

Certificat

Gestion des Équipes de Pentesting



tech universit 
technologique

Certificat Gestion des  quipes de Pentesting

- » Modalit : en ligne
- » Dur e: 6 semaines
- » Dipl me: TECH Universit  Technologique
- » Horaire:   votre rythme
- » Examens: en ligne

Acc s au site web: www.techtitute.com/fr/informatique/cours/gestion-equipes-pentesting

Sommaire

01

Présentation

page 4

02

Objectifs

page 8

03

Direction de la formation

page 12

04

Structure et contenu

page 16

05

Méthodologie

page 20

06

Diplôme

page 28

01

Présentation

La gestion des équipes de pentesting est un aspect fondamental pour les institutions. En effet, elle permet d'exploiter au mieux les ressources humaines et technologiques disponibles pour la réalisation des tests de pénétration. Par conséquent, les entreprises demandent de plus en plus l'incorporation d'experts en cybersécurité afin d'identifier et de résoudre les problèmes de manière optimale. Face à l'augmentation du *hacking* informatique, ces professionnels doivent régulièrement mettre à jour leurs connaissances et appliquer les outils les plus récents afin de prévenir les attaques informatiques. C'est pourquoi TECH lance un programme innovant permettant aux étudiants de mettre en œuvre les tactiques de *pentesting* plus pointues. De plus, ce programme est basé sur un mode 100% en ligne, garantissant ainsi le confort et la flexibilité des étudiants.



```
// Begin Actor overrides
virtual void PostInitiateComponent() override;
virtual void Tick(float DeltaSeconds) override;
virtual void ReceiveHit(class UBasicDamageComponent* DamageComponent, const class FVector& Location, const class UDamageType* DamageType, bool bIsRadial) override;
virtual void FellOutOfOrderId(const class UDamageType* DamageType) override;
// End Actor overrides

// Begin Pawn overrides
virtual void SetupPlayerInputComponent(class UInputComponent* InputComponent) override;
virtual float TakeDamage(float Damage, struct FDamageEvent const& DamageEvent, class AController* Controller, class AActor* Instigator) override;
virtual void TurnOff() override;
// End Pawn overrides

/** Identifies if pawn is in its dying state.
 * @see UPROPERTY(VisibleAnywhere, BlueprintReadWrite)
 */
uint32 bIsDying:1;

/** replicating death on client
 * @see UFUNCTION()
 */
void OnRep_Dying();

/** Returns true if the pawn is in its dying state.
 * @see UPROPERTY(VisibleAnywhere, BlueprintReadWrite)
 */
virtual bool IsDying() const;

```

“

Il propose l'arsenal le plus puissant de l'audit offensif à travers 150 heures du meilleur enseignement numérique"

Grâce aux audits réalisés par des experts en management d'équipe, les entités prennent conscience de leurs obstacles, risques et problèmes potentiels avant qu'il ne soit trop tard. En ce sens, les pentesters facilitent la communication entre les membres de l'équipe, ce qui leur permet de partager des connaissances et des informations. De même, les ressources sont surveillées et des stratégies de contrôle sont appliquées pour atteindre les objectifs fixés par les organisations (à la fois à court et à long terme).

Conscient de cette réalité, TECH a développé un cours de formation pionnier qui couvre tous les aspects, de l'analyse de la vulnérabilité aux techniques d'intrusion avancées. Le programme se penchera sur une série de méthodologies orientées vers la sécurité offensive, parmi lesquelles se distingue le Cyber Security Kill Chain. En outre, il encouragera la créativité par le biais de la technique "think outside the box" (sortir des sentiers battus) et promouvra ainsi des solutions innovantes pour se différencier des autres. Il explorera également les différents rôles du *pentesting*, en insistant sur la nécessité de mener des enquêtes approfondies. Il se penchera également sur l'outil Metasploit, dans le but de réaliser des attaques simulées de manière contrôlée. Enfin, les principaux défis affectant la sécurité offensive seront présentés et les diplômés seront encouragés à en faire des occasions de démontrer leur plein potentiel et leur ingéniosité.

Il convient de noter que, pour consolider la maîtrise des contenus, cette formation applique le système avant-gardiste de *Relearning*. TECH est un pionnier dans l'utilisation de ce modèle d'enseignement, qui favorise l'assimilation de concepts complexes par la répétition naturelle et progressive de ceux-ci. Dans cette optique, le programme utilise également du matériel sous différents formats tels que des infographies, des résumés interactifs et des vidéos explicatives. Tout cela dans un mode pratique 100 % en ligne, qui permet aux étudiants d'adapter leur emploi du temps en fonction de leurs responsabilités et de leur situation personnelle.

Ce **Certificat en Gestion des Équipes de Pentesting** contient le programme le plus complet et le plus actualisé du marché. Ses caractéristiques sont les suivantes:

- ♦ Le développement d'études de cas présentées par des experts en Gestion des Équipes de Pentesting
- ♦ Le contenu graphique, schématique et éminemment pratique de l'ouvrage fournit des informations actualisées et pratiques sur les disciplines essentielles à la pratique professionnelle
- ♦ Exercices pratiques permettant de réaliser le processus d'auto-évaluation afin d'améliorer l'apprentissage
- ♦ Il met l'accent sur les méthodologies innovantes
- ♦ Cours théoriques, questions à l'expert, forums de discussion sur des sujets controversés et travail de réflexion individuel
- ♦ Il est possible d'accéder aux contenus depuis tout appareil fixe ou portable doté d'une connexion à internet



Vous voulez faire un saut professionnel dans votre carrière? Devenez un expert en Intelligence des sources ouvertes grâce à cette formation"

“

Vous atteindrez vos objectifs grâce aux outils didactiques de TECH, y compris les vidéos explicatives et les résumés interactifs”

Le corps enseignant du programme englobe des spécialistes réputés dans le domaine et qui apportent à ce programme l'expérience de leur travail, ainsi que des spécialistes reconnus dans de grandes sociétés et des universités prestigieuses.

Grâce à son contenu multimédia développé avec les dernières technologies éducatives, les spécialistes bénéficieront d'un apprentissage situé et contextuel, ainsi, ils se formeront dans un environnement simulé qui leur permettra d'apprendre en immersion et de s'entraîner dans des situations réelles.

La conception de ce programme est axée sur l'Apprentissage par les Problèmes, grâce auquel le professionnel doit essayer de résoudre les différentes situations de la pratique professionnelle qui se présentent tout au long du programme académique. Pour ce faire, l'étudiant sera assisté d'un innovant système de vidéos interactives, créé par des experts reconnus.

Vous approfondirez vos compétences en matière de recherche pour mener les enquêtes les plus approfondies et vous démarquer des autres.

Maîtrisez le programme Metasploit dans la meilleure université numérique du monde selon Forbes.



02 Objectifs

La conception de ce programme fournira une plongée profonde dans les tactiques et les techniques employées par les professionnels de la sécurité offensive. Dans cette optique, il se concentrera sur le développement de compétences et de stratégies de test de pénétration pour exploiter les vulnérabilités des systèmes et des réseaux. Cela permettra d'acquérir de solides connaissances sur la manière de mener des évaluations de sécurité de manière efficace et éthique. Les étudiants mèneront des sessions pratiques pour apprendre les concepts théoriques dans des environnements simulés, les préparant à faire face aux défis du monde réel dans *Red Team*.



“

Vous souhaitez mettre en œuvre les mesures de sécurité offensives les plus innovantes ? Réalisez-le grâce à ce programme en seulement 6 semaines”



Objectifs généraux

- ◆ Acquérir des compétences avancées en matière de tests de pénétration et de simulations Red Team, afin d'identifier et d'exploiter les vulnérabilités des systèmes et des réseaux
- ◆ Développer des compétences en leadership pour coordonner des équipes spécialisées dans la cybersécurité offensive, en optimisant l'exécution des projets Pentesting et Red Team
- ◆ Développer des compétences dans l'analyse et le développement de logiciels malveillants, en comprenant leur fonctionnalité et en appliquant des stratégies défensives et éducatives
- ◆ Améliorer les compétences en matière de communication en produisant des rapports techniques et exécutifs détaillés, en présentant les résultats de manière efficace à des auditoires techniques et exécutifs
- ◆ Promouvoir une pratique éthique et responsable dans le domaine de la cybersécurité, en tenant compte des principes éthiques et juridiques dans toutes les activités
- ◆ Tenir les étudiants au courant des tendances et des technologies émergentes dans le domaine de la cybersécurité



Tout au long de votre processus d'apprentissage, vous serez soutenu par les meilleurs professionnels de la Cybersécurité"





Objectifs spécifiques

- ♦ Familiariser le diplômé avec les méthodologies de test de pénétration, y compris les phases clés telles que la collecte d'informations, l'analyse de la vulnérabilité, l'exploitation et la documentation
- ♦ Développer des compétences pratiques dans l'utilisation d'outils de Pentesting spécialisés pour identifier et évaluer les vulnérabilités des systèmes et des réseaux
- ♦ 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
- ♦ Appliquer les connaissances théoriques dans des scénarios pratiques et des simulations, en faisant face à des défis réels pour renforcer les compétences de Pentesting
- ♦ Développer des compétences efficaces en matière de documentation, en créant des rapports détaillés reflétant les résultats, les méthodologies utilisées et les recommandations pour l'amélioration de la sécurité
- ♦ Pratiquer une collaboration efficace au sein des équipes de sécurité offensive, en optimisant la coordination et l'exécution des activités de Pentesting

03

Direction de la formation

Dans son engagement d'offrir un enseignement de la plus haute qualité, TECH dispose d'un corps enseignant de haut niveau. Ces experts se caractérisent par une connaissance approfondie de la cybersécurité, tout en disposant d'une large expérience professionnelle. C'est pourquoi ce parcours académique fournit aux étudiants les meilleurs outils et tactiques pour leur permettre d'acquérir de multiples compétences pendant le cours. Les étudiants ont ainsi les garanties nécessaires pour se spécialiser dans un secteur numérique qui offre de nombreuses possibilités d'emploi.



“

Vous accéderez à un système d'apprentissage basé sur la répétition, avec un enseignement naturel et progressif tout au long du programme”

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 Politéchnique de Madrid
- ♦ Il collabore avec des établissements d'enseignement pour la préparation de **Cycles de Formation de Niveau Supérieur** en cybersécurité

Professeurs

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



04 Structure et contenu

Ce programme est abordé d'un point de vue théorique et pratique, avec un corps enseignant expérimenté qui plonge les étudiants dans l'analyse des stratégies de sécurité offensives les plus efficaces. Afin d'acquérir une compréhension globale du fonctionnement des acteurs malveillants, la catégorisation des vulnérabilités (CAPEC, CVSS, etc.) est explorée en profondeur. De plus, l'accent est mis sur l'utilisation des scripts dans le but d'exécuter des scripts qui automatisent des tâches sur un système informatique, y compris JavaScript. Les principes de l'éthique du *hacker* sont également abordés afin de comprendre les implications légales et les conséquences qui peuvent survenir au cours des activités. Pour ce faire, des études de cas réels sont analysées où l'éthique de la cybersécurité a été appliquée.

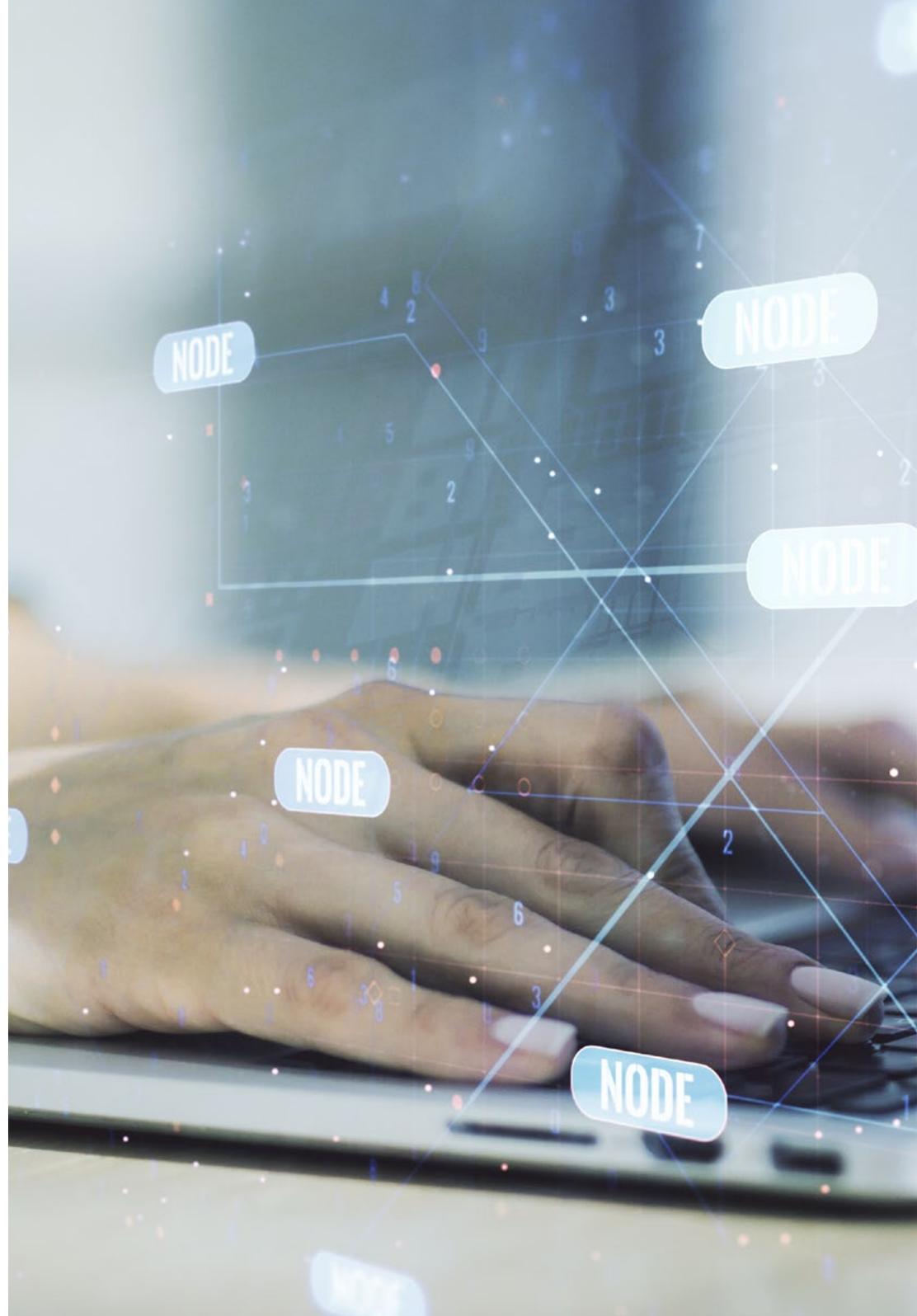


“

*Pas d'horaires préétablis ni
de calendriers d'évaluation:
c'est la raison d'être de ce
programme TECH"*

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 Intelligence 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

“ *La bibliothèque regorge de ressources multimédias dans différents formats audiovisuels* ”

05 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 Relearning, un système qui renonce à l'apprentissage linéaire conventionnel pour vous emmener à travers des systèmes d'enseignement cycliques: une façon d'apprendre qui s'est avérée extrêmement efficace, en particulier dans les matières qui exigent la mémorisation”

Étude de Cas pour mettre en contexte 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”



Vous bénéficierez d'un système d'apprentissage basé sur la répétition, avec un enseignement naturel et progressif sur l'ensemble du cursus.



L'étudiant apprendra, par des activités collaboratives et des cas réels, à résoudre des situations complexes dans des environnements commerciaux réels.

Une méthode d'apprentissage innovante et différente

Cette formation TECH est un programme d'enseignement intensif, créé de toutes pièces, qui propose les défis et les décisions les plus exigeants dans ce domaine, 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 professionnelle la plus actuelle.

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

La méthode des cas est le système d'apprentissage le plus largement utilisé dans les meilleures écoles d'informatique 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.

En 2019, nous avons obtenu les meilleurs résultats d'apprentissage de toutes les universités en ligne du monde.

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 université est la seule université autorisée à utiliser cette méthode qui a fait ses preuves. 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). Par conséquent, chacun de ces éléments est combiné 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 formation, en développant un esprit critique, en défendant des arguments et en contrastant les opinions: une équation directe vers le succès.

À partir des 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 des preuves scientifiques de l'utilité de l'observation par un tiers expert.

La méthode "Learning from an Expert" renforce les connaissances et la mémoire, et donne confiance dans les futures décisions difficiles.



Pratiques en compétences et aptitudes

Les étudiants réaliseront des activités visant à développer des compétences et des aptitudes spécifiques dans chaque domaine. Des activités pratiques et dynamiques pour acquérir et développer les compétences et aptitudes qu'un spécialiste doit développer dans le cadre de la mondialisation dans laquelle 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 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 périodiquement évaluées et réévaluées tout au long du programme, par le biais d'activités et d'exercices d'évaluation et d'auto-évaluation, afin que l'étudiant puisse vérifier comment il atteint ses objectifs.



06 Diplôme

Le Certificat en Gestion des Équipes de Pentesting garantit, outre la formation la plus rigoureuse et la plus actualisée, l'accès à un diplôme de Certificat 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 **Certificat en Gestion des Équipes de Pentesting** contient le programme le plus complet et actualisé du marché.

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

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

Diplôme: **Certificat en Gestion des Équipes de Pentesting**

Heures Officielles: **150 h.**



*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.

future
santé confiance personnes
éducation information tuteurs
garantie accréditation enseignement
institutions technologie apprentissage
communauté engagement
service personnalisé innovation
connaissance présent qualité
en ligne formation
développement institutions
classe virtuelle langues



Certificat Gestion des Équipes de Pentesting

- » Modalité: en ligne
- » Durée: 6 semaines
- » Diplôme: TECH Université Technologique
- » Horaire: à votre rythme
- » Examens: en ligne

Certificat

Gestion des Équipes de Pentesting

