

Fiche descriptive de module

Sécurité

ST220

Orientation(s) / année	STE / 2	Numéro de version: 6.1 Date entrée en vigueur : 01.08.2020 <i>Annule et remplace la version précédente</i>
-------------------------------	----------------	---

Contenu du module	Cours	Titre / Contenu	Nbre périodes
	CRYP ₂₀	Cryptographie	30
	IDST ₂₀	IDS et outils de test	60
	VPNT ₂₀	VPN	60
	FIRE ₂₀	Firewall et filtrage	50
		TOTAL	200

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
Processus PEC associés	01.1-01.2-01.3-01.4-02.1-02.3-03.1-03.2-03.3-03.4-04.1-04.3-04.4-05.1-05.2-05.3-05.4-05.5-05.6-06.1-06.2-06.3-07.1-07.2-08.2-08.3-08.4-08.5-09.1-09.2-09.3-09.4-09.5-10.1-10.2-10.3-11.1-11.2-11.3-11.4-12.1-12.3-12.4-12.5-12.6-12.7-13.1-13.2-13.3-13.4-13.5-13.6-14.1-14.2-14.3-15.1-15.2-15.3
Objectifs de compétences spécifiques du module	<ul style="list-style-type: none"> Mettre en place des systèmes de filtres réseau (firewall et proxy) Comprendre et appliquer les mécanismes de cryptographie Mettre en place et gérer des solutions VPN Utiliser les outils de monitoring et de détection d'intrusion
Modalité d'évaluation du module	<p>La note finale du module est constituée par :</p> <ul style="list-style-type: none"> des notes de contrôles continus et/ou des notes d'applications pratiques et/ou des notes de présentations (orales ou écrites) et d'une note d'épreuve de synthèse <p>L'épreuve de synthèse consiste à :</p> <ul style="list-style-type: none"> mettre en service une infrastructure réseau sécurisée pour entreprise avec pare-feu, système de détection d'intrusion et VPN.
Conditions de réussite du module	<p>Toutes les conditions suivantes doivent être remplies, les notes sont calculées au demi-point et les moyennes au dixième de point.</p> <ul style="list-style-type: none"> 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 du module, composée à 60 % par la moyenne des notes et à 40 % par la note d'épreuve de synthèse, doit être égale ou supérieure à 4,0. <p style="text-align: right;"><i>Les cas particuliers sont traités par la direction</i></p>
Remarques	-

Fiche descriptive de cours

Cryptographie

CRYP₂₀

Nombre de périodes du cours	TOTAL	30
------------------------------------	--------------	-----------

Formes d'enseignement du cours	Enseignements théoriques et applications pratiques en laboratoire
Objectifs de compétences spécifiques du cours	<ul style="list-style-type: none"> • Identifier les différents mécanismes de cryptographie: chiffrement, empreintes (C1) • Appliquer la cryptographie à l'authentification, au chiffrement et au contrôle d'intégrité (C3) • Expérimenter un système PGP (C3)
Contenus (chapitres) du cours	<ul style="list-style-type: none"> • Principes de base de la cryptographie • Calcul et utilisation d'empreintes : authentification et contrôle d'intégrité • Chiffrement symétrique et asymétrique • Certificats • PGP
Modalités d'évaluation du cours	<ul style="list-style-type: none"> • Travaux écrits et/ou • Travaux pratiques et/ou • Présentations (écrites et orales) <hr style="border-top: 1px dotted black;"/> <p>2 travaux notés</p>
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

IDS et outils de test

IDST²⁰

Nombre de périodes du cours	TOTAL	60
------------------------------------	--------------	-----------

Formes d'enseignement du cours	Enseignements théoriques et applications pratiques en laboratoire
Objectifs de compétences spécifiques du cours	<ul style="list-style-type: none"> • Classifier les différents outils de sécurité (Monitoring, IDS, PENTEST) (C2) • Choisir et expérimenter un outil de monitoring (C3) • Choisir et expérimenter un IDS (C3) • Choisir et expérimenter un PENTEST (C3)
Contenus (chapitres) du cours	<ul style="list-style-type: none"> • Outils d'audit et de surveillance • Outils de détection d'intrusions (IDS) • Outils de test de pénétration (PENTEST)
Modalités d'évaluation du cours	<ul style="list-style-type: none"> • Travaux écrits et/ou • Travaux pratiques et/ou • Présentations (écrites et orales) <p>3 travaux notés</p>
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

VPNT₂₀

Nombre de périodes du cours	TOTAL	60
------------------------------------	--------------	-----------

Formes d'enseignement du cours	Enseignements théoriques et applications pratiques en laboratoire	
Objectifs de compétences spécifiques du cours	<ul style="list-style-type: none"> • Identifier les différents composants d'un VPN (C2) • Identifier les différentes architectures VPN (C2) • Choisir l'architecture et les protocoles adaptés selon les besoins (C3) • Proposer, installer et tester un VPN (C4) 	
Contenus (chapitres) du cours	<ul style="list-style-type: none"> • Virtual Private Network (VPN) • SSL / TLS 	
Modalités d'évaluation du cours	<ul style="list-style-type: none"> • Travaux écrits et/ou • Travaux pratiques et/ou • Présentations (écrites et orales) <hr style="border-top: 1px dotted black;"/> <p>3 travaux notés</p>	
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

FIRE₂₀

Nombre de périodes du cours	TOTAL	50
------------------------------------	--------------	-----------

Formes d'enseignement du cours	Enseignements théoriques et applications pratiques en laboratoire	
Objectifs de compétences spécifiques du cours	<ul style="list-style-type: none"> • Planifier une DMZ (C3) • Proposer, installer et tester un firewall réseau (C4) • Proposer, installer et tester un proxy / firewall applicatif (C4) 	
Contenus (chapitres) du cours	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Travaux écrits et/ou • Travaux pratiques et/ou • Présentations (écrites et orales) <hr style="border-top: 1px dotted black;"/> <p>3 travaux notés</p>	
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	-	