Certificat Avancé
Hacking Web Avancé

tech université technologique

tech université technologique

Certificat Avancé
Hacking Web Avancé

- Modalité : **en ligne**
- Durée : **6 mois**
- Quali ication: **TECH Université Technologique**
- Horaire: **à votre rythme**
- Examens: **en ligne**

Accès au site web: www.techtitute.com/fr/informatique/diplome-universite/diplome-universite-hacking-web-avance

Sommaire

01

Présentation

À mesure que les institutions se développent numériquement, elles utilisent de plus en plus la technologie pour stocker des données sensibles. Le *Hacking* Avancé devient donc une menace sérieuse pour les institutions. Si les *hackers* parviennent à accéder à leurs sites web, les conséquences peuvent être désastreuses, allant de l'usurpation d'identité à la fraude financière et au chantage. C'est pourquoi il est important pour les entreprises de disposer d'experts en mesures de sécurité avancées, pour la mise en œuvre de mesures telles que les *firewalls*. C'est pourquoi TECH lance un programme innovant destiné aux étudiants afin qu'ils maîtrisent les techniques les plus efficaces en matière de cybersécurité. En outre, il est basé sur une modalité 100% en ligne, garantissant la commodité et la flexibilité du temps.

Grâce à ce Certificat Avancé, vous transformerez n'importe quelle entreprise en un environnement sûr, à l'abri des cybermenaces"

Les spécialistes des technologies de l'information constituent un atout immatériel précieux pour les organisations d'aujourd'hui. L'une des principales raisons est que leurs audits réguliers permettent d'identifier et de traiter rapidement les vulnérabilités potentielles. Ils anticipent ainsi les délits que les *hackers*informatiques pourraient commettre, tout en transformant les environnements virtuels en zones sûres.

Les utilisateurs sont ainsi assurés de pouvoir naviguer librement et en toute sécurité sur leur réseau et d'acheter des biens et des services. Cependant, face à l'augmentation de ces pratiques, les informaticiens sont confrontés au défi de mettre constamment à jour leurs connaissances, en mettant en œuvre les techniques les plus révolutionnaires pour y faire face.

Dans ce contexte, TECH a développé le Certificat Avancé en *Hacking Web* Avancé le plus complet sur le marché académique. Grâce à ce programme, les diplômés seront à la pointe de la cybersécurité et disposeront d'un large éventail de tactiques pour protéger les informations à diffusion restreinte. En outre, ils approfondiront les stratégies d'exploitation des vulnérabilités sophistiquées.

En outre, le professionnel se concentrera sur la mise en œuvre de mesures de sécurité efficaces, telles que les systèmes de détection d'intrusion. L'accent sera également mis sur le *switching* pour interconnecter les équipements de toutes les sections de l'organisation sur le même réseau. Le programme fournira également les clés pour rédiger des rapports techniques et exécutifs. En ce sens, nous verrons comment exposer des données sensibles, en axant le rapport sur les clients. Enfin, différentes méthodologies pour mesurer la sécurité opérationnelle réelle seront explorées.

Pour consolider la maîtrise des contenus, cette formation applique le système innovant de *Relearning*, qui favorise l'assimilation de concepts complexes par la réitération naturelle et progressive de ceux-ci. De même, le programme utilise du matériel sous différents formats, tels que des infographies ou des vidéos explicatives. Le tout dans un mode pratique 100 % en ligne, qui permet d'adapter l'emploi du temps de chacun à ses responsabilités.

Ce **Certificat Avancé en Hacking Web Avancé** contient le programme éducatif 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 Hacking Web Avancé
- Le contenu graphique, schématique et éminemment pratique de l'ouvrage fournit des informations complètes 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 déchiffrerez les mots de passe stockés sur les ordinateurs et anticiperez les attaques des hackers"

Vous explorerez le modèle OSI et comprendrez les processus de communication dans les systèmes de réseau. Et ce, en 6 mois seulement!"

Vous découvrirez les vulnérabilités des DOM et préviendrez les attaques avancées à l'aide des stratégies les plus efficaces.

Oubliez la mémorisation! Avec la méthodologie Relearning vous intégrerez les concepts de manière naturelle et progressive.

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.

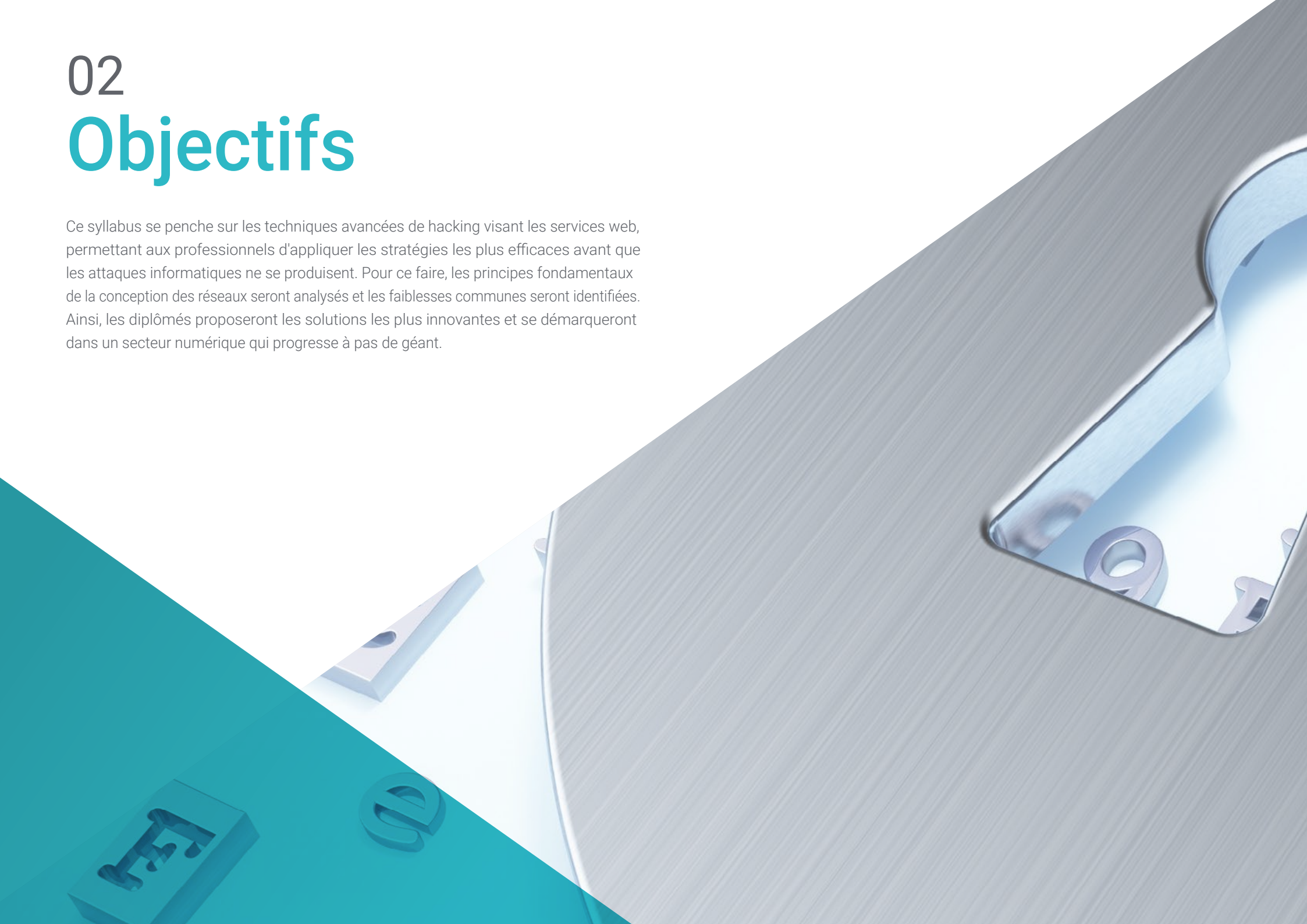
Grâce à son contenu multimédia développé avec les dernières technologies éducatives, les spécialistes bénéficieront d'un apprentissage situé et contextuel, ainsi, ils se formeront dans un environnement simulé qui leur permettra d'apprendre en immersion et de s'entrainer dans des situations réelles.

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.

02

Objectifs

Ce syllabus se penche sur les techniques avancées de hacking visant les services web, permettant aux professionnels d'appliquer les stratégies les plus efficaces avant que les attaques informatiques ne se produisent. Pour ce faire, les principes fondamentaux de la conception des réseaux seront analysés et les faiblesses communes seront identifiées. Ainsi, les diplômés proposeront les solutions les plus innovantes et se démarqueront dans un secteur numérique qui progresse à pas de géant.



Vous voulez sécuriser le réseau et les données qui y sont transmises? Maîtrisez le switching avec la meilleure université numérique au monde, selon Forbes"

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

Vous appliquerez les mesures de sécurité les plus efficaces et éviterez les vulnérabilités telles que le Broken Authentication. Inscrivez-vous maintenant!"

Objectifs spécifiques

Module 1. Hacking Web Avancé

- Développer des compétences pour identifier et évaluer les vulnérabilités des applications web, y compris les injections SQL, le Cross-Site Scripting (XSS) et d'autres vecteurs d'attaque courants
- Apprendre à effectuer des tests de sécurité sur des applications web modernes
- Acquérir des compétences dans les techniques avancées de piratage web, en explorant des stratégies pour contourner les mesures de sécurité et exploiter des vulnérabilités sophistiquées
- 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
- Développer des compétences pour mettre en œuvre des mesures d'atténuation efficaces dans les applications web, en réduisant l'exposition aux attaques et en renforçant la sécurité
- Participer à des simulations pratiques pour évaluer la sécurité dans des environnements web complexes, en appliquant les connaissances à des scénarios du monde réel.
- Développer des compétences dans la formulation de stratégies de défense efficaces pour protéger les applications web contre les cyber-menaces
- Apprendre à aligner les pratiques avancées de hacking web sur les réglementations et les normes de sécurité pertinentes, en veillant au respect des cadres juridiques et éthiques.
- Favoriser une collaboration efficace entre les équipes de développement et de sécurité

Module 2. Architecture et Sécurité des Réseaux

- Acquérir une connaissance avancée de l'architecture des réseaux, y compris les topologies, les protocoles et les composants clés
- Développer des compétences pour identifier et évaluer les vulnérabilités spécifiques des infrastructures de réseau, en tenant compte des menaces potentielles
- Apprendre à mettre en œuvre des mesures de sécurité réseau efficaces, notamment des firewalls, des systèmes de détection d'intrusion (IDS) et la segmentation du réseau
- Familiariser l'étudiant avec les technologies de réseau émergentes, telles que les réseaux définis par logiciel (SDN), et comprendre leur impact sur la sécurité
- Développer des compétences en matière de sécurisation des communications réseau, y compris la protection contre les menaces telles que le sniffing et les attaques intermédiaires
- Apprendre à évaluer et à améliorer les configurations de sécurité dans les environnements de réseaux d'entreprise, afin de garantir une protection adéquate
- Développer des compétences pour mettre en œuvre des mesures d'atténuation efficaces contre les menaces sur les réseaux d'entreprise, qu'il s'agisse d'attaques internes ou de menaces externes
- Favoriser une collaboration efficace avec les équipes de sécurité, en intégrant les stratégies et les efforts visant à protéger l'infrastructure du réseau
- Promouvoir des pratiques éthiques et juridiques dans la mise en œuvre des mesures de sécurité des réseaux, en veillant au respect des principes éthiques dans toutes les activités

Module 3. Rapports Techniques et Exécutifs

- Développer des compétences pour produire des rapports techniques détaillés, présentant les résultats, les méthodologies et les recommandations d'une manière claire et complète
- Apprendre à communiquer efficacement avec des publics techniques, en utilisant un langage précis et approprié pour transmettre des informations techniques complexes
- Développer des compétences pour formuler des recommandations pratiques et réalisables visant à atténuer les vulnérabilités et à améliorer le niveau de sécurité
- Apprendre à évaluer l'impact potentiel des vulnérabilités identifiées, en tenant compte des aspects techniques, opérationnels et stratégiques
- Familiariser l'apprenant avec les meilleures pratiques en matière de rapports exécutifs, en adaptant des informations techniques à des publics non techniques
- Développer des compétences pour aligner les résultats et les recommandations sur les objectifs stratégiques et opérationnels de l'organisation
- Apprendre à utiliser des outils de visualisation des données pour représenter graphiquement les informations contenues dans les rapports, afin d'en faciliter la compréhension
- Promouvoir l'inclusion d'informations pertinentes sur le respect des réglementations et des normes dans les rapports, afin de garantir le respect des exigences légales
- Favoriser une collaboration efficace entre les équipes techniques et exécutives, afin de garantir la compréhension et le soutien des mesures d'amélioration proposées dans le rapport

03

Direction de la formation

Dans le but d'offrir un enseignement d'excellence, TECH a réuni une équipe d'enseignants ayant une vaste expérience professionnelle dans le domaine de la cybersécurité. Avec plus de 13 ans d'expérience, ces spécialistes proposeront l'approche la plus complète et les outils les plus récents pour développer des environnements virtuels sécurisés. Ainsi, les étudiants auront les garanties nécessaires pour se spécialiser dans un secteur numérique qui offre de multiples opportunités.

Vous explorerez les limites du Pentester avec l'appui du meilleur corps enseignant. Vos activités seront 100% légales!"

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 Development*
- Gagnant du Concours AdaByron

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"

04

Structure et contenu

Ce programme couvre 3 modules complets : *Hacking Web* Avancé; Architecture et Sécurité des Réseaux; et Rapports Techniques et Exécutifs Avec le soutien de professeurs expérimentés, des tactiques avancées de sécurisation des réseaux d'entreprise par la mise en œuvre de *firewalls*seront abordées. La détection des intrusions, y compris le HHTP *Request Smuggling*, sera également abordée. Vous explorerez également l'importance d'avoir des VLAN pour séparer le trafic de données dans le même environnement virtuel, et vous vous plongerez dans le processus de reporting afin de présenter des rapports précis et détaillés.

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

Module 1. Hacking Web Avancé

1.1. Fonctionnement d'un site web
- 1.1.1. L'URL et ses composantes
- 1.1.2. Les méthodes HTTP
- 1.1.3. Les en-têtes
- 1.1.4. Comment visualiser les requêtes web avec Burp Suite

1.2. Sessions
- 1.2.1. Les *cookies*
- 1.2.2. *Tokens* JWT
- 1.2.3. Attaques par détournement de session
- 1.2.4. Attaques sur le JWT

1.3. *Cross Site Scripting* (XSS)
- 1.3.1. Qu'est-ce que le XSS
- 1.3.2. Types de XSS
- 1.3.3. Exploiter un XSS
- 1.3.4. Introduction à *XSLeaks*

1.4. Injections dans les bases de données
- 1.4.1. Qu'est-ce qu'une *SQL Injection*
- 1.4.2. Exfiltrer des informations avec *SQLi*
- 1.4.3. *SQLi Blind, Time-Based et Error-Based*
- 1.4.4. Injections NoSQLi

1.5. Path Traversal et Local File Inclusion
- 1.5.1. Qu'est-ce que c'est et quelles sont leurs différences
- 1.5.2. Filtres courants et comment les contourner
- 1.5.3. *Log Poisoning*
- 1.5.4. LFIs en PHP

1.6. *Broken Authentication*
- 1.6.1. *User Enumeration*
- 1.6.2. *Password Bruteforce*
- 1.6.3. *2FA Bypass*
- 1.6.4. *Cookies* contenant des informations sensibles et modifiables

1.7. *Remote Command Execution*
- 1.7.1. *Command Injection*
- 1.7.2. *Blind Command Injection*
- 1.7.3. *Insecure Deserialization* PHP
- 1.7.4. *Insecure Deserialization* Java

1.8. *File Uploads*
- 1.8.1. RCE à travers les *webshells*
- 1.8.2. XSS dans les téléchargements de fichiers
- 1.8.3. XML *External Entity* (XXE) *Injection*
- 1.8.4. *Path traversal* dans les téléchargements de fichiers

1.9. *Broken Acess Control*
- 1.9.1. Accès illimité au panneau
- 1.9.2. *Insecure Direct Object References* (IDOR)
- 1.9.3. *Bypass* des filtres
- 1.9.4. Méthodes d'autorisation insuffisantes

1.10. Vulnérabilités du DOM et attaques plus avancées
- 1.10.1. *Regex Denial of Service*
- 1.10.2. DOM *Clobbering*
- 1.10.3. *Prototype Pollution*
- 1.10.4. HTTP *Request Smuggling*

Module 2. Architecture et Sécurité des Réseaux

2.1. Réseaux informatiques
- 2.1.1. Concepts de base : Protocoles LAN, WAN, CP, CC
- 2.1.2. Modèle OSI et TCP/IP
- 2.1.3. *Commutation :* Concepts de base
- 2.1.4. *Routing:* Concepts de base

2.2. *Switching*
- 2.2.1. Introduction aux VLAN
- 2.2.2. STP
- 2.2.3. *EtherChannel*
- 2.2.4. Attaques de la couche 2

2.3. VLANs
- 2.3.1. Importance des VLAN
- 2.3.2. Vulnérabilités des VLAN
- 2.3.3. Attaques courantes contre les VLAN
- 2.3.4. Atténuations

2.4. *Routing*
- 2.4.1. Adressage IP - IPv4 et IPv6
- 2.4.2. Routage : Concepts clés
- 2.4.3. Routage Statique
- 2.4.4. Routage Dynamique : Introduction

2.5. Protocoles IGP
- 2.5.1. RIP
- 2.5.2. OSPF
- 2.5.3. RIP vs OSPF
- 2.5.4. Analyse des besoins en matière de topologie

2.6. Protection du périmètre
- 2.6.1. DMZ
- 2.6.2. *Firewalls*
- 2.6.3. Architectures communes
- 2.6.4. Zero Trust Network Access

2.7. IDS et IPS
- 2.7.1. Caractéristiques
- 2.7.2. Mise en œuvre
- 2.7.3. SIEM et SIEM CLOUDS
- 2.7.4. Détection basée sur les *HoneyPots*

2.8. TLS y VPN
- 2.8.1. SSL/TLS
- 2.8.2. TLS: Attaques courantes
- 2.8.3. VPN avec TLS
- 2.8.4. VPN avec IPSEC

2.9. Sécurité dans les réseaux sans fil
- 2.9.1. Introduction aux réseaux sans fil
- 2.9.2. Protocoles
- 2.9.3. Éléments clés
- 2.9.4. Attaques courantes

2.10. Les réseaux d'entreprises et la manière de les gérer
- 2.10.1. Segmentation logique
- 2.10.2. Segmentation physique
- 2.10.3. Contrôle d'accès
- 2.10.4. Autres mesures à prendre en compte

Module 3. Rapports Techniques et Exécutifs

3.1. Processus de rapport
- 3.1.1. Structure d'un rapport
- 3.1.2. Processus de rapport
- 3.1.3. Concepts clés
- 3.1.4. Exécutif vs. Technique

3.2. Guide
- 3.2.1. Introduction
- 3.2.2. Types de Guides
- 3.2.3. Types de guides
- 3.2.4. Cas d'utilisation

3.3. Méthodologie
- 3.3.1. Évaluation
- 3.3.2. *Pentesting*
- 3.3.3. Revue des méthodologies communes
- 3.3.4. Introduction aux méthodologies nationales

3.4. Approche technique de la phase de rapport
- 3.4.1. Comprendre les limites du *pentester*
- 3.4.2. Utilisation de la langue et indices
- 3.4.3. Présentation de l'information
- 3.4.4. Erreurs courantes

3.5. Approche exécutive de la phase de rapport
- 3.5.1. Adapter le rapport au contexte
- 3.5.2. Utilisation de la langue et indices
- 3.5.3. Normalisation
- 3.5.4. Erreurs courantes

3.6. OSSTMM
- 3.6.1. Comprendre la méthodologie
- 3.6.2. Reconnaissance
- 3.6.3. Documentation
- 3.6.4. Élaboration du rapport

3.7. LINCE
- 3.7.1. Comprendre la méthodologie
- 3.7.2. Reconnaissance
- 3.7.3. Documentation
- 3.7.4. Élaboration du rapport

3.8. Signalement des vulnérabilités
- 3.8.1. Concepts clés
- 3.8.2. Quantifier la portée
- 3.8.3. Vulnérabilités et preuves
- 3.8.4. Erreurs courantes

3.9. Orienter le rapport vers le client
- 3.9.1. Importance des tests de travail
- 3.9.2. Solutions et atténuations
- 3.9.3. Données sensibles et pertinentes
- 3.9.4. Exemples et cas pratiques

3.10. Rapport sur les *retakes*
- 3.10.1. Concepts clés
- 3.10.2. Comprendre les informations héritées du passé
- 3.10.3. Vérification des erreurs
- 3.10.4. Ajout d'informations

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

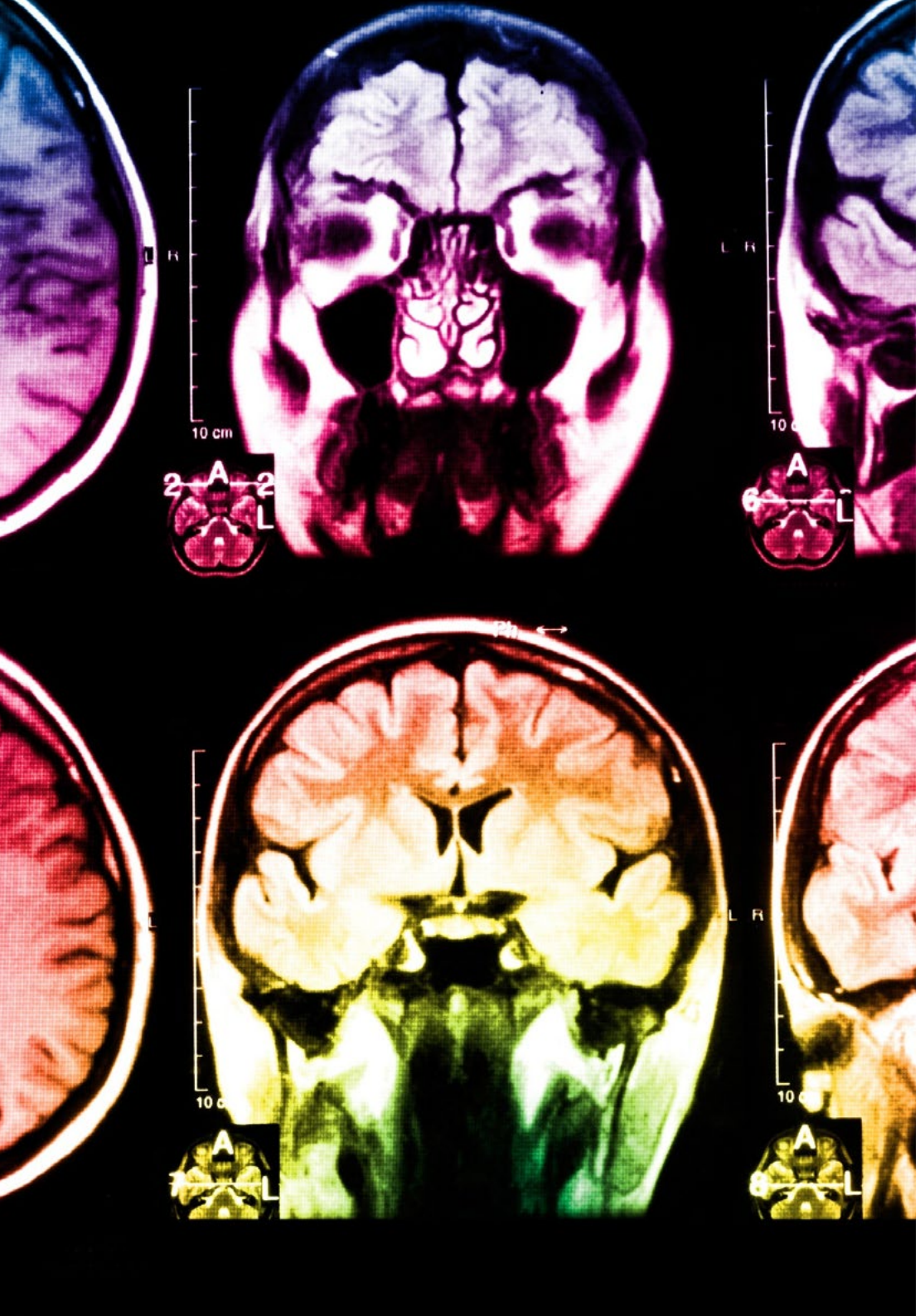
TECH combine efficacement la méthodologie des Études de Cas avec un système d'apprentissage 100% en ligne basé sur la répétition, qui associe différents éléments didactiques dans chaque leçon.

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.

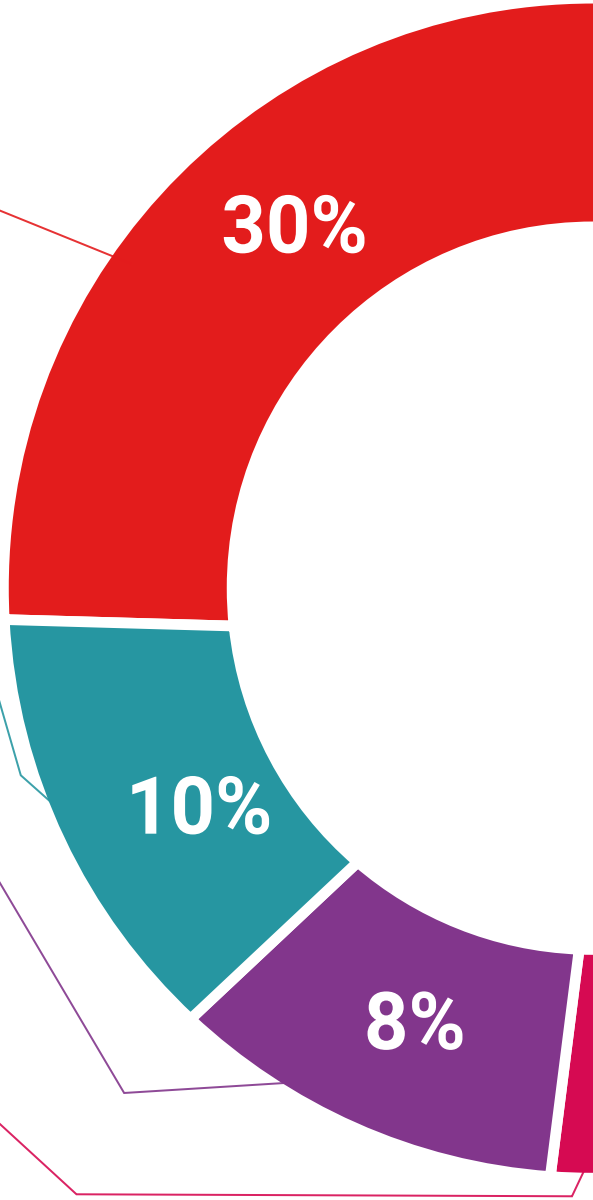
La méthode "Learning from an Expert" renforce les connaissances et la mémoire, et donne confiance dans les futures décisions difficiles.

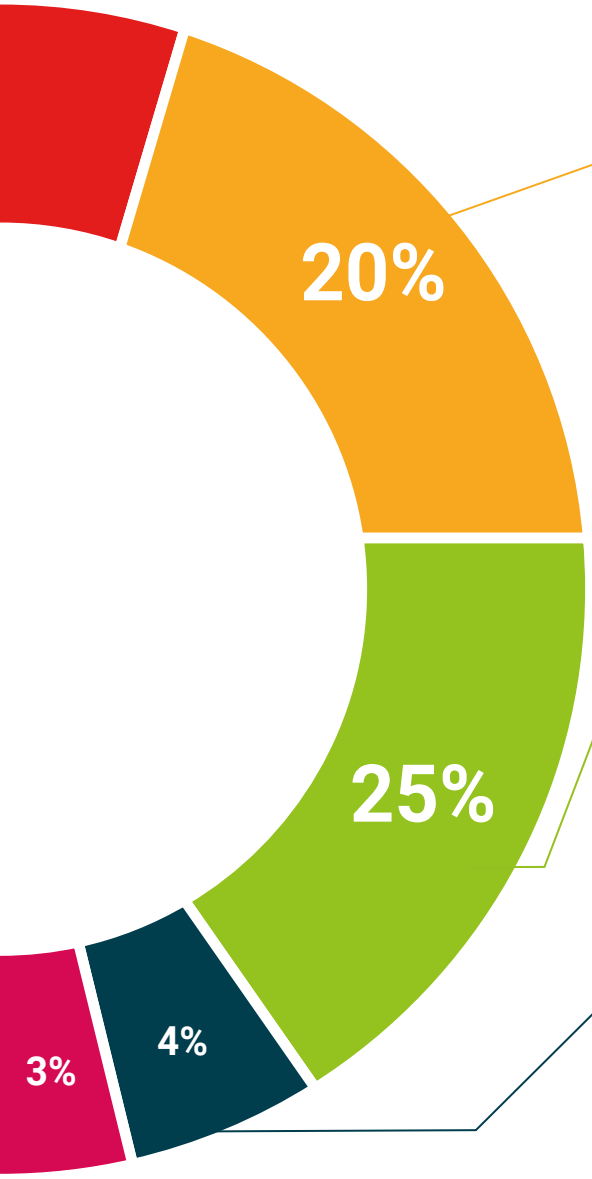
Pratiques en compétences et aptitudes

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 Avancé en Hacking Web Avancé garantit, outre la formation la plus rigoureuse et la plus actualisée, l'accès à un diplôme de Certificat Avancé 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 Avancé en Hacking Web Avancé** 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 Avancé** délivrée par **TECH Université Technologique**

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

Diplôme : **Certificat Avancé en Hacking Web Avancé**

Heures Officielles: **450 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

CERTIFICAT AVANCÉ

en

Hacking Web Avancé

Il s'agit d'un diplôme spécialisé octroyé par cette Université d'une durée de 450 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

*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

Certificat Avancé
Hacking Web Avancé

- Modalité : **en ligne**
- Durée : **6 mois**
- Qualification: **TECH Université Technologique**
- Horaire: **à votre rythme**
- Examens: **en ligne**

Certificat Avancé
Hacking Web Avancé

tech université technologique