

N° action formation :
N° offre catalogue :



› Méthode pédagogique

Alternance de cours collectifs et de travaux pratiques individualisés dans le laboratoire de pen-testing du département R&T

› Effectif

- minimum : 5
- maximum : 8

› Intervenants

Enseignants et professionnels certifiés CEH

› Validation

Diplôme Universitaire qualifiant et certifiant l'acquisition de compétences pour les métiers de la sécurité des systèmes d'information, dans le cadre de la formation professionnelle continue.

› Coût de la formation

Tarif « conventionné employeur » :
6000 €/personne
Tarif « individuel payant » :
4000 €/personne

› Lieux de formation

IUT, Département Réseaux et Télécommunications
40 avenue de Soweto - Terre Sainte Saint-Pierre

› Contact

IUT, Pôle Formation Continue et Alternance
secrétariat :
fc-iut@univ-reunion.fr
responsable pédagogique :
Tahiry RAZAFINDRALAMBO



iut.univ-reunion.fr

IUT de La Réunion Officiel

Mise à jour : 29 novembre 2018

Diplôme Universitaire Cyberattaque Cyberdéfense

› Objectifs de la formation

- Connaître le cadre législatif de la cybersécurité et du hacking éthique
- Comprendre le mécanisme des principales attaques contre un SI
- Mettre en pratique les attaques classiques et récentes contre un SI
- Evaluer les vulnérabilités d'un SI et les risques d'attaque au travers des tests d'intrusion
- Appliquer des contre-mesures et des règles basiques pour défendre le SI

› Public concerné

- Responsable de la sécurité des systèmes d'information (RSSI),
- Référent cybersécurité dans une TPE/PME,
- Délégué aux données personnelles (DPO),
- Formateur, Chef de projet sécurité,
- Administrateur système, réseau et sécurité,
- Consultant Cybersécurité,
- Tout informaticien ayant des connaissances de base en réseau et souhaitant se former à la cybersécurité.

› Pré-requis

Niveau BAC

- Connaître le fonctionnement d'un réseau local (Ethernet, VLANs) et les principaux protocoles d'Internet (IP, TCP, UDP, ICMP)
 - Posséder des bases dans la programmation, l'administration d'un système d'exploitation (Linux, Windows) et la sécurité des systèmes d'information.
- Sélection sur dossier et/ou entretien.

› Programme (140 heures)

Le programme de cette formation contient les enseignements du « Référentiel pédagogique de formation à la cybersécurité des TPE et des PME » élaboré par l'ANSSI (<https://www.ssi.gouv.fr/>)

UE1 : Communication et aspects juridiques de la cybersécurité (35h)

- Communication : intégration professionnelle (rédaction de CV et lettres de motivation), valorisation des compétences
- Cybercriminalité, cybersécurité : notions de base, enjeux et droit commun
- Gestion et organisation de la cybersécurité (entreprise, France, monde)
- Protection de l'innovation
- Cloud computing, infogérance
- Données personnelles : la CNIL, le RGPD, la fonction de DPO
- Audit de sécurité et test d'intrusion, périmètre du hacking éthique
- Rédaction du rapport de test d'intrusion

UE2 : Sécurité des systèmes d'information (35h)

- Réseaux informatiques : modèle OSI, protocoles de l'Internet, présentation de quelques outils (Wireshark, nmap) et de quelques attaques (MAC flooding, ARP spoofing, mots de passe FTP),
- Systèmes d'exploitation (Linux, Windows), scripting, programmation
- Définitions : authenticité, confidentialité, intégrité, disponibilité,



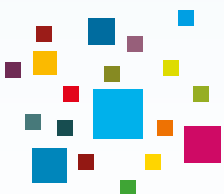
Diplôme Universitaire Cyberattaque Cyberdéfense



SecNumedu
Formation continue

ANSSI

Cette formation a reçu le label
SecNumedu-FC délivré par l'Agence
nationale de la sécurité des
systèmes d'information



- Sécurité des équipements : sécurité physique, durcissement,
- Cryptographie, stéganographie, fonctions de hachage, certificats
- Protocoles sécurisés : HTTPS, SSH...
- Réseaux sans fils,
- Architectures sécurisées : filtrage (pare-feu), IDS/IPS, DMZ

UE3 : Techniques de hacking : l'approche Red Team (42h)

- Méthodologie d'un test d'intrusion
- Collecte d'informations : prise d'empreintes, reconnaissance, scan de réseau, scan de ports, cartographie du réseau, ingénierie sociale, énumération. Contre-mesures.
- Recherche de vulnérabilités : scan de vulnérabilités, réseaux filaires et sans fils, faiblesses dans les protocoles, systèmes d'exploitation, sites web et bases de données (injection SQL), applications. Contre-mesures.
- Exploitation : crackage des mots de passe, élévation des privilèges, buffer overflow, génération de malware et contournement des antivirus, prise en main à distance d'un équipement (backdoor, rootkit), postexploitation et maintien d'accès. Contre-mesures.

UE4 : Projet : challenge de hacking (28h)

- Réalisation d'un test d'intrusion sur le laboratoire de pentesting de l'IUT : mise en application des techniques vues dans l'UE 3, dans une situation analogue à celle d'un véritable réseau d'entreprise
- Restitution des résultats du test d'intrusion : rédaction du rapport
- Recommandations pour améliorer la sécurité du réseau audité

► Calendrier et horaires

Les 140 heures d'enseignement se répartissent sur 17 semaines, à raison de 7 heures par semaine (une journée), sauf la première semaine (21 heures, aspects juridiques) et l'avant dernière (21 heures, projet).

	UE 1	UE2	UE3	UE4
Inscriptions	nous consulter			
Dates *	du 20 février au 5 mars 2019	du 22 mars au 19 avril 2019	du 26 avril au 7 juin 2019	du 12 au 21 juin 2019

* Dates susceptibles de modifications