Fiche descriptive de module

Sécurité avancée SR205

Orientation(s) / année	**SRS / 2**	Numéro de version : **1.1** Date entrée en vigueur : 01.08.2024 ***Annule et remplace la version précédente***

Contenu du module	***Cours***	***Titre / Contenu***	***Nbre de notes***	***Nbre périodes***
	IDST	IDS et outils de test	2	40
	VPN	VPN	3	60
	FIRE	Firewall et filtrage	3	60
		TOTAL	**8**	**160**

Prérequis	Les prérequis sont fixés par le plan modulaire de la filière de formation.
Formes d'enseignement du module	Enseignements et exercices théoriques, applications pratiques en laboratoire.
Objectifs de compétences spécifiques du module	A l'issue de ce module, l'étudiant·e sera capable de : • Mettre en place des systèmes de filtres réseau (firewall et proxy). • Mettre en place et gérer des solutions VPN. • Utiliser les outils de tests et de détection d'intrusion.
Modalité d'évaluation du module	La note finale du module est constituée par : • des notes de contrôles continus et/ou • des notes d'applications pratiques et/ou • des notes de présentations (orales ou écrites) et • d'une **épreuve de synthèse** <u>L'épreuve de synthèse consiste à :</u> • mettre en service une infrastructure réseau sécurisée pour entreprise avec pare-feu, système de détection d'intrusion et VPN.
Conditions de réussite du module	Toutes les conditions suivantes doivent être remplies, les notes sont calculées au demi-point et les moyennes au dixième de point. • Moins de la moitié des notes doivent être inférieures à 4,0. • La note d'épreuve de synthèse, établie au demi-point, doit être égale ou supérieure à 3,0. • La note finale de module, composée à 60 % par la moyenne des notes et à 40 % par l'épreuve de synthèse, doit être égale ou supérieure à 4,0. *Les cas particuliers sont traités par la direction*
Remarques	-

Fiche descriptive de cours

IDS et outils de test IDST

Formes d'enseignement du cours	Cours théoriques et exercices d'applications
Objectifs de compétences spécifiques du cours	A l'issue de ce cours l'étudiant·e sera capable de : • Classifier les différents outils de sécurité (IDS, PENTEST). • Sélectionner et expérimenter un IDS. • Sélectionner et expérimenter des outils de PENTEST.
Contenus (chapitres) du cours	• Outils de test de pénétration (PENTEST) • Outils de détection d'intrusions (IDS)
Modalités d'évaluation du cours	• Travaux écrits et/ou • Travaux pratiques et/ou • Présentations (écrites et orales)
Modalités d'enseignement présentiel / à distance	Ce cours est donné en présentiel Il comprend éventuellement des lectures, des exercices, des laboratoires, des rapports à faire ou à terminer hors des heures de cours en classe ou à domicile.
Conditions de réussite du cours	Il n'y a pas de validation individuelle de ce cours (moyenne de cours). Les notes d'évaluation de ce cours sont établies au demi-point et utilisées dans la validation du module (moyenne de module).
Remarques	-

Fiche descriptive de cours

VPN

VPN

Formes d'enseignement du cours	Cours théoriques et exercices d'applications
Objectifs de compétences spécifiques du cours	A l'issue de ce cours l'étudiant·e sera capable de : • Identifier les différents composants d'un VPN. • Identifier les différentes architectures VPN. • Choisir l'architecture et les protocoles adaptés selon les besoins. • Proposer, installer et tester un VPN.
Contenus (chapitres) du cours	• Virtual Private Network (VPN) • SSL / TLS
Modalités d'évaluation du cours	• Travaux écrits et/ou • Travaux pratiques et/ou • Présentations (écrites et orales)
Modalités d'enseignement présentiel / à distance	Ce cours est donné en présentiel Il comprend éventuellement des lectures, des exercices, des laboratoires, des rapports à faire ou à terminer hors des heures de cours en classe ou à domicile.
Conditions de réussite du cours	Il n'y a pas de validation individuelle de ce cours (moyenne de cours). Les notes d'évaluation de ce cours sont établies au demi-point et utilisées dans la validation du module (moyenne de module).
Remarques	-

Fiche descriptive de cours

Firewall et filtrage FIRE

Formes d'enseignement du cours	Cours théoriques et exercices d'applications
Objectifs de compétences spécifiques du cours	A l'issue de ce cours l'étudiant·e sera capable de : • Planifier une DMZ. • Installer et tester un firewall réseau. • Installer et tester un proxy / firewall applicatif.
Contenus (chapitres) du cours	• Principe de la DMZ • Mécanismes de translation d'adresses (NAT / PAT) • Les différents types de firewall • Principe et utilisation d'ACL (Access Control List) • Appliance Firewall • Proxy et firewall applicatif
Modalités d'évaluation du cours	• Travaux écrits et/ou • Travaux pratiques et/ou • Présentations (écrites et orales)
Modalités d'enseignement présentiel / à distance	Ce cours est donné en présentiel Il comprend éventuellement des lectures, des exercices, des laboratoires, des rapports à faire ou à terminer hors des heures de cours en classe ou à domicile.
Conditions de réussite du cours	Il n'y a pas de validation individuelle de ce cours (moyenne de cours). Les notes d'évaluation de ce cours sont établies au demi-point et utilisées dans la validation du module (moyenne de module).
Remarques	-