EXPER.net
CAMPUS INFORMATIQUE & MARKETING DIGITAL

ESD
Cybersecurity Academy

EXPERT.E EN SÉCURITÉ DIGITALE



FORMATION
BAC+5
RNCP 36399
NIVEAU 7

PROGRAMME

HACKING ETHIQUE

- Ce cours vous permet d'aborder différents types d'attaque comme le hacking système, le sniffing, les injestions SQL, le contournement IDS mais également l'étude de malware ou la mise en place de Honeyspots

SECURITE OFFENSIVE

- Ce cours vous permet d'avoir une vue d'ensemble sur les attaques modernes pesant sur la sécurité de l'information. La double vision (Attaque/Défense) permet de comprendre les choix effectués par attaquants, afin de prévoir l'implémentation des mesures de sécurité les plus efficaces possible. De la prise de contrôle de l'organisation aux différentes phases de rebonds internes qu'un attaquant pourrait être tenté d'utiliser, l'ensemble de ces phases sera analysé.
    - o Identifier et exploiter les vulnérabilités
    - o Attaques avancées : Old School vs New School
    - o Dans la peau d'un Hacker

PYTHON POUR TEST D'INTRUSION

- Ce cours est orienté vers l'utilisation du langage Python et PowerShell pour la fabrication d'outils pour le métier de Pentester. Les bibliothèques telles que Spacy, Beautiful Soup, API.net sont étudiées. Vous étudierez la création de connexion socket avec les techniques de bypass IDS, ARP Poisoning et exflitration de données.
    - o Créer un socket (client/serveur) en liaison avec un reverse shell - FUD
    - o Créer une communication http(s) et évasion d'IDS/IPS
    - o Remplacement du socket proxy, sniffer, arp spoofing, MITM avec Scapy
    - o Utilisation de Python avec Burpsuite
    - o Création d'une charge FUD avec PowerShell

SECURITE DEFFENSIVE

- Ce cours permet d'avoir une vue d'ensemble sur les mécanismes de défense permettant aux organisations de créer une protection efficace et efficiente. Afin d'implémenter et configurer au plus juste les systèmes de défense SI, l'approche par l'attaque sera mise en avant et ce à travers des exercices de simulation confrontant des infrastructures virtuelles à différentes attaques, en conditions réelles.
    - o Réduction des surfaces d'attaque
    - o Bests practices SSI
    - o Attaques et défenses des infrastructures SI
    - o Durcissement des mécanismes de défense

FORENSIC ET REPONSE A INCIDENT

- Ce cours a pour but d'établir un panorama des différentes branches et parties prenantes du Forensic (Forensic légal, Réponse à incident, outils, etc...). La collecte de données sur disque, RAM, fichier d'hibernation est ensuite étudiée avec ses différentes propriétés.
- Observer les mouvements d'exfiltration, de pivoting et de persistance. Pour finir, une analyse statique et dynamique des charges malveillantes est mise en pratique.
    - o Découverte du monde de l'investigation
    - o Présentation d'une méthodologie de relevé de preuves
    - o Collecte de données, timeline, analyse, rapport
    - o Etudes des différentes malware, analyse de malware (statique)
    - o Etude et protection après incident sur les systèmes Windows
    - o Création d'un plan de réponse à incident

ISO 27005 : ANALYSE DE RISQUES SI

- La formation « ISO/CEI 27005 Risk Manager » vous permettra de développer les compétences pour maîtriser les processus liés à tous les actifs pertinents pour la sécurité de l'information en utilisant la norme ISO/CEI 27005 comme cadre de référence. Au cours de cette formation, nous présenterons également d'autres méthodes d'appréciation des risques telle que EBIOS et la méthodologie harmonisée d'EMR. persistance.
    - o Analyse et compréhension d'une stratégie d'entreprise
    - o Etude de la gouvernance SSI et de l'importance de l'alignement stratégique
    - o Mise en œuvre d'une analyse de risques basée sur l'ISO 27005 au travers de la méthode EBIOS
    - o Extrapolation et méthode d'implémentation d'une politique de sécurité de l'information

CDCF : CAHIER DES CHARGES FONCTIONNEL

- Le module CDCF a pour but principal de fournir l'ensemble de moyens, méthodes, et outils nécessaires à la gestion des projets SSI au sein d'une organisation. La formation permettra de prendre en main l'ensemble des phases constituant la construction d'un cahier des charges fonctionnel. L'alignement entre les besoins de l'organisation et le contenu du CDCF sera analysé, ainsi que l'alignement des réponses à appels d'offres.

PROGRAMME

ISO 27001 : SMSI

- SO/IEC 27001 Lead Implementer vous permet de développer l'expertise nécessaire pour aider une organisation à établir, mettre en oeuvre, gérer et maintenir un Système de Gestion de la Sécurité de l'Information (SMSI). Durant cette formation, vous gagnerez aussi une compréhension approfondie des meilleures pratiques des systèmes de gestion de la sécurité de l'information pour sécuriser les informations sensibles de l'organisation et améliorer la performance globale et l'efficacité.
  - o Présentation de la norme ISO 27001/ISO 27002
  - o Contexte d'utilisation et d'implémentation
  - o Compréhension des relations entre le SMSI, le management des risques, les contrôles et les différentes parties prenantes
  - o Analyse détaillée des exigences de la norme 27001
  - o Savoir créer une méthodologie alignée sur l'ISO 27001 pour le déploiement d'un SMSI

PCA/PRA : GESTION DE CRISE ISO 22301

- Ce cours permet d'avoir l'ensemble les éléments pour la compréhension et l'implémentation d'un système de management de la continuité d'activité. Il permet de créer un alignement fort avec les besoins en continuité des processus des organisations et s'intègre parfaitement dans une démarche de gestion par le risque. Ce cours permettra d'avoir une vision claire sur les choix liés à la continuité d'activité ainsi que leurs efficiences en fonctions des besoins identifiés par l'organisation.
  - o PCA/PRA/PSI/PCI Explications
  - o Compréhension des besoins en sécurité de l'information de l'entreprise
  - o Savoir mener une analyse d'impact sur le business (Business Impact Analysis)
  - o Analyse détaillée des exigences de la norme 22301

APPSEC, SECDEVOPS : WEB, MOBILE DEVOPS

- La sécurisation des applications web est primordiale. Ce cours permet d'aborder les attaques les plus connue sur une application web, souvent regroupées par le TOP 10 OWASP (SQLI, XSS, CSRF, IDOR, SSRF, etc.). Mise en pratique du durcissement de code, de l'infrastructure, des serveurs, avec l'insertion de service SAST, DAST, montée de charge en intégration continue.
  - o Compréhension des attaques web les plus utilisées (top 10 OWASP) et protection
  - o Mise en place d'un cycle de développement sécurisé (SDL), ISO 27034, protection DaCP
  - o Mise en place d'un modèle de maturité pour la sécurité des applications
  - o Réduction des attaques de surface, secure by default, séparation des privilèges
  - o Hardening, conception sécurisé (intégration d'outils, durcissement server/client, architecture sécurisé, HTTPOnly, CSP, etc.)
  - o Pentest applicatif (Méthode OWASP)

VEILLE SSI

- Un test d'intrusion bien mené nécessite une méthode rigoureuse afin de rédiger un rapport de test qui ne se contente pas d'énumérer les vulnérabilités détectées chez le client. À ce titre, l'accent a été mis sur la définition des règles de pré-engagement, la réglementation et sur la rédaction du rapport afin qu'il soit clair et en adéquation avec les craintes et les motivations du client.
  - o Textes officiels concernant la réglementation d'un test d'intrusion
  - o Préparation et organisation du projet Pentest
  - o Création de règles de pré-engagement, contrat commercial, devis
  - o Utilisation de la méthode PTES et le respect des différentes phases suivant le périmètre des RE
  - o Création de rapport

DURÉE TOTALE : 18 mois
Durée en formation : 30% Durée en entreprise : 70%

PUBLIC ET PRÉ-REQUIS :

- Bac+3/4 en informatique validé
- Intérêt pour le monde la cybersécurité
- Entretien de motivation + test (1h)

ACCESSIBILITÉ :

- Parcours continu de formation (Alternance)
- Capitalisation des CCP
- VAE
- CPF

MÉTIERS VISÉS :

- Expert-e en sécurité numérique
- Consultant-e en sécurité des SI
- Auditeur-rice en sécurité des SI
- Assistant-e RSSI
- Risk Manager (Junior)
- Administrateur-rice système réseau et sécurité

DÉBOUCHÉS / SECTEURS D'ACTIVITÉ

- Consultant sécurité
- Administrations et grandes entreprises
- Services Sécurité / Informatiques des PME/PMI

COMPÉTENCES / CAPACITES ATTESTÉES :

- Les Experts en Sécurité Digitale sont reconnus par la profession et par leurs responsables hiérarchiques comme des experts dans la conception d'infrastructure informatique ainsi que la sécurisation de celle-ci
- Ils veillent à la sécurité et l'évolution du SI de l'entreprise
- Il prend les décisions stratégiques, négocie et supervise leur mise en œuvre avec les acteurs impliqués. Il assure des positions managériales selon la taille de l'entreprise

VALIDATION

- Titre « **Expert.e en Sécurité Digitale** » reconnu par l'Etat de Niveau 7 (Bac+5), inscrit au RNCP36399
- Arrêté du 25-04-2022 - date d'échéance enregistrement 25/04/2027
- Le passage du titre professionnel se fait en intégralité sur l'ensemble des blocs de compétences

POURSUITE DE PARCOURS :

- Bac+5 " **Directeur.rice de Projets Informatiques**" chez EXPERNET
- Master 2 à l'université
- Titre Professionnel Bac+5

MÉTHODES ORGANISATIONS PEDAGOGIQUES :

- Pratiques professionnelles, apprentissage théorique schématisé, cas pratique / Simulation, retour d'expérience, méthodologie projet, pédagogie différenciée

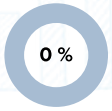
STATISTIQUES EN 2025



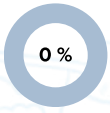
TAUX DE RÉUSSITE



TAUX D'INSERTION



TAUX D'INTERRUPTION



TAUX DE POURSUITE D'ÉTUDE

EXPERNET MET TOUT EN ŒUVRE POUR ACCUEILLIR LES PERSONNES EN SITUATION DE HANDICAP ET A MOBILITÉ RÉDUITE POUR TOUTE INFORMATION,

MERCI DE CONTACTER LA RÉFÉRENTE HANDICAP DU CAMPUS

CHAMAND Murielle
Référente Handicap et Mobilité
Nationale et Internationale

0262 21 90 45
m.chamand@expernet.re