INFRES_7_2_SR Architecture et Sécurité du Système d'information	INFRES	S7

Pourquoi cette UE ?

Ce module permet à l'élève de maîtriser les bases de la cryptographie et la gestion des certificats, essentielles à la sécurisation des communications et des infrastructures. Il met un accent particulier sur la mise en œuvre de ces mécanismes dans un environnement cloud privé basé sur OpenStack. L'élève apprend à déployer, configurer et sécuriser une plateforme OpenStack, compétence stratégique pour la gestion d'infrastructures virtualisées, souveraines et évolutives, en réponse aux besoins actuels des organisations.

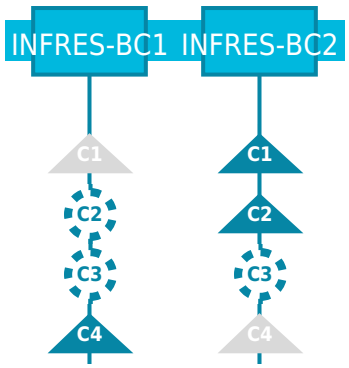
Eléménts constitutifs de l'UE

	coefficient
INFRES_7_2_SR-1 Sécurité des réseaux et systèmes	1
INFRES_7_2_SR-2 Infrastructure: open stack	2

Volume d'heures d'enseignement encadré	Volume d'heures de travail personnel	Nombre d'ECTS
57	20	4

Alignement curriculaire

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



INFRES_7_2_SR Architecture et Sécurité du Système d'information	INFRES

INFRES_7_2_SR-1 Sécurité des réseaux et systèmes

S7

Contexte et enjeux de l'enseignement

Ce cours répond à la nécessité de protéger des infrastructures numériques de plus en plus complexes et interconnectées. Les réseaux constituent la colonne vertébrale des échanges d'information, tandis que les systèmes hébergent données et applications critiques : leur compromission peut avoir des conséquences majeures. Les enjeux sont de sensibiliser aux principales menaces (attaques réseau, malwares, intrusions), de présenter les mécanismes de défense (chiffrement, pare-feu, contrôle d'accès, surveillance), et d'initier aux bonnes pratiques d'administration sécurisée. L'objectif est d'apprendre aux élèves à raisonner en termes de résilience et de défense en profondeur, en intégrant à la fois la dimension technique et organisationnelle. Ce cours fournit ainsi des bases solides pour anticiper, détecter et contrer les attaques, tout en garantissant la disponibilité et l'intégrité des services numériques.

Prise en compte des dimensions socio-environnementales

Prérequis

- Protocoles réseaux - Administration Unix

Modalités d'enseignement et d'évaluation

	Nb d'heures
Cours	
Cours intégré (cours + TD)	31
TD	
TP	
Projets	
Travail en autonomie encadré	
Contrôles et soutenances	2
Travail personnel	10

Objectifs pédagogiques

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

- Estimer le niveau de sécurité d'un réseau,
- Minimiser les risques sans nuire aux autres services réseaux,
- Déployer une politique de sécurité pour un réseau.

Activités

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

Cours et TP (GNS3)

Évaluations et retours faits aux élèves

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

QCM
TP

INFRES_7_2_SR Architecture et Sécurité du Système d'information	INFRES
INFRES_7_2_SR-1 Sécurité des réseaux et systèmes	**S7**

Plan de cours

- Iptables : Firewalling sous Linux
  - Bref historique des technologie de filtrage
  - Présentation de la solution Netfilter/IPtables
  - Mise en place d'un firewall stateless
  - Mise en place d'un firewall statefull
- Mitm (l'homme du milieu) : Détournement de trafic réseau
  - Découverte du fonctionnement de la technique
  - Présentation du cas ARP-Poisonning
  - Mise en place d'un détournement de traffic par ARP-Poisonning

Ressources et références

Les supports pédagogiques sont disponibles en ligne sous Campus.

INFRES_7_2_SR Architecture et Sécurité du Système d'information	INFRES
INFRES_7_2_SR-2 Infrastructure: open stack	**S7**

Contexte et enjeux de l'enseignement

Le développement rapide des services numériques exige des infrastructures cloud flexibles, scalables et maîtrisées. OpenStack, solution open source de cloud computing, permet de déployer des environnements IaaS (Infrastructure as a Service) comparables à ceux des grands fournisseurs commerciaux, tout en gardant le contrôle sur les données et l'architecture. Son adoption croissante dans les secteurs publics, industriels et scientifiques répond à un besoin d'autonomie technologique, d'optimisation des ressources matérielles, et de standardisation des déploiements. Cet enseignement prépare les élèves ingénieurs à concevoir, administrer et sécuriser des infrastructures cloud complexes basées sur OpenStack, en lien avec les enjeux actuels de souveraineté numérique, d'automatisation des systèmes et d'intégration DevOps.

Prise en compte des dimensions socio-environnementales

Prérequis

Administration Linux Virtualisation

Modalités d'enseignement et d'évaluation

	Nb d'heures
Cours	
Cours intégré (cours + TD)	24
TD	
TP	
Projets	
Travail en autonomie encadré	
Contrôles et soutenances	
Travail personnel	10

Objectifs pédagogiques

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

- Expliquer l'architecture et les composants d'OpenStack.
- Déployer une infrastructure OpenStack sur un cluster.
- Gérer les services IaaS (réseaux, instances, volumes).
- Intégrer OpenStack dans un environnement DevOps.
- Diagnostiquer et sécuriser une infrastructure cloud OpenStack.

Activités

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

Cours
TP de mise en place d'une architecture Open Stack sur machine virtuelle

Évaluations et retours faits aux élèves

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

QCM
TP évalué

INFRES_7_2_SR Architecture et Sécurité du Système d'information	INFRES
INFRES_7_2_SR-2 Infrastructure: open stack	**S7**

Plan de cours

ntroduction au cloud computing et à OpenStack
Présentation des paradigmes IaaS, PaaS, SaaS. Architecture modulaire d'OpenStack. Cas d'usage industriels et publics. Comparaison avec les offres cloud propriétaires.

- Installation et configuration de base d'OpenStack
Prise en main des outils de déploiement (DevStack, Packstack, kolla-ansible). Configuration réseau, stockage et compute. Mise en place d'un environnement de test sur machines virtuelles ou cluster réel.
- Administration des services OpenStack
Gestion des projets, utilisateurs et droits. Création et gestion d'instances virtuelles. Configuration des réseaux virtuels (Neutron), des volumes (Cinder), et des images (Glance). Monitoring et journalisation.
- Sécurité, haute disponibilité et performances
Principes de sécurité dans OpenStack. Isolation des tenants, gestion des accès. Approches de redondance, tolérance aux pannes et mise à l'échelle. Optimisation des ressources.
- Automatisation, intégration et supervision
Automatisation des déploiements avec Ansible. Intégration CI/CD dans un environnement OpenStack. Supervision avancée avec Prometheus, Grafana, ou Stacklight. Perspectives d'évolution du cloud souverain.

Ressources et références

Les supports pédagogiques sont disponibles en ligne sous Campus.