PECB BEYOND RECOGNITION

Manuel du candidat

CERTIFIED LEAD ETHICAL HACKER

PECB

Table des matières

SECTION I : INTRODUCTION

À propos de PECB

PECB est un organisme de certification qui propose des services d'éducation[1] et de certification de personnes selon la norme ISO/IEC 17024, dans un large éventail de disciplines.

Nous aidons les professionnels à faire preuve d'engagement et de compétence en leur fournissant des services d'évaluation et de certification en fonction de normes reconnues internationalement. Notre mission est de fournir des services qui inspirent la confiance, l'amélioration continue, assurent la reconnaissance et profitent à la société dans son ensemble.

Les principaux objectifs de PECB sont les suivants :

1. Établir les exigences minimales nécessaires pour certifier les professionnels
2. Examiner et vérifier les qualifications des candidats pour s'assurer qu'ils sont éligibles à la certification
3. Développer et maintenir des évaluations de certification fiables
4. Délivrer des certifications aux candidats qualifiés, tenir des registres et publier un répertoire des détenteurs de certifications valides
5. Établir les exigences pour le renouvellement périodique de la certification et veiller au respect de ces exigences
6. S'assurer que les candidats respectent les normes éthiques dans leur pratique professionnelle
7. Représenter ses membres, le cas échéant, dans les questions d'intérêt commun
8. Promouvoir les avantages de la certification auprès des organisations, des employeurs, des fonctionnaires, des praticiens dans des domaines connexes et auprès du public

[1] Éducation fait référence aux formations développées par PECB, et offertes dans le monde entier par les Revendeurs PECB.

Valeur de la certification PECB

Pourquoi choisir PECB en tant qu'organisme de certification ?

Reconnaissance mondiale
Nos certifications sont reconnues à l'échelle internationale et accréditées par l'IAS (International Accreditation Service), signataire du Multilateral Recognition Arrangement (MLA) de l'IAF qui assure la reconnaissance mutuelle de la certification accréditée entre les signataires du MLA et l'acceptation de la certification accréditée dans de nombreux marchés. Par conséquent, les professionnels qui obtiennent un titre de certification de PECB bénéficieront de la reconnaissance de PECB sur les marchés nationaux et internationaux.

Personnel compétent
L'équipe centrale de PECB est composée de personnes compétentes qui possèdent une expérience pertinente des différents domaines.
Tous nos employés détiennent des titres professionnels et sont constamment formés pour fournir des services plus que satisfaisants à nos clients.

Conformité aux normes
Nos certifications sont une démonstration de la conformité à la norme ISO/IEC 17024. Elles garantissent que les exigences de la norme ont été remplies et validées avec la cohérence, le professionnalisme et l'impartialité adéquats.

Service client
Nous sommes une entreprise centrée sur le client et nous traitons tous nos clients avec estime, importance, professionnalisme et équité. PECB dispose d'une équipe d'experts qui se consacrent au soutien des demandes, problèmes, préoccupations, besoins et opinions des clients. Nous faisons de notre mieux pour maintenir un temps de réponse maximum de 24 heures sans compromettre la qualité du service.

Code de déontologie de PECB

Les professionnels de PECB sont tenus de :

1. Se comporter de manière professionnelle, avec honnêteté, exactitude, équité, responsabilité et indépendance
2. Agir en tout temps uniquement dans le meilleur intérêt de leur employeur, de leurs clients, du public et de la profession, en respectant les normes professionnelles et les techniques applicables tout en offrant des services professionnels
3. Maintenir leurs compétences dans leurs domaines respectifs et s'efforcer d'améliorer constamment leurs capacités professionnelles
4. Ne proposer que des services professionnels pour lesquels ils sont qualifiés et informer correctement les clients de la nature des services proposés, y compris de toute préoccupation ou risque pertinent
5. Informer chaque employeur ou client de tout intérêt commercial ou affiliation qui pourrait influencer leur jugement ou nuire à leur équité
6. Traiter de manière confidentielle et privée les informations obtenues dans le cadre des relations professionnelles et commerciales de tout employeur ou client, actuel ou ancien
7. Se conformer à toutes les lois et réglementations des juridictions dans lesquelles les activités professionnelles sont exercées
8. Respecter la propriété intellectuelle et la contribution d'autrui
9. Ne pas communiquer, intentionnellement ou non, des informations fausses ou falsifiées qui pourraient compromettre l'intégrité du processus d'évaluation d'un candidat à un titre professionnel
10. Ne pas agir d'une manière qui pourrait compromettre la réputation de PECB ou de ses programmes de certification
11. Coopérer pleinement à l'enquête menée à la suite d'une prétendue violation du présent Code de déontologie

La version complète du Code de déontologie de PECB peut être téléchargée ici.

Introduction à la norme Certified Lead Ethical Hacker

La formation Certified Lead Ethical Hacker permet aux participants de maîtriser les techniques de tests d'intrusion et d'acquérir les connaissances et les compétences nécessaires pour réaliser des tests d'intrusion des systèmes d'information en effectuant les laboratoires inclus dans la formation à l'aide d'une machine virtuelle.

Être un pirate éthique est l'une des professions les plus demandées sur le marché, permettant aux organismes de rechercher et de découvrir des vulnérabilités exploitables. La formation PECB Certified Ethical Hacker offre une nouvelle expérience pratique des méthodologies et outils de piratage éthique utilisés par les pirates éthiques et les professionnels de la sécurité de l'information.

La certification « **Lead Ethical Hacker** » est une certification professionnelle destinée aux personnes qui souhaitent démontrer leur compétence à planifier, réaliser et gérer des tests d'intrusion de la sécurité de l'information. Cette certification reconnue au plan international peut vous aider à exploiter votre potentiel de carrière et à atteindre vos objectifs professionnels.

Il est important de préciser que les certifications de PECB ne sont pas une licence ou une simple adhésion. Il s'agit d'une reconnaissance par les pairs qu'une personne a démontré sa maîtrise et sa compréhension d'un ensemble de compétences. Les certifications PECB sont accordées aux candidats qui peuvent fournir la preuve de leur expérience et qui ont réussi un examen normalisé dans le domaine de la certification.

Ce manuel du candidat présente le programme de certification PECB Lead Ethical Hacker conformément à la norme ISO/IEC 17024:2012. Il contient également des informations sur le processus par lequel les candidats peuvent obtenir et renouveler leur certification. Il est très important que vous lisiez toutes les informations contenues dans ce manuel avant de remplir et de soumettre votre candidature. Si vous avez des questions après la lecture de ce document, veuillez contacter le bureau international de PECB à certification.team@pecb.com.

PECB

SECTION II : PROCESSUS DE CERTIFICATION ET PRÉPARATION, POLITIQUES ET RÈGLEMENTS RELATIFS À L'EXAMEN DE PECB

Décidez de la certification qui vous convient

Toutes les certifications PECB ont des exigences spécifiques en matière de formation et d'expérience professionnelle. Pour déterminer le titre de compétence qui vous convient, vérifiez les critères d'admissibilité des diverses certifications et vos besoins professionnels.

Préparer et programmer l'examen

Les candidats sont responsables de leur propre étude et de leur préparation aux examens de certification. Aucun ensemble spécifique de cours ou de programmes d'études n'est requis dans le cadre du processus de certification. Toutefois, la participation à une session de formation peut augmenter de manière significative les chances de réussite à l'examen PECB.

Pour programmer un examen de certification PECB, les candidats ont deux options :

1. Contacter l'un de nos revendeurs qui proposent des sessions de formation et d'examen. Les candidats trouveront un Revendeur de formations dans une région donnée sur la page Liste des revendeurs. Le calendrier des sessions de formation PECB est également disponible sous l'onglet Calendrier des formations.
2. Passer un examen PECB à distance de chez eux ou de n'importe quel endroit qu'ils préfèrent grâce à l'application PECB Exams, qui est accessible ici : Sessions d'examens.

Pour en savoir plus sur les examens, les domaines de compétences et les énoncés de connaissances, veuillez vous référer à la *section III* du présent document.

Frais de demande d'examen et de certification

PECB propose aussi les examens directement, où un candidat peut se présenter à l'examen sans assister à la formation. Les prix sont les suivants :

- Examen Lead : 1000 $ US
- Examen Manager : 700 $ US
- Examens Foundation et Transition : 500 $ US

Les frais de demande de certification sont de 500 $ US.

Pour tous les candidats qui ont suivi la formation et passé l'examen auprès d'un revendeur PECB, le coût de la session de formation comprend les frais associés à l'examen (examen et première reprise) et à la demande de certification, ainsi que la première année de frais annuels de maintenance (FAM).

Domaines de compétence

La certification « **Certified Lead Ethical Hacker** » est une certification professionnelle qui démontre la capacité d'un candidat à mener des tests d'intrusion dans un système d'information. L'objectif de l'examen Certified Lead Ethical Hacker est de s'assurer que le candidat a acquis les connaissances et l'expertise nécessaires pour réaliser un test d'intrusion basé sur un cadre prédéfini.

La certification Certified Lead Ethical Hacker est destinée aux :

- Professionnels de la cybersécurité et membres des équipes des systèmes d'information
- Professionnels de la sécurité de l'information souhaitant maîtriser les techniques de piratage éthique
- Managers ou consultants souhaitant maîtriser le processus de test d'intrusion
- Personnes responsables du maintien de la sécurité des systèmes d'information au sein d'un organisme
- Experts techniques souhaitant se préparer à réaliser des tests d'intrusion
- Experts en audit souhaitant réaliser des tests d'intrusion professionnels

Le contenu de l'examen est réparti comme suit :

- **Domaine 1 :** Outils et techniques de collecte d'informations
- **Domaine 2 :** Modélisation des menaces et identification des vulnérabilités
- **Domaine 3 :** Techniques d'exploitation
- **Domaine 4 :** Escalade des privilèges
- **Domaine 5 :** Pivotement et transferts de fichiers
- **Domaine 6 :** Rapport

PECB

Domaine 1 : Outils et techniques de collecte d'informations **Objectif principal :** S'assurer que le candidat comprend et est capable de sélectionner et d'adapter l'approche des tests d'intrusion en fonction des informations recueillies	
Compétences	**Énoncés de connaissances**
1. Aptitude à comprendre et à interpréter les concepts et principes fondamentaux du piratage éthique et de la cybersécurité 2. Aptitude à comprendre les normes et les cadres des tests d'intrusion 3. Aptitude à comprendre les méthodologies de piratage éthique 4. Aptitude à collecter des informations pendant la phase de reconnaissance 5. Aptitude à sélectionner et à adapter l'approche des tests d'intrusion en fonction des informations recueillies 6. Aptitude à comprendre et à utiliser les outils et techniques appropriés pour collecter des informations précieuses 7. Aptitude à recueillir efficacement des informations sur la cible à l'aide de renseignements open source 8. Capacité à comprendre et à expliquer la différence entre la reconnaissance passive et active	1. Connaissance des principaux concepts et de la terminologie du piratage éthique et de la cybersécurité 2. Connaissance des stratégies et méthodologies de tests d'intrusion 3. Connaissance des techniques courantes de piratage 4. Connaissance des différentes méthodes de collecte et d'analyse d'informations précieuses 5. Connaissance des outils de reconnaissance inclus dans la boîte à outils du pirate éthique et de leur utilisation 6. Connaissance des techniques de collecte d'informations qui évitent la détection 7. Connaissance des outils et techniques de renseignement open source et de leur utilisation, notamment OSINT Framework, Shodan, Maltego et Google Hacking 8. Connaissance des outils et techniques de reconnaissance passive et active et de leur utilisation

PECB

Domaine 2 : Modélisation des menaces et identification des vulnérabilités **Objectif principal :** S'assurer que le candidat comprend et est capable d'effectuer une modélisation des menaces sur la cible et de découvrir les vulnérabilités cachées qui peuvent être exploitées	
Compétences	**Énoncés de connaissances**
1. Aptitude à comprendre et à expliquer la relation entre les menaces et les vulnérabilités 2. Aptitude à créer un modèle de menace offensive à partir des informations recueillies lors de la phase de reconnaissance 3. Aptitude à analyser les informations et à adapter le modèle de menace 4. Aptitude à utiliser les outils et techniques d'analyse de vulnérabilité appropriés 5. Aptitude à comprendre et à expliquer la différence entre les types de vulnérabilité et leur efficacité 6. Aptitude à adapter le modèle de menace sur la base des nouvelles informations collectées	1. Connaissance des principales méthodes de collecte et d'analyse d'informations précieuses pour créer un modèle de menace efficace 2. Connaissance des vulnérabilités de type « zero-day » et des autres vulnérabilités et menaces 3. Connaissance des outils d'analyse des vulnérabilités présents dans la boîte à outils du hacker éthique 4. Connaissance de la manière d'évaluer les différents types de vulnérabilité et de déterminer lequel utiliser pour assurer une exploitation efficace de la vulnérabilité 5. Connaissance des catégories de plans d'attaque

PECB

Domaine 3 : Techniques d'exploitation **Objectif principal :** S'assurer que le candidat comprend et peut interpréter et appliquer les principales techniques d'exploitation	
Compétences	**Énoncés de connaissances**
1. Aptitude à contourner les systèmes de détection d'intrusion (IDS) et les systèmes de prévention d'intrusion, les pare-feu et les honeypots 2. Aptitude à comprendre, interpréter et réaliser des attaques côté serveur 3. Aptitude à comprendre et à réaliser des attaques côté client 4. Aptitude à réaliser des attaques sur les applications Web 5. Aptitude à comprendre et à réaliser des attaques sur des réseaux sans fil	1. Connaissance des différents types de systèmes de détection d'intrusion et du processus de contournement des IDS 2. Connaissance des mesures de protection contre les attaques côté serveur 3. Connaissance des dernières tendances en matière d'exploitation pour réaliser des attaques côté serveur 4. Connaissance des derniers outils et techniques d'exploitation pour les attaques côté client 5. Connaissance des méthodes de renforcement des serveurs Web, des vulnérabilités des applications Web, des menaces et des contre-mesures 6. Connaissance de la technologie sans fil et des méthodes de piratage sans fil 7. Connaissance des outils et techniques de sécurité des réseaux sans fil et de leur utilisation

PECB

Domaine 4 : Escalade des privilèges **Objectif principal :** S'assurer que le candidat est capable de comprendre et de mettre en œuvre les processus nécessaires pour accéder à un réseau ou à un système et réaliser une escalade des privilèges	
Compétences	**Énoncés de connaissances**
1. Aptitude à comprendre et à interpréter le concept d'escalade des privilèges 2. Aptitude à comprendre et expliquer les méthodes d'escalade des privilèges 3. Aptitude à effectuer une escalade de privilèges sur une machine 4. Aptitude à comprendre et à effectuer une escalade des privilèges sur un système 5. Aptitude à effectuer une escalade des privilèges sur un réseau	1. Connaissance de la procédure d'escalade des privilèges et de ses avantages 2. Connaissance des différentes méthodes d'escalade des privilèges : récolte des certificats et mots de passe structurés 3. Connaissance de la procédure d'escalade des privilèges dans les applications Web 4. Connaissance des outils et techniques appropriés pour l'escalade des privilèges des utilisateurs sur les machines et les réseaux

PECB

Domaine 5 : Pivotement et transfert de fichiers **Objectif principal :** S'assurer que le candidat est capable de comprendre et de mener des actions appropriées pour effectuer le pivotement d'une machine à l'autre et transférer les fichiers pertinents	
Compétences	**Énoncés de connaissances**
1. Aptitude à comprendre et à expliquer la définition du processus de pivotement 2. Aptitude à pivoter vers un réseau différent 3. Aptitude à comprendre et à utiliser de manière appropriée les outils et techniques de pivotement 4. Aptitude à comprendre et à expliquer la définition du transfert de fichiers 5. Aptitude à transférer en toute sécurité des fichiers depuis l'hôte cible 6. Aptitude à comprendre et à utiliser différents outils pour maintenir l'accès à un réseau 7. Aptitude à nettoyer et détruire les artefacts	1. Connaissance des outils et techniques appropriés pour pivoter vers un autre réseau, tels que Netcat ou SSH 2. Connaissances des méthodes et outils de transfert des fichiers, notamment FTP, HTTP, Netcat, wget, et curl 3. Connaissance des outils et des approches utilisés pour maintenir l'accès à un réseau, tels que les enregistreurs de frappe (keylogger), les rootkits et les chevaux de Troie 4. Connaissance du processus de nettoyage et de destruction des artefacts, tels que les agents, les scripts, les exécutables et les portes dérobées (backdoors)

PECB

Domaine 6 : Rapport **Objectif principal :** S'assurer que le candidat est capable de créer un rapport de test d'intrusion compréhensible	
Compétences	**Énoncés de connaissances**
1. Aptitude à recueillir efficacement des informations pendant toutes les phases des tests d'intrusion 2. Aptitude à interpréter les vecteurs et mécanismes d'attaque 3. Aptitude à proposer des recommandations appropriées sur les techniques d'atténuation à inclure dans le rapport de test 4. Aptitude à établir un rapport de test d'intrusion 5. Aptitude à comprendre la classification du rapport de test d'intrusion en fonction de la politique de classification de l'information du client 6. Aptitude à rédiger le rapport de test d'intrusion de manière compréhensible et claire	1. Connaissance des outils de collecte et de structuration de l'information, tels que CherryTree 2. Connaissance des mécanismes d'attaque et des vecteurs d'atténuation 3. Connaissance des approches à suivre pour définir des recommandations visant à atténuer les vulnérabilités 4. Connaissance de la manière de protéger les informations recueillies au cours du processus de test d'intrusion et d'éviter la divulgation des vulnérabilités 5. Savoir comment rédiger un rapport concis et utiliser des outils de visualisation pour mieux présenter les résultats des tests d'intrusion

Sur la base des domaines susmentionnés et de leur pertinence, les candidats devront compromettre au moins deux machines sur trois et documenter correctement le processus par un rapport d'examen. Les tâches qui sont incluses dans l'examen sont résumées dans le tableau ci-dessous :

				Niveau de compréhension (Cognitif/Taxonomique) requis				
		Nombre de points par tâche	Tâches qui mesurent la compréhension, l'application et l'analyse	Tâches qui mesurent la synthèse et l'évaluation	Nombre de tâches par domaine de compétence	% de l'examen consacré à chaque domaine de compétence	Nombre de points par domaine de compétence	% de points par domaine de compétence
Domaines de compétence	Collecte d'information	5		X	3	25	15	15
		5		X				
		5		X				
	Modélisation des menaces et identification des vulnérabilités	5		X	1	8,33	5	5
	Techniques d'exploitation	10	X		3	25	30	30
		10	X					
		10	X					
	Escalade des privilèges	10	X		3	25	25	25
		10	X					
		5	X					
	Pivotement et transferts de fichiers	15	X		1	8,33	15	15
	Rapport	10		X	1	8,33	10	10
	Total des points	100						
	Nombre de tâches par niveau de compréhension		7	5				
	Pourcentage de l'examen consacré à chaque niveau de compréhension (cognitif/taxonomie)		58,3	41,66				

La note de passage est établie à **70 %**. Ce score peut être atteint en documentant correctement le processus de compromission d'au moins deux machines dans un rapport écrit.

Après avoir réussi l'examen, les candidats pourront demander la certification « PECB Certified Lead Ethical Hacker » en fonction de leur niveau d'expérience.

Faire l’examen

Informations générales sur l’examen

Les candidats sont tenus d'être présents au moins 30 minutes avant le début de l'examen. Les candidats qui arrivent en retard ne disposeront pas de temps supplémentaire pour compenser leur retard et pourraient se voir refuser l'accès à l'examen.

Les candidats doivent être en possession d'une carte d'identité valide (carte d'identité nationale, permis de conduire ou passeport) et la présenter au surveillant.

Format et type d’examen PECB

- **Examen en ligne :** Les examens sont fournis par voie électronique via l'application PECB Exams. L'utilisation d'appareils électroniques, tels que les tablettes et les téléphones portables, n'est pas autorisée. La session d'examen est supervisée à distance par un surveillant de PECB via l'application PECB Exams et une caméra externe/intégrée.

Pour des informations plus détaillées sur le format d’examen en ligne, veuillez vous référer au PECB Online Exam Guide.

L'examen PECB Certified Lead Ethical Hacker comprend deux parties :
1. Examen pratique
2. Rapport écrit

L’examen pratique dure six heures et l’écriture du rapport dure huit heures. Si la demande en est faite le jour de l'examen, une heure supplémentaire peut être accordée pour la rédaction du rapport aux candidats qui passent l'examen dans une langue autre que leur langue maternelle.

L'examen PECB Certified Lead Ethical Hacker est fait en ligne. L'examen est utilisé pour déterminer et évaluer si un candidat est capable d'obtenir un accès à distance au réseau cible en compromettant pas moins de deux machines. Ce type de format d'examen a été choisi comme moyen de déterminer si un candidat peut appliquer les connaissances acquises pendant la formation dans un environnement réel. En outre, l'examen exige du candidat qu'il documente ce processus dans le rapport d'examen.

L'examen est à livre ouvert et n'est pas destiné à mesurer la mémorisation ou le rappel d'informations. Il vise à évaluer la compréhension, les capacités d'analyse et les connaissances appliquées des candidats. Les candidats doivent donc être en mesure de justifier leurs réponses en fournissant des explications à l'aide de captures d'écran. Vous trouverez ci-dessous un exemple d'une des tâches d'examen.

L'examen étant « à livre ouvert », les candidats sont autorisés à utiliser les documents de référence suivants :
- Support de formation du participant (accessible sur l'application PECB Exams ou imprimé)
- Notes personnelles prises pendant la session de formation (accessibles sur l'application PECB Exams ou papier)
- Livres et support en ligne
- Dictionnaire au format papier

Toute tentative de plagiat pendant la session d'examen entraînera un échec automatique.

Les examens PECB sont disponibles en anglais et dans d'autres langues. Pour savoir si l'examen est disponible dans une langue particulière, veuillez contacter examination.team@pecb.com.

Exemples de tâches d'examen

Tâche 1 :
Effectuer un scan du réseau sur le système cible pour recueillir des informations sur la plage IP.

Réponse possible :
Pour comprendre la plage IP d'un réseau, nous devons effectuer un scan du réseau à l'aide de Nmap. Nmap nous fournira les informations nécessaires pour passer à l'étape suivante.

```
kali@kali:~$ nmap -sP 192.168.10.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-19 14:48 UTC
Nmap scan report for ip-192-168-10-10.us-east-2.compute.internal (192.168.10.10)
Host is up (0.000058s latency).
Nmap scan report for ip-192-168-10-25.us-east-2.compute.internal (192.168.10.25)
Host is up (0.00099s latency).
Nmap scan report for ip-192-168-10-54.us-east-2.compute.internal (192.168.10.54)
Host is up (0.00052s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.55 seconds
```

Sur la base du scan, nous déterminons que deux machines autres que la nôtre sont actives sur le réseau, les machines ont les IP internes suivantes : 192.168.10.25 et 192.168.10.54.

Transmission des résultats d'examen

Les résultats d'examens seront communiqués par e-mail. Les seuls résultats possibles sont la réussite ou l'échec ; aucune note ne sera incluse. Le délai de communication commence à la date de l'examen et dure de trois à huit semaines pour les examens à développement.

Les candidats qui réussissent l'examen pourront se porter candidats à l'un des titres de compétences du programme de certification correspondant.

En cas d'échec à l'examen, une liste des domaines dans lesquels le candidat a obtenu une note inférieure à la note de passage sera ajoutée à l'e-mail pour aider les candidats à mieux se préparer à une reprise.

Les candidats qui ne sont pas d'accord avec les résultats peuvent demander une réévaluation en écrivant à examination.team@pecb.com dans les 30 jours suivant la réception des résultats. Les demandes de réévaluation reçues après 30 jours ne seront pas traitées. Si les candidats ne sont pas d'accord avec les résultats de la réévaluation, ils disposent de 30 jours à compter de la date de réception des résultats de l'examen réévalué pour déposer une plainte via le système de ticket de PECB. Toute plainte reçue après 30 jours ne sera pas traitée.

Politique de reprise d'examen

Il n'y a pas de limite au nombre de fois qu'un candidat peut reprendre un examen. Toutefois, il existe certains délais à respecter entre les reprises d'examen.

- Si le candidat échoue à l'examen à la 1re tentative, il doit attendre 15 jours à compter de la date de l'examen initial avant la prochaine tentative (1re reprise). Des frais s'appliquent.
  Note : *Le candidat ayant suivi la formation complète et qui échoue à l'examen est éligible à reprendre l'examen gratuitement une fois dans un délai de 12 mois à compter de la date de l'examen initial.*
- Si le candidat échoue à l'examen à la 2e tentative, il doit attendre 3 mois à compter de la date de l'examen initial avant la prochaine tentative (2e reprise). Des frais s'appliquent.
  Note : Aux candidats qui échouent à l'examen à la 2e reprise, PECB recommande de reprendre une session de formation afin de mieux se préparer à l'examen.
- Si le candidat échoue à l'examen à la 3e tentative, il doit attendre 6 mois à compter de la date de l'examen initial avant la prochaine tentative (3e reprise). Des frais s'appliquent.
- Après la 4e tentative, une période d'attente de 12 mois à compter de la date de la dernière reprise est requise. Des frais s'appliquent.

Pour organiser une reprise d'examen (date, heure, lieu, coûts), le candidat doit contacter le revendeur/distributeur PECB qui a organisé la session d'examen initiale.

Sécurité de l'examen

Une composante importante de la certification professionnelle est le maintien de la sécurité et de la confidentialité de l'examen. PECB compte sur le comportement éthique des titulaires et des candidats à la certification pour maintenir la sécurité et la confidentialité des examens PECB. Toute divulgation d'informations sur le contenu des examens PECB constitue une violation directe du Code de déontologie de PECB. PECB prendra des mesures à l'encontre de toute personne qui enfreint les politiques et règlements, y compris l'interdiction permanente d'obtenir les certifications PECB et la révocation de toute certification antérieure. PECB intentera également une action en justice contre les personnes ou les organisations qui enfreignent ses droits d'auteur, ses droits de propriété et sa propriété intellectuelle.

Reprogrammer l'examen

Pour tout changement concernant la date, l'heure, le lieu de l'examen ou d'autres détails, veuillez contacter. online.exams@pecb.com.

Demander la certification

Tous les candidats qui réussissent cet examen (ou un équivalent accepté par PECB) peuvent demander les titres de compétences de PECB pour lesquels ils ont été examinés. Des exigences spécifiques en matière d'éducation et d'expérience professionnelle doivent être remplies afin d'obtenir une certification PECB. Le candidat doit remplir le formulaire de demande de certification en ligne (accessible via son compte PECB), y compris les coordonnées des références qui seront contactées pour valider l'expérience professionnelle du candidat. Le candidat peut soumettre sa demande en plusieurs langues. Il peut choisir de payer en ligne ou d'être facturé. Pour de plus amples informations, veuillez contacter certification.team@pecb.com.

Le processus de demande de certification en ligne est très simple et ne prend que quelques minutes :

- Inscrivez-vous.
- Vérifier vos e-mails pour activer le lien de confirmation.
- Connectez-vous pour demander la certification

Pour plus d'informations sur le processus de demande, suivez les instructions du manuel Faire une demande de certification.

La demande est approuvée dès que le Service de certification valide que le candidat remplit toutes les exigences de certification relatives au titre concerné. Un e-mail sera envoyé à l'adresse électronique fournie au cours du processus de demande pour communiquer l'état de la demande. Si la demande est approuvée, le candidat pourra télécharger la certification à partir de son compte PECB.

PECB offre un soutien en anglais et en français.

Renouveler la certification

Les certifications PECB sont valides pour une période de trois ans à compter de la date de délivrance. Pour les conserver, les candidats doivent démontrer chaque année qu'ils effectuent toujours les activités liées à la certification. Les professionnels certifiés par PECB doivent fournir chaque année des unités de formation professionnelle continue (FPC) et payer 120 $ US de frais annuels de maintien (FAM) pour conserver leur certification. Pour de plus amples renseignements, veuillez consulter la page Maintien de la certification sur le site Web de PECB.

Fermeture d'un dossier

Si un candidat ne demande pas la certification dans les trois ans, son dossier sera fermé. Toutefois, même si la période de certification expire, le candidat a le droit de rouvrir son dossier. Cependant, PECB ne sera plus responsable de tout changement concernant les conditions, les normes, les politiques et le Manuel du candidat qui étaient applicables avant la fermeture du dossier. Un candidat qui demande la réouverture de son dossier doit le faire par écrit et payer les frais requis.

PECB

SECTION III : EXIGENCES DE CERTIFICATION

Certified Lead Ethical Hacker

Les exigences pour les certifications PECB Certified Lead Ethical Hacker sont les suivantes :

Titre de compétence	Examen	Expérience professionnelle	Expérience de projet	Autres exigences
PECB Certified Lead Ethical Hacker	Examen PECB Certified Lead Ethical Hacker	Deux années d'expérience en matière de tests d'intrusion et de cybersécurité	Aucune	Signature du Code de déontologie de PECB et du Code de conduite pour les CLEH de PECB

Pour être considérée comme valide, l'expérience en matière de tests d'intrusion et de cybersécurité devrait inclure les activités suivantes :

1. Déterminer le périmètre du piratage éthique
2. Définir une approche de test d'intrusion
3. Exécuter les étapes à suivre lors d'un test d'intrusion
4. Définir les critères des tests d'intrusion
5. Évaluer les scénarios de tests d'intrusion et les options de traitement
6. Utiliser les méthodes qui permettent d'accroître la sécurité des systèmes d'exploitation
7. Établir les rapports des résultats des tests d'intrusion

SECTION IV : POLITIQUES ET RÈGLEMENTS RELATIFS À LA CERTIFICATION

Références professionnelles

Pour chaque demande de certification, deux références professionnelles sont requises. Les références professionnelles doivent provenir de personnes ayant travaillé avec le candidat dans un environnement professionnel et pouvant ainsi attester de son son expérience en test d'intrusion, en cybersécurité, ainsi que de ses antécédents professionnels actuels et antérieurs. Les références professionnelles de personnes qui sont sous la supervision du candidat ou qui sont ses proches ne sont pas valables.

Expérience professionnelle

Le candidat doit fournir des informations complètes et exactes concernant son expérience professionnelle, notamment le titre de chaque poste, les dates de début et de fin, la description des postes, etc. Il est conseillé au candidat de résumer ses missions précédentes et actuelles, en fournissant suffisamment de détails pour décrire la nature des responsabilités de chaque emploi. Des informations plus détaillées peuvent être incluses dans le CV.

Évaluation des demandes de certification

Le Service de certification évaluera chaque demande afin de valider l'éligibilité du candidat à la certification. Le candidat dont la demande est examinée en sera informé par écrit et disposera d'un délai raisonnable pour fournir tout document supplémentaire si nécessaire. Si un candidat ne répond pas dans le délai imparti ou ne fournit pas les documents requis dans le délai imparti, le service de certification validera la demande sur la base des informations initiales fournies, ce qui peut éventuellement conduire à la rétrogradation du candidat à un titre inférieur.

Refus de la demande de certification

PECB peut refuser la demande de certification si le candidat :

- Falsifie la demande
- Enfreint les procédures d'examen
- Enfreint le Code de déontologie de PECB
- Échoue à l'examen

Pour des informations plus détaillées, reportez-vous à la section **Plainte et appel**.

Le paiement de la demande de certification n'est pas remboursable.

Suspension de la certification

PECB peut suspendre temporairement la certification si le candidat ne satisfait pas aux exigences de PECB. D'autres raisons peuvent justifier la suspension de la certification :

- PECB reçoit des plaintes excessives ou sérieuses de la part des parties intéressées (la suspension sera appliquée jusqu'à ce que l'enquête soit terminée).
- Les logos de PECB ou des organismes d'accréditation sont délibérément utilisés de manière abusive.
- Le candidat ne corrige pas l'usage abusif d'une marque de certification dans le délai déterminé par PECB.
- La personne certifiée a volontairement demandé une suspension.
- Toute autre condition jugée appropriée pour la suspension de la certification.

Révocation de la certification

PECB peut révoquer (c'est-à-dire retirer) la certification si le candidat ne satisfait pas aux exigences de PECB. Le candidat n'est alors plus autorisé à se présenter comme un professionnel certifié par PECB. D'autres raisons de révocation de la certification peuvent être invoquées si le candidat :

- Enfreint le Code de déontologie de PECB
- Fait une fausse déclaration et fournit de fausses informations sur la portée du certificat
- Enfreint toute autre règle de PECB

Mise à niveau des titres de compétences

Les professionnels peuvent demander à passer à une certification supérieure dès qu'ils peuvent démontrer qu'ils remplissent les conditions requises.

Pour faire une demande de mise à niveau, les candidats doivent se connecter à leur compte PECB, visiter l'onglet ***Mes certifications*** et cliquer sur le lien ***Mise à niveau***. Les frais de demande de mise à niveau sont de 100 $ US.

Déclassement des titres de compétences

Une certification PECB peut être déclassée à un titre inférieur pour les raisons suivantes :

- Les FAM n'ont pas été payés.
- Les heures de FPC n'ont pas été soumises.
- Un nombre insuffisant d'heures de FPC a été soumis.
- La preuve des heures de FPC n'a pas été soumise sur demande.

Note : *Les professionnels certifiés par PECB qui détiennent des certifications Lead et qui ne fournissent pas de preuves des exigences de maintien de la certification verront leurs titres déclassés. D'autre part, les détenteurs de certifications Master qui ne soumettent pas les FPC et ne paient pas les FAM verront leurs certifications révoquées.*

Autres statuts

En plus d'être active, suspendue ou révoquée, une certification peut être retirée volontairement. Pour plus d'informations sur ces statuts et sur le statut de cessation permanente, ainsi que sur la manière de les appliquer, veuillez consulter la page État de la certification.

SECTION V : POLITIQUES GÉNÉRALES DE PECB

Code de déontologie de PECB
L'adhésion au Code de déontologie de PECB est un engagement volontaire. Il est important que les professionnels certifiés par PECB non seulement adhèrent aux principes de ce Code, mais aussi qu'ils encouragent et soutiennent les autres à faire de même. Plus d'informations sont disponibles ici.

Autres examens et certifications
PECB accepte les certifications et les examens d'autres organismes de certification accrédités et reconnus. PECB évaluera les demandes par le biais de son processus d'équivalence pour décider si la ou les certifications ou examens respectifs peuvent être acceptés comme équivalents à la certification PECB respective (par exemple, la certification ISO/IEC 27001 Lead Auditor).

Non-discrimination et aménagements spéciaux
Toutes les candidatures seront évaluées objectivement, sans considération d'âge, de sexe, de race, de religion, de nationalité ou d'état civil du candidat.

Afin de garantir l'égalité des chances à toutes les personnes qualifiées, PECB fera des aménagements raisonnables pour les candidats, le cas échéant. Si un candidat a besoin d'aménagements spéciaux en raison d'un handicap ou d'une condition physique particulière, il devrait en informer le revendeur/distributeur afin que celui-ci puisse prendre les dispositions nécessaires. Toute information fournie par les candidats concernant leur handicap/besoin sera traitée de manière strictement confidentielle.

Cliquez ici pour télécharger le Formulaire pour les candidats présentant un handicap.

Plainte et appel
Toute plainte doit être déposée au plus tard 30 jours après la réception de la décision de certification (y compris la décision d'examen). PECB fournira une réponse écrite au candidat dans les 30 jours ouvrables suivant la réception de la plainte. Si la réponse de PECB n'est pas satisfaisante, le candidat a le droit de faire appel. Pour plus d'informations, consultez la Politique de plainte et d'appel de PECB ici.

(1) Selon le Americans with Disabilities Act (ADA), le terme « aménagement raisonnable » peut inclure : (A) rendre les installations existantes utilisées par les employés facilement accessibles et utilisables par les individus souffrant d'invalidité ; et (B) la restructuration des tâches, les horaires de travail à temps partiel ou modifiés, la réaffectation à un poste vacant, l'acquisition ou la modification d'équipement ou d'appareils, l'adaptation ou la modification appropriée des examens, du matériel de formation ou des politiques, la fourniture de personnel qualifié.

ADA Amendments Act of 2008 (P.L. 110-325) Sec. 12189. Examens et cours. [Section 309] : Toute personne qui propose des examens ou des cours liés à des demandes, des licences, des certifications ou des habilitations pour l'enseignement secondaire ou post-secondaire, à des fins professionnelles ou commerciales, doit proposer ces examens ou ces cours dans un lieu et d'une manière accessibles aux personnes handicapées ou proposer d'autres arrangements accessibles à ces personnes.

Adresse
Siège social
6683, rue Jean-Talon Est,
bureau 336 Montréal
QC H1S 0A5
CANADA

Tel./Fax.
T : +1-844-426-7322
F : +1-844-329-7322

Centre d'aide de PECB
Visitez notre Centre d'aide pour parcourir la Foire aux questions (FAQ), consulter les manuels d'utilisation du site Web et des applications de PECB, lire les documents relatifs aux processus de PECB ou nous contacter via le système de suivi en ligne du centre d'aide.

E-mails
Examen : examination.team@pecb.com
Certification : certification.team@pecb.com
Service client : customer@pecb.com

Copyright © 2021 PECB. La reproduction ou le stockage sous quelque forme que ce soit et à quelque fin que ce soit n'est pas autorisé sans une autorisation écrite préalable de PECB.

www.pecb.com