






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
Thèmes abordés	<ul style="list-style-type: none"> • e-mail falsifiés, courriers 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	<p>A la fin de cette unité d'enseignement, l'étudiant est capable de :</p> <p>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 :</p> <ul style="list-style-type: none"> • INFO1.1-3 • INFO2.1-5 • INFO5.2, INFO4-5 • INFO6.1, INFO6.3, INFO6.4 <p>Eu égard au référentiel AA du programme « Master [120] en sciences informatiques », ce cours contribue au développement, à l'acquisition et à l'évaluation des acquis d'apprentissage suivants :</p> <ul style="list-style-type: none"> • SIN1.M1 • SIN2.1-5 • SIN5.2, SIN4-5 • SIN6.1, SIN6.3, SIN6.4 <p>Le cours offre une vision large de la sécurité de systèmes informatiques qui constitue un bon aperçu du domaine pour des non-spécialistes et une bonne introduction pour les futurs spécialistes.</p> <p>Un étudiant qui termine avec succès ce cours seront capables de :</p> <ul style="list-style-type: none"> • défendre le besoin de protection et de sécurité , et le rôle des considérations éthiques dans l'utilisation des ordinateurs , • 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	<p>Mode d'évaluation pour la session de juin :</p> <ul style="list-style-type: none"> • Examen (50% de la note finale) • Activités de projet en groupe (35% de la note finale) • Activité de project individuel (15% de la note finale) <p>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.</p> <p>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.</p>
Méthodes d'enseignement	<ul style="list-style-type: none"> • Cours magistraux • Lecture d'articles scientifique • Travaux pratiques • Activités de projet

<p>Contenu</p>	<p>Le cours propose une introduction à un large éventail de problèmes de sécurité liés aux réseaux informatiques et aux appareils connectés à ces réseaux.</p> <p>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.</p> <p>Quelques thèmes abordés les années précédentes :</p> <ul style="list-style-type: none"> • 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
<p>Ressources en ligne</p>	<p>Teams et/ou Moodle</p>
<p>Autres infos</p>	<p>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:</p> <ul style="list-style-type: none"> • Réseaux: LINFO1341 ou LELEC2920 • Systèmes informatiques et C: LINFO1252 ou LINFO2241
<p>Faculté ou entité en charge:</p>	<p>INFO</p>

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		
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		