Ethical Hacking and Computer Forensics [HAC]

MRU

TIC / HEIG-VD

Responsable

Junod Pascal

Domaine de spécialisation

Technologies de l'information et de la communication

Capacité d'accueil

30

Objectifs détaillés

A la fin de ce cours, l'étudiant-e est capable de :

- d'expliquer les principes éthiques inhérents à la découverte de vulnérabilités
- d'appliquer des techniques de reconnaissance de topologie de réseaux
- d'utiliser un scanner de vulnérabilités et d'en interpréter les résultats
- d'expliquer les principes de craquage de mots de passe et leurs limites
- d'expliquer les principes de découverte de vulnérabilités software
- d'expliquer en détail les concepts de "backdoor" et de "rootkit"
- de décrire et d'expliquer les limites des outils de surveillance communs
- d'expliquer les principes économiques de la cybercriminalité
- d'expliquer la méthodologie précise d'une analyse forensique
- et d'utiliser des outils forensiques de base

Connaissances préalables

- Notions de base en sécurité informatique (menaces, mécanismes de défenses, etc.) qui peuvent être acquises par exemple avec le module central "Sécurité Informatique".
- Notions de programmation
- Réseaux TCP/IP

Contenu

Sujet	Temps [%]
1) Reconnaissance : Principes éthiques et légaux - Découverte de la topologie de réseaux filaires/sans-fil - Scanners de vulnérabilités (Windows/UNIX) - Principes d'ingénierie sociale - Travail pratique : reconnaissance d'un réseau	15
2) Pénétration de réseaux et d'applications : Craquage de mots de passe (Windows/UNIX) - Craquage de réseaux sans-fil (WEP, WPA/WPA2) - Concept de shellcode et leur conception - Outils (Metasploit, ...) - Techniques de fuzzing - Techniques de Reverse-engineering (OllyDbg)	20
3) Contrôle d'un système : Backdoors : Rootkits (Windows/UNIX)	10
4) Surveillance : Outils de capture et analyse réseaux - Pots de miel - Systèmes de Détection d'Intrusions (IDS) - Intégrité des fichiers (Tripwire,...)	15
5) Bases de Cyber-Forensique : Économie dans la cybercriminalité - Renseignement criminel (processus, types) - Processus dans l'informatique forensique - Préparation (formation, outils, environnements)	10
6) Collecte des données : Démarches : à chaud (live) ou à froid (dead), préservation des preuves (imaging), rapport de garde - Traces numériques dans les équipements réseaux - Traces dans les systèmes d'exploitation, les fichiers et applications - Autres équipements : PDAs, téléphones mobiles, appareils de photo, etc. - Portes dérobées troyennes utilisées dans la collecte de données	10
7) Analyse des données : Diagramme de décision typique - Outils (TCT, FTK, EnCase, Sleuth Kit, ...) - Fiabilité des informations analysées - Travail pratique : analyse d'un malware, de son activité sur un système compromis et récupération de données	20

Méthodes d'enseignement

Mode	Périodes d'enseignement	Volume de travail (en heures)
Exposés	28	60
Exercices	7	15
Travaux pratiques	7	15
TOTAL	42	90
Crédits ECTS		3

Évaluation

Examen écrit

Ethical Hacking and Computer Forensics [HAC]

Compétences visées

	Ingénierie logicielle	Réseaux d'entreprises et sécurité IT	Systèmes d'information et multimédia	Systèmes embarqués et mobiles
Gérer le projet				
Sait choisir et appliquer la méthode adéquate de gestion de projet, pour des projets de complexité moyenne				
Sait identifier les contraintes économiques et les formuler (business plan)				
Sait exploiter les ressources internes et identifier les ressources externes permettant de mettre en oeuvre une solution				
Est capable de s'intégrer dans un groupe; est en mesure d'animer, motiver et convaincre les membres du groupe				
A le sens de l'initiative personnelle et des responsabilités				
Analyser et spécifier des produits / services				
Est capable d'analyser les besoins du client dans le domaine de spécialisation et sait traduire les exigences et contraintes dans le contexte technico-scientifico-économique et environnemental adéquat	X	X	X	X
Est capable de spécifier, planifier, concevoir et mettre en oeuvre des architectures de systèmes spécifiques au domaine de spécialisation, en intégrant des composants hétérogènes et en respectant les exigences d'interopérabilité et d'évolutivité des systèmes, ainsi que les normes et standards				
Est capable de mener des études de faisabilité et de proposer des services de conseil				
Est capable de superviser et analyser (monitoring) la sécurité d'un système IT et développer des tableaux de bord renseignant sur l'état du système				
Est capable d'effectuer une analyse du risque IT et sait choisir la méthode adéquate et, le cas échéant, l'adapter ou en développer une nouvelle				
Est capable de spécifier, dans un cahier des charges, les besoins du client, après les avoir traduits dans le contexte technico-économique adéquat				
Est en mesure de proposer et comparer des solutions et peut justifier un choix avec des arguments techniques, économiques, organisationnels ou environnementaux appropriés				
Est capable de se mettre à la place de l'utilisateur pour conce-voir un produit répondant à ses attentes				
Développer et réaliser				
Sait choisir et mettre en oeuvre efficacement un outil de modé-lisation dans son domaine de spécialisation	X	X	X	X
Est capable de choisir et mettre en oeuvre efficacement une approche d'aide à la décision pour résoudre des problèmes complexes et, le cas échéant, de l'adapter ou en développer une nouvelle				
Est capable de choisir et mettre en oeuvre efficacement une méthode d'optimisation et, le cas échéant, de l'adapter ou en développer une nouvelle				
Est capable de choisir et mettre en oeuvre efficacement une méthode de gestion et de configuration de réseaux et de services				
A appris à comparer entre elles diverses méthodes de recherche et de traitement de l'information multimédia et est capable d'en développer de nouvelles				
A appris à comparer entre elles diverses méthodes de développement logiciel, de gestion de versions, de gestion de problèmes, de automatisée de logiciel et est capable de les appliquer, les adapter ou d'en développer de nouvelles				
Sait appliquer les bonnes pratiques et modèles de conception (design patterns) pour des systèmes logiciels				
Sait utiliser à bon escient les concepts et techniques d'ingénierie et de stockage de l'information				
Est capable d'évaluer et choisir des systèmes de transport (SAN, WAN, ?) et serveurs de stockage de l'information multimédia				
Est capable de proposer des approches innovantes pour la réalisation d'interfaces d'utilisateur adaptatives et adaptables en fonction des besoins et des profils des utilisateurs, en adoptant une approche ergonomique				
Est capable de proposer des approches innovantes pour la réalisation d'interfaces adaptatives en fonction du contexte (p. ex. drivers, type de réseau)				
Maîtrise les technologies de simulation graphiques tri-dimensionnelles et réalité virtuelle, p. ex. les GIS (Geographic Information Systems)				
Sait évaluer et choisir une méthode de traitement de l'information multimédia appropriée				
Connaît les principes de l'informatique pervasive (ubiquitous computing) et sait les appliquer pour concevoir des solutions d'interaction homme-machine efficaces				
Connaît les techniques de parallélisation logicielles et matérielles et de distribution des processus et des données				
Sait comparer les méthodes de co-design et est en mesure de choisir la méthode appropriée				
Est capable de mettre en oeuvre un outil de simulation de système complexe et d'optimiser son architecture, sa performance (p. ex. qualité de service)				
Est capable de concevoir, vérifier, réaliser et valider un système numérique				
Sait appliquer les techniques de poly-publishing et de cross-média				
Est capable de développer, porter, adapter des composants logiciels de bas niveau (bootstrap, moniteur, driver, os, etc.) sur différentes architectures, en maîtrisant les aspects liés aux interactions logiciel-matériel				
Est capable de développer de nouvelles applications en respectant les contraintes propres aux environnements mobiles (os, transmission, consommation, interfaces, etc.)				
Est capable de modéliser un système physique en vue d'une implémentation informatique				
Sait appliquer des méthodologies de travail appropriées et organiser son temps	X	X	X	X
A été sensibilisé aux règles d'éthique et du développement durable	X	X	X	X
Valider, améliorer et disséminer				
Sait choisir et mettre en oeuvre efficacement un outil de test et de validation				
A appris à auditer un système d'information et est capable de proposer des mesures appropriées pour son amélioration				
A appris à auditer la sécurité d'un système IT et est capable de proposer des mesures appropriées pour son amélioration	X	X	X	X
A appris à auditer l'architecture d'un système de commu-nication et est capable de proposer des mesures appropriées pour son amélioration	X	X	X	X
A appris à auditer une architecture logicielle et le code y relatif et est capable de proposer des mesures appropriées pour son amélioration	X	X	X	X
Est capable de choisir et mettre en oeuvre efficacement une approche d'ontologie informationnelle et de gestion de connaissances et, le cas échéant, de l'adapter ou en développer une nouvelle				
Est capable de concevoir et réaliser une plate-forme d'essai permettant de valider des architectures de systèmes ainsi que des composants matériels ou logiciels et d'optimiser leur fonctionnement				
Est en mesure d'assurer la veille technologique dans son domaine et d'intégrer les connaissances nouvelles	X	X	X	X
Sait rédiger, présenter, communiquer et convaincre de manière pertinente				
Est intégré dans des réseaux profession-nels lui facilitant les échanges d'information, les expériences et la veille technologique				
Est en mesure d'acquérir de façon autonome des connaissances et compétences nouvelles	X	X	X	X