INFRES_5_5 Architecture et Sécurité du Système d'information	INFRES	S5

Pourquoi cette UE ?

En maîtrisant les techniques d'attaque et de défense, ainsi que les outils de virtualisation, les étudiants seront en mesure de concevoir des systèmes d'information robustes et de répondre aux défis croissants de la sécurité informatique.

Eléménts constitutifs de l'UE

	coefficient
INFRES_5_5-1 Ethical hacking	1
INFRES_5_5-2 Virtualisation et conteneurisation : fondamentaux	1

Volume d'heures d'enseignement encadré	Volume d'heures de travail personnel	Nombre d'ECTS
54	0	3

Alignement curriculaire

Parmi les compétences visées par la formation, lesquelles sont développées dans cette UE ?

INFRES_5_5 Architecture et Sécurité du Système d'information	INFRES
INFRES_5_5-1 Ethical hacking	**S5**

Contexte et enjeux de l'enseignement

Des enjeux économiques et financiers très importants imposent à l'entreprise la valorisation et la protection permanentes de toutes les composantes de son patrimoine immatériel. Ce cours présente les différentes failles et techniques d'attaque du SI. Ainsi, l'apprenti aura les outils lui permettant de vérifier le niveau de sécurité de son SI, et de le protéger plus efficacement.

Prise en compte des dimensions socio-environnementales

Prérequis

Connaissances élémentaires en informatique et en réseaux/télécoms.

Modalités d'enseignement et d'évaluation

	Nb d'heures
Cours	10
Cours intégré (cours + TD)	
TD	
TP	12
Projets	
Travail en autonomie encadré	
Contrôles et soutenances	2
Travail personnel	

Objectifs pédagogiques

(à la fin de cet enseignement, l'étudiant sera capable de ...)

Avoir connaissance des différentes techniques d'attaque d'un SI.
Identifier les facteurs de vulnérabilité d'un SI.
Mettre en œuvre des mesures de sécurité.

Activités

(CM, TD, TP, projet, sortie terrain, etc.)

Cours illustré par de nombreux TP.

Évaluations et retours faits aux élèves

(évaluations qui comptent pour la note ou qui permettent à l'étudiant de se situer, corrigés, feedback personnalisé...)

TP et contrôle QCM.

INFRES_5_5 Architecture et Sécurité du Système d'information	INFRES
INFRES_5_5-1 Ethical hacking	**S5**

Plan de cours

• Le Hacking et la sécurité
◦ Formes d'attaques, modes opératoires, acteurs, enjeux.
◦ Audits et tests d'intrusion, place dans un SMSI.
• Sniffing, interception, analyse, injection réseau
◦ Anatomie d'un paquet, tcpdump, Wireshark, tshark.
◦ Détournement et interception de communications (Man-in-the-Middle,
◦ attaques de VLAN, les pots de miel).
◦ Paquets : Sniffing, lecture/analyse à partir d'un pcap, extraction des donnés
◦ utiles, représentations graphiques.
◦ Scapy : architecture, capacités, utilisation.
◦ Travaux pratiques (Ecouter le réseau avec des sniffers. Utiliser scapy (ligne de commande, script python) : injections, interception, lecture de pcap, scan, DoS, MitM).
• La reconnaissance, le scanning et l'énumération
◦ L'intelligence gathering, le hot reading, l'exploitation du darknet, l'Ingénierie Sociale.
◦ Reconnaissance de service, de système, de topologie et d'architectures.
◦ Types de scans, détection du filtrage, firewalking, fuzzing.
◦ Le camouflage par usurpation et par rebond, l'identification de chemins avec traceroute, le source routing.
◦ L'évasion d'IDS et d'IPS : fragmentations, covert channels. Nmap : scan et d'exportation des résultats, les options.
◦ Les autres scanners : Nessus, OpenVAS.
◦ Travaux pratiques (Utilisation de l'outil nmap, écriture d'un script NSE en LUA. Détection du filtrage)
• Les attaques Web
◦ OWASP : organisation, chapitres, Top10, manuels, outils.
◦ Découverte de l'infrastructure et des technologies associées, forces et
◦ faiblesses.
◦ Côté client : clickjacking, CSRF, vol de cookies, XSS, composants (flash, java). Nouveaux vecteurs.
◦ Côté serveur : authentification, vol de sessions, injections (SQL, LDAP, fichiers, commandes).
◦ Inclusion de fichiers locaux et distants, attaques et vecteurs cryptographiques.
◦ Évasion

Ressources et références

Les supports pédagogiques sont disponibles en ligne sous Campus

INFRES_5_5 Architecture et Sécurité du Système d'information	INFRES
INFRES_5_5-2 Virtualisation et conteneurisation : fondamentaux	**S5**

Contexte et enjeux de l'enseignement

Ce cours présente les concepts de conteneurisation et de virtualisation. Ces notions sont fondamentales dans l'informatique moderne, notamment dans le contexte des microservices et du cloud.

Prise en compte des dimensions socio-environnementales

Prérequis

Aucun

Modalités d'enseignement et d'évaluation

	Nb d'heures
Cours	30
Cours intégré (cours + TD)	
TD	
TP	
Projets	
Travail en autonomie encadré	
Contrôles et soutenances	
Travail personnel	

Objectifs pédagogiques

(à la fin de cet enseignement, l'étudiant sera capable de ...)

Ce cours permet aux étudiants de créer et manipuler des conteneurs à l'aide de l'outil Docker, la solution la plus conviviale et la plus populaire en matière de conteneurisation.

Activités

(CM, TD, TP, projet, sortie terrain, etc.)

- TD : 8 séances de 3h30
- Installation d'une VM Linux + Docker
- Exposé théorique des notions
- Nombreux ateliers pratiques pour l'assimilation par la pratique
- Exercices pour chacune des notions

Évaluations et retours faits aux élèves

(évaluations qui comptent pour la note ou qui permettent à l'étudiant de se situer, corrigés, feedback personnalisé...)

Examen 2h (20 questions)

INFRES_5_5 Architecture et Sécurité du Système d'information	INFRES
INFRES_5_5-2 Virtualisation et conteneurisation : fondamentaux	**S5**

Plan de cours

Présentation de Docker & Installation sous Rocky Linux 8
Les commandes de base
Gérer les images des conteneurs
Exécuter un conteneur
Exposer un conteneur
Se connecter à un conteneur
Gérer les logs de Docker
Utiliser les registres
Construire une image
Gérer les volumes
Conteneurs et réseaux
Combiner les conteneurs
Docker Compose

Ressources et références

https://blog.microlinux.fr/formation-docker/