

NUMÉRIQUE

CYB-151

Tests d'intrusion et hacking éthique

Conduire un test d'intrusion encadré : cadre juridique et autorisation, reconnaissance, recherche et exploitation de vulnérabilités, élévation de privilèges et rapport utile à la remédiation.



DURÉE

21 heures

FORMAT

Visio

TARIF

Sur devis

FINANCEMENT

Étude OPCO

NIVEAU

Selon prérequis

Validation et reconnaissance

Attestation de fin de formation et certificat de réalisation. Cette formation ne prépare pas à une certification enregistrée au RNCP ou au répertoire spécifique.



Une formation adaptée à vos besoins

Questionnaire avant la session avec un court exercice technique : fonction, environnement (systèmes, réseau, cloud), outils, niveau. Les travaux pratiques sont adaptés au contexte des participants.



Délai d'accès

Sous 15 jours selon les disponibilités, après analyse du besoin.



Accessibilité

Les besoins d'aménagement sont étudiés avant la session avec notre référent handicap.



Ce que vous saurez faire à l'issue de la formation



Objectif 01

Cadrer un test d'intrusion : autorisation écrite, périmètre, règles d'engagement, conformément au cadre pénal.



Objectif 02

Mener une reconnaissance et cartographier une cible de laboratoire.



Objectif 03

Identifier et exploiter des vulnérabilités systèmes et applicatives en laboratoire.



Objectif 04

Réaliser une élévation de privilèges et un mouvement latéral en laboratoire.



Objectif 05

Rédiger un rapport classant les vulnérabilités par risque avec des recommandations de remédiation.



Public visé et prérequis



Pour qui

Analystes sécurité et administrateurs confirmés. Développeurs et ingénieurs qui veulent comprendre l'attaque. Auditeurs en sécurité.



Prérequis

Administrer Linux et Windows et connaître les protocoles réseau.



Déroulement de la formation

Dates, horaires, lieu ou accès à distance sont confirmés dans la convocation. Le livret d'accueil, le règlement et les contacts utiles sont transmis avant la session.

Programme détaillé

01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16
----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----

21 heures · 16 séquences · programme adapté après positionnement



1

Cadre et méthodologie - Code pénal

atteintes aux systèmes de traitement automatisé (art. 323-1 et suivants)



2

Cadre et méthodologie - Autorisation écrite et contrat



3

Cadre et méthodologie - Méthodologies de référence



4

Cadre et méthodologie - Règles d'engagement et périmètre



5

Reconnaissance - Sources ouvertes



6

Reconnaissance - Découverte réseau et services



7

Reconnaissance - Énumération



8

Reconnaissance - Cartographie



9

Exploitation - Vulnérabilités connues et correctifs manquants



10

Exploitation - Failles applicatives web



11

Exploitation - Mots de passe et authentification



12

Exploitation - Élévation de privilèges et mouvements latéraux



13

Rapport et remédiation - Notation des risques



14

Rapport et remédiation - Rédaction du rapport



15

Rapport et remédiation - Présentation aux équipes



16

Rapport et remédiation - Contre-test

✓ Méthodes pédagogiques et évaluation

Méthodes pédagogiques

Apports techniques et démonstrations. Travaux pratiques en laboratoire isolé, jamais sur des systèmes de production. Études de cas d'incidents réels anonymisés. Supports et fiches réflexes remis à chaque participant.

✓ Évaluation des acquis

Pendant : document relu, cartographie et objectifs vérifiés. En fin de formation : rapport noté et quiz. Questionnaire de satisfaction à chaud.

Moyens et supports pédagogiques

Un ordinateur par participant avec droits d'administration ou machine virtuelle. Laboratoire virtuel isolé fourni pour les travaux pratiques. En classe virtuelle : connexion stable, webcam et micro.

Financement

Financement possible par l'entreprise ou son OPCO selon les règles applicables et après accord écrit. Aucune prise en charge n'est garantie avant cet accord.

NOVA ACADEMY - société par actions simplifiée (SAS) - SIRET 993 541 879 00017. Déclaration d'activité n° 76 34 14584 34. Cet enregistrement ne vaut pas agrément de l'État. Certification CERT_S0626_0811 délivrée par CEVA Solution, pour les actions de formation. Contact : formation@capsulecom-nova.fr.