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

Mis à jour le 17-07-2026

Code : CYB108

Unité d'enseignement de type mixte

6 crédits

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

Responsabilité nationale :
EPN05 - Informatique / Pierre SWEID

Contact national :

EPN05- Informatique

2 rue Conté
33.1.14A
75003 Paris

Sanaz MANSOURI
sanaz.mansouri@lecnam.net

Présentation

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.

Objectifs pédagogiques

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.

Programme

Contenu

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 (https://technet.microsoft.com)
    - 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 (https://technet.microsoft.com)
    - 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)

Modalités de validation

- Contrôle continu
- Projet(s)

Bibliographie

Titre	Auteur(s)
1. Red_Hat_Enterprise_Linux-8-Security_hardening. Enhancing security of Red Hat Enterprise Linux 8 systems	Collectif
2. Linux Hardening in Hostile Networks. Server Security from TLS to Tor. KYLE RANKIN	Collectif
3. CIS_Microsoft_Windows_Server_2019_Stand-alone_v2.0.0	Collectif
4. Syngress - Security Sage's Guide to Hardening the Network. Steven Andrés et Brian Kenyon. SYNGRESS	Collectif
5. CCNA Security 210-260 Official Cert Guide, https://community.cisco.com/legacyfs/online/ccna_security_chapter_18_9781587205668_.pdf. Omar Santos et John Stuppi. Copyright© 2015 Pearson Education, Inc. Published by: Cisco Press 800 East 96th Street	Collectif