anglais	1.1 Utilisation appropriée de formules et des termes relatifs au métier en français et en anglais	05
		2. Utilisation du français	2.1 Application appropriée du code grammatical du français	05
		3. Making use of English language	3.1 Appropriated use of English language rules	05
		4. Exploitation d'un texte et des ressources documentaires	4.1 Détermination des éléments pertinents d'un texte	05
		5. Exploitation of documentary resources	5.1 Détermination of pertinent éléments of a document	05
Interagir avec les membres de l'équipe et la hiérarchie	Produit	6. Identification des attitudes à adopter dans un contexte professionnel.	6.1 Reconnaissance des attitudes à adopter dans un contexte professionnel.	05
		7. Utilisation des comportements éthiques, d'intégrité et de conduite responsable	7.1 Démonstration de comportements éthiques, d'intégrité et de conduite responsable.	05
		8. Use of means of communication	Use of appropriate means of communication	05
Produire des écrits généraux et professionnels		9. Subjet analysis	15.1 Réponse correcte aux questions portant sur un texte.	05
			15.2 Pertinent analysis of the subjet	05
		10. Redaction d'une production dans la	9.1 Rédaction correcte d'une production dans	05

		langue recommandée.	la langue recommandée.	
		11. Utilisation des ouvrages relatifs à la qualité de la langue	o Utilisation efficace des ouvrages relatifs à la qualité de la langue	05
		12. Redaction des messages et des rapports	12.1 Rédaction claire et concise de messages.	05
			12.2 Production de rapports clairs et concis.	
		13. Vérification de l'efficacité et de la qualité de la communication écrite	13.1 Vérification judicieuse de l'efficacité et de la qualité de la communication écrite.	05
Établir une relation conseil	Produit	14. Détermination of needs	14.1 Precise détermination of needs	05
		15. Utilisation des moyens d'intervention	1.1 Détermination des moyens d'intervention appropriés.	
			1.2 Mise en œuvre adéquate des moyens d'intervention.	05
		16. Vérification de l'atteinte des objectifs	o Communication appropriée de l'information pertinente.	
			16.2 Vérification objective de l'atteinte des objectifs.	05
Encadrer une équipe de travail	Produit	17. Établissement d'un bilan de compétence	o Établissement judicieuse d'un bilan de compétence	05
		18. Application des techniques d'encadrement	18.1 Identification des aspects favorables à la conduite de réunions.	
			22.2 Application judicieuse des techniques d'encadrement	05
		19. Writing of report	19.1 Judicious writing of report	05

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

FICHE D'ÉVALUATION			CODE :
N° 02 et Énoncé de la compétence	**Communiquer en milieu professionnel**		**Durée 2 h**
Nom de l'apprenant: Établissement d'enseignement: Date de l'évaluation: Signature du formateur:			Résultat SUCCÈS ☐ ÉCHEC ☐
ÉLÉMENTS D'OBSERVATION	OUI	NON	RÉSULTATS
1. APPROPRIATION DES TERMES ET EXPRESSIONS RELATIFS AU MÉTIER EN FRANÇAIS ET EN ANGLAIS 1.1 Utilisation appropriée de formules et des termes relatifs au métier en français et en anglais			0 ou 5
2. UTILISATION DU FRANÇAIS 2.1 Application appropriée du code grammatical du français			0 ou 5
3. MAKING USE OF ENGLISH LANGUAGE 3.1 Appropriated use of English language rules			0 ou 5
4. EXPLOITATION D'UN TEXTE ET DES RESSOURCES DOCUMENTAIRES 4.1 Détermination des éléments pertinents d''un texte			0 ou 5
5. EXPLOITATION OF DOCUMENTARY RESOURCES 5.1 Détermination of pertinent éléments of a document			0 ou 5
6. IDENTIFICATION DES ATTITUDES À ADOPTER DANS UN CONTEXTE PROFESSIONNEL 6.1 Reconnaissance des attitudes à adopter dans un contexte professionnel.			0 ou 5
7. UTILISATION DES COMPORTEMENTS ÉTHIQUES, D'INTÉGRITÉ ET DE CONDUITE RESPONSABLE 7.1 Démonstration de comportements éthiques, d'intégrité et de conduite responsable.			0 ou 5
8. Use of means of communication 8.1 Use of appropriate means of communication			0 ou 5
9. RÉSOLUTION DES QUESTIONS PORTANT SUR UN TEXTE. 9.1 Réponse correcte aux questions portant sur un texte. 9.2 Analyse pertinente d'un sujet.			0 ou 5 0 ou 5
10. RÉDACTION D'UNE PRODUCTION DANS LA LANGUE RECOMMANDÉE. 10.1 Rédaction correcte d'une production dans la langue recommandée.			0 ou 5
11. UTILISATION DES OUVRAGES RELATIFS À LA QUALITÉ DE LA LANGUE 11.1 Utilisation efficace des ouvrages relatifs à la			0 ou 5

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

TABLEAU DE SPÉCIFICATIONS				
METIER :	**PENTESTER**		**Code**	**APSC03**
N° et libellé de la compétence	**3. Appliquer les principes de la sécurité des comptes**		Durée d'apprentissage	60heures
Éléments de la compétence	**Stratégie**	**Indicateurs**	**Critères d'évaluation**	**Points**
S'informer des lois et des règlements sur la santé et la sécurité au travail	Processus	1. Identification du corpus et du dispositif juridique	1.1 Interprétation juste de la législation du travail	**05**
			1.2 Relevé approprié des normes et des procédures de santé et de sécurité au travail	**05**
		2. Repérage de l'information dans les documents et les pictogrammes	2.1. Repérage adéquat de l'information dans les documents et les pictogrammes	**05**
Gérer les identités	Processus	3. Techniques et règles de gestion des identités	3.1. Respect judicieux du nombre d'identités	**05**
			3.2. Respect judicieux du délai de provisioning d'une nouvelle identité	**05**
		4. Renouvellement des mots de passe	4.1 Renouvellement approprié des mots de passe	**05**
Contrôler les mots de passe	Processus	5. Utilisation des mesures de sécurité des mots de passe	5.1. Sécurisation correcte des mots de passe ;	**05**
			5.2. Respect de la complexité des mots de passe ;	**05**
		6. Respect du délai de réinitialisation d'un mot de passe oublié/compromis	6.1. Respect du délai de réinitialisation d'un mot de passe oublié/compromis	**05**
Contrôler les accès	Processus	7.Identification des accès	7.1. Authentification correcte des accès	**05**

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

DESCRIPTION DE L'ÉPREUVE		Code : APSC03
METIER :	**PENTESTER**	
N° et énoncé de la compétence	**3. Appliquer les principes de la sécurité des comptes**	**Durée :4h**

Renseignements généraux

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

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

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

Déroulement de l'épreuve

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

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

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

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

Matériel *(Pour un groupe de 25 apprenants)*

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

Consigne particulière

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

FICHE D'ÉVALUATION			Code : APSC03
Métier	**PENTESTER**		
N° et énoncé de la compétence	**3. Appliquer les principes de la sécurité des comptes**		
Nom de l'apprenant: Établissement d'enseignement: Date de l'évaluation: Signature du formateur:			**Résultat** **SUCCÈS** ☐ **ÉCHEC** ☐
ÉLÉMENTS D'OBSERVATION	**OUI**	**NON**	**RÉSULTATS**
1. Identification du corpus et du dispositif juridique 1.1 Interprétation juste de la législation du travail 1.2 Relevé approprié des normes et des procédures de santé et de sécurité au travail			0 ou 05 0 ou 05
2. Repérage de l'information dans les documents et les pictogrammes 2.1 Repérage adéquat de l'information dans les documents et les pictogrammes			0 ou 05
3. Techniques et règles de gestion des identités 3.1. Respect judicieux du nombre d'identités 3.2. Respect judicieux du délai de provisioning d'une nouvelle identité			0 ou 05 0 ou 10
4. Renouvellement des mots de passe 4.1. Renouvellement approprié des mots de passe			0 ou 05
5. Application des mesures de sécurité des mots de passe 5.1. Sécurisation correcte des mots de passe 5.2. Respect de la complexité des mots de passe ;			0 ou 05 0 ou 05
6. Respect du délai de réinitialisation d'un mot de passe oublié/compromis 6.1. Respect du délai de réinitialisation d'un mot de passe oublié/compromis			0 ou 05
7.Identification des accès 7.1. Respect strict du délai d'approbation d'une demande d'accès			0 ou 05
8. Détection correcte du Nombre de violations 8.1. Détection du Nombre de violations			0 ou 05
9.Respect du temps moyen de détection des incidents 9.1. Respect strict du délai entre la survenue et détection d'un incident			0 ou 05

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

TABLEAU DE SPÉCIFICATIONS			
METIER :	**PENTESTER**	**Code**	**EASI04**
No et libellé de la compétence	**4. Exploiter l'architecture des systèmes informatiques des réseaux et des protocoles**	**Durée d'apprentissage**	
Éléments de la compétence	**Stratégie**	**Indicateurs**	**Critères d'évaluation**
Identifier les composants des systèmes informatiques	Processus	1.Interpretation des traitements applicatifs	1.1 Choix exact du matériel ;
		2.Optimisation des ressources systèmes	2.1. Identification correcte des données ;
		3. Choix des logiciels	3.1 Identification correcte des logiciels
Utiliser l'architecture système et applicative	Processus	3. Utilisation de l'architecture système et applicative	4.1. Utilisation correcte l'architecture systèm applicative
		4. Suivi de l'architecture système et applicative	5.1. Suivi correcte de l'architecture systèm applicative
		6. Isolation/Sécurisation correcte des applications	6.1 Isolation/Sécurisation correcte applications.
Utiliser les réseaux	Processus	7. Contrôle des latences des communications	7.1. Contrôle efficace des latences des communications
		8.Gestion de la fiabilité des transmissions	8.1. Gestion appropriée de la fiabilité transmissions
		9.Assurer la Sécurité et confidentialité des échanges	9.1. Sécurité et confidentialité correctes échanges
Appliquer les protocoles de communication	Processus	10. Choix des types de protocole	10.1. Identification judicieuse des types protocole
		11. Contrôle de la charge réseau	11.1. Contrôle correcte de la charge réseau
		12. Vérification de la Robustesse et résistance aux aléas	12.1. Vérification correcte de la Robustess résistance aux aléas.

DESCRIPTION DE L'ÉPREUVE		Code : EASI04
N° 4	**Énoncé de la compétence : Exploiter l'architecture des systèmes informatiques des réseaux et des protocoles**	

Renseignements généraux

L'épreuve a pour but d'évaluer l'engagement de l'apprenant dans une démarche qui vise à assurer l'acquisition de la compétence relative à « Exploiter l'architecture des systèmes informatiques des réseaux et des protocoles Il s'agit d'une épreuve d'évaluation qui prend en considération l'évaluation des connaissances théoriques et pratiques et elle pourrait être administrée individuellement à l'écrit.
L'évaluation des connaissances théoriques pourrait être réalisée avec l'ensemble des apprenants et l'évaluation des connaissances pratiques pourrait être administrée par groupes en fonction du nombre de postes informatiques disponibles pour les dessins assistés par ordinateur.
L'évaluation portera sur les points suivants :

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

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

Liens avec les autres compétences

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

Contenu de l'épreuve

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

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

Matériel *(Pour un groupe de 25 apprenants)*

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

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

Consigne particulière

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

FICHE D'ÉVALUATION			Code : EASI04
Énoncé de la compétence :	4. **Exploiter l'architecture des systèmes informatiques des réseaux et des protocoles**		**Durée : 4 h**

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

ÉLÉMENTS D'OBSERVATION	**OUI**	**NON**	**RÉSULTATS**
1. Interprétation des traitements applicatifs et des ressources systèmes 1.1 Gestion efficace des Performance des traitements applicatifs ;			0 ou 10
2.Optimisation des ressources systèmes 2.1. Optimisation correcte des ressources systèmes			0 ou 10
3.Choix des logiciels 3.1 Identification correcte des logiciels			0 ou 10
4. Utilisation de l'architecture système et applicative 4.1. Utilisation correcte l'architecture système et applicative			0 ou 10 0 ou 05
5. Suivi de l'architecture système et applicative. 5.1. Suivi correcte de l'architecture système et applicative			0 ou 05
5.Isolation/Sécurisation des applications 6.1 Isolation/Sécurisation correcte des applications			0 ou 05
7. Contrôle des latences des communications 7.1. Contrôle efficace des latences des communications			0 ou 05
8.Gestion de la fiabilité des transmissions 8.1. Gestion appropriée de la fiabilité des transmissions			0 ou 10
9. Sécurité et confidentialité des échanges 9.1. Sécurité et confidentialité correctes des échanges			0 ou 05
10.Choix des types de protocole 10.1. Identification judicieuse des types de protocole			0 ou 05
11.Gestion de la charge réseau 11.1. Gestion correcte de la charge réseau			0 ou 10
12. Robustesse et résistance aux aléas 12.1. Robustesse et résistance efficace aux aléas			0 ou 10
		TOTAL :	**/100**

Seuil de réussite : 70%

Règle de verdict : Néant

Remarque :

TABLEAU DE SPÉCIFICATIONS				
METIER	**PENTESTER**		**Code**	**CSEP05**
N° et énoncé de la compétence	**5. Configurer les systèmes d'exploitation.**		**Durée d'apprentissage**	**60 h**
Éléments de la compétence	**Stratégie**	**Indicateurs**	**Critères d'évaluation**	**Points**
Effectuer l'administration système	Processus	1.Organisation de l'administration système	1.1. Gestion efficace de l'administration système	10
			1.2 Suivi correcte des actions d'administration système.	5
		2. Respect des procédures d'administration système	2.1. Respect des procédures d'administration système	5
Organiser les utilisateurs et les droits	Processus	3. Supervision de l'Intégrité des comptes utilisateurs	3.1 Supervision efficace des mécanismes d'authentification	5
			3.2. Supervision efficace de l'Intégrité des comptes utilisateurs	10
		4. Suivi des actions sur les comptes	4.1. Suivi correcte des actions sur les comptes	5
Appliquer la sécurité des systèmes d'exploitation	Processus	5. Identification des taux de correction des vulnérabilités	5.1 Gestion efficace de protection contre les vulnérabilités	5
			5.2. Résistance efficace aux attaques ciblées	5
		6.Détection des compromissions	6.1. Détection correcte des compromissions	5
Contrôler la sécurité OS:	Processus	7. Description des mécanismes de défense	7.1 Gestion efficace des mécanismes de défense	10
		8. Découverte des menaces avancées	8.1 Détection correcte des menaces avancées	5

		9. identification et analyses des événements de sécurité	9.1. Détermination correcte du Journal des événements de sécurité	5
		10.Détection d'incident à courte durée	10.1. Réponse efficace aux incidents.	5
Gérer les périphériques	Processus	11. Échanges des données avec les périphériques	11.1. Échanges efficaces avec les périphériques	5
			11.2. Échange minutieuse des données	5
		12. Vérification de l'Intégrité des données échangées	12.1. Vérification correcte de l'Intégrité des données échangées	5
		Suivi des actions sur les périphériques.	Suivi correcte des actions sur les périphériques.	5

DESCRIPTION DE L'ÉPREUVE	Code : CSEP05
N° et énoncé de la compétence	**5. Configurer les systèmes d'exploitation.**

Renseignements généraux

L'épreuve a pour but d'évaluer l'engagement de l'apprenant dans une démarche qui vise à assurer l'acquisition de la compétence relative à « Configurer les systèmes d'exploitation ».
Il s'agit d'une épreuve d'évaluation qui prend en considération l'évaluation des connaissances théoriques et pratiques et elle pourrait être administrée individuellement à l'écrit.
L'évaluation des connaissances théoriques pourrait être réalisée avec l'ensemble des apprenants et l'évaluation des connaissances pratiques pourrait être administrée par groupes en fonction du nombre de postes disponibles.
L'évaluation portera sur les points suivants :

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

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

Liens avec les autres compétences

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

Contenu de l'épreuve

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

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

Matériel *(Pour un groupe de 25 apprenants)*

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

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

Consigne particulière

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

excellentes, seul cet élément pourrait être repris.

FICHE D'ÉVALUATION		Code : CSEP05	
N° et énoncé de la compétence	**5. Configurer les systèmes d'exploitation**		**Durée : 4h**
Nom de l'apprenant :		**Résultat**	
Établissement d'enseignement :		**SUCCÈS**	**ÉCHEC**
Date de l'évaluation :			
Signature du formateur :			

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

11.1. Échanges efficaces avec les périphériques ; 11.2. Échange minutieuse des données			0 ou 05
12. Vérification de Intégrité des données échangées 12.1. Vérification correcte de l'Intégrité des données échangées			0 ou 05
13.Suivi des actions sur les périphériques 13.1. Suivi correcte des actions sur les périphériques.			0 ou 05
		TOTAL :	**/100**
Seuil de réussite : 70%			
Règle de verdict : Néant			
Remarque :			

TABLEAU DE SPÉCIFICATIONS				
METIER	**PENTESTER**		**Code**	**UASI04**
N° et énoncé de la compétence	**6. Utilisation des langages de programmation**		**Durée d'apprentissage**	**120h**
Éléments de la compétence	**Stratégie**	**Indicateurs**	**Critères d'évaluation**	**Points**
Identifier le langage de programmation généralistes :	Processus	1. Identification des caractéristiques et spécificités	1.1. Identification correcte des caractéristiques et spécificités	10
		2. Comparaison des langages	2.1. Comparaison minutieuse des langages entre eux ;	05
		3. Acquisition des nouveaux langages	3.1. Gestion efficace sur les évolutions et nouveaux langages	05
Acquérir les notions en Développement web, applicatif et bases de données	Processus	4.Identification des types de langage	4.1. Acquisition correcte du HTML/CSS, frameworks front-end comme React, Angular, PHP, Node.js, langage de base de données	05
		5.Elaboration du développement défensif	5.1. Acquisition correcte du développement défensif	05
		6.Gestion des vulnérabilités	6.1. Gestion correcte des vulnérabilités	05
		7.Description de la Cryptographie	7.1. Acquisition correcte de la Cryptographie	05
		8.Utilisation des identités	8.1. Gestion correcte des identités	05
Acquérir les notions d'algorithmie et structures de	Produit		9.1. Gestion efficace de la complexité des algorithmes ;	05

données		9.Acquisition de la Gestion, de l'Implémentation et de l'Optimisation des algorithmes "		
			9.2. Implémentation correcte d'algorithmes courants ;	05
		10. Analyse et optimisation d'algorithmes	10.1. Analyse et optimisation efficace d'algorithmes	**05**
Utiliser la programmation système	Processus	11.Utilisation de la mémoire et threads	11.1. Utilisation appropriée de la mémoire et threads	**05**
		12.Utilisation des Langages de bas niveau comme C, assemblage	12.1 Utilisation correcte des Langages de bas niveau comme C, assemblage	05
		13.Utilisation du Développement embarqué/temps réel	13.1. Utilisation appropriée du Développement embarqué/temps réel.	05
Sécuriser le code source	Processus	14.Exécution des tests de vulnérabilités	14.1. Exécution correcte des tests de vulnérabilités	05
		15.Attribution des droits et permissions	15.1. Attribution appropriée des droits et permissions	05
		16.Utilisation du développement défensif	16.1. Utilisation correcte du développement défensif	05
		17.Gestion des vulnérabilités	17.1Gestion efficace des vulnérabilités	05
	Processus .	18.Utilisation judicieuse de la Cryptographie	18.1. Utilisation judicieuse de la Cryptographie	05

DESCRIPTION DE L'ÉPREUVE	Code : UASI04

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

Renseignements généraux

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

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

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

L'évaluation portera sur les points suivants :

1.Identifier le langage de programmation généralistes ;
2.Acquérir les notions en Développement web et applicatif ;
3. Acquérir les notions d'algorithmie et structures de données.
4. Utiliser la programmation système ;
5. Sécuriser le code source.

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

Liens avec les autres compétences

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

Contenu de l'épreuve

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

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

Matériel *(Pour un groupe de 25 apprenants)*

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

Consigne particulière

L'épreuve pourrait être administrée dès la fin du temps d'apprentissage de la compétence.

En cas d'échec, l'épreuve devrait être reprise dans son ensemble. Si un seul élément est très faible comparativement aux autres pour lesquels les performances de l'apprenant seraient excellentes, seul

cet élément pourrait être repris.

FICHE D'ÉVALUATION			**Code : UASI04**
Compétence 6: Utilisation des langages de programmation			**Durée :8h**
Nom de l'apprenant: Établissement d'enseignement: Date de l'évaluation: Signature du formateur:			**Résultat** **SUCCÈS** ☐ **ÉCHEC** ☐
ÉLÉMENTS D'OBSERVATION	**OUI**	**NON**	**RÉSULTATS**
1**. Identification des caractéristiques et spécificités** 1.1. Identification correcte des caractéristiques et spécificités			0 ou 05
2. **Comparaison des langages** 2.1. Comparaison minutieuse des langages entre eux			0 ou 05
3. **Acquisition des nouveaux langages** 3.1. Gestion efficace sur les évolutions et nouveaux langages			0 ou 05
4.**Identification des types de langage** 4.1. Acquisition correcte du HTML/CSS, frameworks front-end comme React, Angular, PHP, Node.js.			0 ou 05
5.**Elaboration du développement défensif** 5.1. Acquisition correcte du développement défensif			0 ou 05
6.**Gestion des vulnérabilités** 6.1. Gestion correcte des vulnérabilités			0 ou 05
7.**Description de la Cryptographie** 7.1. Acquisition correcte de la Cryptographie			0 ou 05
8.**Utilisation des identités** 8.1. Gestion correcte des identités			0 ou 05
9.**Acquisition de la Gestion, de l'Implémentation et de l'Optimisation des algorithmes** 9.1. Gestion efficace de la complexité des algorithmes			0 ou 05
9.2. Implémentation correcte d'algorithmes courants			0 ou 05
10 **Analyse et optimisation d'algorithmes** 10.1. Analyse et optimisation efficace d'algorithmes			0 ou 05

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

TABLEAU DE SPÉCIFICATIONS				
Métier	**PENTESTER**		Code	**IVPS07**
N° et libellé de la compétence	**7 Identifier les vulnérabilités potentielles dans les Systèmes informatiques**		Durée d'apprentissage/d'évaluation	**60h**
Éléments de la compétence	Stratégie	Indicateurs	Critères d'évaluation	Points
Acquérir les connaissances approfondies en sécurité informatique	Processus	1. transmission des connaissances de référence	1. 1. Acquisition parfaite des concepts, modèles et normes de référence	05
			1.2. Transmission correcte des connaissances	05
		2. détection des nouvelles menaces.	2.1 Identification correcte des nouvelles menaces.	05
		3. identification des nouvelles avancées dans le domaine	3.1 Contrôle exact de l'évolution des connaissances.	05
Décrire un audit de configuration	Processus	4. Vérification du périmètre couvert et des tests réalisés	4.1 Vérification correcte du périmètre couvert	10
			4.2 Vérification correcte des tests réalisé ;	10
		5.Élaboration du rapport d'audit	5.1 Précision -pertinente du rapport d'audit produit	05
Effectuer une analyse statique et dynamique de code source	Processus	6. Identification des vulnérabilités	6.1. Détection correcte des vulnérabilités	10
		7.Acquisition des résultats et des recommandations	7.1 Précision pertinente des résultats produits	05
			7.2. Détermination Pertinente des recommandation	05
Effectuer les tests d'intrusion	Processus	8.Analyse des failles de sécurité	8.1 Exploitation correcte des vulnérabilités	10

("penetration testing") .		9. précision des prévisions	9.1 Détermination correcte des résultats	10
Veiller sur les vulnérabilités	Processus	10. anticipation des tendances émergentes à partir des sources identifiées	10.1. Identification judicieuse des sources de veille	05
		11. Exploitation des alertes sur les vulnérabilités	11.1 Exploitation correcte des alertes sur les vulnérabilités	05
		12. Contextualisation du Niveau de Précision de la sécurité	12.1 Contextualisation efficace par rapport au système audité	05

DESCRIPTION DE L'ÉPREUVE	Code : IVPS07
Métier	**PENTESTER**
N° et énoncé de la compétence	**7. Identifier les vulnérabilités potentielles dans les Systèmes informatiques**

Renseignements généraux

L'épreuve a pour but d'évaluer la compétence relative à « *: Identifier les vulnérabilités potentielles dans les Systèmes informatiques* ». Il s'agit d'une épreuve d'évaluation qui prend en considération une portion d'évaluation des connaissances théoriques et une portion de type pratique.

L'évaluation de type pratique pourrait être administrée individuellement.

L'évaluation des connaissances théoriques pourrait être réalisée avec l'ensemble des apprenants.

L'environnement de réalisation de l'épreuve de type pratique devrait s'inspirer le plus possible d'une situation en milieu de travail.

La durée cumulée de l'ensemble des épreuves pourrait être d'environ 4 heures, et inclure la portion pratique combinée à celle de l'évaluation des connaissances théoriques pour les différents éléments de compétence.

Déroulement de l'épreuve

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

Matériel (Pour un effectif de 25 apprenants)

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

Consignes particulières

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

FICHE D'ÉVALUATION		Code : IVPS07
N° et énoncé de la compétence	**7. Identifier les vulnérabilités potentielles dans les Systèmes informatiques**	**Durée :4h:**

Nom de l'apprenant:
Établissement d'enseignement:
Date de l'évaluation:
Signature du formateur:

Résultat	
SUCCÈS	**ÉCHEC**
☐	☐

ÉLÉMENTS D'OBSERVATION	OUI	NON	RÉSULTATS
1. **transmission des connaissances de référence** 1. 1. Acquisition parfaite des concepts, modèles et normes de référence ;			0 ou 05
1.2. Transmission correcte des connaissances			0 ou 05
2. **détection des nouvelles menaces.** 2.1 Identification correcte des nouvelles menaces ;			0 ou 05
3. **identification des nouvelles avancées dans le domaine** 3.1 Contrôle exact de l'évolution des connaissances			0 ou 05
4. **Vérification du périmètre couvert et des tests réalisés**			0 ou 10
4.1 Vérification correcte du périmètre couvert 4.2 Vérification correcte des tests réalisé ;			0 ou 10
5.**Élaboration du rapport d'audit** 5.1 Précision -pertinente du rapport d'audit produit			0 ou 05
6. **Identification des vulnérabilités** 6.1. Détection correcte des vulnérabilités			0 ou 10
7.**Acquisition des résultats et des recommandations** 7.1 Exploitation correcte des vulnérabilités			0 ou 05
8. **précision des prévisions** 8.1 Détermination correcte des résultats			0 ou 10
9. **anticipation des tendances émergentes à partir des sources identifiées** 9.1. Identification judicieuse des sources de veille			0 ou 05
10**.** anticipation des tendances émergentes à partir des sources identifiées 10.1. Identification judicieuse des sources de veille			0 ou 10
11. **Exploitation des alertes sur les vulnérabilités** 11.1 Exploitation correcte des alertes sur les vulnérabilités			0 ou 05

12. Contextualisation du Niveau de Précision de la sécurité 12.1 Contextualisation efficace par rapport au système audité			0 ou 010
		TOTAL:	**/100**
Seuil de réussite: 70 % et obligation de satisfaire aux exigences des critères 2.1;3.1;4.1;6.1;11.1			
Règle de verdict: Le formateur devra s'assurer qu'en dehors de la maîtrise des opérations, l'apprenant adopte des attitudes respectant les règles de sécurité pour lesquelles il aura été évalué.	**Oui** ☐	**Non** ☐	
Remarque :			

TABLEAU DE SPÉCIFICATIONS				
Métier	**PENTESTER**		**Code**	**COPS08**
N° et Énoncé de la compétence	8. **Configurer les outils de test de pénétration des systèmes d'exploitation**		**Durée d'apprentissage**	**120h**
Éléments de la compétence	**Stratégie**	**Indicateurs**	**Critères d'évaluation**	**Points**
Utiliser des outils de tests de pénétration d'intrusion	Processus	1. Exploitation des fonctionnalités des outils	1.1 Exploitation efficace des fonctionnalités des outils	
		2**.** Identification des outils en fonction des tests	2.1. Choix pertinent des outils en fonction des tests	10
	Processus	3. Documentation des résultats	3.1 Documentation pertinente des résultats	
Configurer les outils	Processus	4. Réalisation des paramétrages	4. **1.** Réalisation correcte des paramétrages	10
	Produit	5. Choix des options/modules	5.1. Sélection pertinente des options/modules	10
	Processus	6. Exécution des tâches de configuration	6.1. Exécution appropriée des tâches de configuration	10
		7. protection des configurations déployées	7.1. Sécurisation correcte des configurations déployées	10
Configurer les systèmes d'exploitation cibles	Processus	8. Spécification des OS ciblés	8.1 Spécification efficace des OS ciblés	10
		9.. Documentation des services et ports testés	9.1. Documentation pertinente des services et ports testé	
	Processus	10. Utilisation **des** mises à jour des configurations	10.1 Exploitation efficace des mises à jour des configurations	10

Elaborer les Scripts	Processus	11.Exploitation des codes langage	11.1. Utilisation correcte du code /langage	10
	Processus	12. Utilisation des fonctionnalités	12.1. Gestion Pertinente des fonctionnalités	10
	Produit	13 Vérification de l'efficacité des scripts	13.1 Vérification correcte de l'efficacité des scripts	10
	Processus	14 Documentation pertinente des techniques des scripts	14.1 Documentation pertinente des techniques des scripts	

DESCRIPTION DE L'ÉPREUVE	Code : COPS08
N° et énoncé de la compétence	**8. Configurer les outils de test de pénétration des systèmes d'exploitation**

Renseignements généraux

L'épreuve a pour but d'évaluer la compétence relative à « *Configurer les outils de test de pénétration des systèmes d'exploitation* ». Il s'agit d'une épreuve d'évaluation qui prend en considération une portion d'évaluation des connaissances théoriques et une portion de type pratique.

L'évaluation de type pratique pourrait être administrée individuellement.

L'évaluation des connaissances théoriques pourrait être réalisée avec l'ensemble des apprenants.

L'environnement de réalisation de l'épreuve de type pratique devrait s'inspirer le plus possible d'une situation en milieu de travail.

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

Déroulement de l'épreuve

Par l'entremise d'une épreuve de connaissances théoriques, on pourrait demander à l'apprenant d'Utiliser des outils de tests de pénétration d'intrusion, de Configurer les outils, les systèmes d'exploitation cibles et d'Elaborer les Scripts intelligents.

Matériel (Pour un effectif de 25 apprenants)

- Matériel informatique
- Outils de test d'intrusion
- Environnement de test
- Matériel de réseau :
- Outils de capture de trafic
- Stylo à bille, crayons de dessin ;

Consignes particulières

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

FICHE D'ÉVALUATION		Code : COPS08
N° et libellé de la compétence	**8. Configurer les outils de test de pénétration des systèmes d'exploitation**	**Durée :8h**

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

ÉLÉMENTS D'OBSERVATION	**OUI**	**NON**	**RÉSULTATS**
1**. Exploitation des fonctionnalités des outils** 1.1. Exploitation efficace des fonctionnalités des outils			
2. **Identification** des outils en fonction des tests 2.1. Choix pertinent des outils en fonction des tests			0 ou 010
3. **Documentation des résultats** 3.1 Documentation pertinente des résultats			
4. **Réalisation des paramétrages** 4. **1.** Réalisation correcte des paramétrages			0 ou 10
5**.** Choix **des options/modules** 5.1. Sélection pertinente des options/modules			0 ou 10
6. **Exécution appropriée des tâches de configuration** 6.1. Exécution appropriée des tâches de configuration			0 ou 10
7. **protection des configurations déployées** 7.1. Sécurisation correcte des configurations déployées			0 ou 10
8. **Spécification des OS ciblés** 8.1 Spécification efficace des OS ciblés			0 ou 10
9.. Documentation des services et ports testés 9.1. Documentation pertinente des services et ports testés			
10. **Utilisation** des mises à jour des configurations 10.1 Exploitation efficace des mises à jour des configurations			0 ou 10
11.**Exploitation des codes langage** 11.1. Utilisation correcte du code /langage			0 ou 10
12. **Utilisation des fonctionnalités** 12.1. Gestion Pertinente des fonctionnalités			0 ou 10
13. **Vérification de l'efficacité des scripts** 13.1 Vérification correcte de l'efficacité **des scripts**			0 ou 10
14 **Documentation pertinente des techniques des scripts** 14.1 Documentation pertinente des techniques des scripts			
EXIGENCES L'évaluation des connaissances pratiques pourrait être utilisée au cas où une observation (évaluation pratique) ne pourrait pas être réalisée. Si tel est le cas, l'apprenant devra répondre adéquatement à 80 % des questions			

FICHE D'ÉVALUATION		Code : COPS08	
N° et libellé de la compétence	**8. Configurer les outils de test de pénétration des systèmes d'exploitation**	**Durée :8h**	
qui lui sont posées afin d'obtenir la totalité des points associés au critère d'évaluation			
		TOTAL:	**/100**
Seuil de réussite: 70 points			
Règle de verdict: Le formateur devra s'assurer qu'en dehors de la maîtrise des opérations, l'apprenant adopte des attitudes respectant les règles de sécurité.		**Oui** ☐	**Non** ☐
Remarque			

TABLEAU DE SPÉCIFICATIONS				
Métier	**PENTESTER**		**Code**	**RVAP09**
N° et Énoncé de la compétence	**9. Tester la vulnérabilité sur les Réseaux, les applications, site web et les systèmes d'exploitation**		**Durée d'apprentissage/d'évaluation**	**150h**
Éléments de la compétence	**Stratégie**	**Indicateurs**	**Critères d'évaluation**	**Points**
Analyser la topologie et les flux réseau	Produit	1. Production des informations	1.1.Production correcte des informations	**05**
		2. Réalisation de la cartographie réseaux	2.1..Réalisation correcte de la cartographie réseau	**05**
	Processus	3.Gestion des flux	3.1.Gestion efficace des flux	**05**
		4.Evaluation des métriques réseau	4.1.Evaluation correcte des métriques réseau	**05**
Identifier les vecteurs d'intrusion réseau	Processus	5.Identification des techniques d'attaque réseau	5.1. Identification correcte des techniques d'attaque réseau ;	**05**
		6. Analyse appropriée des logs et alertes	6.1. Analyse appropriée des logs et alertes	**05**
		7. Collecte minutieuse des vecteurs potentiels couverts	7.1. Collecte minutieuse des vecteurs potentiels couverts.	**05**
Décrire les outils de tests de vulnérabilités	Processus	8. Acquisition des outils de test d'intrusion des réseaux /applications	8.1 Présentation correcte des outils de tests d'intrusion/pentesting	10
			8.2 Description parfaite des fonctionnalités	05
		9. Détection des vulnérabilités des réseaux/applications	9.1. Détection correcte des vulnérabilités des réseaux/applications	05
Tester l'efficacité du réseau et des applications :	Processus	10.Description des résultats de tests	10.1. Analyse judicieuse des résultats de tests	10
		11.Utilisation des préconisations	11.1. Application efficace des préconisations	05
		12.Identification des failles	12.1. Détection correcte de failles dans les APIs, services web	05
Tester les systèmes	Processus	13. Description des configurations	13.1. Gestion efficace des configurations et	05

d’exploitation :		et services testés	services testés ;	
		14.Scanne des vulnérabilités	14.1Précision correcte du diagnostic de vulnérabilité	05
	Produit	15. Recommandation des correctifs et mesures	15. 1. Recommandation des correctifs et mesures	10

DESCRIPTION DE L'ÉPREUVE		Code : RVAP09
N° et énoncé de la compétence	*9* **Tester la vulnérabilité sur les Réseaux, les applications, site web et les systèmes d'exploitation**	
Renseignements généraux		
L'épreuve a pour but d'évaluer la compétence relative à « *Effectuer les tests de vulnérabilité, sur les Réseaux, les applications, site web et les systèmes d'exploitation* ». Il s'agit d'une épreuve d'évaluation qui prend en considération une portion d'évaluation des connaissances théoriques et une portion de type pratique. L'évaluation de type pratique pourrait être administrée individuellement. L'évaluation des connaissances théoriques pourrait être réalisée avec l'ensemble des apprenants. L'environnement de réalisation de l'épreuve de type pratique devrait s'inspirer le plus possible d'une situation en milieu de travail. La durée cumulée de l'ensemble des épreuves pourrait être d'environ 10 heures, et inclure la portion pratique combinée à celle de l'évaluation des connaissances théoriques pour les différents éléments de compétence.		
Déroulement de l'épreuve Par l'entremise d'une épreuve de connaissances théoriques, on pourrait demander à l'apprenant d'Analyser la topologie et les flux réseau, d' Analyser les risques et menaces, de Décrire les outils de tests de vulnérabilités, de Tester l'efficacité du réseau, des applications, du système d'exploitation, et de présenter un rapport des résultats. On pourrait également demander à l'apprenant, dans le cadre d'une évaluation pratique, de Tester l'efficacité d'un serveur web à partir des outils de test de son choix.		
Matériel (Pour un effectif de 25 apprenants) • Ordinateurs portables puissants, • Outils de test d'intrusion • Environnement de test • Matériel de réseau : • Outils de capture de trafic		
Consignes particulières • L'épreuve pourrait être administrée durant le temps d'apprentissage d'une compétence subséquente ou d'une compétence évaluée en parallèle. • En cas d'échec, l'épreuve devrait être reprise dans son ensemble. Si un seul élément est très faible comparativement aux autres pour lesquels les performances de l'apprenant seraient excellentes, seul cet élément pourrait être repris.		

FICHE D'ÉVALUATION			Code : RVAP09
N° et énoncé de la compétence	9. **Tester la vulnérabilité sur les Réseaux des applications, site web et les systèmes d'exploitation**		
Nom de l'apprenant: Établissement d'enseignement: Date de l'évaluation: Signature du forma :			**Résultat** **SUCCÈS** ☐ **ÉCHEC** ☐
ÉLÉMENTS D'OBSERVATION	**OUI**	**NON**	**RÉSULTATS**
1.Production des informations 1.1.Production correcte des informations			0 ou 10
2.Réalisation de la cartographie réseaux 2.1..Réalisation correcte de la cartographie réseau			0 ou 05
3.Evaluation des métriques réseau **3.1.** Evaluation correcte des métriques réseau			0 ou 05
4.Identification des techniques d'attaque réseau 4.1.Identification correcte des techniques d'attaque réseau			0 ou 05
5.**Gestion des logs et alertes** 5.1**.** Gestion efficace des logs et alertes			0 ou 05
6.**Utilisation des modèles de compromission** 6.1.Utilisation parfaite des modèles de compromission			0 ou 05
7.Calcul des métriques de propagation 7.1. Calcul correct des métriques de propagation			0 ou 05
8. Acquisition des outils de test d'intrusion des réseaux /applications 8.1 Présentation correcte des outils de tests d'intrusion/pentesting 8.2 Description parfaite des fonctionnalités			0 ou 10 0 ou 05
9. **Détection des vulnérabilités des réseaux ou applications** 9.1 Détection des vulnérabilités des réseaux ou applications			0 ou 05
10.Description des résultats de tests 10.1. Analyse judicieuse des résultats de tests			0 ou 10
11.**Utilisation des préconisations** 11.1. Application efficace des préconisations			0 ou 05
12.**Identification des failles** 12.1. Détection correcte de failles dans les APIs, services web			0 ou 05
13. **Description des configurations et services testés** 13.1. Gestion efficace des configurations et services testés.			0 ou 05
14.**Scanne des vulnérabilités** 14.1Précision correcte du diagnostic de vulnérabilité			0 ou 05

FICHE D'ÉVALUATION			Code : RVAP09
N° et énoncé de la compétence	9. **Tester la vulnérabilité sur les Réseaux des applications, site web et les systèmes d'exploitation**		
15. **Recommandation des correctifs et mesures** 15.1 Conduite rigoureuse des tests, mesures et contrôles permettant de valider ou non les hypothèses			0 ou 10
EXIGENCES L'évaluation des connaissances pratiques pourrait être utilisée au cas où une observation (évaluation pratique) ne pourrait pas être réalisée. Si tel est le cas, l'apprenant devra répondre adéquatement à 70 % des questions qui lui sont posées afin d'obtenir la totalité des points associés au critère d'évaluation			
		TOTAL :	**/100**
Seuil de réussite: 70 points			
Règle de verdict.	**Oui** ☐	**Non** ☐	
Remarque			

TABLEAU DE SPÉCIFICATIONS				
Métier	**PENTESTER**		**Code**	**PSAT10**
N° et libellé de la compétence	**10. Proposition des stratégies d'atténuation**		**Durée d'apprentissage**	**150h**
Éléments de la compétence	**Stratégie**	**Indicateurs**	**Critères d'évaluation**	**Points**
Évaluer la propagation latérale de l'attaquant	**Processus**	1.Utilisation des modèles de compromission	1.1.Utilisation parfaite des modèles de compromission ;	; **05**
		2.Simulation des scénarios de propagation	2.2.Simulation efficace des scénarios de propagation	05
	Produit	**3.** Calcul des métriques de propagation	3.1.Calcul correct des métriques de propagation	**05**
Concevoir des scénarios de segmentation réseau	**Processus**	4.Elaboration d'un microsegmentation du réseau ;	4.1.Elaboration correcte d'un microsegmentation du réseau ;	**05**
	Processus	5.Gestion des scénarios	5.1.Gestion efficace des scénarios	**05**
	Produit	6.documentation de la technique proposée	6.1.documentation pertinente de la technique proposée	**05**
Analyser les risques et menaces	**Processus**	6.Analyse des menaces et vulnérabilités ;	6.1Analyse efficace des menaces et vulnérabilités ; .	**05**
	Processus	7.Exploitation du contexte organisationnel et règlementaire ;	7.1.Exploitation correcte du contexte organisationnel et règlementaire ;	**05**
	Processus	8.Analyse efficace des mises à jour	8.1.Analyse efficace des mises à jour	**05**
Réaliser des conseils sur l'architecture sécurité	Produit	9. Elaboration d'une microsegmentation du réseau	9.1.Elaboration correcte d'une microsegmentation du réseau	**05**

	Processus	10. Gestion des scénarios	10.1 Gestion efficace des scénarios	**05**
		11. Documentation de la technique proposée	11.1 Documentation correcte de la technique proposée	**05**
Élaborer une politique de sécurité	Processus	12. Gestion des bonnes pratiques et référentiels reconnus ;	12.1 Production efficace d'une documentation présentant la politique de sécurité	
			12.2. Utilisation correcte des bonnes pratiques et référentiels reconnus ;	**05**
	Produit	13 Elaboration d'un plan d'action de suivi et d'audit	13.1. Elaboration correcte d'un plan d'action de suivi et d'audit	**05**
Préconiser des mesures techniques	Processus	14.Proposition des solutions exhaustives ;	14.1.Proposition pertinente des solutions exhaustives ; .	**05**
		15. Déploiement et administration correctes d'une politique de sécurité ;	15.1.Déploiement et administration correctes d'une politique de sécurité ;	**05**
		16.Reduction efficace des risques	16.1.Reduction efficace des risques	**05**
Valider la mise en œuvre	Processus	17. Validation des tests	17.1.Utilisation correcte des scénarios de tests	**05**
			17.2 Gestion efficace des tests effectués	**05**
		18. .Contrôle du respect des spécifications définies	18.1Contrôle efficace du respect des spécifications définies	**05**

DESCRIPTION DE L'ÉPREUVE	Code : PSAT10
N° et énoncé de la compétence	**10. Proposition des stratégies d'atténuation**

Renseignements généraux

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

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

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

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

Déroulement de l'épreuve

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

Matériel et équipements (Pour un groupe de 25 apprenants)

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

Les Bics et crayons

Consigne particulière

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

FICHE D'ÉVALUATION		Code : PSAT10
N° et énoncé de la compétence	**10. Proposition des stratégies d'atténuation**	**Durée :10h**

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

ÉLÉMENTS D'OBSERVATION	**OUI**	**NON**	**RÉSULTATS**
1.**Utilisation des modèles de compromission** 1.1.Utilisation parfaite des modèles de compromission ;			0 ou 05
2.Simulation des scénarios de propagation 2.2.Simulation efficace des scénarios de propagation			0 ou 05
3.Calcul des métriques de propagation 3.1.Calcul correct des métriques de propagation			0 ou 05
4.Elaboration d'un microsegmentation du réseau 4.1.Elaboration correcte d'un microsegmentation du réseau			0 ou 05
5.Gestion des scénarios 5.1.Gestion efficace des scénarios			0 ou 05
6.documentation de la technique proposée 6.1.documentation pertinente de la technique proposée			0 ou 05
7.**Exploitation du contexte organisationnel et règlementaire** 7.1.Exploitation correcte du contexte organisationnel et règlementaire ;			0 ou 05
8.Analyse efficace des mises à jour 8.1.Analyse efficace des mises à jour			0 ou 05
9.Elaboration d'une microsegmentation du réseau 9.1.Elaboration correcte d'une microsegmentation du réseau			0 ou 05
10.**Gestion des scénarios** 10.1.Gestion efficace des scénarios			0 ou 05
11.**Documentation de la technique proposée** 11.1.Documentation correcte de la technique proposée			0 ou 05
12.**Gestion des bonnes pratiques et référentiels reconnus** 12.1.Production efficace d'une documentation présentant la politique de sécurité 12.2. Utilisation correcte des bonnes pratiques et référentiels reconnus ;			 0 ou 05
13.Elaboration d'un plan d'action de suivi et d'audit 13.1.Elaboration correcte d'un plan d'action de suivi et d'audit			0 ou 05
14.**Proposition des solutions exhaustives** ; 14.1.Proposition pertinente des solutions exhaustives			0 ou 05

15.**Déploiement et administration correctes d'une politique de sécurité** 15.1.Déploiement et administration correctes d'une politique de sécurité ;			0 ou 05
16.**Reduction efficace des risques** 16.1.Reduction efficace des risques			0 ou 05
17.Validation des tests 17.1.Utilisation correcte des scénarios de tests 17.2.Gestion efficace des tests effectués			0 ou 05 0 ou 05
18. .Contrôle du respect des spécifications définies 18.1Contrôle efficace du respect des spécifications définies			0 ou 05
		TOTAL:	**/100**
Seuil de réussite: 70 % et obligation de satisfaire aux exigences des critères 1.1;5.1 ,7.1, 13.2			
Règle de verdict: Le formateur devra s'assurer qu'en dehors de la maîtrise des opérations, l'apprenant adopte des attitudes respectant les règles de sécurité pour lesquelles il aura été évalué à la compétence 03.	**Oui** ☐	**Non** ☐	
Remarque :			

TABLEAU DE SPÉCIFICATIONS				
Métier	**PENTESTER**		**Code : CPFDI11**	**CPFDI11**
N° et énoncé de la compétence	**11. Configurer les pares-feux et des systèmes de détection d'intrusions**		**Durée d'apprentissage**	**75h**
Éléments de la compétence	**Stratégie**	**Indicateurs**	**Critères d'évaluation**	**Points**
Configurer les pare-feux et des IDS/IPS		1 Validation des tests	1.1. Définition Précise des règles/signatures	**5**
			1.2. Validation correcte des tests effectués	**5**
	Produit	3 Documentation des techniques produites	3.1. Documentation correcte des techniques produites	**10**
Implémenter une politique de filtrage et de détection	Processus	4 Utilisation des bonnes pratiques de sécurité ;	4.1. Utilisation correcte des bonnes pratiques de sécurité ;	**10**
		5 Déploiement sur l'infrastructure cible ;	5.1. Déploiement approprié sur l'infrastructure cible ;	**10**
		6 Mesure de la politique de filtrage et de détection	6.1. Mesure efficace de la politique de filtrage et de détection	**10**
Gérer les règles, les signatures et les listes blanches/noires	Processus	7 Réactivité aux nouvelles menaces ;	7.1. Réactivité appropriée aux nouvelles menaces ;	**10**
		8 Gestion des configurations	8.1. Contrôle efficace d'impact des modifications ;	**5**
			8.2. Exploitation correcte de la supervision des configurations.	**5**
Superviser les événements de sécurité générés	Processus	9 Exploitation des corrélations et alertes remontées ;	9.1. Exploitation rationnelle des corrélations et alertes remontées ;	**10**
	Produit	10 Collecte des logs et	10.1. Collecte Exhaustive des logs et	**10**

		métriques	métriques	
	Processus	11 Description de reporting des incidents	11.1. Description correcte de reporting des incidents	**10**

DESCRIPTION DE L'ÉPREUVE	Code : CPFDI11
N° et énoncé de la compétence	**11. Configurer les pares-feux et des systèmes de détection d'intrusions**

Renseignements généraux

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

Déroulement de l'épreuve

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

Matériel et équipements (Pour un groupe de 25 apprenants)

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

Consigne particulière

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

FICHE D'ÉVALUATION		Code : CPFDI11
N° et énoncé de la compétence	**11. Configurer les pares-feux et des systèmes de détection d'intrusions**	**Durée : 5h**

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

ÉLÉMENTS D'OBSERVATION	**OUI**	**NON**	**RÉSULTATS**
1. **Validation des tests** 1.1. Définition Précise des règles/signatures ;			0 ou 05
1.2. Validation correcte des tests effectués ;			0 ou 05
2. **Production des documents techniques** 2.1. Documentation correcte des techniques produites			0 ou 10
3. Utilisation des bonnes pratiques de sécurité ; 3.1 Utilisation correcte des bonnes pratiques de sécurité ;			0 ou 10
4. Déploiement sur l'infrastructure cible 4.1 Déploiement approprié sur l'infrastructure cible			0 ou 10
5. Mesure de la politique de filtrage et de détection 5.1. Mesure efficace de la politique de filtrage et de détection			0 ou 10
6. Réactivité aux nouvelles menaces ; 6.1. Réactivité appropriée aux nouvelles menaces ;			0 ou 10
7. Gestion des configurations 7.1 Contrôle efficace d'impact des modifications ;			0 ou 05
7.2 Exploitation correcte de la supervision des configurations.			0 ou 05
8. Exploitation des corrélations et alertes remontées ; 8.1. Exploitation rationnelle des corrélations et alertes remontées ;			0 ou 10
9. Collecte des logs et métriques 9.1. Collecte Exhaustive des logs et métriques			0 ou 10
6. Description de reporting des incidents 10.1 Description correcte de reporting des incidents			0 ou 10
		TOTAL:	**/100**
Seuil de réussite: 70 %			
Règle de verdict: Le formateur devra s'assurer qu'en dehors de la maîtrise des opérations, l'apprenant adopte des attitudes respectant les règles de sécurité pour lesquelles il aura été évalué à la compétence 03.	**Oui** ☐	**Non** ☐	
Remarque :			

TABLEAU DE SPÉCIFICATIONS				
Métier	**PENTESTER**		**Code :VTCY12**	**VTCY12**
N° et énoncé de la compétence	**12. Assurer la veille technologique en cyberattaque**		**Durée d'apprentissage**	**75h**
Éléments de la compétence	**Stratégie**	**Indicateurs**	**Critères d'évaluation**	**Points**
Assurer la veille technologique et sécuritaire	Processus	1. diffusion des alertes sur les nouvelles menaces ;	1.1. diffusion correcte des alertes sur les nouvelles menaces ;	**05**
		2. analyse des tendances et évolutions ;	2.1 analyse pertinente des tendances et évolutions ;	**10**
	Produit	3. Collecte de la documentation	3.1 Collecte efficace de la documentation des informations	**05**
Analyser les nouvelles techniques d'attaques	Processus	4. Identification des vecteurs et failles exploités ;	4.1. Identification précise des vecteurs et failles exploités ;	**05**
		5. Évaluation de la criticité et de l'impact potentiel	5.1 Évaluation correcte de la criticité et de l'impact potentiel	**10**
		6. Exploitation des mises à jour	6.1 Exploitation efficace des mises à jour de l'analyse en fonction des retours	**05**
Évaluer l'impact sur l'architecture existante	Processus	7. Analyse des risques encourus ;	7.1. Analyse correcte des risques encourus ;	**10**
		8. Gestion des scénarios de test	8.1 Utilisation correcte des scénarios de tests ;	**05**
			8.2 Exploitation Précise de la documentation des résultats	**05**
Préconiser des mesures correctives	Processus	10. Gestion des risques	9.1. Rapprochement correcte entre les objectifs de sécurité et le niveau de risque ;	**05**

			9.2. Implémentation et pertinence correcte des solutions ;	**05**
		12. Exploitation du rapport coût/bénéfice et des contraintes	10.1 Exploitation correcte du rapport coût/bénéfice et des contraintes	**05**
		13. Adaptation du délai de mise en œuvre à la criticité.	11.1 Adaptation correcte du délai de mise en œuvre à la criticité.	**05**
				05
Valider la réponse apportée	Processus	15. Exécution des tests	12.1 exécution correcte des tests;	**05**
		16. Production d'une documentation des résultats	13.1 Production exacte d'une documentation des résultats ;	**05**
		17. Respect des spécifications définies	14.1 Respect correct des spécifications définies.	**05**

DESCRIPTION DE L'ÉPREUVE	Code : VTCY12
N° et énoncé de la compétence	12.. Assurer la veille technologique en cyberattaque

Renseignements généraux

L'épreuve a pour but d'évaluer la compétence relative à « Assurer la veille technologique en cyberattaque ».

Il s'agit d'une épreuve d'évaluation qui prend en considération l'évaluation des connaissances théoriques et petite portion de type pratique.

L'évaluation de type pratique pourrait être administrée à un groupe restreint d'apprenants en raison de la disponibilité du matériel, de la matière d'œuvre et de la capacité du formateur à observer plusieurs personnes à la fois.

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

L'épreuve pourrait être d'une durée d'environ (5 heures), ce qui inclut la portion combinée à celle de l'évaluation des connaissances théoriques et pratique.

Déroulement de l'épreuve

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

Matériel et équipements (Pour un groupe de 25 apprenants)

- Ordinateurs
- Internet ;
- Les logiciels

Consigne particulière

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

N° et énoncé de la compétence	12.. Assurer la veille technologique en cyberattaque	Durée :5h

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

ÉLÉMENTS D'OBSERVATION	OUI	NON	RÉSULTATS
1. Diffusion des alertes sur les nouvelles menaces 1.1. Diffusion correcte des alertes sur les nouvelles menaces			0 ou 05
2. Analyse des tendances et évolutions ; 2.1. Analyse pertinente des tendances et évolutions ;			0 ou 10
3. Collecte de la documentation 3.1. Collecte efficace de la documentation des informations			0 ou 05
4. Identification des vecteurs et failles exploités ; 4.1. Identification précise des vecteurs et failles exploités ;			0 ou 05
5. Évaluation de la criticité et de l'impact potentiel 5.1 Évaluation correcte de la criticité et de l'impact potentiel			0 ou 10
6. Exploitation des mises à jour 6.1 Exploitation efficace des mises à jour de l'analyse en fonction des retours			0 ou 05
7. Analyse des risques encourus ; 7.1. Analyse correcte des risques encourus ;			0 ou 10
8. Gestion des scénarios de test 8.1 Utilisation correcte des scénarios de tests ; 8.2 Exploitation Précise de la documentation des résultats			0 ou 05
9. Gestion des risques 9.1. Rapprochement correcte entre les objectifs de sécurité et le niveau de risque ; 9.2. Implémentation et pertinence correcte des solutions ;			0 ou 05
7. Exploitation du rapport coût/bénéfice et des contraintes 10.1 Exploitation correcte du rapport coût/bénéfice et des contraintes			0 ou 05
8. Adaptation du délai de mise en œuvre à la criticité. 11.1 Adaptation correcte du délai de mise en œuvre à la criticité.			0 ou 05

9. Exécution des tests 12.1 exécution correcte des tests;			0 ou 05
10. Production d'une documentation des résultats 13.1 Production exacte d'une documentation des résultats ;			0 ou 05
11. Respect des spécifications définies 14.1 Respect correct des spécifications définies.			0 ou 05
		TOTAL:	**/100**
Seuil de réussite: 70 %			
Règle de verdict: Le formateur devra s'assurer qu'en dehors de la maîtrise des opérations, l'apprenant adopte des attitudes respectant les règles de sécurité pour lesquelles il aura été évalué à la compétence 03.	**Oui** ☐	**Non** ☐	
Remarque :			

REFERENCES BIBLIOGRAPHIQUES

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

3 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.

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

5 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

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

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

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

9 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)

10 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 »

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

12 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.

13 Samurçay R. et Pastré, P. (2004), Stratégie de la formation professionnelle, République du Cameroun, Toulouse : Octarès, 187 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 des études sectorielles et préliminaires, 77 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 réalisation d'un référentiel de métier-compétences, 83 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, Guide - Conception et production d'un guide pédagogique, 61 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'évaluation, 86 pages.
18 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