FORMATION COURTE

DIPLÔME UNIVERSITAIRE

CYBER-ATTAQUE CYBER-DÉFENSE

sous réserve de validation dans les instances et d'effectif atteint

IUT DE LA RÉUNION
Institut Universitaire de Technologie

UR | UNIVERSITÉ DE LA RÉUNION

METHODE PÉDAGOGIQUE

Alternance de cours collectifs et de travaux pratiques individualisés dans le laboratoire de pen-testing du département Réseaux et Télécommunications de l'IUT.

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.

INTERVENANTS

Enseignants et professionnels certifiés CEH, Stormshield, Cisco, ITILv4, ISO 27001

EFFECTIF

minimum : 6

maximum : 12

TARIF

Tarif conventionné employeur : **9000 €** par personne

Tarif individuel payant : **7000 €** par personne

LIEU DE FORMATION

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

CANDIDATURE

en ligne sur :
candidature.univ-reunion.fr
du 19/12/2023 au 15/03/2024

OBJECTIFS DE LA FORMATION

- Connaître le cadre législatif de la cybersécurité et du hacking éthique
- Comprendre et mettre en pratique les principales attaques 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

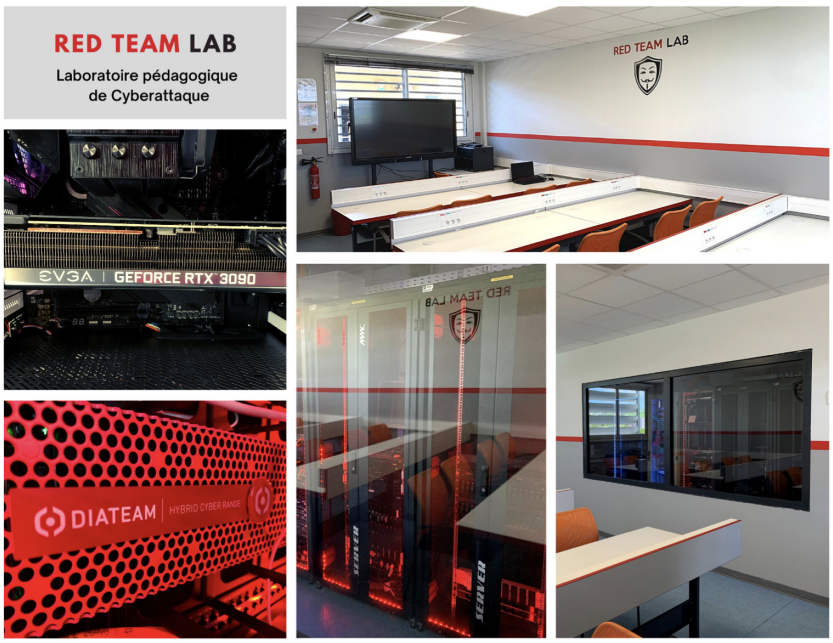
Toute personne intéressée et concernée par la cybersécurité (Responsable de la Sécurité des Systèmes d'Information - RSSI, Administrateur Système / Réseau / Sécurité, Consultant Cybersécurité...)

UNE INFRASTRUCTURE À LA POINTE DES DERNIÈRES TECHNOLOGIES

Profitez d'un environnement technique de haut-niveau pour un apprentissage optimal des techniques d'attaque des hackers. Le RED TEAM LAB c'est :
- Un laboratoire pédagogique de Cybersécurité dédié au pen-testing
- Une plateforme d'entraînement et de simulation Cyber Range - DIATEAM, utilisée par de grands groupes du secteur privé et ministères (www.diateam.net)
- Une cracking box équipée de la carte graphique Nvidia RTX 3090
- Du matériel de terrain : Mouchards réseau, Keylogger, Clé USB verolée, Rogue Access Point...

diateam® military & civil cybersecurity solutions

NVIDIA GEFORCE RTX



CONTACTS

Contact administratif
Pôle formation continue et alternance
fc-iut@univ-reunion.fr

Responsable pédagogique
Tahiry RAZAFINDRALAMBO

Les réseaux sociaux

IUT de la Réunion Officiel

Site internet

iut.univ-reunion.fr

mise à jour : 21 décembre 2023

PROGRAMME DE LA FORMATION (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, infogérence
- 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
- Réponse à incident

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,
- 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 overfow, 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

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 des notions de sécurité des systèmes d'information.

CALENDRIER ET HORAIRES

Les 140 heures d'enseignement se répartissent sur 17 semaines, à raison de 7 heures par semaine (une journée, le vendredi), sauf la dernière semaine 14 heures (2 jours, le jeudi et vendredi)

Candidatures	Date limite fixée au 15 mars 2024
Dates de formation	Du 26 avril au 29 novembre 2024