HEH be Sciences et technologies

8a avenue Maistriau
7000 Mons

www.heh.be

Intitulé de l'UE	Malware analysis
Section(s)	- **(2 ECTS)** Master en sciences de l'Ingénieur industriel / Finalité Informatique / Cycle 2 Bloc 2 option Réseaux et Sécurité

Responsable(s)	Heures	Période
Jean-Sébastien LERAT	30	**Quad 1**

Activités d'apprentissage	Heures	Enseignant(s)
Analysis techniques	15h	**Jean-Sébastien LERAT**
Reverse engineering	15h	**Jean-Sébastien LERAT**

Prérequis	Corequis
- Systèmes d'exploitation	

Répartition des heures
Analysis techniques : 10h de théorie, 5h d'exercices/laboratoires
Reverse engineering : 5h de théorie, 10h d'exercices/laboratoires

Langue d'enseignement
Analysis techniques : Français, Anglais
Reverse engineering : Français, Anglais

Connaissances et compétences préalables
Maîtrise des notions abordées à l'AA d'introduction à la sécurité informatique ainsi que de ses prérequis.

Objectifs par rapport au référentiel de compétences ARES

Cette UE contribue au développement des compétences suivantes

- Master en Sciences de l'ingénieur industriel :

- Identifier, conceptualiser et résoudre des problèmes complexes
  - Intégrer les savoirs scientifiques et technologiques afin de faire face à la diversité et à la complexité des problèmes rencontrés
  - Analyser des produits, processus et performances, de systèmes techniques nouveaux et innovants
  - Concevoir, développer et améliorer des produits, processus et systèmes techniques
  - Sélectionner et exploiter les logiciels et outils conceptuels les plus appropriés pour résoudre une tâche spécifique
  - Établir ou concevoir un protocole de tests, de contrôles et de mesures.
- Concevoir et gérer des projets de recherche appliquée
  - Réaliser des simulations, modéliser des phénomènes afin d'approfondir les études et la recherche sur des sujets technologiques ou scientifiques

- Mener des études expérimentales, en évaluer les résultats et en tirer des conclusions
- Valider les performances et certifier les résultats en fonction des objectifs attendus
- Exploiter les résultats de recherche

- Master en Sciences de l'ingénieur industriel en Informatique :

- Analyser, concevoir, implémenter et maintenir des systèmes informatiques logiciels et matériels
  - Maîtriser et mettre en oeuvre les techniques de sécurité logicielle et matérielle (cryptologie, architectures d'authentifications, …)

Acquis d'apprentissage spécifiques

- Enumérer, expliquer et illustrer les différents types de maliciels vus au cours
- Enumérer, expliquer et illustrer les différents types d'analyse de maliciels vus au cours
- Identifier les constructions de codes assembleurs C et C++
- Citer les composants principaux de l'API Windows et de ses concepts associés
- Expliquer et illustrer le comportement des malwares et leurs shellcodes
- Expliquer et illustrer les concepts propres aux fonctionnement de Windows
- Expliquer et illustrer l'architecture des fichiers PE
- Expliquer et illustrer l'architecture x86, x64 et ARM
- Expliquer et illustrer les notions de polymorphisme, métamorphisme, cracking, patching and keygenning et les packers
- Expliquer et illustrer les notions d'anti-désassembleur, d'anti-débugueur et d'anti-virtualisation
- Expliquer et illustrer les notions d'encodage et de signatures réseaux
- Mettre en oeuvre les notions de cracking, patching et keygenning sur des exemples simples
- Utiliser les outils IDA Pro, OllyDBG, WinDBG

Contenu de l'AA Analysis techniques

- Basic malware analysis : static analysis, virtual machine, dynamic analysis (sandbox, process, network)
- IDA Pro, OllyDBG, WinDBG, Ghidra, Volatility
- C and C++ code constructs
- Windows malware (API, registry and traces)
- Advanced malware analysis
- Malware behavior and launching
- Encoding and network signatures
- Malware shellcodes
- Packers
- Anti-disassembly, Anti-debugging and Anti-virtualization
- Rootkits & Bootkits
- Mobile malware

Contenu de l'AA Reverse engineering

- Windows fundamentals (architecture, memory, object and handles), process and threads
- Tools
- Complexity : polymorphism, metamorphism
- Cracking, patching and keygenning
- Architecture : x86, x64 and ARM
- PE file format, packing, obfuscation, linked import
- Debugging

Méthodes d'enseignement

Analysis techniques : cours magistral, travaux de groupes, approche par projets, approche interactive, étude de cas, utilisation de logiciels

Reverse engineering : cours magistral, travaux de groupes, approche par projets, approche interactive, étude de cas, utilisation de logiciels

Supports

Analysis techniques : copies des présentations

Reverse engineering : copies des présentations

Ressources bibliographiques de l'AA Analysis techniques
Sikorski, M., & Honig, A. (2012). Practical malware analysis: The hands-on guide to dissecting malicious software. No Starch Press.

Ressources bibliographiques de l'AA Reverse engineering
Dang, B. (2014). Practical reverse engineering: x86, x64, arm, windows kernel, reversing tools, and obfuscation. Wiley. Eilam, E. (2005). Reversing: Secrets of reverse engineering. Wiley.

Évaluations et pondérations	
Évaluation	Note globale à l'UE
Langue(s) d'évaluation	Français, Anglais
Méthode d'évaluation	20% de travaux et d'évaluation continue, 80% examen oral où l'étudiant est confronté à une mise en situation de malware. L'étudiant doit expliquer sa méthodologie d'analyse en justifiant ses choix à l'aide des concepts théoriques abordés au cours. En cas d'examen à distance, une partie préliminaire pratique peut être demandée à l'étudiant afin de personnaliser l'examen. Ceci comprend notamment la réalisation d'un projet. Les supports de cours sont anglais mais le cours est enseigné en Français
Report de note d'une année à l'autre pour l'AA réussie en cas d'échec à l'UE	
Analysis techniques : **non** Reverse engineering : **non**	

Année académique : **2020 - 2021**