RÉFÉRENTIEL DE CERTIFICATION ET DE COMPÉTENCES

Intitulé de la certification

Analyser et protéger un système informatique dans un environnement de cybercriminalité

Objectif de la certification

La certification vise l'appropriation des techniques et méthodes permettant l'analyse et la protection de systèmes informatiques dans un environnement de cybercriminalité.

Elle s'inscrit dans le développement de compétences complémentaires au métier de Technicien Supérieur Systèmes et Réseaux, également appelé Technicien systèmes et réseaux, Technicien Réseau, Technicien informatique, ou encore Technicien Support, en réponse à un besoin important de professionnels qualifiés pour analyser et protéger les systèmes informatiques des entreprises et des particuliers afin de faire face aux attaques cybercriminelles en constante augmentation.

Elle permet le développement de compétences s'appuyant sur une pédagogie participative, en immersion dans le cadre d'ateliers et de mises en situations professionnelles, reposant sur les pratiques de formateurs professionnels de l'ingénierie informatique et de la cybersécurité.

Prérequis

Titulaire du Titre professionnel de Technicien Supérieur Systèmes et Réseaux de niveau 5, ou en cours de formation au Titre professionnel de Technicien Supérieur Systèmes et Réseaux, ou Titulaire d'un Titre professionnel d'assistance en informatique ou équivalent de niveau 4 ayant 2 ans d'expérience dans le métier de Technicien Réseau.

Durée du parcours

105 heures de formation soit 3 semaines de 35 heures

RÉFÉRENTIEL DE CERTIFICATION ET DE COMPÉTENCES

REFERENTIEL DE COMPETENCES	REFERENTIEL D'EVALUATION	
Compétences professionnelles	**Modalités d'évaluation**	**Critère d'évaluation**
C1 : Effectuer des recherches sur les sites underground avec mise en place d'une protection maximale. **C2 :** Etablir une recherche de découverte réseaux en mode actif/passif puis éditer un tableau de résultats. **C3 :** Analyser et détecter des failles informatiques puis établir un plan de mise à niveau selon la criticité. **C4 :** Mettre en œuvre une sécurité intermédiaire d'authentification radius, et VPN client-serveur. **C5 :** Etablir les règles principales de sécurité informatique. **C6 :** Mettre en place un système d'exploitation Windows chiffré et effectuer des résolutions cryptographiques de base.	**Durée**. 4 heures dont 3 heures de mise en situation, 45 minutes de questionnement oral avec le jury et 15 minutes d'entretien final avec le jury. **Première partie : Mise en situation professionnelle sur un réseau test virtuel.** La mise en situation vise à analyser et protéger un système informatique virtuel afin de faire face à des cyberattaques. Un sujet décrira au candidat la série de tests et d'analyses qu'il devra réaliser, sur un réseau test mis à disposition sur un plateau technique. Les objectifs seront de : ▪ Découvrir et analyser un réseau informatique. A cet effet le candidat devra : - Etablir une recherche active. - Désigner la méthode employée. - Détecter et énumérer les acteurs et les failles. - Faire une recherche de CVE (Common vulnerabilities and exposures). - Concevoir et rédiger un plan de mise à niveau selon la criticité. ▪ Mettre en place et installer un Firewall dans un environnement virtuel.	**Cr1** : Le candidat met en place les mesures de sécurité requises pour son immersion underground. Il possède les connaissances requises en matière de menaces cybercriminelles, de cycles d'attaque et de vulnérabilités communes. **Cr2 :** La méthode de recherche active/passive est clairement désignée et pertinente. Le tableau de résultats est précis, motivé et bien présenté. **Cr3** : Le plan de mise à niveau s'appuie sur les analyses réalisées et les résultats obtenus. Il évalue les facteurs de risque, les possibilités, les forces et faiblesses avec une approche critique. Les niveaux sont clairement définis. **Cr4** : Le protocole d'authentification client-serveur RADIUS (Remote Authentication Dial-In User Service) et VPN sont correctement configurés. **Cr5** : Les règles strictes de sécurité du système informatique de l'entreprise test sont établies dans un document clairement identifié.

	▪ Etablir les règles principales de sécurité. ▪ Mettre en place et gérer un accès VPN utilisateur. **Le candidat devra rédiger :** ◊ Une fiche d'intervention dans laquelle il décrira les méthodes de recherche et d'analyse employées, les acteurs concernés et les failles détectées. ◊ Un plan de mise à niveau selon la criticité. ◊ Un plan décrivant les règles principales de sécurité mises en place. **<u>Deuxième partie : Entretien Technique avec un jury</u>** Le jury contrôle et questionne le candidat sur les différents paramétrages et déploiements qu'il a réalisé sur son réseau test. Le candidat soutient devant le jury le plan de mise à niveau ainsi que les règles de sécurité qu'il aura établies pendant la phase de mise en situation professionnelle. **<u>Troisième partie : Entretien final avec le jury</u>** Le jury questionne le candidat afin de vérifier son niveau de maîtrise des compétences requises pour l'exercice des activités composant le certificat. **NB : Le jury tient compte des résultats des évaluations passées en cours de formation pour les candidats issus d'un parcours de formation.**	Il établit les règles relatives au téléchargement de document et à l'installation de nouveaux logiciels. Il contient des conseils sur le choix d'un mot de passe fort. Les sauvegardes automatiques des données sont définies et mises en œuvre. Les commandements de la sécurité sur l'Internet de l'ANSSI sont appliqués, de même que les règles en matière de protection des données personnelles. **Cr6** : Le système d'exploitation Windows installé est chiffré et fonctionnel. Les techniques et protocoles de cryptographie sont maîtrisés.