le cnam
Nouvelle-Aquitaine

Fiche récapitulative

CYB108 | Durcissement et mise en oeuvre de mesures de sécurité avancées pour les données, les réseaux et les systèmes (Hardening)

Mise à jour le 29/04/2026

50
Total d'heures d'enseignement

6
Crédits ECTS

Date non définie
Début des cours prévu

Programme

Sujet 01 - Introduction générale sur la sécurité informatique et principe de hardening

- Mise en place d'un atelier de machines Linux/Windows vulnérables et à durcir
- Cartographie d'un système d'information : identification de la topologie réseau
- Cartographie d'un système d'information : identifier les machines accessibles avec NMap
- Cartographie d'un système d'information : identifier les machines affectées par des vulnérabilités connues
- Introduction au durcissement systèmes et réseaux
- Concept de défense en profondeur
- L'attaque comme moyen pour mieux se défendre : survol des techniques avancées comme ;
- Cyber kill chaine
- Cyber kill chaine unifié
- Le framework MITRE ATT&CK

- Lab : identification de vulnérabilité système et mise en place d'une solution de sécurisation. Environnement : Kali Linux & Metasploitable2 / Plateforme VMWare ou équivalent

Sujet 02 - Durcissement de systèmes Linux

- Définition des besoins de durcissement
- Mise en place d'une base de sécurité (Security Baseline)
- Désactivation des services qui ne sont pas nécessaires
- Suppression des processus inutiles
- Gestion des patchs
- Gestion et vérification des permissions des fichiers
- Gestion de modification des permissions sur les fichiers
- Contrôle et vérification des permissions sur le fichiers et répertoires critiques
- Restreindre l'exécution des applications et des commandes sur Linux

- Protection par pare-feu basée sur l'hôte avec le pare-feu linux IPtables
- Protection du système linux à l'aide de Fail2ban
- Menace, vulnérabilité, besoin et HIDS ?
- Lab01 : Auditer les configurations avec buck-security et Lynis.
- Lab02 : durcissement périmétrique d'un système et réseau à l'aide du pare-feu IPtables.
- Lab03 : mise en place de la protection et durcissement d'un système Linux à l'aide de IDS Snort. Environnaient : Kali comme machine d'attaque, Ubuntu, la machine à protéger. Outils exploités : nmap, scapy

Sujet 03 - Durcissement de systèmes Windows

- Définition des besoins de durcissement

- Checklist de sécurité de base des systèmes d'exploitation
- Configuration d'un mot de passe BIOS
- Audit de Registry de Windows
- Outil Process Monitor (/> - Gestion des mots de passes et comptes utilisateurs
- Configuration de l'authentification utilisateur
- Checklist de sécurité de base des systèmes d'exploitation
- Configuration d'un mot de passe BIOS
- Audit de registry de Windows
- Outil Process Monitor (/> - Gestion des mots de passes et comptes utilisateurs
- Configuration de l'authentification utilisateur

- Construction de contrôles de base pour Windows (Building Baseline Controls)
- Centre pour la sécurité Internet (CIS® ó Center for Internet Security)
- Windows Security Baseline « Les lignes de base de sécurité Windows »

- Outils pour le durcissement de Windows
- Lab01 : audit du système avec GFI'sLANguard
- Lab02 : LAB Sécurisation des données avec VeraCrypt
- Lab03 : améliorer la protection du système hôte Windows à l'aide du IDS SNORT.

Sujet 04 - Durcissement des flux de données réseau

- Durcissement des flux de données (IP sec, TLS, Equipement réseaux)
- Atelier, LAB
- Durcissement des flux sur l'interface Radio (cas de 4G et 5G)
- Lab01 : mise en place et configuration de VPN IPsec entre deux sites

Sujet 05 - Hardening Windows et réseaux

- Durcissement de serveurs Linux
- Durcissement des serveurs Windows (Active Directory, Kerberos, etc.)
- Lab01 : Windows Server 2008 (comme cas intéressant pour ses vulnérabilités)

Objectifs : aptitudes et compétences

Objectifs :

Le cours adresse des sujets technologiques avancées et cible plus particulièrement les systèmes d'exploitation Linux et Windows (systèmes hôtes et serveurs), les infrastructures réseaux et la sécurisation des échanges sur la voie radio pour le système 4G et 5G.

Le Harding des systèmes, des réseaux et de données joue un rôle fondamental dans la stratégie de la mise en place de la défense en profondeur.

Le cours permettra aux auditeurs de maitriser les stratégies et appréhender les techniques permettant d'améliorer la sécurité des systèmes ainsi que l'évaluation de l'efficacité de ces techniques.

Les objectifs pédagogiques sont les suivants :

- Comprendre et apprendre à garantir la sécurité des systèmes d'exploitation windows
- Comprendre et apprendre à garantir la sécurité des systèmes d'exploitation linux
- Maitriser les approches de base pour garantir la sécurité des systèmes serveurs Windows et Linux
- Comprendre et maitriser les techniques et solutions de sécurisation des flux de données échangés flux réseaux et des services et aussi sur la voie radio.

Comprendre et apprendre les différents outils et techniques pour mettre en place le durcissement

Compétences :

- Choisir les mécanismes utiles à la mise en place du durcissement (configurations, gestion des patchs, etc.)
- Choisir les solutions et techniques appropriés selon le type de durcissement mis en place.
- Optimiser la sécurité des principaux systèmes d'exploitation (linux et Microsoft Windows, MS Active directory, serveurs Window et

Linux).
- Définir la stratégie de sécurisation des flux réseaux et des services.
- Mettre en place des mesures techniques avancées sur un systèmes d'information en exploitation : système d'exploitation et réseaux.

Prérequis

Bac+2 informatiques (ou L2)

RSX101-Réseaux et protocoles pour l'Internet

SEC102-Menaces informatiques et codes malveillants : analyse et lutte

Disposer de connaissances :

- En techniques du chiffrement, d'authentification et de la signature numérique,
- En administration système (Windows et Linux) ainsi qu'en réseaux et équipements réseaux.

Délais d'accès

Le délai d'accès à la formation correspond à la durée entre votre inscription et la date du premier cours de votre formation.

- UE du 1er semestre et UE annuelle : inscription entre mai et octobre
- UE du 2e semestre : inscription de mai jusqu'à mi-mars

Exemple : Je m'inscris le 21 juin à FPG003 (Projet personnel et professionnel : auto-orientation pédagogique). Le premier cours a lieu le 21 octobre. Le délai d'accès est donc de 4 mois.

Modalités

Modalités pédagogiques :

Pédagogie qui combine apports académiques, études de cas basées sur des pratiques professionnelles et expérience des élèves. Équipe pédagogique constituée pour partie de professionnels. Un espace numérique de formation (ENF) est utilisé tout au long du cursus.

Modalités de validation :

Les centres de présentation des examens sont Angoulême, Bordeaux, Dax, Limoges, Niort, Pau et Poitiers.

Tarif

Plusieurs dispositifs de financement sont possibles en fonction de votre statut et peuvent financer jusqu'à 100% de votre formation.

Salarié : Faites financer votre formation par votre employeur

Demandeur d'emploi : Faites financer votre formation par Pôle emploi

Votre formation est éligible au CPF ? Financez-la avec votre CPF

Si aucun dispositif de financement ne peut être mobilisé, nous proposons à l'élève une prise en charge partielle de la Région Nouvelle-Aquitaine avec un reste à charge. Ce reste à charge correspond au tarif réduit et est à destination des salariés ou demandeurs d'emploi.

Pour plus de renseignements, consultez la page Financer mon projet formationopen_in_new ou contactez nos conseillers pour vous accompagner pas à pas dans vos démarches.

Passerelles : lien entre certifications

- CYC9106A - Diplôme d'ingénieur Cybersécurité

Taux de réussite

Les dernières informations concernant le taux de réussite des unités dcenseignement composant les diplômes

↓ Taux de réussite