Executive Mastère

Pentesting et Red Team

MPRT

tech université technologique

tech université technologique

Executive Mastère
Pentesting et Red Team

- Modalité: **en ligne**
- Durée: **12 mois**
- Diplôme: **TECH Université Technologique**
- Temps estimé: **16 heures/semaine**
- Horaire: **à votre rythme**
- Examens: **en ligne**
- Dirigé aux: **Diplômés de l'Université, les Titulaires de Diplômes qui ont précédemment obtenu un diplôme dans le domaine des Sciences Sociales et Juridiques, de l'Administration et des Affaires**

Accès au site web: **www.techtitute.com/fr/ecole-de-commerce/master/master-pentesting-red-team**

Sommaire

01

Présentation

Actuellement, les cyberattaques ont pris une ampleur et une force considérables, inquiétant la population et les entreprises elles-mêmes. En conséquence, les entreprises ont souffert de façon exponentielle de ces menaces et ont dû mettre en place une protection maximale des bases de données et des informations sensibles de leurs clients. C'est pourquoi ce secteur est constamment à la recherche d'experts hautement qualifiés en cybersécurité. TECH a donc conçu ce programme académique, avec des ressources technologiques et d'autres développements autour des tactiques, techniques et procédures utilisées par les acteurs malveillants. Tout cela, grâce à la méthodologie *Relearning* et à une plateforme complète 100 % en ligne, qui offre flexibilité et commodité de temps.

Mastère Spécialisé en Pentesting et Red Team
TECH Université Technologique

Grâce à ce programme 100% en ligne, vous vous spécialiserez dans la promotion de pratiques éthiques et légales dans l'exécution d'attaques et de tests sur les systèmes Windows"

02

Pourquoi étudier à TECH?

TECH est la plus grande école de commerce 100% en ligne au monde. Il s'agit d'une École de Commerce d'élite, avec un modèle de normes académiques des plus élevées. Un centre international performant pour la formation intensive aux techniques de gestion.

TECH est une université à la pointe de la technologie, qui met toutes ses ressources à la disposition de l'étudiant pour l'aider à réussir dans son entreprise"

À TECH Université Technologique

Innovation

L'université propose un modèle d'apprentissage en ligne qui associe les dernières technologies éducatives à la plus grande rigueur pédagogique. Une méthode unique, bénéficiant de la plus haute reconnaissance internationale, qui fournira aux étudiants les clés pour évoluer dans un monde en constante évolution, où l'innovation doit être l'engagement essentiel de tout entrepreneur.

« Histoire de Succès Microsoft Europe » pour avoir incorporé un système multi-vidéo interactif innovant dans les programmes.

Exigence maximale

Le critère d'admission de TECH n'est pas économique. Vous n'avez pas besoin de faire un gros investissement pour étudier avec nous. Cependant, pour obtenir un diplôme de TECH, les limites de l'intelligence et des capacités de l'étudiant seront testées. Les normes académiques de cette institution sont très élevées...

95 % | **des étudiants de TECH finalisent leurs études avec succès**

Networking

Chez TECH, des professionnels du monde entier participent, de sorte que les étudiants pourront créer un vaste réseau de contacts qui leur sera utile pour leur avenir.

+100 000 **dirigeants formés chaque année**

+200 **nationalités différentes**

Empowerment

L'étudiant évoluera main dans la main avec les meilleures entreprises et des professionnels de grand prestige et de grande influence. TECH a développé des alliances stratégiques et un précieux réseau de contacts avec les principaux acteurs économiques des 7 continents.

+500 | **accords de collaboration avec les meilleures entreprises**

Talent

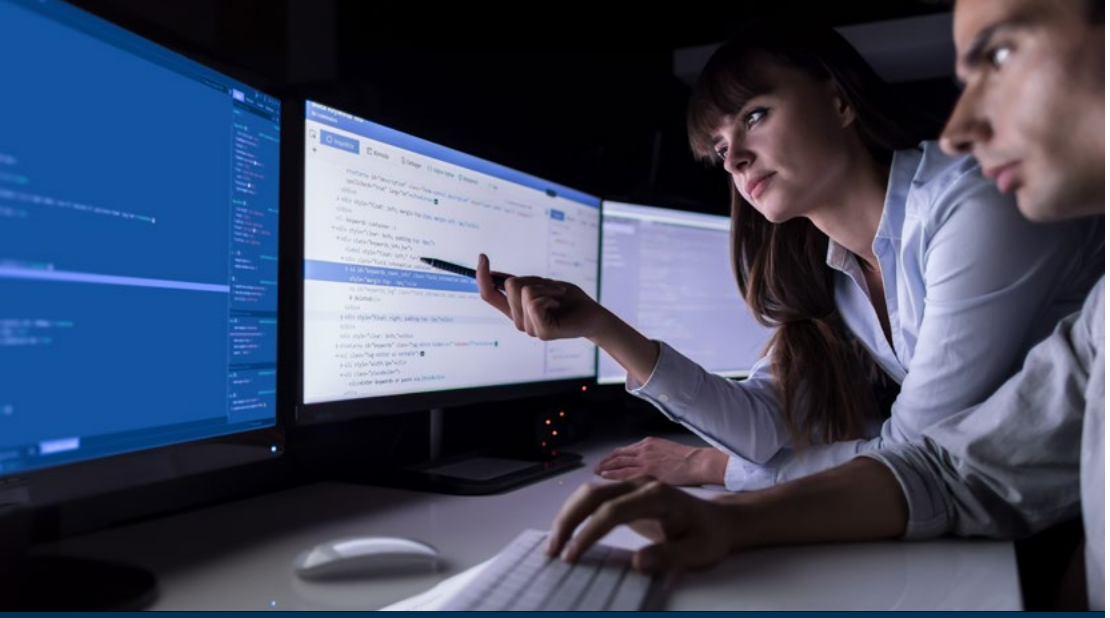
Ce programme est une proposition unique visant à faire ressortir le talent de l'étudiant dans le domaine des affaires. C'est l'occasion de mettre en avant leurs intérêts et leur vision de l'entreprise.

TECH aide les étudiants à montrer leur talent au monde entier à la fin de ce programme.

Contexte Multiculturel

En étudiant à TECH, les étudiants bénéficieront d'une expérience unique. Vous étudierez dans un contexte multiculturel. Dans un programme à vision globale, grâce auquel vous apprendrez à connaître la façon de travailler dans différentes parties du monde, en recueillant les dernières informations qui conviennent le mieux à votre idée d'entreprise.

Les étudiants TECH sont issus de plus de 200 nationalités.



Apprenez avec les meilleurs

L'équipe d'enseignants de TECH explique en classe ce qui les a conduits au succès dans leurs entreprises, en travaillant dans un contexte réel, vivant et dynamique. Des enseignants qui s'engagent pleinement à offrir une spécialisation de qualité permettant aux étudiants de progresser dans leur carrière et de se distinguer dans le monde des affaires.

Des professeurs de 20 nationalités différentes.

Chez TECH, vous aurez accès aux études de cas les plus rigoureuses et les plus récentes du monde académique"

TECH recherche l'excellence et, à cette fin, elle possède une série de caractéristiques qui en font une université unique:

Analyse

TECH explore la pensée critique, le questionnement, la résolution de problèmes et les compétences interpersonnelles des étudiants.

Excellence académique

TECH offre aux étudiants la meilleure méthodologie d'apprentissage en ligne. L'université combine la méthode *Relearning* (la méthode d'apprentissage de troisième cycle la plus reconnue au niveau international) avec l'Étude de Cas. Entre tradition et innovation dans un équilibre subtil et dans le cadre d'un parcours académique des plus exigeants.

Économie d'échelle

TECH est la plus grande université en ligne du monde. Elle possède un portefeuille de plus de 10 000 diplômes de troisième cycle. Et dans la nouvelle économie, **volume + technologie = prix de rupture**. De cette manière, elle garantit que les études ne sont pas aussi coûteuses que dans une autre université.

03

Pourquoi notre programme?

Suivre le programme TECH, c'est multiplier les possibilités de réussite professionnelle dans le domaine de la gestion supérieure des affaires.

C'est un défi qui implique des efforts et du dévouement, mais qui ouvre la porte à un avenir prometteur. Les étudiants apprendront auprès de la meilleure équipe d'enseignants et avec la méthodologie éducative la plus flexible et la plus innovante.

Nous disposons du corps enseignant le plus prestigieux et du programme le plus complet du marché, ce qui nous permet de vous offrir une formation du plus haut niveau académique"

Ce programme apportera une multitude d'avantages aussi bien professionnels que personnels, dont les suivants:

01 Donner un coup de pouce définitif à la carrière des étudiants

En étudiant à TECH, les étudiants seront en mesure de prendre en main leur avenir et de développer tout leur potentiel. À l'issue de ce programme, ils acquerront les compétences nécessaires pour opérer un changement positif dans leur carrière en peu de temps.

70% des participants à cette spécialisation réalisent un changement positif dans leur carrière en moins de 2 ans.

02 Vous acquerrez une vision stratégique et globale de l'entreprise

TECH offre un aperçu approfondi de la gestion générale afin de comprendre comment chaque décision affecte les différents domaines fonctionnels de l'entreprise.

Notre vision globale de l'entreprise améliorera votre vision stratégique.

03 Consolidation des étudiants en gestion supérieure des affaires

Étudier à TECH, c'est ouvrir les portes d'un panorama professionnel de grande importance pour que les étudiants puissent se positionner comme des managers de haut niveau, avec une vision large de l'environnement international.

Vous travaillerez sur plus de 100 cas réels de cadres supérieurs.

04 Vous obtiendrez de nouvelles responsabilités

Au cours du programme, les dernières tendances, évolutions et stratégies sont présentées, afin que les étudiants puissent mener à bien leur travail professionnel dans un environnement en mutation.

À l'issue de cette formation, 45% des étudiants obtiennent une promotion professionnelle au sein de leur entreprise.

05

Accès à un puissant réseau de contacts

TECH met ses étudiants en réseau afin de maximiser les opportunités. Des étudiants ayant les mêmes préoccupations et le même désir d'évoluer. Ainsi, les partenaires, les clients ou les fournisseurs peuvent être partagés.

Vous y trouverez un réseau de contacts essentiel pour votre développement professionnel.

06

Développer des projets d'entreprise de manière rigoureuse

Les étudiants acquerront une vision stratégique approfondie qui les aidera à élaborer leur propre projet, en tenant compte des différents domaines de l'entreprise.

20 % de nos étudiants développent leur propre idée entrepreneuriale.

07

Améliorer les *soft skills* et les compétences de gestion

TECH aide les étudiants à appliquer et à développer les connaissances acquises et à améliorer leurs compétences interpersonnelles pour devenir des leaders qui font la différence.

Améliorez vos compétences en communication ainsi que dans le domaine du leadership pour booster votre carrière professionnelle.

08

Vous ferez partie d'une communauté exclusive

L'étudiant fera partie d'une communauté de managers d'élite, de grandes entreprises, d'institutions renommées et de professeurs qualifiés issus des universités les plus prestigieuses du monde : la communauté de TECH Université Technologique.

Nous vous donnons la possibilité de vous spécialiser auprès d'une équipe de professeurs de renommée internationale.

04

Objectifs

Cette formation universitaire fournira aux étudiants des actualisations innovantes concernant les réglementations et la conformité dans les projets de cybersécurité dans le domaine du *Pentesting*, apportant ainsi une plus grande valeur à leur carrière professionnelle. En ce sens, TECH fournira des ressources didactiques tout au long du développement du programme, en améliorant les compétences liées à la détection des anomalies et des comportements suspects. Ainsi, à la fin de ce programme, e diplômé aura élargi ses connaissances en matière de *Pentesting et Red Team*. Tout cela pendant 12 mois de formation en ligne.

Après ce Mastère Spécialisé, vous serez au fait de l'utilité de la Recherche Forensique Numérique (DFIR) pour résoudre les problèmes de cybercriminalité"

TECH prend en compte les objectifs de ses étudiants
Ils travaillent ensemble pour les atteindre

Le **Executive Mastère en Pentesting et Red Team** formera les étudiants à:

01 Étudier et comprendre les tactiques, les techniques et les procédures utilisées par les acteurs malveillants, ce qui permet d'identifier et de simuler les menaces

02 Appliquer les connaissances théoriques dans des scénarios pratiques et des simulations, en faisant face à des défis réels pour renforcer les compétences de *Pentesting*

03 Apprendre à allouer efficacement les ressources au sein d'une équipe de cybersécurité, en tenant compte des compétences individuelles et en maximisant la productivité des projets

04 Améliorer les compétences de communication spécifiques aux environnements techniques, en facilitant la compréhension et la coordination entre les membres de l'équipe

05 Apprendre les techniques de suivi et de contrôle des projets, en identifiant les écarts et en prenant les mesures correctives nécessaires

06 Développer des compétences pour évaluer et améliorer les configurations de sécurité dans les systèmes Windows, en assurant la mise en œuvre de mesures efficaces

07 Promouvoir des pratiques éthiques et légales dans l'exécution d'attaques et de tests sur les systèmes Windows, en tenant compte des principes éthiques de la cybersécurité

08 Familiariser le diplômé avec l'évaluation de la sécurité des API et des services web, en identifiant les points de vulnérabilité possibles et en renforçant la sécurité des interfaces de programmation

09 Favoriser une collaboration efficace avec les équipes de sécurité, en intégrant les stratégies et les efforts visant à protéger l'infrastructure du réseau

10 Promouvoir des pratiques éthiques et juridiques dans l'analyse et le développement des logiciels malveillants, en garantissant l'intégrité et la responsabilité dans toutes les activités

11 Appliquer les connaissances théoriques dans des environnements simulés, participer à des exercices pratiques pour comprendre et contrer les attaques malveillantes

12 Acquérir une solide compréhension des principes fondamentaux de l'Investigation Numérique (DFIR) et de leur application dans la résolution des cyberincidents

13 Apprendre à produire des rapports détaillés documentant les résultats, les méthodologies utilisées et les recommandations issues des exercices *Red Team* avancés

14 Développer des compétences pour formuler des recommandations pratiques et réalisables visant à atténuer les vulnérabilités et à améliorer le niveau de sécurité

15 Familiariser l'apprenant avec les meilleures pratiques en matière de rapports exécutifs, en adaptant des informations techniques à des publics non techniques

05

Compétences

Cette proposition académique fournira au diplômé un point de vue actuel sur le *Pentesting*. Vous aurez ainsi l'occasion d'accroître vos compétences, d'assumer des rôles de gestion, de faire face à des situations difficiles et changeantes, et même de travailler main dans la main et de manière efficace avec d'autres entreprises du secteur informatique. Ainsi, le professionnel aura à sa disposition de multiples outils, tels que des infographies et des vidéos, qui présenteront une perspective plus pratique de ce domaine d'étude.

Améliorez vos compétences pour une détection et une prévention efficaces des logiciels malveillants, en résolvant les situations les plus difficiles dans le secteur informatique"

01 Acquérir des compétences en matière de *coaching* pour le développement professionnel des membres de l'équipe, en favorisant la croissance et l'amélioration

02 Développer des compétences en matière de prise de décision stratégique dans des situations de cybersécurité, en tenant compte de l'impact à court et à long terme sur la sécurité de l'organisation

03 Acquérir des compétences dans l'identification, l'évaluation et l'atténuation des risques spécifiques des projets de cybersécurité

04 Développer des compétences pour mettre en œuvre des mesures de défense active, en renforçant la sécurité des systèmes et des réseaux

05 Apprendre les techniques d'analyse du trafic web afin d'identifier les modèles et les comportements anormaux, facilitant ainsi la détection d'éventuelles menaces

06 Acquérir des compétences en matière d'analyse criminalistique appliquée aux environnements de réseau, permettant une identification et une réponse efficaces aux cyberincidents

07 Apprendre des stratégies de détection et de prévention efficaces des malware, y compris le déploiement de solutions de sécurité avancées

08 Développer des compétences dans l'identification d'indicateurs de compromission (IoC) au cours d'une enquête médico-légale, afin de faciliter la détection et la réponse aux incidents

09 Acquérir des compétences en matière de planification stratégique des exercices du *Red Team*, en tenant compte des objectifs, de la portée, des ressources et des scénarios réalistes

10 Acquérir des compétences en matière d'identification et de hiérarchisation des vulnérabilités, en mettant en évidence celles qui présentent le plus grand risque pour la sécurité

06

Structure et contenu

Le programme en Pentesting et Red Team est un programme essentiellement axé sur l'acquisition par le diplômé des compétences liées à la criminalistique informatique dans le domaine de la cybersécurité. En tant que telle, cette qualification académique est orientée vers une structure théorique-pratique, accompagnée d'une large expérience et d'un vaste bagage d'une équipe d'experts hautement spécialisés.

Pas d'horaires prédéfinis ni d'évaluations continues: TECH vous garantit l'accès le plus rapide et le plus flexible à son contenu académique"

Programme d'études

Cette qualification universitaire consiste en 1 500 heures d'apprentissage continu à travers un enseignement de haut niveau, grâce auquel le diplômé atteindra les meilleures positions dans le secteur des technologies de l'information et des entreprises. De cette manière, les étudiants surmonteront les différents obstacles imposés par l'environnement de travail. Cette qualification permet d'acquérir de multiples compétences en matière de techniques avancées dans le domaine de Kerberos, d'atténuation et de protection.

D'autre part, l'équipe enseignante a développé un programme exclusif, qui comprend 10 modules, dans le but de permettre à l'étudiant d'acquérir des compétences fondamentales liées à l'évaluation de la sécurité des API et des services web, en identifiant les points de vulnérabilité possibles.

De même, le professionnel approfondira les recommandations pratiques et réalisables visant à atténuer les vulnérabilités et à améliorer la posture de sécurité. En ce sens, ils deviendront d'importants spécialistes dans le domaine de la prévention des conflits et des méthodes de mesure.

Pour ce programme académique, les entrepreneurs seront soutenus par la méthodologie unique *Relearning*, qui leur permettra d'examiner des concepts complexes et d'assimiler leur application quotidienne de manière transparente. En même temps, la formation sera dispensée sur une plateforme d'apprentissage innovante 100% en ligne, qui n'est pas soumise à des horaires fixes ou à des calendriers d'évaluation continue.

Ce Mastère Spécialisé est développé sur 12 mois et est divisé en 10 modules:

Module 1	Sécurité Offensive
Module 2	Gestion des Équipes de Cybersécurité
Module 3	Gestion des Projets de Sécurité
Module 4	Attaques des Réseaux et des Systèmes Windows
Module 5	***Hacking Web*** Avancé
Module 6	Architecture et Sécurité des Réseaux
Module 7	Analyse et Développement de ***Malware***
Module 8	Principes Fondamentaux de la Criminalistique et DFIR
Module 9	Exercices Avancés du ***Red Team***
Module 10	Rapports Techniques et Exécutifs

Où, quand et comment l'enseignement est dispensé?

TECH offre la possibilité d'étudier ce programme de Mastère Spécialisé en Pentesting et Red Team entièrement en ligne. Pendant les 12 mois de la spécialisation, les étudiants pourront accéder à tous les contenus de ce programme à tout moment, ce qui leur permettra d'auto gérer leur temps d'étude.

Une expérience éducative unique, clé et décisive pour stimuler votre développement professionnel.

Module 1. Sécurité Offensive

1.1. Définition et contexte
1.1.1. Concepts fondamentaux de la sécurité offensive
1.1.2. Importance de la cybersécurité aujourd'hui
1.1.3. Défis et opportunités en matière de sécurité offensive

1.2. Bases de la cybersécurité
1.2.1. Les premiers défis et l'évolution des menaces
1.2.2. Les étapes technologiques et leur impact sur la cybersécurité
1.2.3. La cybersécurité à l'ère moderne

1.3. Bases de la sécurité offensive
1.3.1. Concepts clés et terminologie
1.3.2. *Think Outside the Box*
1.3.3. Différences entre hacking offensif et hacking défensif

1.4. Méthodologies de sécurité offensives
1.4.1. PTES (*Penetration Testing Execution Standard*)
1.4.2. OWASP (*Open Web Application Security Project*)
1.4.3. *Cyber Security Kill Chain*

1.5. Rôles et responsabilités en matière de sécurité offensive
1.5.1. Profils principaux
1.5.2. *Bug Bounty Hunters*
1.5.3. *Researching*: L'art de la recherche

1.6. L'arsenal offensif de l'auditeur
1.6.1. Systèmes d'exploitation pour *hacking*
1.6.2. Introduction au C2
1.6.3. *Metasploit*: Principes de base et Utilisation
1.6.4. Ressources utiles

1.7. OSINT: Renseignement de Sources Ouvertes
1.7.1. Les bases de la OSINT
1.7.2. Techniques et outils OSINT
1.7.3. Applications OSINT en matière de sécurité offensive

1.8. *Scripting*: Introduction à l'automatisation
1.8.1. Principes de base de *scripting*
1.8.2. *Scripting* en Bash
1.8.3. *Scripting* en Python

1.9. Catégorisation des vulnérabilités
1.9.1. CVE (*Common Vulnerabilities and Exposure*)
1.9.2. CWE (*Common Weakness Enumeration*)
1.9.3. CAPEC (*Common Attack Pattern Enumeration and Classification*)
1.9.4. CVSS (*Common Vulnerability Scoring System*)
1.9.5. MITRE ATT & CK

1.10. Éthique et *hacking*
1.10.1. Principes de l'éthique du *hacker*
1.10.2. La frontière entre le *hacking* éthique et le *hacking* malveillant
1.10.3. Implications et conséquences juridiques
1.10.4. Étude de cas: Situations éthiques en cybersécurité

Module 2. Gestion des Équipes de Cybersécurité

2.1. Gestion des équipes
2.1.1. Qui est qui
2.1.2. Le manager
2.1.3. Conclusions

2.2. Rôles et responsabilités
2.2.1. Identification des rôles
2.2.2. Délégation effective
2.2.3. Gestion des attentes

2.3. Formation et développement des équipes
2.3.1. Étapes de la formation des équipes
2.3.2. Dynamique de groupe
2.3.3. Évaluation et retour d'information

2.4. Gestion des talents
2.4.1. Identification des talents
2.4.2. Développement des capacités
2.4.3. Fidélisation des talents

2.5. Direction et motivation de l'équipe
2.5.1. Styles de leadership
2.5.2. Théories de la motivation
2.5.3. Reconnaissance des résultats

2.6. Communication et coordination
2.6.1. Outil de communication
2.6.2. Obstacles à la communication
2.6.3. Stratégies de coordination

2.7. Planification stratégique pour le développement du personnel
2.7.1. Identification des besoins de formation
2.7.2. Plans de développement individuel
2.7.3. Suivi et évaluation

2.8. Résolution des conflits
2.8.1. Identification des conflits
2.8.2. Méthodes de mesure
2.8.3. Prévention des conflits

2.9. Gestion de la qualité et amélioration continue
2.9.1. Principes de qualité
2.9.2. Techniques d'amélioration continue
2.9.3. *Feedback* et retour d'information

2.10. Outils et technologies
2.10.1. Plateformes de collaboration
2.10.2. Gestion de projets
2.10.3. Conclusions

Module 3. Gestion des Projets de Sécurité

3.1. Gestion des projets de sécurité
3.1.1. Définition et objectif de la gestion de projet de cybersécurité
3.1.2. Principaux défis
3.1.3. Considérations

3.2. Cycle de vie d'un projet de sécurité
3.2.1. Étapes initiales et définition des objectifs
3.2.2. Mise en œuvre et exécution
3.2.3. Évaluation et révision

3.3. Planification et estimation des ressources
3.3.1. Concepts de base de la gestion économique
3.3.2. Détermination des ressources humaines et techniques
3.3.3. Budgétisation et coûts associés

3.4. Mise en œuvre et contrôle du projet
3.4.1. Contrôle et suivi
3.4.2. Adaptation et modifications du projet
3.4.3. Évaluation à mi-parcours et révisions

3.5. Communication et rapports sur le projet
3.5.1. Stratégies de communication efficaces
3.5.2. Préparation de rapports et de présentations
3.5.3. Communication avec le client et la direction

3.6. Outils et technologies
3.6.1. Outils de planification et d'organisation
3.6.2. Outils de collaboration et de communication
3.6.3. Outils de documentation et de stockage

3.7. Documentation et protocoles
3.7.1. Structuration et création de la documentation
3.7.2. Protocoles d'action
3.7.3. Guide

3.8. Réglementation et conformité dans les projets de cybersécurité
3.8.1. Lois et réglementations internationales
3.8.2. Conformité
3.8.3. Audits

3.9. Gestion des risques dans les projets de sécurité
3.9.1. Identification et analyse des risques
3.9.2. Stratégies d'atténuation
3.9.3. Surveillance et examen des risques

3.10. La clôture des projets
3.10.1. Examen et évaluation
3.10.2. Documentation finale
3.10.3. *Feedback*

Module 4. Attaques des Réseaux et des Systèmes Windows

4.1. Windows et Active Directory
4.1.1. Histoire et évolution de Windows
4.1.2. Principes de base d'Active Directory
4.1.3. Fonctions et services d'Active Directory
4.1.4. Architecture générale d'Active Directory

4.2. Réseaux dans les environnements Active Directory
4.2.1. Protocoles de réseau dans Windows
4.2.2. DNS et son fonctionnement dans Active Directory
4.2.3. Outils de diagnostic réseau
4.2.4. Mise en œuvre du réseau dans Active Directory

4.3. Authentification et autorisation dans Active Directory
4.3.1. Processus et flux d'authentification
4.3.2. Types de certificats
4.3.3. Stockage et gestion des certificats
4.3.4. Sécurité de l'authentification

4.4. Permissions et stratégies dans Active Directory
4.4.1. GPOs
4.4.2. Application et gestion des GPO
4.4.3. Gestion des autorisations dans Active Directory
4.4.4. Vulnérabilités en matière de permissions et mesures d'atténuation

4.5. Principes de base de Kerberos
4.5.1. Qu'est-ce que Kerberos?
4.5.2. Composants et fonctionnement
4.5.3. Tickets dans Kerberos
4.5.4. Kerberos dans le contexte d'Active Directory

4.6. Techniques avancées de Kerberos
4.6.1. Attaques courantes contre Kerberos
4.6.2. Atténuations et protections
4.6.3. Surveillance du trafic Kerberos
4.6.4. Attaques avancées contre Kerberos

4.7. *Active Directory Certificate Services* (ADCS)
4.7.1. Les bases du PKI
4.7.2. Rôles et composants ADCS
4.7.3. Configuration et déploiement de l'ADCS
4.7.4. Sécurité ADCS

4.8. Attaques et défenses des *Active Directory Certificate Services* (ADCS)
4.8.1. Vulnérabilités courantes dans ADCS
4.8.2. Attaques et techniques d'exploitation
4.8.3. Défenses et atténuations
4.8.4. Surveillance et audit des ADCS

4.9. Audit de l'Active Directory
4.9.1. Importance de l'audit de l'Active Directory
4.9.2. Outils d'audit
4.9.3. Détection des anomalies et des comportements suspects
4.9.4. Réponse aux incidents et récupération

4.10. Azure AD
4.10.1. Principes de base d'Azure AD
4.10.2. Synchronisation avec l'Active Directory local
4.10.3. Gestion des identités dans Azure AD
4.10.4. Intégration avec les applications et les services

Module 5. *Hacking* Web Avancé

5.1. Fonctionnement d'un site web
5.1.1. L'URL et ses composantes
5.1.2. Les méthodes HTTP
5.1.3. Les en-têtes
5.1.4. Comment visualiser les requêtes web avec Burp Suite

5.2. Sessions
5.2.1. Les *cookies*
5.2.2. *Tokens* JWT
5.2.3. Attaques par détournement de session
5.2.4. Attaques sur le JWT

5.3. *Cross Site Scripting* (XSS)
5.3.1. Qu'est-ce que le XSS
5.3.2. Types de XSS
5.3.3. Exploiter un XSS
5.3.4. Introduction à *XSLeaks*

5.4. Injections dans les bases de données
5.4.1. Qu'est-ce qu'une SQL *Injection*
5.4.2. Exfiltrer des informations avec SQLi
5.4.3. SQLi Blind, Time-Based et Error-Based
5.4.4. Injections NoSQLi

5.5. *Path Traversal et Local File Inclusion*
5.5.1. Qu'est-ce que c'est et quelles sont leurs différences
5.5.2. Filtres courants et comment les contourner
5.5.3. *Log Poisoning*
5.5.4. LFIs en PHP

5.6. *Broken Authentication*
5.6.1. *User Enumeration*
5.6.2. *Password Bruteforce*
5.6.3. 2FA Bypass
5.6.4. *Cookies* contenant des informations sensibles et modifiables

5.7. *Remote Command Execution*
5.7.1. *Command Injection*
5.7.2. *Blind Command Injection*
5.7.3. *Insecure Deserialization* PHP
5.7.4. *Insecure Deserialization* Java

5.8. *File Uploads*
5.8.1. RCE à travers les *webshells*
5.8.2. XSS dans les téléchargements de fichiers
5.8.3. XML *External Entity* (XXE) *Injection*
5.8.4. *Path traversal* dans les téléchargements de fichiers

5.9. *Broken Acess Control*
5.9.1. Accès illimité au panneau
5.9.2. *Insecure Direct Object References* (IDOR)
5.9.3. *Bypass* des filtres
5.9.4. Méthodes d'autorisation insuffisantes

5.10. Vulnérabilités du DOM et attaques plus avancées
5.10.1. *Regex Denial of Service*
5.10.2. DOM *Clobbering*
5.10.3. *Prototype Pollution*
5.10.4. HTTP *Request Smuggling*

Module 6. Architecture et Sécurité des Réseaux

6.1. Réseaux informatiques
6.1.1. Concepts de base: Protocoles LAN, WAN, CP, CC
6.1.2. Modèle OSI et TCP/IP
6.1.3. *Commutation:* Concepts de base
6.1.4. *Routing*: Concepts de base

6.2. *Switching*
6.2.1. Introduction aux VLAN
6.2.2. STP
6.2.3. *EtherChannel*
6.2.4. Attaques de la couche 2

6.3. VLANs
6.3.1. Importance des VLAN
6.3.2. Vulnérabilités des VLAN
6.3.3. Attaques courantes contre les VLAN
6.3.4. Atténuations

6.4. *Routing*
6.4.1. Adressage IP - IPv4 et IPv6
6.4.2. Routage: Concepts clés
6.4.3. Routage Statique
6.4.4. Routage Dynamique: Introduction

6.5. Protocoles IGP
6.5.1. RIP
6.5.2. OSPF
6.5.3. RIP vs OSPF
6.5.4. Analyse des besoins en matière de topologie

6.6. Protection du périmètre
6.6.1. DMZ
6.6.2. *Firewalls*
6.6.3. Architectures communes
6.6.4. *Zero Trust Network Access*

6.7. IDS et IPS
6.7.1. Caractéristiques
6.7.2. Mise en œuvre
6.7.3. SIEM et SIEM CLOUDS
6.7.4. Détection basée sur les *HoneyPots*

6.8. TLS y VPN
6.8.1. SSL/TLS
6.8.2. TLS: Attaques courantes
6.8.3. VPN avec TLS
6.8.4. VPN avec IPSEC

6.9. Sécurité dans les réseaux sans fil
6.9.1. Introduction aux réseaux sans fil
6.9.2. Protocoles
6.9.3. Éléments clés
6.9.4. Attaques courantes

6.10. Les réseaux d'entreprises et la manière de les gérer
6.10.1. Segmentation logique
6.10.2. Segmentation physique
6.10.3. Contrôle d'accès
6.10.4. Autres mesures à prendre en compte

Module 7. Analyse et Développement de *Malware*

7.1. Analyse et développement de *malware*
7.1.1. Histoire et évolution des *malware*
7.1.2. Classification et types de *malware*
7.1.3. Analyse des *malware*
7.1.4. Développement de *malware*

7.2. Préparation de l'environnement
7.2.1. Configuration de la Machine Virtuelle et *Snapshots*
7.2.2. Outils d'analyse des *malware*
7.2.3. Outils de développement de *malware*

7.3. Principes de base de Windows
7.3.1. Format de fichier PE (*Portable Executable*)
7.3.2. Processus et *Threads*
7.3.3. Système de fichiers et registre
7.3.4. *Windows Defender*

7.4. Techniques de *malware* de base
7.4.1. Génération de *shellcode*
7.4.2. Exécution du *shellcode* sur le disque
7.4.3. Disque vs mémoire
7.4.4. Exécution du *shellcode* en mémoire

7.5. Techniques de malware intermédiaires
7.5.1. Persistance sur Windows
7.5.2. Dossier d'accueil
7.5.3. Clés de registre
7.5.4. Économiseur d'écran

7.6. Techniques des *malwares* avancés
7.6.1. Cryptage du *Shellcode* (XOR)
7.6.2. Cryptage du *shellcode* (RSA)
7.6.3. Obfuscation de *strings*
7.6.4. Injection de processus

7.7. Analyse statique du *malware*
7.7.1. Analyse des *packers* avec DIE (*Detect It Easy*)
7.7.2. Analyse des sections avec PE-Bear
7.7.3. Décompilation avec Ghidra

7.8. Analyse dynamique du *malware*
7.8.1. Observation du comportement avec Process Hacker
7.8.2. Analyse des appels avec API Monitor
7.8.3. Analyser les modifications du registre avec Regshot
7.8.4. Observer les requêtes réseau avec TCPView

7.9. Analyse en .NET
7.9.1. Introduction à .NET
7.9.2. Décompilation avec dnSpy
7.9.3. Débogage avec dnSpy

7.10. Analyser de vrais *malware*
7.10.1. Préparation de l'environnement
7.10.2. Analyse statique du *malware*
7.10.3 Analyse dynamique du *malware*
7.10.4. Création de règles YARA

Module 8. Principes Fondamentaux de la Criminalistique et DFIR

8.1. La criminalistique numérique
8.1.1. Histoire et évolution de la criminalistique informatique
8.1.2. Importance de l'informatique légale dans la cybersécurité
8.1.3. Histoire et évolution de la criminalistique informatique

8.2. Principes fondamentaux de l'Informatique légale
8.2.1. La chaîne de contrôle et son application
8.2.2. Types de preuves numériques
8.2.3. Processus d'acquisition des preuves

8.3. Systèmes de fichiers et structure des données
8.3.1. Principaux systèmes de fichiers
8.3.2. Méthodes de dissimulation des données
8.3.3. Analyse des métadonnées et des attributs des fichiers

8.4. Analyse des Systèmes d'Exploitation
8.4.1. Analyse criminalistique des systèmes Windows
8.4.2. Analyse légale des systèmes Linux
8.4.3. Analyse légale des systèmes macOS

8.5. Récupération de données et analyse de disques
8.5.1. Récupération de données à partir de supports endommagés
8.5.2. Outils d'analyse de disque
8.5.3. Interprétation des tables d'allocation de fichiers

8.6. Analyse du réseau et du trafic
8.6.1. Capture et analyse des paquets réseau
8.6.2. Analyse du journal du *firewall*
8.6.3. Détection des intrusions sur le réseau

8.7. *Malware* et analyse des codes malveillants
8.7.1. Classification des *malwares* et de leurs caractéristiques
8.7.2. Analyse statique et dynamique des *malwares*
8.7.3. Techniques de désassemblage et de débogage

8.8. Analyse des journaux et des événements
8.8.1. Types de journaux dans les systèmes et les applications
8.8.2. Interprétation des événements pertinents
8.8.3. Outils d'analyse des journaux

8.9. Réaction aux incidents de sécurité
8.9.1. Processus de réponse aux incidents
8.9.2. Création d'un plan de réponse aux incidents
8.9.3. Coordination avec les équipes de sécurité

8.10. Présentation des preuves et aspects juridiques
8.10.1. Règles de la preuve numérique dans le domaine juridique
8.10.2. Préparation des rapports médico-légaux
8.10.3. Comparaître au procès en tant que témoin expert

Module 9. Exercices Avancés du *Red Team*

9.1. Techniques avancées de reconnaissance
9.1.1. Énumération avancée des sous-domaines
9.1.2. *Google Dorking* avancé
9.1.3. Les Réseaux Sociaux et theHarvester

9.2. Campagnes de *phishing* avancées
9.2.1. Qu'est-ce que le *Reverse-Proxy Phishing*
9.2.2. *2FA Bypass* avec Evilginx
9.2.3. Exfiltration de données

9.3. Techniques avancées de persistance
9.3.1. *Golden Tickets*
9.3.2. *Silver Tickets*
9.3.3. Technique *DCShadow*

9.4. Techniques d'évasion avancées
9.4.1. *Bypass* de l'AMSI
9.4.2. Modification des outils existants
9.4.3. Obfuscation de *Powershell*

9.5. Techniques avancées de déplacement latéral
9.5.1. *Pass-the-Ticket* (PtT)
9.5.2. *Overpass-the-Hash* (Pass-the-Key)
9.5.3. NTLM Relay

9.6. Techniques avancées de post-exploitation
9.6.1. *Dump* de LSASS
9.6.2. *Dump* de SAM
9.6.3. Attaque *DCSync*

9.7. Techniques avancées de *pivoting*
9.7.1. Qu'est-ce que le *pivoting*
9.7.2. Tunnel SSH
9.7.3. *Pivoting* avec un Ciseau

9.8. Intrusions physiques
9.8.1. Surveillance et reconnaissance
9.8.2. *Tailgating et Piggybacking*
9.8.3. *Lock-Picking*

9.9. Attaques *Wi-Fi*
9.9.1. Attaques WPA/WPA2 PSK
9.9.2. Attaques des Rogue AP
9.9.3. Attaques WPA2 *Enterprise*

9.10. Attaques RFID
9.10.1. Lecture de cartes RFID
9.10.2. Manipulation de cartes RFID
9.10.3. Création de cartes clonées

Module 10. Rapports Techniques et Exécutifs

10.1. Processus de rapport
10.1.1. Structure d'un rapport
10.1.2. Processus de rapport
10.1.3. Concepts clés
10.1.4. Exécutif vs. Technique

10.2. Guide
10.2.1. Introduction
10.2.2. Types de Guides
10.2.3. Types de guides
10.2.4. Cas d'utilisation

10.3. Méthodologie
10.3.1. Évaluation
10.3.2. *Pentesting*
10.3.3. Revue des méthodologies communes
10.3.4. Introduction aux méthodologies nationales

10.4. Approche technique de la phase de rapport
10.4.1. Comprendre les limites du *pentester*
10.4.2. Utilisation de la langue et indices
10.4.3. Présentation de l'information
10.4.4. Erreurs courantes

10.5. Approche exécutive de la phase de rapport
10.5.1. Adapter le rapport au contexte
10.5.2. Utilisation de la langue et indices
10.5.3. Normalisation
10.5.4. Erreurs courantes

10.6. OSSTMM
10.6.1. Comprendre la méthodologie
10.6.2. Reconnaissance
10.6.3. Documentation
10.6.4. Élaboration du rapport

10.7. LINCE
10.7.1. Comprendre la méthodologie
10.7.2. Reconnaissance
10.7.3. Documentation
10.7.4. Élaboration du rapport

10.8. Signalement des vulnérabilités
10.8.1. Concepts clés
10.8.2. Quantifier la portée
10.8.3. Vulnérabilités et preuves
10.8.4. Erreurs courantes

10.9. Orienter le rapport vers le client
10.9.1. Importance des tests de travail
10.9.2. Solutions et atténuations
10.9.3. Données sensibles et pertinentes
10.9.4. Exemples et cas pratiques

10.10. Rapport sur les *retakes*
10.10.1. Concepts clés
10.10.2. Comprendre les informations héritées du passé
10.10.3. Vérification des erreurs
10.10.4. Ajout d'informations

07

Méthodologie

Ce programme de formation offre une manière différente d'apprendre. Notre méthodologie est développée à travers un mode d'apprentissage cyclique: ***le Relearning***.

Ce système d'enseignement est utilisé, par exemple, dans les écoles de médecine les plus prestigieuses du monde et a été considéré comme l'un des plus efficaces par des publications de premier plan telles que le ***New England Journal of Medicine.***

Découvrez le Relearning, un système qui laisse de côté l'apprentissage linéaire conventionnel au profit des systèmes d'enseignement cycliques: une façon d'apprendre qui a prouvé son énorme efficacité, notamment dans les matières dont la mémorisation est essentielle"

TECH Business School utilise l'Étude de Cas pour contextualiser tout le contenu.

Notre programme offre une méthode révolutionnaire de développement des compétences et des connaissances. Notre objectif est de renforcer les compétences dans un contexte changeant, compétitif et hautement exigeant.

Avec TECH, vous pouvez expérimenter une manière d'apprendre qui ébranle les fondations des universités traditionnelles du monde entier"

Notre programme vous prépare à relever les défis commerciaux dans des environnements incertains et à faire réussir votre entreprise.

Notre programme vous prépare à relever de nouveaux défis dans des environnements incertains et à réussir votre carrière.

Une méthode d'apprentissage innovante et différente

Ce programme TECH est un parcours de formation intensif, créé de toutes pièces pour offrir aux managers des défis et des décisions commerciales au plus haut niveau, tant au niveau national qu'international. Grâce à cette méthodologie, l'épanouissement personnel et professionnel est stimulé, faisant ainsi un pas décisif vers la réussite. La méthode des cas, technique qui constitue la base de ce contenu, permet de suivre la réalité économique, sociale et commerciale la plus actuelle.

> *Vous apprendrez, par le biais d'activités collaboratives et de cas réels, la résolution de situations complexes dans des environnements professionnels réels"*

La méthode des cas est le système d'apprentissage le plus utilisé dans les meilleures écoles de commerce du monde depuis qu'elles existent. Développée en 1912 pour que les étudiants en Droit n'apprennent pas seulement le droit sur la base d'un contenu théorique, la méthode des cas consiste à leur présenter des situations réelles complexes afin qu'ils prennent des décisions éclairées et des jugements de valeur sur la manière de les résoudre. En 1924, elle a été établie comme méthode d'enseignement standard à Harvard.

Dans une situation donnée, que doit faire un professionnel? C'est la question à laquelle nous sommes confrontés dans la méthode des cas, une méthode d'apprentissage orientée vers l'action. Tout au long du programme, les étudiants seront confrontés à de multiples cas réels. Ils devront intégrer toutes leurs connaissances, faire des recherches, argumenter et défendre leurs idées et leurs décisions.

Relearning Methodology

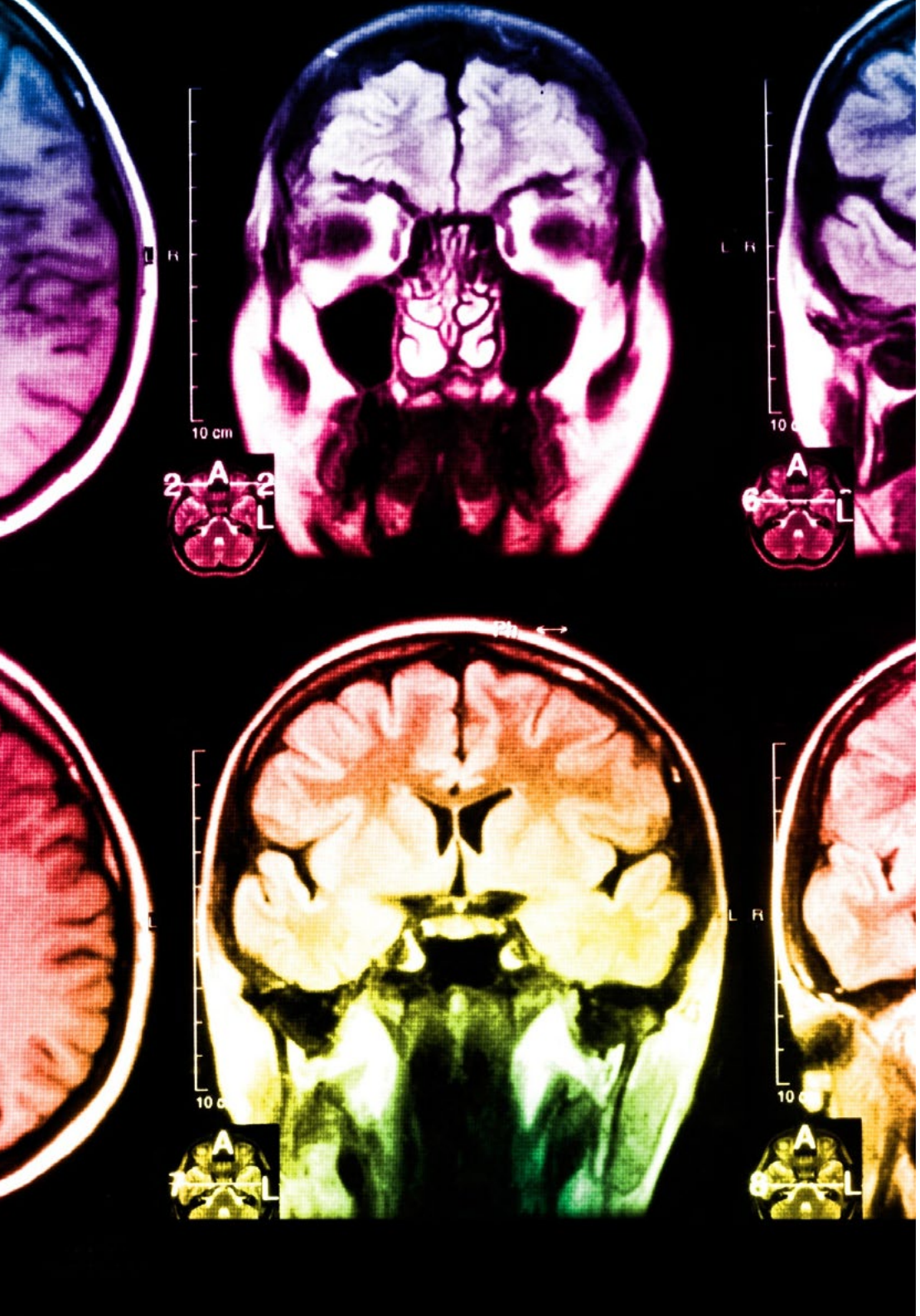
TECH combine efficacement la méthodologie des Études de Cas avec un système d'apprentissage 100% en ligne basé sur la répétition, qui associe différents éléments didactiques dans chaque leçon.

Nous enrichissons l'Étude de Cas avec la meilleure méthode d'enseignement 100% en ligne: le Relearning.

> *Notre système en ligne vous permettra d'organiser votre temps et votre rythme d'apprentissage, en l'adaptant à votre emploi du temps. Vous pourrez accéder aux contenus depuis n'importe quel appareil fixe ou mobile doté d'une connexion Internet.*

À TECH, vous apprendrez avec une méthodologie de pointe conçue pour former les managers du futur. Cette méthode, à la pointe de la pédagogie mondiale, est appelée Relearning.

Notre école de commerce est la seule école autorisée à employer cette méthode fructueuse. En 2019, nous avons réussi à améliorer les niveaux de satisfaction globale de nos étudiants (qualité de l'enseignement, qualité des supports, structure des cours, objectifs...) par rapport aux indicateurs de la meilleure université en ligne.



Dans notre programme, l'apprentissage n'est pas un processus linéaire, mais se déroule en spirale (apprendre, désapprendre, oublier et réapprendre). C'est pourquoi nous combinons chacun de ces éléments de manière concentrique. Cette méthodologie a permis de former plus de 650.000 diplômés universitaires avec un succès sans précédent dans des domaines aussi divers que la biochimie, la génétique, la chirurgie, le droit international, les compétences en gestion, les sciences du sport, la philosophie, le droit, l'ingénierie, le journalisme, l'histoire, les marchés financiers et les instruments. Tout cela dans un environnement très exigeant, avec un corps étudiant universitaire au profil socio-économique élevé et dont l'âge moyen est de 43,5 ans.

Le Relearning vous permettra d'apprendre avec moins d'efforts et plus de performance, en vous impliquant davantage dans votre spécialisation, en développant un esprit critique, en défendant des arguments et en contrastant les opinions: une équation directe vers le succès.

D'après les dernières preuves scientifiques dans le domaine des neurosciences, non seulement nous savons comment organiser les informations, les idées, les images et les souvenirs, mais nous savons aussi que le lieu et le contexte dans lesquels nous avons appris quelque chose sont fondamentaux pour notre capacité à nous en souvenir et à le stocker dans l'hippocampe, pour le conserver dans notre mémoire à long terme.

De cette manière, et dans ce que l'on appelle Neurocognitive context-dependent e-learning, les différents éléments de notre programme sont reliés au contexte dans lequel le participant développe sa pratique professionnelle.

Ce programme offre le support matériel pédagogique, soigneusement préparé pour les professionnels:

Support d'étude

Tous les contenus didactiques sont créés par les spécialistes qui enseigneront le cours, spécifiquement pour le cours, afin que le développement didactique soit vraiment spécifique et concret.

Ces contenus sont ensuite appliqués au format audiovisuel, pour créer la méthode de travail TECH en ligne. Tout cela, avec les dernières techniques qui offrent des pièces de haute qualité dans chacun des matériaux qui sont mis à la disposition de l'étudiant.

Cours magistraux

Il existe de nombreux faits scientifiques prouvant l'utilité de l'observation par un tiers expert.

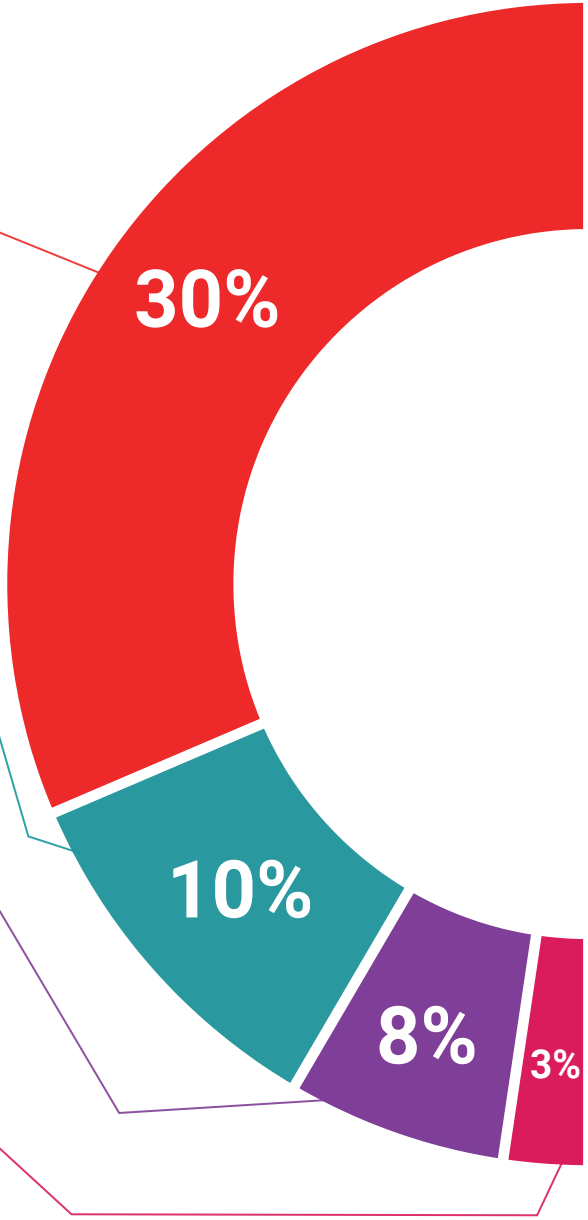
La méthode "Learning from an Expert" permet au professionnel de renforcer ses connaissances ainsi que sa mémoire, puis lui permet d'avoir davantage confiance en lui concernant la prise de décisions difficiles.

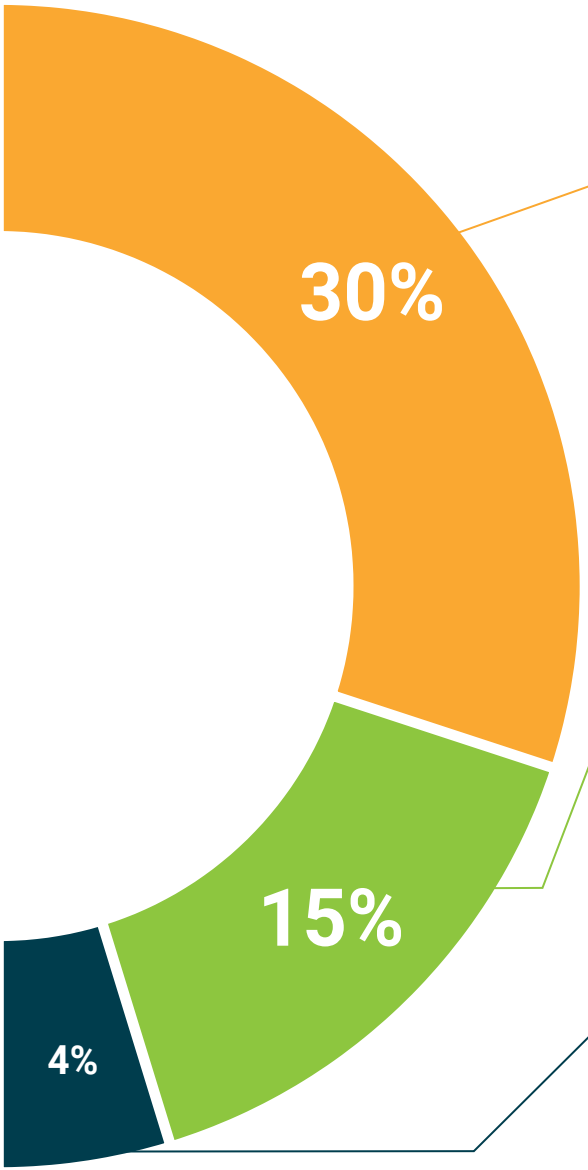
Stages en compétences de gestion

Ceux-ci mèneront des activités visant à développer des compétences de gestion spécifiques dans chaque domaine thématique. Pratiques et dynamiques pour acquérir et développer les compétences et les capacités dont un cadre supérieur a besoin dans le contexte de la mondialisation dans lequel nous vivons.

Lectures complémentaires

Articles récents, documents de consensus et directives internationales, entre autres. Dans la bibliothèque virtuelle de TECH, l'étudiant aura accès à tout ce dont il a besoin pour compléter sa formation.





Case studies

Ils réaliseront une sélection des meilleures études de cas choisies spécifiquement pour ce diplôme. Des cas présentés, analysés et tutorés par les meilleurs spécialistes de la direction d'entreprise sur la scène internationale.

Résumés interactifs

L'équipe TECH présente les contenus de manière attrayante et dynamique dans des pilules multimédia comprenant des audios, des vidéos, des images, des diagrammes et des cartes conceptuelles afin de renforcer les connaissances.

Ce système éducatif unique pour la présentation de contenu multimédia a été récompensé par Microsoft en tant que "European Success Story".

Testing & Retesting

Les connaissances de l'étudiant sont évaluées et réévaluées périodiquement tout au long du programme, par des activités et des exercices d'évaluation et d'auto-évaluation, afin que l'étudiant puisse vérifier comment il atteint ses objectifs.

08

Profil de nos étudiants

Le programme s'adresse aux titulaires d'un certificat ou d'un diplôme universitaire ayant déjà obtenu l'un des diplômes suivants dans les domaines des Sciences Sociales et Juridiques, de l'Administration et de l'Économie.

La diversité des participants aux différents profils académiques et aux multiples nationalités, constitue l'approche multidisciplinaire de ce programme.

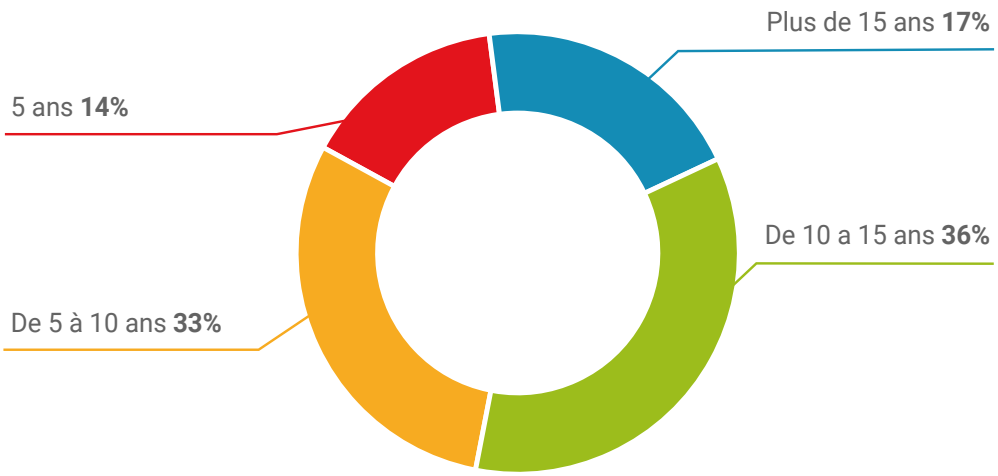
Les professionnels titulaires d'un diplôme universitaire dans n'importe quel domaine et ayant deux ans d'expérience professionnelle dans le domaine de l'Informatique peuvent également participer à ce programme.

Si vous avez de l'expérience dans le domaine de Pentesting et Red Team et que vous recherchez une évolution intéressante de votre carrière tout en continuant à travailler, ce programme est fait pour vous"

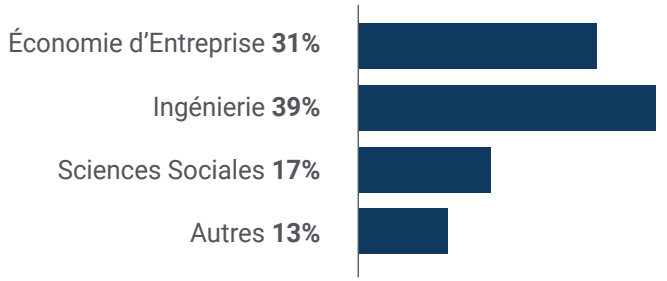
Âge moyen

Entre **35** et **45** ans

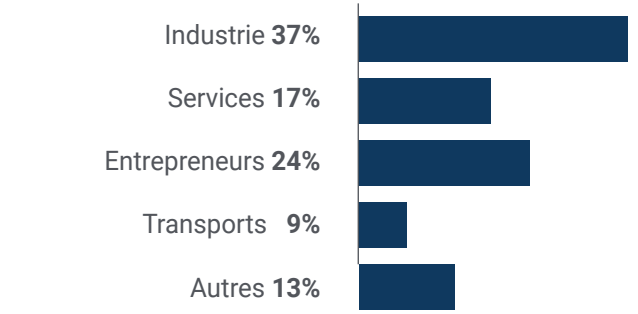
Années d'expérience



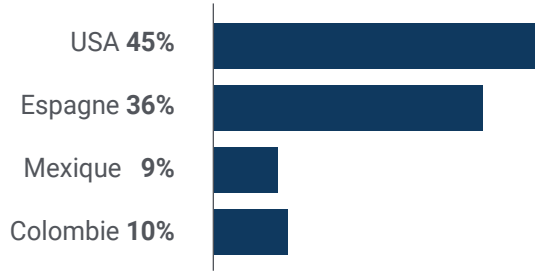
Formation



Profil académique



Distribution géographique



Salomón Galvis

Analyste de la sécurité de l'information

"De cette qualification, je voudrais souligner que j'ai pu approfondir ma compréhension de l'importance des évaluations régulières et à quel point il est essentiel de mesurer la cybersécurité. Un grand investissement qui se reflétera dans l'avenir, grâce aux outils clés que l'équipe enseignante met en œuvre dans le développement du programme"

09

Direction de la formation

Ce Mastère Spécialisé dispose d'une équipe enseignante de grande renommée internationale et d'une grande expertise dans les domaines des Logiciels et Technologies de la Société de l'Information et de la Cybersécurité dans l'Intégration des Technologies de l'Entreprise. Ainsi, la formation d'élite se traduit par une approche dynamique et innovante du programme d'études, mettant en œuvre les dernières tendances en matière de cybersécurité. Ainsi, des cas simulés et l'analyse de situations réelles sont combinés pour fournir aux étudiants une praxis de première classe, leur permettant de relever différents défis professionnels sur le lieu de travail.

De grands experts en Pentesting et Red Team enseigneront ce programme innovant et rigoureux"

Direction

M. Gómez Pintado, Carlos

- Directeur de l'Équipe de Cybersécurité et de Réseau Cipherbit dans le Grupo Oesía
- Directeur, *Conseiller et Investisseur* chez Wesson App
- Diplôme en Ingénierie Logicielle et Technologies de la Société de l'Information, Université Politécnique de Madrid
- Il collabore avec des établissements d'enseignement pour la préparation de Cycles de Formation de Niveau Supérieur en cybersécurité

Professeurs

M. Siles Rubia, Marcelino

- Cibersecurity Engineer
- Ingénieur en Cybersécurité à l'Université Rey Juan Carlos
- Connaissances: Programmation Compétitive, *Hacking Web, Active Directory et Malware Developmen*t
- Gagnant du Concours AdaByron

M. González Sanz, Marcos

- Cybersecurity Consultant-Red Teamer Cipherbit chez Groupe Oesía
- Ingénieur en Logiciel de l'Université Polytechnique de Madrid
- Spécialiste en *Cybersécurité Tutor* et Core *Dumped*

M. Redondo Castro, Pablo

- Pentester chez Groupe Oesía
- Ingénieur en Cybersécurité de l'Université Rey Juan Carlos
- Vaste expérience en tant que *Cibersecurity Evaluator Traineev*
- Il accumule de l'expérience dans l'enseignement, en donnant des formations liées aux tournois "Capture The Flag"

M. Gallego Sánchez, Alejandro

- Pentester chez Groupe Oesía
- Consultant en Cybersécurité à Integration Technologique Empresarial, S.L.
- Technicien Audiovisuel chez Ingénierie Audiovisuelle S.A.
- Diplômé en Ingénierie de la Cybersécurité de l'Université Rey Juan Carlos

M. Mora Navas, Sergio

- Consultant en Cybersécurité chez Groupe Oesía
- Ingénieur en Cybersécurité de l'Université Rey Juan Carlos
- Ingénieur Informaticien de l'Université de Burgos

M. González Parrilla, Yuba

- Coordinateur de la Ligne de Sécurité Offensive et Red Team
- Spécialiste en Gestion *Prédictive* de Projet à l'Institut de Gestion de Projet
- Spécialiste de *SmartDefense*
- Expert en *Web Application Penetration Tester* chez eLearnSecurity
- *Junior Penetration Tester* chez eLearnSecurity
- Diplômé en Ingénierie Informatique à l'Université Polytechnique de Madrid

“Une expérience de formation unique, clé et décisive pour stimuler votre développement professionnel”

10

Impact sur votre carrière

Ce programme universitaire a été conçu dans le but d'orienter le diplômé vers les connaissances qui lui permettront de faire face à toute situation dans le domaine de la cybersécurité. Ainsi, TECH se concentrera spécifiquement sur un enseignement de la plus haute qualité, en recherchant l'efficacité dans chacune de ses formations. Ainsi, le professionnel aura la garantie d'un apprentissage spécialisé dans le *Pentesting* et *Red Team*.

Red Team et d'autres aspects informatiques de la cybersécurité peuvent être intégrés au Pentesting grâce à cette formation intensive"

Les techniques avancées de pivotement sont quelques-unes des compétences que vous aurez en main à l'issue de ce programme complet de 12 mois.

Êtes-vous prêt à faire le grand saut? Vous allez booster votre carrière professionnelle.

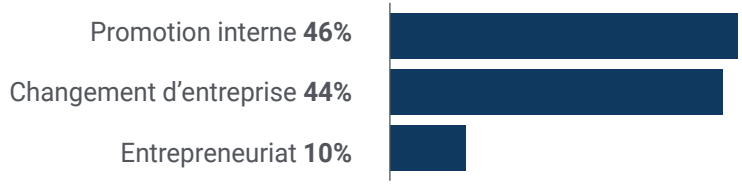
Le Mastère Spécialisé Pentesting et Red Team de TECH est un programme intensif qui prépare les étudiants à relever les défis et à prendre des décisions commerciales dans le domaine de l'Informatique. Son principal objectif est de favoriser votre épanouissement personnel et professionnel. Vous aider à réussir.

Si vous voulez vous améliorer, réaliser un changement positif au niveau professionnel et interagir avec les meilleurs, c'est l'endroit idéal pour vous.

Profitez de cette opportunité rigoureuse et complète pour développer vos compétences en Pentesting grâce à TECH, la meilleure université en ligne au monde selon Forbes.

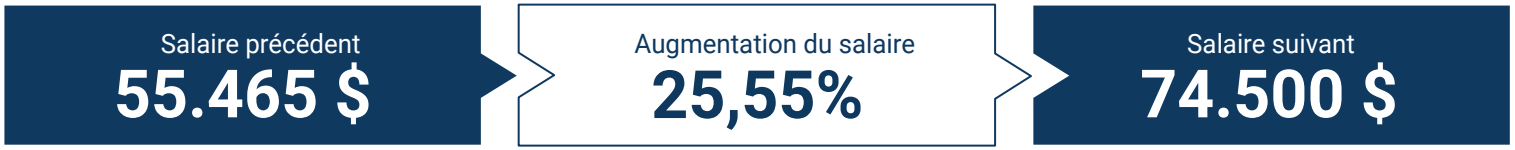
Moment du changement

Type de changement



Amélioration du salaire

L'achèvement de ce programme signifie une augmentation de salaire de plus de **25,55%** pour nos étudiants.



11

Bénéfices pour votre entreprise

Ce programme contribue à élever le talent de l'organisation à son potentiel maximal grâce à la formation de dirigeants de haut niveau.

En outre, la participation à cette option universitaire est une occasion unique d'accéder à un puissant réseau de contacts dans lequel trouver de futurs partenaires professionnels, clients ou fournisseurs.

À l'ère du numérique, les managers doivent intégrer de nouveaux processus et de nouvelles stratégies qui entraînent des changements importants et un développement organisationnel. Cela n'est possible que par une formation universitaire et une actualisation des connaissances"

Développer et retenir les talents dans les entreprises est le meilleur investissement à long terme.

01

Accroître les talents et le capital intellectuel

Le professionnel apportera à l'entreprise de nouveaux concepts, stratégies et perspectives susceptibles d'entraîner des changements importants dans l'organisation.

02

Conserver les cadres à haut potentiel et éviter la fuite des talents

Ce programme renforce le lien entre l'entreprise et le professionnel et ouvre de nouvelles perspectives d'évolution professionnelle au sein de l'entreprise.

03

Former des agents du changement

Vous serez en mesure de prendre des décisions en période d'incertitude et de crise, en aidant l'organisation à surmonter les obstacles.

04

Des possibilités accrues d'expansion internationale

Grâce à ce programme, l'entreprise entrera en contact avec les principaux marchés de l'économie mondiale.

05

Développement de projets propres

Le professionnel peut travailler sur un projet réel, ou développer de nouveaux projets, dans le domaine de la R+D ou le Business Development de son entreprise.

06

Accroître la compétitivité

Ce programme permettra à exiger de leurs professionnels d'acquérir les compétences nécessaires pour relever de nouveaux défis et pour faire progresser l'organisation.

12

Diplôme

Le Executive Mastère en Pentesting et Red Team garantit, outre la formation la plus rigoureuse et la plus actualisée, l'accès à un diplôme de Mastère Spécialisé délivré par TECH Université Technologique.

Terminez ce programme avec succès et recevez votre diplôme sans avoir à vous soucier des déplacements ou des formalités administratives”

Ce **Executive Mastère en Pentesting et Red Team** contient le programme le plus complet et le plus actualisé du marché

Après avoir passé l'évaluation, l'étudiant recevra par courrier* avec accusé de réception son diplôme de **Executive Mastère** délivrée par **TECH Université Technologique.**

Le diplôme délivré par **TECH Université Technologique** indiquera la note obtenue lors du **Executive Mastère**, et répond aux exigences communément demandées par les bourses d'emploi, les concours et les commissions d'évaluation des carrières professionnelles.

Diplôme: **Executive Mastère en Pentesting et Red Team**

Heures Officielles **1.500 h.**


tech université technologique

Délivre le présent

DIPLÔME

à

Mme/M. _____, avec nº d'identification _____

Pour avoir finalisé et accrédité avec succès le programme de

EXECUTIVE MASTÈRE

en

Pentesting et Red Team

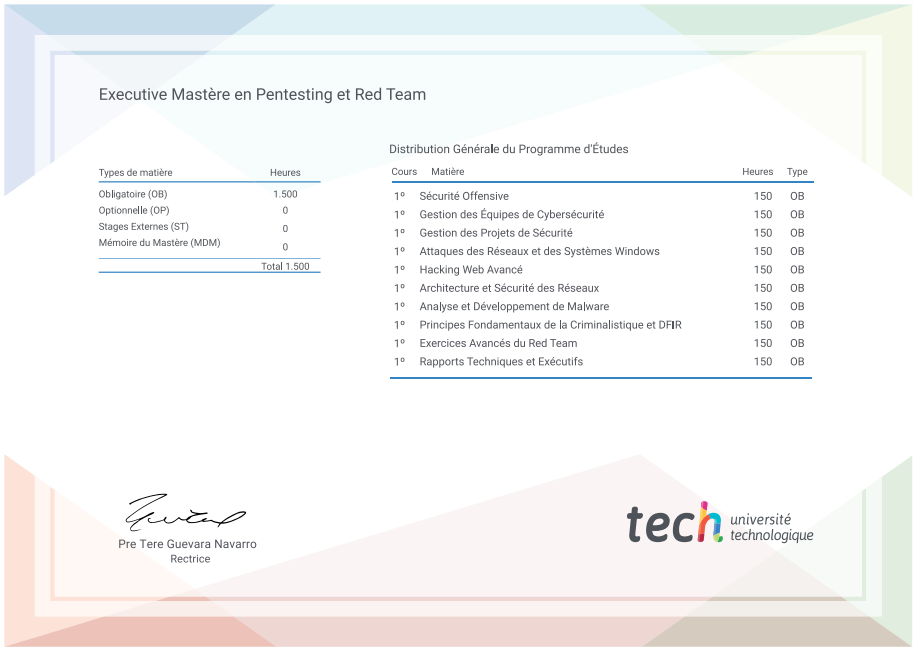
Il s'agit d'un diplôme spécialisé octroyé par cette Université d'une durée de 1.500 heures, débutant le dd/mm/aaaa et finalisant le dd/mm/aaaa.

TECH est une Institution Privée d'Enseignement Supérieur reconnue par le Ministère de l'Enseignement Public depuis le 28 juin 2018.

Fait le 17 juin 2020

Pre Tere Guevara Navarro
Rectrice

Code Unique TECH: AFWOR23S techtitute.com/diplômes


Executive Mastère en Pentesting et Red Team

Distribution Générale du Programme d'Études

Types de matière	Heures
Obligatoire (OB)	1.500
Optionnelle (OP)	0
Stages Externes (ST)	0
Mémoire du Mastère (MDM)	0
	Total 1.500

Cours	Matière	Heures	Type
1º	Sécurité Offensive	150	OB
1º	Gestion des Équipes de Cybersécurité	150	OB
1º	Gestion des Projets de Sécurité	150	OB
1º	Attaques des Réseaux et des Systèmes Windows	150	OB
1º	Hacking Web Avancé	150	OB
1º	Architecture et Sécurité des Réseaux	150	OB
1º	Analyse et Développement de Malware	150	OB
1º	Principes Fondamentaux de la Criminalistique et DFIR	150	OB
1º	Exercices Avancés du Red Team	150	OB
1º	Rapports Techniques et Exécutifs	150	OB

Pre Tere Guevara Navarro
Rectrice

tech université technologique

*Si l'étudiant souhaite que son diplôme version papier possède l'Apostille de La Haye, TECH EDUCATION fera les démarches nécessaires pour son obtention moyennant un coût supplémentaire.

tech université technologique

Executive Mastère
Pentesting et Red Team

- Modalité: **en ligne**
- Durée: **12 mois**
- Diplôme: **TECH Université Technologique**
- Temps estimé: **16 heures/semaine**
- Horaire: **à votre rythme**
- Examens: **en ligne**

Executive Mastère
Pentesting et Red Team

tech université technologique