SEC108 - Durcissement et mise en œuvre de mesures de sécurité avancées pour les données, les réseaux et les systèmes (Hardening)

Mis à jour le 02-01-2023

Code : SEC108

Unité d'enseignement de type mixte

6 crédits

Volume horaire de référence (+/- 10%) : **50 heures**

Responsabilité nationale :
EPN05 - Informatique / 1

Contact national :

EPN05 - Informatique

2 rue Conté
accès 33.1.13B
75003 Paris
01 40 27 28 21
Mmadi Hamida
hamida.mmadi@lecnam.net

Présentation

Prérequis

Bac+2 informatique (ou L2)
SEC105

SEC106
Disposer de connaissances en administration système (Windows et Linux) ainsi qu'en réseaux et équipements réseaux.

Objectifs pédagogiques

Ce cours vise la connaissance avancée des technologies de la sécurité informatique : cryptographie, systèmes d'exploitation (Linux et Windows), infrastructures réseaux.
Il permet d'acquérir des compétences de durcissement ainsi que de l'évaluation de ces mesures de sécurité, il répond à la stratégie de sécurité "tout ce qui n'est pas utile au fonctionnement est inutile et sera désactivé" afin d'éviter les brèches.
Il permettra en conséquence de n'activer que les services utiles et de désactiver tous les autres.
Le cours propose d'apprendre la mise en place d'outillage pour le hardening et la conception et le maintien de l'outillage de cyber défense, de détection d'intrusion sur les systèmes Linux et windows pour mettre en place un système de défense plus robuste pour amélioration continue et l'atténuation de la menace.

Les objectifs pédagogiques sont les suivants :

- Comprendre et apprendre à se prémunir des attaques sur le chiffrement des données et des données sensibles
- Comprendre et apprendre à garantir la sécurité des systèmes d'exploitation principaux linux et windows,
- Comprendre et apprendre les exigences et contraintes spécifiques à la mise en place de chacune des briques techniques du systèmes d'information : système d'exploitation et réseaux.
- Comprendre et apprendre les différents dispositifs présents pour les optimiser en fonction des flux réseaux et des services,
- Comprendre et apprendre les mécanismes utiles à la mise en place du hardening (configurateur avancé, contrôle des configurations),
- Comprendre et apprendre les différents outils et techniques pour mettre en place le hardening.

Compétences

- Choisir les techniques de chiffrement adaptés aux contraintes techniques, organisationnelles et de conformité.
- Anticiper les attaques sur le chiffrement des données et des données sensibles.
- Choisir les mécanismes utiles à la mise en place du hardening (configurateur avancé, contrôle des configurations.
- Adapter les différents outils et techniques selon le type de durcissement mis en place.
- Optimiser la sécurité des principaux systèmes d'exploitation (linux et MS Windows, MS Active directory).
- Optimiser en fonction 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.

Programme

Contenu

Cours 1 Introduction aux systèmes durcis

TEMPS 1 – Cryptographie avancée

Cours 2 – Chiffrement des données en réseau (symétrique par bloc)

Cours 3 – Chiffrement des données en réseau (asymétrique)

Cours 4 – Durcissement par chiffrement de disque

TEMPS 2 – Durcissement de systèmes Windows

Cours 5 - Menace, vulnérabilité, besoin et HIDS

Cours 6 – Outils pour la réduction des surfaces d'attaques systèmes

Cours 7 – Autres outils pour le durcissement de Windows

TEMPS 3 – Durcissement de systèmes Linux

Cours 8 - Menace, vulnérabilité, besoin et HIDS

Cours 9 – Outils pour la réduction des surfaces d'attaques systèmes Linux

Cours 10 – Autres outils pour le durcissement de Linux

TEMPS 4 – Durcissement Réseaux +protocole

Cours 11 – Durcissement SSH

Cours 12 –Utilisation de Netfilter et iWatch

Cours 13 : Révision Modalités de validation

Modalités de validation

- Projet(s)
- Mémoire
- Examen final

Description des modalités de validation

Examen final Projet(s)
Dossier Ou examen sur table Ou les 2

Bibliographie

Titre	Auteur(s)
CCNA Security 210-260 Certification Guide	Auteur: Singh, Glen D.,Vinod, Michael,Anandh, Vijay Editeur: Packt Publishing - 2018
Mastering Linux Security and Hardening	Auteur: Tevault, Donald A. Editeur: Packt Publishing - 2018
Identifying and Mitigating Vulnerabilities of Hardened Windows Operating System. In : Information and Communication Technology for Competitive Strategies (ICTCS 2020). Springer, Singapore, 2022. p. 623-632. OLENCIN, Michal et PERHÁC, Ján. Automated Hardening of a Linux Web Server.	SREERAG, M., SETHUMADHAVAN, M., et AMRITHA, P. P.

Automated Hardening of a Linux Web Server.	OLENCIN, Michal et PERHÁC, Ján.