Expert.e
en Sécurité Digitale

FORMATION
BAC +5
RNCP
NIVEAU 7

Durée en formation	Durée en entreprise
15 semaines	40 semaines

CONDITIONS D'ADMISSION :

- Bac+3/4 en informatique validé
- Intérêt pour le monde la cybersécurité
- Entretien de motivation (40min)

TYPES D'EMPLOI ACCESSIBLES A LA SORTIE :

- Administrateur.rice Système et/ou Réseau
- Administrateur.rice de Bases de données
- Administrateur.rice de Messagerie
- …

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.
    - Identifier et exploiter les vulnérabilités
    - Attaques avancées : Old School vs New School
    - 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 exfiltration de données.

- Créer un socket (client/serveur) en liaison avec un reverse shell - FUD
- Créer une communication http(s) et évasion d'IDS/IPS
- Remplacement du socket proxy, sniffer, arp spoofing, MITM avec Scapy
- Utilisation de Python avec Burpsuite
- 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.

- Réduction des surfaces d'attaque
- Bests practices SSI
- Attaques et défenses des infrastructures SI
- Durcissement des mécanismes de défenses
- Audit et sécurité SI & Plan 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.

- Découverte du monde de l'investigation
- Présentation d'une méthodologie de relevé de preuves
- Collecte de données, timeline, analyse, rapport
- Etudes des différentes malware, analyse de malware (statique)
- Etude et protection après incident sur les systèmes Windows
- Création d'un plan de réponse à incident

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.

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.

- Analyse et compréhension d'une stratégie d'entreprise
- Etude de la gouvernance SSI et de l'importance de l'alignement stratégique
- Mise en œuvre d'une analyse de risques basée sur l'ISO 27005 au travers de la méthode EBIOS
- Extrapolation et méthode d'implémentation d'une politique de sécurité de l'information

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.

- Présentation de la norme ISO 27001/ISO 27002
- Contexte d'utilisation et d'implémentation
- Compréhension des relations entre le SMSI, le management des risques, les contrôles et les différentes parties prenantes
- Analyse détaillée des exigences de la norme 27001
- 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.

- PCA/PRA/PSI/PCI Explications
- Compréhension des besoins en sécurité de l'information de l'entreprise
- Savoir mener une analyse d'impact sur le business (Business Impact Analysis)
- 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.

- Compréhension des attaques web les plus utilisées (top 10 OWASP) et protection
- Mise en place d'un cycle de développement sécurisé (SDL), ISO 27034, protection DaCP
- Mise en place d'un modèle de maturité pour la sécurité des applications
- Réduction des attaques de surface, secure by default, séparation des privilèges
- Hardening, conception sécurisé (intégration d'outils, durcissement server/client, architecture sécurisé, HTTPOnly, CSP, etc.)
- Pentest applicatif (Méthode OWASP)

Expert.e
en Sécurité Digitale

FORMATION
BAC +5
RNCP
NIVEAU 7

VEILLE SSI

Choix des étudiants d'un sujet sur la sécurité des systèmes d'information pour une recherche approfondie et documentation dans le but de savoir sensibiliser une équipe au sein d'un système d'information sur un sujet concernant la sécurité.

MENER UN TEST D'INTRUSION

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.

- Textes officiels concernant la réglementation d'un test d'intrusion
- Préparation et organisation du projet Pentest
- Création de règles de pré-engagement, contrat commercial, devis
- Utilisation de la méthode PTES et le respect des différentes phases suivant le périmètre des RE
- Création de rapport

COMPETENCES / CAPACITES ATTESTEES :

- 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'évolutivité 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

DEBOUCHES / SECTEURS D'ACTIVITE :

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

VALIDATION :

- Titre « Expert en Sécurité Digitale » reconnu par l'Etat de Niveau 7 (Bac+5), inscrit au RNCP
- Arrêté du 16/12/16, J.O du 03/03/17

ACCESSIBILITE :

- PARCOURS CONTINU DE FORMATION (Alternance)
- CAPITALISATION DES CCP
- VAE
- CPF (Code 248562)

POUR TOUTES INFORMATIONS OU DEMANDES D'INSCRIPTION, CONTACTEZ :

MAXIME COURBET – RESPONSABLE DEVELOPPEMENT ECOLE

0692 85 79 94 – 02 62 21 90 45 – m.courbet@expernet.re

EXPERNET MET TOUT EN ŒUVRE POUR ACCUEILLIR LES PERSONNES EN SITUATION DE HANCICAP ET A MOBILITE REDUITE
POUR TOUTE INFORMATION MERCI DE CONTACTER LA REFERENTE HANDICAP DE NOTRE ORGANISME :
NELLY SEGUIN - 0693 03 62 55 – n.seguin@expernet.re

MAJ mardi 1er juin 2021