Sécurité des Systèmes d'exploitation	Semestre 8	**Responsable :** David DUVIVIER et Jérôme RIDET

Objectifs de l'ECUE en termes de compétences et d'acquis d'apprentissage visés

A l'issue de cette UE, l'apprenant aura progressé sur les compétences suivantes du référentiel de la formation :

- BC2.1 : Modéliser un problème ou un besoin fonctionnel exprimé par un client et spécifier une solution informatique
- BC2.3 : Concevoir et développer les applications informatiques : web, mobiles, logicielles
- BC2.4 : Documenter une étude et une solution informatique
- BC2.5 : Analyser et identifier les aspects réglementaires et techniques
- BC3.1 : Analyser une solution informatique et en mesurer les performances en utilisant les outils et métriques adaptés (réseaux, systèmes, accès aux données, sécurité, etc.)
- BC3.5 : Fiabiliser et sécuriser

Plus précisément, il sera capable de :

- Spécifier le comportement attendu de la solution de sécurité des systèmes d'exploitation
- Configurer un système d'exploitation pour renforcer sa sécurité, en utilisant des outils d'administration et des pratiques de sécurité recommandées
- Présenter une solution de sécurité des systèmes d'exploitation
- Analyser les normes de sécurité des systèmes d'exploitation, telles que ISO 27001 ou NIST 800-53, et identifier les bonnes pratiques à mettre en œuvre
- Identifier les propriétés de sécurité indispensables pour la protection des données manipulées par un poste de travail ou un serveur
- Identifier les risques et les vulnérabilités pouvant affecter un système d'exploitation
- Concevoir des mécanismes permettant de renforcer la sécurité d'un système d'exploitation ;
- Supprimer ou conserver les fonctionnalités d'un système d'exploitation en fonction de leur adéquation aux contraintes de sécurité

Description de l'ECUE

Sécurité Linux et Windows

- Attaques du noyau depuis l'espace utilisateur
- Mécanismes de protection de l'espace utilisateur
- Protection contre les attaques depuis l'espace utilisateur

Durcissement Linux

- Durcissement niveau 1 (pré-requis, gestion des droits, des services et des packages, Options FS, options kernel, durcissement des paramètres réseaux)
- Durcissement niveau 2 (gestion des droits, des utilisateurs et des packages)
- Durcissement niveau 3 (BIOS-séquence de boot, gestion des packages, implémentation de SELINUX)

Prérequis
Fondements de la sécurité, modèles de sécurité, systèmes d'exploitation, système et programmation sécurisée

Références
S. Ghernaouti, Cybersécurité, Sécurité informatique et réseaux, Dunod, 5ème édition, 2016 G. Avoine, P. Junod, P. Oechslin et S. Pasinin, Sécurité informatique, Vuibert, 2015