Réaliser des tests d'intrusions (Sécurité Pentesting)

La certification « Réaliser des tests d'intrusions (Sécurité Pentesting) » permet aux candidats d'acquérir l'ensemble des compétences indispensables afin d'effectuer des tests d'intrusions, consistant à examiner l'ensemble du système d'information en simulant les actions d'un intrus potentiel à l'intérieur de leur environnement de travail.

Prérequis : Une compréhension globale de la sécurité informatique et les infrastructures SI.

Public cible : Pentester, Ingénieur cybersécurité, administrateur sécurité, RSSI, professionnels en informatique.

Niveau d'expérience : une première expérience dans la sécurité informatique.

<table>
<tr><th>REFERENTIEL DE COMPETENCES</th><th>MODALITÉS D'ÉVALUATION</th><th>CRITÈRES D'ÉVALUATION</th></tr>
<tr><td>C.1.1 Définir les enjeux et contraintes du test d'intrusion dans l'objectif de définir les scénarios les plus probables ainsi que l'obtention du consentement légal.</td><td rowspan="3">E.1- Etude de cas
Dans le cadre d'un mini-projet réalisé individuellement, en temps limité de 4 heures, à partir d'un besoin exprimé ou généré, le/la candidat(e) doit :
- Identifier les objectifs du test d'intrusion
- Identifier les contraintes du test d'intrusion

E.2 Mise en situation professionnelle
- Appliquer une méthodologie se basant sur les étapes de la killchain
- Utiliser les outils adaptés
- Évaluer le niveau de sécurité d'un SI

E.3 Choisir des outils afin d'effectuer un test d'intrusion
- Déterminer des failles potentielles
- Réajuster les outils d'intrusion
- Classifications de criticité des failles</td><td>CRIT 1
Les éléments d'encadrement du test d'intrusion ont été identifié
Les scénarios d'intrusion les plus pertinents sont identifiés vis-à-vis du contexte du test d'intrusion
La méthodologie est conforme aux objectifs du test d'intrusion</td></tr>
<tr><td>C.1.2 Appliquer une méthodologie de test d'intrusion clair et reproductible afin de pouvoir restituer des éléments comparables dans leurs approches.</td><td>CRIT 2
Une méthodologie de test d'intrusion a été sélectionné
Les phases de la méthodologie sélectionnées sont détaillées
Les outils adaptés pour chaque phase sont sélectionnés</td></tr>
<tr><td>C.1.3 Concevoir et réaligner des outils d'intrusions dans l'objectif de répondre aux différents besoins d'un test d'intrusion.</td><td>CRT 3
Les vulnérabilités pesant sur l'organisation ont été identifié et classer
Les défauts de conception de sécurité ont été remonté</td></tr>
</table>

C.1.4 *Identifier les différentes vulnérabilités présentes en réalisant les différentes phases des tests d'intrusions évoqués dans les enjeux initiaux dans le but de découvrir les points de faiblesses de l'organisation.*	**E.4 Exploiter différentes vulnérabilités afin d'effectuer un test d'intrusion** - *Exploiter les failles identifiées* - *Exploiter différents systèmes* - *Attaquer des systèmes critiques*	CRT 4 Les vulnérabilités les plus critiques sont exploiter Des systèmes plus critiques sont découverts et exploités
C.1.5 *Remonter et restituer les différentes vulnérabilités identifiées ainsi qu'un plan d'action contenant les mesures de sécurité permettant à l'organisation de corriger ses failles.*	**E.5 Restituer les différentes vulnérabilités identifiées** - *Proposer des actions correctives ciblées vis à vis de scénarios identifiés* - *Proposer un plan d'action priorisant les vulnérabilités critiques* - Produire un rapport de Penteste	CRT 5 Les mesures de sécurité l'organisation ont été cartographiées et mesurées Les mécanismes de sécurité ont été réajustés Les mesures de sécurité sélectionnées sont efficaces vis-à-vis des menaces et vulnérabilités précédemment identifiés.

Dérouler de l'examen

Après l'étude cas de 4heures le candidat présentera un rapport au jury qu'il défendra à l'oral durant un temps maximum de 1H30 en détaillant la méthode, les outils choisis ainsi que les contre mesure adéquates vis-à-vis des menaces et vulnérabilités identifiées lors de son penteste.

1) *Analyse du rapport par le jury sans candidat*
2) *Présentation du rapport par le candidat devant le jury = 60min*
3) *Question du jury au candidat = 30min*
    a. *Rapport*
    b. *L'étude de cas*
    c. *Technique*
    d. *Qualité oratoire*

Jury de certification

Grille d'évaluation complétée par le jury d'évaluation avec un score minimal de 70/100 pour la validation de l'ensemble des compétences de la certification.

Le jury de certification analysera les éléments de l'étude de cas et de la mise en situation afin de valider la certification.

Grilles de notations

Nom du candidat	*Date*	*Numéro de certification*
Les enjeux et contraintes	*Note sur 10*	*Commentaire du jury*
Évaluer les vulnérabilités	*Note sur 10*	*Commentaire du jury*
Exploiter les failles	*Note sur 20*	*Commentaire du jury*
Rapport ***Qualité*** ***Pertinence*** ***Recommandations de sécurité***	*Note sur 30*	*Commentaire du jury*
Oral ***Expression*** ***Explication*** ***Méthode***	*Note sur 30*	*Commentaire du jury*

Résultat du candidat	*Total sur 100*	*Commentaire du jury*