

Sécurité des systèmes d'exploitation

Domaine	Ingénierie et Architecture
Filière	Télécommunications
Orientation	Sécurité de l'information (TS)
Mode de formation	Plein temps

Informations générales

Nom:	:	Sécurité des systèmes d'exploitation
Identifiant:	:	SOS
Année académique	:	2019-2020
Responsable:	:	Sylvain Pasini
Charge de travail:	:	90 heures d'études
Périodes encadrées:	:	64 (= 48 heures)

Semestre	E1	S1	S2	E2	S3	S4	E3	S5	S6
Cours						32			
Laboratoire						32			

Connaissances préalables recommandées

- Bases de la programmation procédurale
- Principes fondamentaux de la sécurité de l'information
- Principes fondamentaux des réseaux

Objectifs

À la fin de ce cours, l'étudiant sera capable:

- connaître les principales vulnérabilités et attaques visant des systèmes d'exploitation;
- comprendre les mécanismes sécuritaires les plus importants des principaux systèmes d'exploitation modernes (Linux, Microsoft Windows, Android, iOS);
- comprendre les modèles de contrôle d'accès et être capable de les utiliser;
- mettre en place des mécanismes de restrictions, d'isolation et/ou de virtualisation;
- être capable de concevoir et d'appliquer une stratégie de durcissement d'un système d'exploitation et de son interaction avec les applications;

Contenu et formes d'enseignement

Répartition des périodes indiquée à titre informatif.

Cours: 32 périodes

- Linux : Concepts de base et outils de consolidation	2
- LinuxÂ : Limitation des opportunités de vulnérabilité, supervision et contrôle d'intégrité	2
- LinuxÂ : Gestion avancée des contrôles d'accès et SELinux	2
- LinuxÂ : Limitation des ressources et des accès aux ressources, isolation et virtualisation	2
- LinuxÂ : Limitation des accès au réseau, gestion centralisée des configurations et des patches	2

- WindowsÂ : Introduction et composants de sécurité	2
- WindowsÂ : Attaques, outils et exploitation de vulnérabilités	3
- WindowsÂ : Vol de mots de passe et persistance	3
- WindowsÂ : Protection de mots de passe, sécurité physique et authentification avancée	2
- Sécurité mobile	8
- Travaux pratiques	4
Laboratoire: 32 périodes	
- Exercices pratiques de sécurité Linux	8
- Laboratoire de sécurité Linux	4
- Exercices pratiques de sécurité Windows	6
- Laboratoire de sécurité Windows	6
- Laboratoire de sécurité Mobile	8

Bibliographie

N/A

Contrôle de connaissances

Cours:

l'acquisition des matières de cet enseignement sera contrôlée au fur et à mesure par des tests et des travaux personnels tout au long de son déroulement. Il y aura au moins 2 tests d'une durée totale d'au moins 2 périodes.

Laboratoire:

ils seront évalués sur la base des rapports de manipulation, à 3 reprises au minimum.

Examen:

L'atteinte de l'ensemble des objectifs de formation sera vérifiée lors d'un contrôle final commun écrit d'une durée de 90 minutes.

Matériel autorisé:

- Information communiquée directement par l'enseignant.

Calcul de la note finale

Note finale = moyenne cours x 0.3 + moyenne laboratoire x 0.2 + moyenne examen x 0.5

Fiche validée le 17.09.2019 par Donini Pier