CYBER LABS – TESTS D'INTRUSIONS ET REMÉDIATIONS

Durée et lieu de la formation : 4 jours à Nanterre (92) – ou à distance le temps de la crise sanitaire (matériel de formation fournis par Devenez)

Pour connaitre les dates de la prochaine formation :
https://www.devenez.fr/espace-candidats/les-offres-en-cours/formation-modules-boosters/

PRÉ-REQUIS

- *Connaissance de base en réseau : IP, MAC, couches OSI*
- *Connaissance de base en système : commandes linux de base*

OBJECTIFS :

- *A l'issue de la formation, les stagiaires auront acquis les compétences suivantes :*
- *Préparer un test d'intrusion*
- *Maîtriser toutes les phases d'un test d'intrusion (de la découverte à la post exploitation) :*
- *Découvrir facilement et rapidement le réseau cible*
- *Exploiter en toute sécurité les vulnérabilités identifiées*
- *Elever ses privilèges pour accéder aux ressources critiques*
- *Comprendre les vulnérabilités exposées par les réseaux externes et internes*
- *Utiliser efficacement les outils de pentes*

PROGRAMME

Jour 1 : Introduction et prise d'information

- *Types d'audits*
- *Types d'attaques*
- *Préparation d'un test d'intrusion*
- *Déroulement d'un test d'intrusion*
- *Prestation de Kali Linux*
- *Récolte d'information active/passive (DNS, scan de ports et prise d'empreintes…)*
- *Rappels du protocole TCP/IP*
- *Fonctionnement d'un scanner de ports*
- *TP : prise d'information*

CYBER LABS – TESTS D'INTRUSIONS ET REMÉDIATIONS

Jour 2 : Vulnérabilités système et réseau

- *Vulnérabilités réseau*
- *Vulnérabilités système*
- *Fonctionnement des scanners de vulnérabilités*
- *TP : Utilisation d'un scanner de vulnérabilité*
- *Exploitation des vulnérabilités système et réseau*
- *Présentation de Metasploit*
- *TP : Exploitation de vulnérabilités système*
- *Techniques d'élévation de privilège*

Jour 3 : Vulnérabilités web

- *Présentation de l'OWASP TOP 10*
- *Présentation des différents types d'injection (XSS, CSRF, SQL)*
- *Présentation des RFI, LFI*
- *Utilisation des outils de pentest web (Burp, SQLMAP, Dirb…)*
- *TP : Attaques sur une application web vulnérable (SQL injection, XSS, force brute…)*

Jour 4 : Mise en situation

- *TP : tests d'intrusion sur une adresse IP (mise en pratique de l'exploitation des vulnérabilités*
- *système, réseau et web)*
- *TP : social engineering*
- *Rédaction d'un rapport de tests d'intrusion et recommandations*

CYBER LABS – TESTS D'INTRUSIONS ET REMÉDIATIONS

APPROCHE PEDAGOGIQUE ET MODALITES D'EVALUATION

- **En temps normal** : formation présentielle alternant présentation théoriques et TP – sur le site de FITEC NANTERRE
- **En période de crise sanitaire** : Idem qu'en temps normal, mais à distance via VISIO CONFERENCE en SYNCHRONE
- **A la sortie de la crise sanitaire :** La formation reste accessible en visio-conférence.

FORMATEUR ET PÉDAGOGIE

Chaque formateur à FITEC doit avoir une double casquette celle d'expert et de pédagogue. C'est cette double compétence qui garantit une acquisition de compétences optimum pour chaque stagiaire.
Tous les formateurs ont suivi une formation et maîtrisent l'outil Teams. Ils ont également été formés quant à l'organisation de la formation à distance et cela dès sa mise en place.

QUALITÉ DES CONDITIONS TECHNIQUES

Un formateur anime le cours sur un **groupe Teams**, partage sa **vidéo** et son **écran**, diffuse ses **supports**, met une **base documentaire** à disposition, **interagit** avec les stagiaires, lance les TP sur des outils et plateformes cloud, peut **prendre la main** sur les postes.
Enregistrement de la session possible pour consultation hors créneaux horaires.

RYTHME ET SÉQUENÇAGE D'APPRENTISSAGE

Les formations à distance sont donc des cours **synchrones** qui requièrent la présence de tous comme une salle de formation en virtuel.
Le **rythme** est de 9h à 13h et 14h à 18h par jour.

INTERACTIVITÉ

A tout moment, les stagiaires peuvent **interagir** avec le formateur, poser des **questions orales** grâce au micro ou par écrit sur le **chat** de Teams.
Les micros des stagiaires sont coupés par défaut et chacun peut l'activer pour intervenir.

ACCOMPAGNEMENT

Pour chaque session de formation, en plus du formateur, un **modérateur** membre de l'équipe pédagogique veille à la bonne marche de la formation à distance. Il reste connecté à la formation, vérifie les connexions, répond aux questions ou difficultés des stagiaires, enregistre la session.
Le formateur peut ainsi se concentrer sur l'animation pédagogique de son cours.
Un **questionnaire en ligne de satisfaction** est rempli par les stagiaires.

MODALITES D'EVALUATION - VALIDATION DE LA MISE EN OEUVRE DE LA COMPETENCE

20% du temps est consacré au cours théorique et 80% du temps est consacré aux travaux pratiques, exercices et projets.
Les cursus complets de Reskilling sont validés par une **soutenance en ligne** face un jury de professionnels du métier.
Toute notre approche pédagogique est basée sur le respect des critères de la norme ISO 9001.

CYBER LABS – TESTS D'INTRUSIONS ET REMÉDIATIONS

TARIFS ET FINANCEMENTS (possibilité de prise en charge partielle ou intégrale)

Tarif public de cette formation : 1 000€ HT soit 1200€ TTC (tarif indicatif)

Votre formation peut être prise en charge par un organisme de financement. Dans le cadre d'un FNE, CPF, AIF, CSP, n'hésitez pas à nous contacter à recrutement@devenez.fr

En fonction de votre statut au moment de l'entrée en formation (salarié ou demandeur d'emploi), cette prise en charge pourra être **partielle ou intégrale**.
Plus d'informations sur les financements : https://www.devenez.fr/financements/

MODALITES ET DELAIS D'ACCES

Délai d'inscription variable selon le mode de financement.

INSCRIPTION SUR NOTRE SITE INTERNET :
https://www.devenez.fr/espace-candidats/les-offres-en-cours/formation-modules-boosters/

ACCESSIBILITE :

Public en situation de handicap, contactez notre Référent : M. Olivier BENANOU – o_benanou@devenez.fr

POUR TOUTE DEMANDE DE RENSEIGNEMENT :

Contactez-nous à recrutement@devenez.fr