UCLouvain

linfo2347

2026

Computer system security

5.00 crédits	30.0 h + 15.0 h	Q2

Enseignants	Sadre Ramin ;
Langue d'enseignement	Anglais > Facilités pour suivre le cours en français
Lieu du cours	Louvain-la-Neuve
Préalables	Requis#: principes des systèmes informatiques, tels que visés par le cours LINFO1252 Requis#: compétences en réseaux informatiques telles que visées par le cours LINFO1341
Thèmes abordés	· e-mail falsifiés, couriers non désirés, logiciels malveillants , · Principes de base de la cryptographie , · Vulnérabilité des réseaux et des applications: usurpation d'adresse IP , détournement de session , exploits , reniflage de paquets , · Pare-feu, · Proxy , IDS , méthodes de piratage, · Sécurité des communications · Sécurité au niveau de l'utilisateur
Acquis d'apprentissage	**A la fin de cette unité d'enseignement, l'étudiant est capable de :** Eu égard au référentiel AA du programme « Bachelier en sciences informatiques », ce cours contribue au développement, à l'acquisition et à l'évaluation des acquis d'apprentissage suivants: · S1.L8 · S2.1-4 · S4.3-4 · S5.1-2 Eu égard au référentiel AA du programme « Master ingénieur civil en informatique », ce cours contribue au développement, à l'acquisition et à l'évaluation des acquis d'apprentissage suivants : · INFO1.1-3 · INFO2.1-5 · INFO5.4-5 · INFO6.1, INFO6.4, INFO6.5 Le cours offre une vision large de la sécurité de systèmes informatiques. Les étudiant·e·s qui terminent avec succès ce cours seront capables de: · défendre le besoin de protection et de sécurité; · identifier les points forts et les faiblesses en matière de sécurité des systèmes informatiques; · expliquer les problèmes liés à la criminalité numérique et exposer les principes fondamentaux impliqués dans la lutte contre celle-ci; · comparer et mettre en lumière les différences entre les méthodes actuelles de mise en oeuvre de la sécurité.

Modes d'évaluation des acquis des étudiants	Mode d'évaluation pour la session de juin : · Examen (50% de la note finale) · Activités de projet en groupe (40% de la note finale) · Activité de project individuel (10% de la note finale) Session d'août: Les activités de projet (en groupe et individuel) **ne pourront pas** être faites ou refaites pour la session d'août et l'étudiant.e conservera les notes obtenues pour celles-ci lors de la session de juin avec les pondérations pour la note finale comme indiqué ci-dessus. La non participation aux activités de projet aux dates indiquées par l'enseignant entraînera la note zéro pour la partie concernée. Concernant l'utilisation de l'IA générative : les étudiants sont autorisés à utiliser des outils d'IA générative pour soutenir leur travail de projet, par exemple pour comparer des approches de solution, trouver des erreurs dans le code ou améliorer la formulation des rapports. Cependant, les soumissions, qu'il s'agisse de code source, de rapports ou d'autres formes, doivent être principalement votre propre travail. Si des outils d'IA générative ont été utilisés, leur nature et leur portée doivent être décrites en détail dans le travail remis (voir les instructions du projet concerné) et seule la partie originale du travail de l'étudiant sera évaluée. Cela s'applique également lorsque l'on s'inspire du travail de tiers, qu'il provienne d'Internet ou d'une autre personne. Le non-respect de ces directives peut entraîner une réduction des notes ou d'autres sanctions académiques. Le professeur peut demander à un.e étudiant.e de passer un examen oral supplémentaire en complément de l'examen et/ou des activités de projet, dans des cas incluant, mais non limités à, des problèmes techniques, ou des suspicions d'irrégularités.
Méthodes d'enseignement	· Cours magistraux · Lecture d'articles scientifique · Travaux pratiques · Activités de projet
Contenu	Le cours propose une introduction à un large éventail de problèmes de sécurité liés aux réseaux informatiques et aux appareils connectés à ces réseaux. Nous verrons les principaux mécanismes d'attaque (déni de service, empoisonnement de cache, XSS, injection de code, etc.), ainsi que les mécanismes de défense tels que le cryptage, les pare-feu et la détection d'intrusion. Cette dernière comprend la détection basée sur les signatures et la détection d'anomalies basée sur l'apprentissage automatique. Dans les exercices, vous apprendrez à réaliser de telles attaques, à les identifier et à sécuriser un système contre elles. Quelques thèmes abordés les années précédentes : · Injection de code (y compris injection SQL et XSS) · Attaques DDoS et réflexion · Surveillance du réseau avec netflow et protection avec les pare-feux · Systèmes de détection d'intrusion · Introduction à la cryptographie et à son utilisation pour sécuriser les communications réseau et DNS
Ressources en ligne	Teams et/ou Moodle
Autres infos	Vous aurez besoin de connaissances de base en matière de protocoles de réseau, de systèmes informatiques et de programmation en C, par exemple dans les cours suivants: · Réseaux: LINFO1341 ou LINFO2147 · Systèmes informatiques et C: LINFO1252 ou LINFO2241
Faculté ou entité en charge:	INFO

Programmes / formations proposant cette unité d'enseignement (UE)

Intitulé du programme	Sigle	Crédits	Prérequis	Acquis d'apprentissage
Master [120] : ingénieur civil électricien	ELEC2M	5		
Master [120] : ingénieur civil en informatique	INFO2M	5		
Master [120] en sciences informatiques	SINF2M	5		
Bachelier en sciences informatiques	SINF1BA	5		
Master [120] : ingénieur civil en mathématiques appliquées	MAP2M	5		
Master [120] : ingénieur civil en science des données	DATE2M	5		
Master [120] en science des données, orientation technologies de l'information	DATI2M	5		