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

PADESCE

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)

DRAFT DE RAPPORT D'ANALYSE DE SITUATION DE TRAVAIL

SECTEUR : NUMERIQUE

METIER : PENTESTER

NIVEAU DE QUALIFICATION : TECHNICIEN

EQUIPE D'ANIMATION DE L'AST (ANALYSE DE SITUATION DE TRAVAIL)

N°	NOMS ET PRÉNOM	STRUCTURE	QUALIFICATION
1	Mme ZANGA MOUTONG	**MINEFOP**	**METHODOLOGUE**
2	Mme WANKY Evelyne	**MINEFOP**	**METHODOLOGUE**
3	Mme DJANDA NZUATOM Epse NDOUOH Sylvie	**MINEFOP**	**METHODOLOGUE**

LISTE DES PARTICIPANTS AU FOCUS GROUP

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

EQUIPE DE REDACTION

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

TABLE DES MATIERES

REMERCIEMENTS

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

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

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

ABREVIATIONS ET ACRONYMES

APC	Approche Par Compétences
RAST	Rapport de l'Analyse de la Situation de Travail
CQP	Certificat de Qualification Professionnelle
CVE	Common Vulnerabilities and Exposures
DFOP	Direction de la Formation et de l'Orientation Professionnelles
DQP	Diplôme de Qualification Professionnelle
DTS	Diplôme de Technicien Spécialisé
ISO	International Organization for Standardization
NIST	National Institute of Standards and Technology
OWASP	Open Web Application Security Project
PME	Petite et Moyenne Entreprise
RSS	Really Simple Syndication
SA	Société Anonyme
SARL	Société à Responsabilité Limité
VAE	Validation des Acquis de l'Expérience

1 LISTE DES PERSONNES CONSULTEES

- **Les professionnels**

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

INTRODUCTION

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

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

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

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

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

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

PREMIERE PARTIE : DESCRIPTION GÉNÉRALE DE LA PROFESSION

1. DEFINITION DE LA FONCTION DE TRAVAIL

Un pentester est un professionnel de la cybersécurité du secteur numérique capable d'évaluer la sécurité des systèmes d'information en identifiant et en exploitant les vulnérabilités potentielles. C'est un professionnel qualifié qui utilise des méthodes et des outils spécialisés pour simuler des attaques informatiques et aider les organisations à renforcer leur sécurité en identifiant les failles et en fournissant des recommandations pour y remédier.

Il a pour missions principales de :

- Évaluer la sécurité des systèmes afin d'identifier les vulnérabilités potentielles qui pourraient être exploitées par des attaquants malveillants ;
- Réaliser les tests d'intrusion en simulant des attaques ciblées pour mettre à l'épreuve la résistance des systèmes de l'organisation ;
- Analyse des résultats et fournir des recommandations détaillées pour améliorer la sécurité ;
- Rédiger les rapports ;
- Sensibiliser à la sécurité afin de réduire les risques d'attaques informatiques.

2. CONTEXTE PROFESSIONNEL

2.1. Description de l'environnement de travail

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

Secteur d'activité

Selon les professionnels, le secteur d'activité d'un pentester est principalement lié à la sécurité informatique. Il travaille dans une variété d'industries, y compris les services financiers, les technologies de l'information, les entreprises de la cybersécurité, les gouvernements, les institutions de santé, les entreprises de commerce électronique, etc. Les entreprises de toutes tailles et de tous secteurs reconnaissent l'importance de protéger leurs systèmes et leurs données contre les cyberattaques. Par conséquent, le pentester a une demande croissante dans tous les secteurs où la sécurité de l'information est une priorité. Il peut être employés directement par ces organisations ou travailler en tant que consultants externes pour réaliser des tests d'intrusion, évaluer les vulnérabilités et fournir des recommandations pour renforcer la sécurité des systèmes informatiques.

Condition de travail

La condition de travail d'un pentester varie en fonction de plusieurs facteurs, y compris l'employeur, le type de contrat (permanent ou indépendant), et la nature des projets sur lesquels il travaille. Le pentester est souvent confronté à des horaires flexibles, car il doit s'adapter aux besoins et aux contraintes des clients. Il peut être amené à travailler en dehors des heures de travail normales pour éviter les interruptions des tests d'intrusion sur les systèmes en production. Le travail peut être intense et exigeant, car le pentester est souvent confronté à des délais serrés pour réaliser les tests de sécurité et produire des rapports détaillés. Il doit également être prêt à se maintenir constamment à jour sur les dernières techniques et outils de piratage et de sécurité.

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

a) Évolution technologique et conséquences

L'évolution technologique a un impact significatif sur le métier de pentester. D'une part, elle crée des nouvelles opportunités pour les attaques et les vulnérabilités, car des nouveaux systèmes, applications et infrastructures émergent constamment. Les pentesters doivent donc rester constamment à jour sur les dernières technologies et tendances en matière de sécurité pour comprendre les nouvelles méthodes d'attaque potentielles. D'autre part, l'évolution technologique offre également des nouveaux outils et techniques aux pentesters pour renforcer la sécurité. Par exemple, l'intelligence artificielle et l'apprentissage automatique peuvent être utilisés pour détecter les anomalies et les comportements suspects, tandis que l'automatisation peut accélérer les tests de sécurité. Cependant, les technologies émergentes, telles que l'Internet des objets (IoT) et l'intelligence artificielle, présentent également des nouveaux défis en matière de sécurité, nécessitant une compréhension approfondie des risques potentiels.

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

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

La rémunération est comment

3. APPELLATIONS COURANTES DE LA FONCTION DE TRAVAIL

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

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

4. PERSPECTIVES ET CHEMINEMENT D'EMPLOI

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

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

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

Conditions d'embauche

L'accès au métier passe généralement par les offres d'emplois qui sont publiées à travers divers canaux de diffusion, notamment la presse écrite, la radio et même la télévision. De plus en plus, ces offres sont également diffusées sur le réseau Internet dans des sites spécialisés. Enfin, certaines entreprises recourent aux services des Cabinets de recrutement dont le fonctionnement est régi par une règlementation fixée par le Ministère des Postes et Télécommunications.

Le technicien ou la technicienne spécialisé en pentester peut être recruté à partir :

- Du DTS en pentester ;
- Du CQP en sécurité informatique avec une expérience d'au moins deux ans dans le domaine ;
- etc.
- Les équivalents du sous-système anglophone sont également admis.

En plus du diplôme requis, les employeurs peuvent également demander une expérience préalable dans le domaine de la cybersécurité.

Rémunération

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

Horaires de travail

Quant aux horaires de travail, ils sont définis par la règlementation en vigueur. Le technicien pentester travaille généralement pendant 8 à 12 heures de travail par jour. Toutefois, ces durées peuvent être influencées par l'affluence et les conditions de travail, les heures supplémentaires sont rémunérées. Le travail nécessite parfois des horaires adaptés (temps perdu pendant une panne du réseau, intempéries etc.…).

.

b) Conditions d'accès à la formation

L'accès à la formation est ouvert aux personnes des deux sexes remplissant les conditions ci-après :

- Être âgées d'au moins dix-sept ans ;
- Avoir un BACCALAUREAT Scientifique C, D, TI ou Technique industrielle F2 ;
- Avoir un BT MISE (Maintenance et Installation des Systèmes Electroniques) ;
- Avoir le niveau Terminale avec VAE dans le domaine ;
- Être titulaire d'un DQP en Informatique avec une expérience d'au moins 3 ans dans le domaine ;
- Subir avec succès à un test de sélection à l'entrée en formation.

Les équivalents du sous-système anglophone sont également admis.

6. ACCESSIBILITE DES FEMMES AU METIER

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

7. IMPACT DU METIER SUR L'ENVIRONNEMENT

a) Au niveau de la santé et de la sécurité

Le métier de pentester a un impact sur la santé et la sécurité des professionnels qui l'exercent. Les pentesters sont souvent confrontés à des scénarios de test d'intrusion qui peuvent être stressants et exigeants, car ils doivent essayer d'exploiter les vulnérabilités des systèmes pour évaluer leur sécurité. Cela peut entraîner une pression psychologique et émotionnelle importante.

De plus, les pentesters sont exposés à des risques liés à la manipulation d'outils et de logiciels potentiellement dangereux, ainsi qu'à des environnements informatiques instables.

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

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

b) Au niveau de l'environnement

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

8. FORMATION EN MILIEU DE TRAVAIL

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

DEUXIEME PARTIE : DESCRIPTION DU TRAVAIL

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

1. CONCEPTS ET DEFINITIONS

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

- **Les tâches :**
  - sont les principales activités qu'une personne doit mener dans l'exercice de sa profession;
  - sont les différents types de travaux qui sont exécutés de façon régulière ou ponctuelle ;
  - correspondent à un ensemble d'actions permettant d'obtenir un résultat précis, un service ou un produit particulier.
- **Les opérations :**
  - correspondent aux étapes à franchir pour remplir une tâche donnée;
  - décrivent de quelle manière est exécutée une tâche.
- **Les conditions de réalisation :**
  - renvoient à la situation dans laquelle la tâche s'effectue;
  - précisent le degré d'autonomie entourant l'exécution de la tâche, les consignes et les normes à respecter;
  - renseignent sur les lieux de travail, les conditions environnementales et l'équipement utilisé pour exécuter une tâche;
  - indiquent les références à consulter et le matériel nécessaire à l'exécution d'une tâche donnée.
- **Les critères de performance :**
  - indiquent les caractéristiques observables et mesurables pour évaluer les éléments essentiels d'une réalisation satisfaisante d'une tâche;
  - indiquent les caractéristiques observables et mesurables pour évaluer les produits réalisés pendant le processus de réalisation d'une tâche;
  - sont énoncés sous forme d'exigences, de normes de qualité et de règles qui permettent de voir que la tâche est bien exécutée.
- **Processus de Travail**

Le processus de travail vise à mettre en évidence les principales étapes d'une démarche logique pour l'exécution de l'ensemble des tâches d'un métier ou d'une profession. Le processus de travail suivant est couramment observé et est assez générique pour coller aux différentes situations de travail :

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

2. DETERMINATION DES TACHES ET DES OPERATIONS

Les tâches sont les actions qui correspondent aux principales activités de l'exercice du métier analysé. Une tâche est structurée, autonome et observable. Elle a un début déterminé et une fin précise. Dans l'exercice d'un métier, qu'il s'agisse d'un produit, d'un service ou d'une décision, le résultat d'une tâche doit présenter une utilité particulière et significative.

Les informations recueillies permis de :

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

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

3. Tableau des tâches et des opérations du Pentester

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

4. CONDITIONS DE REALISATION DES TACHES ET CRITERES DE PERFORMANCE

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

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

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

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

Tâche 1 Analyser les vulnérabilités du système informatique	
Conditions de réalisation	**Critères de performance**
Autonomie Travail individuel ou en équipe. . **Références** • Normes, • Frameworks • Publications de l'OWASP, • Guides de sécurité de l'ISO, • Rapports de vulnérabilités du NIST, etc. **Consignes particulières** Consignes spécifiques données par le client ou l'organisation. Respect des consignes et suivi des directives fournies concernant les systèmes à tester, les méthodes à utiliser, les horaires de test, les restrictions, etc **Conditions environnementales**	• Détection judicieuse d'un pourcentage de vulnérabilités, • Production correcte de rapports détaillés et clairs, • Identification judicieuse de scénarios d'attaque réalistes, • Conformité correcte aux normes de sécurité, etc.

L'accès physique aux locaux, l'accès aux systèmes informatiques, les autorisations d'utilisation des outils de test, la disponibilité des ressources réseau, etc. **Matériel/moyens** • Ordinateurs portables, • Outils de scan de vulnérabilité ; • Outils de test d'intrusion, • Logiciels spécifiques, • Environnements de test isolés, • Machines virtuelles, • Outils de capture de trafic, etc.	

Tâche 2– Réaliser des tests d'intrusion sur les réseaux et les applications	
Conditions de réalisation	Critères de performance
Autonomie Travail individuel ou en équipe. **Références** • Les publications de l'Open Web Application Security Project (OWASP), • Les guides de sécurité du National Institute of Standards and Technology (NIST), • Les rapports de vulnérabilités de Common Vulnerabilities and Exposures (CVE), **Consignes particulières** Consignes spécifiques données par le client ou l'organisation. Respect des consignes et suivi des directives fournies concernant les systèmes à tester, les méthodes à utiliser, les horaires de test, les restrictions, etc. **Conditions environnementales** L'accès physique aux locaux, l'accès aux systèmes informatiques, les autorisations d'utilisation des outils de test, la disponibilité des ressources réseau, etc. **Matériel/moyens** • Ordinateurs portables puissants, • Outils de scan de vulnérabilité ; • Outils de test d'intrusion spécialisés, • Logiciels de sécurité, • Environnements de test isolés, virtuelles • Outils de capture de trafic réseau, etc.	• Identification correcte du nombre de vulnérabilités, • Exploitation minutieuse des failles du système • Classification et gravité correctes des vulnérabilités, • Clarté et qualité correctes des rapports de test, • Conformité correcte aux normes de sécurité spécifiques, etc

Tâche 3– Elaborer des stratégies de sécurité

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

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

environnement de travail propice à la recherche et à la collecte d'informations. **Matériel/moyens** • Agrégateurs de flux RSS, • Moteurs de recherche spécialisés, • Outils de surveillance des vulnérabilités, • Plateformes de partage de connaissances, • Forums de discussion, etc.	

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

Tâche 6 – Assurer une veille permanente sur les nouvelles menaces et les techniques de piratage	
Conditions de réalisation	Critères de performance
Autonomie	• Fréquence minutieuse des mises à

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

5.IMPORTANCE RELATIVE, FREQUENCE ET COMPLEXITE DES TACHES

IMPORTANCE

L'importance de la tâche est exprimée selon une échelle variant de très important à peu important en comparant les tâches les unes aux autres. Les données obtenues sont converties en pourcentage selon l'information reçue des professionnels de façon individuelle.

On constate que les tâches énumérées sont toutes très importantes ou moyennement importantes, cela justifie évidemment leur choix au sein du métier.

Sachant que l'importance de la tâche est déterminée par les conséquences plus ou moins fâcheuses que peut avoir le fait de mal l'exécuter ou de ne pas l'exécuter du tout, il est logique que certaines tâches soient celles nettement considérées plus importantes. En fait, elles apparaissent comme des tâches qui sont au cœur du métier.

FRÉQUENCE

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

COMPLEXITE DES TACHES

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

Les professionnels du secteur présents à l'AST ont évalué la complexité de chacune des tâches. Les données présentées dans le tableau suivant correspondent aux moyennes des résultats obtenus pour chacun des éléments identifiés.

les données sur le degré de complexité des tâches, fréquence sont présentées dans le tableau ci-dessus.

Les professionnels présents à l'AST ont évalué la fréquence relative des tâches et leur importance. Les données présentées dans le tableau suivant correspondent aux moyennes des résultats obtenus pour chacun des éléments identifiés.

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

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

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

L'évolution technologique a un impact significatif sur le métier de pentester. D'une part, elle crée des nouvelles opportunités pour les attaques et les vulnérabilités, car des nouveaux systèmes, applications et infrastructures émergent constamment. Les pentesters doivent donc rester constamment à jour sur les dernières technologies et tendances en matière de sécurité pour comprendre les nouvelles méthodes d'attaque potentielles. D'autre part, l'évolution technologique offre également des nouveaux outils et techniques aux pentesters pour renforcer la sécurité. Par

exemple, l'intelligence artificielle et l'apprentissage automatique peuvent être utilisés pour détecter les anomalies et les comportements suspects, tandis que l'automatisation peut accélérer les tests de sécurité. Cependant, les technologies émergentes, telles que l'Internet des objets (IoT), l'intelligence artificielle et le Big Data, présentent également de nouveaux défis en matière de sécurité, nécessitant une compréhension approfondie des risques potentiels.

7. CONNAISSANCES, HABILETES ET ATTITUDES

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

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

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

. Connaissances

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

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

- L'Intégration des aspects juridiques de la cybersécurité ;
- La mise en place d'une politique de cybersécurité ;
- Supervision de la sécurité du SI ;
- Construction de la stratégie cybersécurité de l'organisation ;

- Réalisation d'une rétro-ingénierie ;

. **Habiletés**

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

Attitudes

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

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

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

ATTITUDES ET COMPORTEMENTS	Très Important	Important	Moyen	Négligeable
Capacité de gérer le temps (et ponctualité)	X			
Honnêteté	X			
Intégrité	X			
Attitude positive		X		
Responsable /Sens des responsabilités		X		
Recherche de perfectionnement	X			
Esprit d'initiative / Autonomie/ Débrouillardise	X			
Persévérance /Endurance physique/	X			

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

SUGGESTIONS CONCERNANT LA FORMATION

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

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

- La formation initiale qui regroupe un contenu de formation obligatoire.

Ainsi, il a été mentionné que :

- La formation doit être davantage axée sur la pratique et les réalités de la cyber sécurité.
- Les formateurs doivent être des professionnels ayant de l'expérience.
- Le matériel et l'équipement utilisés au centre doivent être représentatifs des pratiques en entreprises.
- Les apprenants doivent se familiariser avec la réalité du terrain par le biais de visites et de stages en entreprise.
- Appliquer les règles de conduite en entreprise au centre de formation, et développer l'autodiscipline, la responsabilisation des apprenants.
- Développer chez les futurs lauréats le souci de concilier la qualité et le rendement satisfaisant des prestations.
- Développer chez les apprenants le sens de l'initiative et l'autonomie.
- Former les apprenants à s'adapter au changement et à l'innovation.
- Développer leur capacité à être responsable de tout ce qui se passe sur les postes de travail.
- Montrer la meilleure méthode et manière pendant qu'ils effectuent les opérations.
- Développer la polyvalence dans la formation, pour permettre aux apprenants d'exécuter différentes opérations sur une variété d'équipements.
- Les formateurs doivent suivre des formations continues en entreprises et dans les structures spécialisées pour être à jour des innovations technologiques et pédagogiques.
- Tous sont d'avis qu'une ou qu'un lauréat a besoin d'une période d'intégration dans l'entreprise avant de pouvoir prendre en charge la totale responsabilité de son poste de travail.
- La connaissance de l'anglais et du français ainsi que la capacité de pouvoir lire et comprendre des documents écrits et technique sont des éléments importants pour exercer le métier, sans oublier les connaissances fondamentales de secourisme et de premiers soins, les connaissances en calculs professionnels sont incontournables.

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

REFERENCES BIBLIOGRAPHIQUES

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

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

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

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

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

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

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

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

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

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

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

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

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