شهادة الخبرة الجامعية
قرصنة الويب المتقدمة

tech الجامعة التيكنولوجية

الجامعة التيكنولوجية

شهادة الخبرة الجامعية
قرصنة الويب المتقدمة

- طريقة التدريس: **أونلاين**
- مدة الدراسة: **6 اشهر**
- المؤهل الجامعي من: **TECH الجامعة التكنولوجية**
- مواعيد الدراسة: **وفقًا لوتيرتك الخاصّة**
- الامتحانات: **أونلاين**

رابط الدخول إلى الموقع الإلكتروني: www.techtitute.com/ae/information-technology/postgraduate-diploma/postgraduate-diploma-advanced-web-hacking

الفهرس

01

المقدمة

مع توسع المؤسسات رقمياً، فإنها تستخدم التكنولوجيا بشكل متزايد لتخزين البيانات الحساسة. بالتالي، تصبح القرصنة Hacking المتقدمة تهديدًا خطيرًا للمؤسسات. إذا تمكن القراصنة hackersمن الوصول إلى مواقعك الإلكترونية، فقد تكون العواقب وخيمة، بدءاً من سرقة الهوية إلى الاحتيال المالي والابتزاز. لذلك، من المهم أن يكون لدى الشركات خبراء في التدابير الأمنية المتقدمة، لتطبيق تدابير مثل جدران الحماية firewalls.. استجابةً لهذا الأمر، تطلق TECH برنامجاً مبتكراً لمساعدة الطلاب على إتقان تقنيات الأمن السيبراني الأكثر فعالية. علاوةً على ذلك، فهو يعتمد على طريقة الإنترنت 100%، مما يضمن الراحة والمرونة في الوقت.

ستحول أي شركة إلى بيئة آمنة خالية من التهديدات
الإلكترونية بفضل شهادة الخبرة الجامعية هذه"

يُعد المتخصصون في تكنولوجيا المعلومات من الأمور القيمة غير الملموسة بالنسبة للمؤسسات اليوم. أحد الأسباب الرئيسية لذلك هو أن عمليات التدقيق المنتظمة تساعد على تحديد نقاط الضعف المحتملة ومعالجتها مسبقًا. بهذه الطريقة، فإنها تستبق الجرائم التي قد يرتكبها القراصنة hackers، مع تحويل البيئات الافتراضية إلى مناطق آمنة.

بهذه الطريقة، نضمن للمستخدمين القدرة على التصفح بأمان وحرية على شبكتهم وشراء سلعهم وخدماتهم. مع ذلك، ونظراً لتزايد هذه الممارسات، يواجه علماء الحاسوب تحدياً يتمثل في تحديث معارفهم باستمرار، وتطبيق أحدث التقنيات للتعامل معها.

وفي هذا السياق، طورت TECH شهادة الخبرة الجامعية في مجال قرصنة الويب المتقدمة الأكثر اكتمالاً في السوق الأكاديمية. من خلال هذا البرنامج، سيكون الخريجون في طليعة مجال الأمن السيبراني وسيكون لديهم مجموعة واسعة من التكتيكات لحماية المعلومات المحظورة. بالإضافة إلى ذلك، سيتم استكشاف استراتيجيات استغلال نقاط الضعف المتطورة بتعمق.

سيركز الممارس أيضاً على وضع تدابير أمنية فعالة، مثل أنظمة كشف التسلل. كما سيتم التأكيد على التحويل switching لربط المعدات من جميع أقسام المخطط التنظيمي على نفس الشبكة. كما سيوفر أيضًا مفاتيح كتابة التقارير الفنية والتنفيذية. في هذا الصدد، سيتطرق التقرير إلى كيفية الكشف عن البيانات الحساسة، مع التركيز على العملاء. أخيراً، سيتم استكشاف منهجيات مختلفة لقياس الأمن التشغيلي الفعلي.

من أجل تعزيز إتقان المحتويات، يطبق هذا التدريب نظام إعادة التعلم Relearningالمبتكر الذي يعزز استيعاب المفاهيم المعقدة من خلال التكرار الطبيعي والتدريجي لها. بالمثل، يعتمد البرنامج على مواد بتنسيقات مختلفة، مثل الرسوم البيانية أو مقاطع الفيديو التوضيحية. كل هذا بطريقة مريحة 100% عبر الإنترنت، مما يسمح بتعديل جداول كل شخص بما يتناسب مع مسؤولياته.

تحتوي **شهادة الخبرة الجامعية في قرصنة الويب المتقدمة** على البرنامج التعليمي الأكثر اكتمالاً وحداثة في السوق. أبرز خصائصها هي:

- تطوير الحالات العملية المقدمة من قبل خبراء في قرصنة الويب المتقدمة
- يجمع المحتوى الرسومي والتخطيطي والعملي البارز الذي تم تصميمه به معلومات كاملة وعملية عن تلك التخصصات الأساسية للممارسة المهنية
- التمارين العملية حيث يمكن إجراء عملية التقييم الذاتي لتحسين التعلم
- تركيزه على المنهجيات المبتكرة
- كل هذا سيتم استكماله بدروس نظرية وأسئلة للخبراء ومنتديات مناقشة حول القضايا المثيرة للجدل وأعمال التفكير الفردية
- توفر المحتوى من أي جهاز ثابت أو محمول متصل بالإنترنت

ستفك تشفير كلمات المرور المخزنة على أجهزة الكمبيوتر وتتوقع هجمات القراصنة"

سوف تستكشف نموذج OSI وتفهم عمليات الاتصال في الأنظمة المتصلة بالشبكة. خلال 6 أشهر فقط!"

سوف تتعمق في نقاط ضعف DOM وتمنع الهجمات المتقدمة باستخدام الاستراتيجيات الأكثر فعالية.

انسى حفظ المناهج الدراسية!" مع منهجية إعادة التعلّم سوف تدمج المفاهيم بطريقة طبيعية وتدريجية.

البرنامج يضم أعضاء هيئة تدريس محترفين يصبون في هذا التدريب خبرة عملهم، بالإضافة إلى متخصصين معترف بهم من الشركات الرائدة والجامعات المرموقة.

سيتيح محتوى البرنامج المتعدد الوسائط، والذي صيغ بأحدث التقنيات التعليمية، للمهني التعلم السياقي والموقعي، أي في بيئة محاكاة توفر تدريبا غامرا مبرمجا للتدريب في حالات حقيقية.

يركز تصميم هذا البرنامج على التعلّم القائم على حل المشكلات، والذي يجب على المهني من خلاله محاولة حل مختلف مواقف الممارسة المهنية التي تنشأ على مدار العام الدراسي. للقيام بذلك، سيحصل على مساعدة من نظام فيديو تفاعلي مبتكر من قبل خبراء مشهورين.

02

الأهداف

سوف تتعمق هذه المحاضرة الدراسية في تقنيات القرصنة المتقدمة التي تستهدف خدمات الويب، مما يمكّن المحترفين من تنفيذ الاستراتيجيات الأكثر فعالية قبل وقوع هجمات القرصنة. لتحقيق ذلك، سيتم تحليل المبادئ الأساسية لتصميم الشبكة وتحديد نقاط الضعف المشتركة. بهذه الطريقة، سيقدم الخريجون الحلول الأكثر ابتكاراً ويبرزون في قطاع رقمي يتقدم بسرعة فائقة.

هل تريد تأمين الشبكة والبيانات المرسلة عليها؟ سوف تتقن التحويل switching في أفضل جامعة رقمية في العالم، وفقًا لمجلة "Forbes

الأهداف العامة

- الأهداف العامة لاكتساب مهارات متقدمة في اختبار الاختراق ومحاكاة فريق الشبكة، ومعالجة ومحاكاة Red Team، ومعالجة تحديد واستغلال نقاط الضعف في الأنظمة والشبكات
- تطوير المهارات القيادية لتنسيق الفرق المتخصصة في الأمن السيبراني الهجومي، وتحسين تنفيذ مشاريع فريق الاختبار الخماسي وفريق الشبكة
- تطوير المهارات في تحليل وتطوير البرمجيات الخبيثة وفهم وظائفها وتطبيق الاستراتيجيات الدفاعية والتعليمية
- صقل مهارات التواصل من خلال إنتاج تقارير تقنية وتنفيذية مفصلة، وعرض النتائج بفعالية على الجمهور التقني والتنفيذي
- تعزيز الممارسة الأخلاقية والمسؤولة في مجال الأمن السيبراني، مع مراعاة المبادئ الأخلاقية والقانونية في جميع الأنشطة
- إبقاء الطلاب على اطلاع دائم بالاتجاهات والتقنيات الناشئة في مجال الأمن السيبراني

الأهداف المحددة

الوحدة 1. قرصنة الويب المتقدمة

- تطوير مهارات تحديد وتقييم نقاط الضعف في تطبيقات الويب، بما في ذلك حقن SQL، والبرمجة النصية عبر المواقع (XSS)، وغيرها من نواقل الهجوم الشائعة
- تعلّم كيفية إجراء اختبارات الأمان على تطبيقات الويب الحديثة
- اكتساب مهارات في تقنيات اختراق الويب المتقدمة، واستكشاف استراتيجيات التحايل على التدابير الأمنية واستغلال الثغرات الأمنية المتطورة
- تعريف الخريج بتقييم الأمن في واجهات برمجة التطبيقات وخدمات الويب، وتحديد نقاط الضعف المحتملة وتعزيز الأمن في واجهات البرمجة
- تطوير المهارات اللازمة لتنفيذ تدابير التخفيف الفعّالة في تطبيقات الويب، والحد من التعرض للهجمات وتعزيز الأمن
- المشاركة في المحاكاة العملية لتقييم الأمن في بيئات الويب المعقدة، وتطبيق المعرفة في مواقف العالم الحقيقي
- تطوير الكفاءات في صياغة استراتيجيات دفاعية فعالة لحماية تطبيقات الويب من التهديدات الإلكترونية
- تعلّم كيفية مواءمة ممارسات اختراق الويب المتقدمة مع اللوائح والمعايير الأمنية ذات الصلة، بما يضمن الالتزام بالأطر القانونية والأخلاقية
- تعزيز التعاون الفعال بين فرق التطوير وفرق الأمن

> ستطبق أكثر التدابير الأمنية فعالية وتتجنب الثغرات الأمنية مثل المصادقة المعطلة. سجل الآن!"

الوحدة 2. بنية الشبكات وأمنها

- اكتساب معرفة متقدمة ببنية الشبكة، بما في ذلك الطوبولوجيات والبروتوكولات والمكونات الرئيسية
- تطوير المهارات اللازمة لتحديد وتقييم نقاط الضعف المحددة في البنى التحتية للشبكة، مع مراعاة التهديدات المحتملة.
- تعلّم كيفية تنفيذ تدابير أمنية فعّالة للشبكة، بما في ذلك جدران الحماية وأنظمة كشف التسلل (IDS) وتجزئة الشبكة
- تعريف الطالب بتقنيات الشبكات الناشئة، مثل الشبكات المعرفة بالبرمجيات (SDN)، وفهم تأثيرها على الأمن
- تطوير المهارات في تأمين اتصالات الشبكة، بما في ذلك الحماية من التهديدات مثل sniffing وهجمات الوسطاء
- التعرف على كيفية تقييم تكوينات الأمان وتحسينها في بيئات شبكات المؤسسات، بما يضمن توفير الحماية الكافية
- تطوير المهارات اللازمة لتنفيذ تدابير التخفيف الفعالة ضد التهديدات التي تتعرض لها شبكات المؤسسات، بدءاً من الهجمات الداخلية وحتى التهديدات الخارجية
- تعزيز التعاون الفعال مع فرق الأمن، ودمج الاستراتيجيات والجهود المبذولة لحماية البنية التحتية للشبكة
- تعزيز الممارسات الأخلاقية والقانونية في تنفيذ تدابير أمن الشبكة، وضمان الالتزام بالمبادئ الأخلاقية في جميع الأنشطة

الوحدة 3. التقرير التقني والتنفيذي

- تطوير المهارات اللازمة لإعداد تقارير تقنية مفصلة، وعرض النتائج والمنهجيات المستخدمة والتوصيات بشكل واضح وشامل
- تعلم كيفية التواصل الفعال مع الجمهور التقني باستخدام لغة دقيقة ومناسبة لنقل المعلومات التقنية المعقدة
- تطوير المهارات اللازمة لصياغة توصيات عملية وقابلة للتنفيذ تهدف إلى التخفيف من نقاط الضعف وتحسين الوضع الأمني
- تعلم كيفية تقييم التأثير المحتمل لنقاط الضعف التي تم تحديدها، مع مراعاة الجوانب التقنية والتشغيلية والاستراتيجية
- إطلاع المتعلم على أفضل الممارسات لإعداد التقارير التنفيذية، وتكييف المعلومات التقنية للجمهور غير التقني
- تطوير الكفاءات لمواءمة النتائج والتوصيات مع الأهداف الاستراتيجية والتشغيلية للمؤسسة
- تعلّم كيفية استخدام أدوات عرض البيانات لتمثيل المعلومات الواردة في التقارير بيانياً، مما يسهل فهمها
- الترويج لإدراج المعلومات ذات الصلة بالامتثال للوائح والمعايير في التقارير، وضمان الالتزام بالمتطلبات القانونية
- تعزيز التعاون الفعال بين الفرق التقنية والتنفيذية، بما يضمن فهم ودعم إجراءات التحسين المقترحة في التقرير

03

هيكل الإدارة وأعضاء هيئة تدريس الدورة التدريبية

بهدف تقديم التميز التعليمي، جمعت TECH فريقاً تعليمياً يتمتع بخلفية مهنية واسعة في مجال الأمن السيبراني. مع أكثر من 13 عاماً من الخبرة، سيقدم هؤلاء المتخصصون النهج الأكثر شمولاً وأحدث الأدوات لتطوير بيئات افتراضية آمنة. بهذه الطريقة، سيحصل الطلاب على الضمانات التي يحتاجونها للتخصص في القطاع الرقمي الذي يوفر فرصاً متعددة.

سوف تتعمق في حدود مختبر الاختراقات Pentester بدعم من أفضل أعضاء هيئة التدريس. ستكون أنشطتك قانونية 100%!"

هيكل الإدارة

أ. Gómez Pintado, Carlos

- مدير فريق الأمن السيبراني والشبكات Cipherbit في Grupo Oesía
- Advisor إداري ومستثمر Investo في تطبيق Wesson App
- بكالوريوس في هندسة البرمجيات وتقنيات مجتمع المعلومات، جامعة مدريد التقنية السياسية
- التعاون مع المؤسسات التعليمية لتطوير دورات تدريبية عالية المستوى في مجال الأمن السيبراني

الأساتذة

أ. Siles Rubia, Marcelino

- Cibersecurity Engineer
- هندسة الأمن السيبراني في جامعة Rey Juan Carlos
- خبرته: البرمجة التنافسية Hacking Web, Active Directory و Malware Development
- فائز في مسابقة AdaByron

أ. Redondo Castro, Pablo

- خبير اختراقات Pentester في مجموعة Oesía
- مهندس الأمن السيبراني من جامعة Rey Juan Carlos
- خبرة واسعة في *Cibersecurity Evaluator Traineev*
- يكتسب خبرة في التدريس، حيث يقدم دورات تدريبية متعلقة ببطولات التقاط العلم

أ. Villaverde, David

- مستشار الأمن السيبراني في Cipherbit
- خبير منصات تحدي القرصنة HackTheBoxg
- أخصائي اختبارات الاختراق
- خبير البرمجيات الخبيثة
- مهندس برمجيات متخصص في الأمن السيبراني من المركز الجامعي للتكنولوجيا والفنون الرقمية في Las Rozas

أ. Castillo, Carlos

- Cybersecurity Consultant y Red Teamer en Cipherbit
- Offensive Security Wireless Professional
- eLearnSecurity Web Application Penetration Tester
- eLearnSecurity Certified Professional Penetration Tester v٢
- eLearnSecurity Junior Penetration Tester
- استشاري الأمن السيبراني
- مهندس البرمجيات من من جامعة Politécnica بمدريد

"سوف تكتسب المعرفة دون قيود جغرافية أو توقيت محدد مسبقًا"

04

الهيكل والمحتوى

يتألف هذا البرنامج من 3 وحدات شاملة: قرصنة الويب Hacking Web المتقدمة، وبنية الشبكات وأمنها، والتقارير التقنية والتنفيذية. وبدعم من أعضاء هيئة التدريس المخضرمين، سيتم تناول التكتيكات المتقدمة لتأمين شبكات المؤسسات من خلال تنفيذ جدران الحماية firewalls. كما سيتم مواصلة تطوير الكشف عن الاختراق، بما في ذلك HHTP Request Smuggling. ستتم مناقشة أهمية شبكات النطاقات المحلية الافتراضية VLANs لفصل حركة مرور البيانات في نفس البيئة الافتراضية، وسيتم استكشاف عملية إعداد التقارير من أجل تقديم تقارير دقيقة ومفصلة.

ستصل إلى نظام تعليمي يعتمد على التكرار، مع التدريس
الطبيعي والتقدمي في جميع أنحاء المنهج الدراسي بأكمله"

الوحدة 1. قرصنة الويب المتقدمة

1.1. طريقة عمل الموقع الإلكتروني
1.1.1. عنوان URL وأجزاؤه
2.1.1. طرق HTTP
3.1.1. رؤوس الصفحات
4.1.1. كيفية عرض طلبات الويب باستخدام حزمة Burp Suite
2.1. الحسابات
1.2.1. ملفات تعريف الارتباط
2.2.1. رموز JWT Tokens
3.2.1. هجمات سرقة الحسابات
4.2.1. هجمات JWT
3.1. *Cross Site Scripting*(XSS)
1.3.1. ما هو ال XSS؟
2.3.1. أنواع XSS
3.3.1. استغلال XSS
4.3.1. مقدمة في *XSLeaks*
4.1. الضخ إلى قاعدة البيانات
1.4.1. ما هو حقن *SQL*
2.4.1. استخراج المعلومات باستخدام *SQLi*
3.4.1. *SQLi Blind, Time-Based y Error-Based*
4.4.1. حقن NoSQLi
5.1. Path Traversal y Local File Inclusion
1.5.1. ماهيتهما واختلافاتهما
2.5.1. المرشحات الشائعة وكيفية تجاوزها
3.5.1. Log poisoning
4.5.1. LFIs en PHP
6.1. Broken Authentication
1.6.1. User Enumeration
2.6.1. Password Bruteforce
3.6.1. FA Bypass2
4.6.1. ملفات تعريف Cookies الارتباط التي تحتوي على معلومات حساسة وقابلة للتعديل
7.1. Remote Command Execution
1.7.1. Command Injection
2.7.1. Blind Command Injection
3.7.1. *Insecure deserialization* PHP
4.7.1. *Insecure deserialization* Java

8.1. *File Uploads*
1.8.1. Remote Code Execution عبر *webshells*
2.8.1. XSS في تحميل الملفات
3.8.1. XML External Entity (XXE) Injection
4.8.1. اجتياز المسار Path traversal في تحميل الملفات
9.1. التحكم في الوصول المعطل
1.9.1. الوصول غير المقيد إلى اللوحات
2.9.1. Insecure direct object references (IDOR)
3.9.1. تجاوز المرشح
4.9.1. طرق التفويض غير كافية
10.1. نقاط ضعف DOM والهجمات الأكثر تقدمًا
1.10.1. *Regex Denial of Service*
2.10.1. DOM *Clobbering*
3.10.1. *Prototype Pollution*
4.10.1. HTTP *Request Smuggling*

الوحدة 2. بنية الشبكات وأمنها

1.2. شبكات الحاسوب
1.1.2. مفاهيم أساسية: بروتوكولات LAN, WAN, CP, CC
2.1.2. نموذج OSI TCP / IP
3.1.2. *Switching*. مفاهيم أساسية
4.1.2. *Routing*. مفاهيم أساسية
2.2. *Switching*
1.2.2. مقدمة في VLAN's
2.2.2. بروتوكول الشجرة المتفرعة STP
3.2.2. *EtherChannel*
4.2.2. الهجمات على الطبقة 2
3.2. الشبكات المحلية الافتراضية VLAN´s
1.3.2. أهمية الشبكات المحلية الافتراضية VLAN
2.3.2. ثغرات الشبكات المحلية الافتراضية VLAN's
3.3.2. الهجومات الشائعة في VLAN
4.3.2. تخفيف الآثار
4.2. *Routing*
1.4.2. عنونة IPv - 4IP و 6IPv
2.4.2. التوجيه: المفاهيم الرئيسية
3.4.2. التوجيه الثابت
4.4.2. التوجيه الديناميكي: المقدمة
5.2. بروتوكول IGP
1.5.2. Routing Information Protocol RIP
2.5.2. Open Shortest Path First OSPF
3.5.2. مقابلOSPF RIP
4.5.2. تحليل احتياجات الطوبولوجيا
6.2. الحماية المحيطية
1.6.2. المناطق العازلة DMZs
2.6.2. **جدران الحماية**
3.6.2. البنى الشائعة
4.6.2. Zero Trust Network Access
7.2. IPS (Intrusion Prevention System) و IDS (Intrusion Detection System)
1.7.2. الخصائص
2.7.2. التنفيذ
3.7.2. SIEM و SIEM CLOUDS
4.7.2. الكشف المستند إلى *HoneyPots*
8.2. TLS وشبكات VPN
1.8.2. SSL/TLS
2.8.2. TLS: الهجمات الشائعة
3.8.2. شبكات VPN مع TLS
4.8.2. شبكات VPN مع IPSEC
9.2. أمان الشبكة اللاسلكية
1.9.2. مقدمة إلى الشبكات اللاسلكية
2.9.2. بروتوكولات
3.9.2. العناصر الرئيسية
4.9.2. الهجمات الشائعة
10.2. شبكات الأعمال وكيفية التعامل معها
1.10.2. التقسيم المنطقي
2.10.2. التقسيم المادي
3.10.2. التحكم في الوصول
4.10.2. التدابير الأخرى التي يجب أخذها في الاعتبار

الوحدة 3. التقرير التقني والتنفيذي

1.3. عملية إعداد التقارير
1.1.3. هيكل التقرير
2.1.3. عملية إعداد التقارير
3.1.3. المفاهيم الرئيسية
4.1.3. تنفيذي مقابل تقني
2.3. الدليل
1.2.3. المقدمة
2.2.3. أنواع الدلائل
3.2.3. الدلائل الإرشادية الوطنية
4.2.3. حالات الاستخدام
3.3. المنهجيات
1.3.3. التقييم
2.3.3. أختبارات الاختراق
3.3.3. مراجعة المنهجيات الشائعة
4.3.3. مقدمة في المنهجيات الوطنية
4.3. النهج التقني لمرحلة إعداد التقارير
1.4.3. فهم حدود مختبر الاختراق pentester
2.4.3. استخدام اللغة والإشارات
3.4.3. عرض المعلومة
4.4.3. الأخطاء الشائعة
5.3. النهج التنفيذي لمرحلة إعداد التقارير
1.5.3. تكييف التقرير مع السياق
2.5.3. استخدام اللغة والإشارات
3.5.3. التوحيد القياسي
4.5.3. الأخطاء الشائعة
6.3. Open Source Security Testing Methodology Manual, OSSTMM
1.6.3. فهم المنهجية
2.6.3. الاعتراف
3.6.3. الوثائق
4.6.3. صياغة التقرير

7.3. شهادة LINCE
1.7.3. فهم المنهجية
2.7.3. الاعتراف
3.7.3. الوثائق
4.7.3. صياغة التقرير
8.3 الإبلاغ عن الثغرات الأمنية
1.8.3. المفاهيم الرئيسية
2.8.3. تحديد النطاق الكمي
3.8.3. نقاط الضعف والأدلة
4.8.3. الأخطاء الشائعة
9.3 تركيز التقرير على العميل
1.9.3. أهمية اختبارات العمل
2.9.3. الحلول والتخفيف
3.9.3. البيانات الحساسة و المهمة
4.9.3. أمثلة عملية وحالات
10.3. الإبلاغ عن retakes
1.10.3. المفاهيم الرئيسية
2.10.3. فهم المعلومات الموروثة
3.10.3. التحقق من الأخطاء
4.10.3. إضافة المعلومات

05

المنهجية

يقدم هذا البرنامج التدريبي طريقة مختلفة للتعلم. فقد تم تطوير منهجيتنا من خلال أسلوب التعليم المرتكز على التكرار: ***Relearning*** أو ما يعرف بمنهجية إعادة التعلم.

يتم استخدام نظام التدريس هذا، على سبيل المثال، في أكثر كليات الطب شهرة في العالم، وقد تم اعتباره أحد أكثر المناهج فعالية في المنشورات ذات الصلة مثل مجلة نيو إنجلند الطبية ***(New England Journal of Medicine)***.

اكتشف منهجية *Relearning* (منهجية إعادة التعلم)، وهي نظام يتخلى عن التعلم الخطي التقليدي ليأخذك عبر أنظمة التدريس التعليم المرتكزة على التكرار: إنها طريقة تعلم أثبتت فعاليتها بشكل كبير، لا سيما في المواد الدراسية التي تتطلب الحفظ"

منهج دراسة الحالة لوضع جميع محتويات المنهج في سياقها المناسب

يقدم برنامجنا منهج ثوري لتطوير المهارات والمعرفة. هدفنا هو تعزيز المهارات في سياق متغير وتنافسي ومتطلب للغاية.

مع جامعة TECH يمكنك تجربة طريقة تعلم تهز أسس الجامعات التقليدية في جميع أنحاء العالم"

سيتم توجيهك من خلال نظام التعلم القائم على إعادة التأكيد على ما تم تعلمه، مع منهج تدريس طبيعي وتقدمي على طول المنهج الدراسي بأكمله.

منهج تعلم مبتكرة ومختلفة

إن هذا البرنامج المُقدم من خلال TECH هو برنامج تدريس مكثف، تم خلقه من الصفر، والذي يقدم التحديات والقرارات الأكثر تطلبًا في هذا المجال، سواء على المستوى المحلي أو الدولي. تعزز هذه المنهجية النمو الشخصي والمهني، متخذة بذلك خطوة حاسمة نحو تحقيق النجاح. ومنهج دراسة الحالة، وهو أسلوب يرسي الأسس لهذا المحتوى، يكفل اتباع أحدث الحقائق الاقتصادية والاجتماعية والمهنية.

> يعدك برنامجنا هذا لمواجهة تحديات جديدة في بيئات غير مستقرة ولتحقيق النجاح في حياتك المهنية"

كان منهج دراسة الحالة هو نظام التعلم الأكثر استخدامًا من قبل أفضل كليات الحاسبات في العالم منذ نشأتها. تم تطويره في عام 1912 بحيث لا يتعلم طلاب القانون القوانين بناءً على المحتويات النظرية فحسب، بل اعتمد منهج دراسة الحالة على تقديم مواقف معقدة حقيقية لهم لاتخاذ قرارات مستنيرة وتقدير الأحكام حول كيفية حلها. في عام 1924 تم تحديد هذه المنهجية كمنهج قياسي للتدريس في جامعة هارفارد.

أمام حالة معينة، ما الذي يجب أن يفعله المهني؟ هذا هو السؤال الذي سنواجهك بها في منهج دراسة الحالة، وهو منهج تعلم موجه نحو الإجراءات المتخذة لحل الحالات. طوال المحاضرة الجامعية، سيواجه الطلاب عدة حالات حقيقية. يجب عليهم دمج كل معارفهم والتحقيق والجدال والدفاع عن أفكارهم وقراراتهم.

سيتعلم الطالب،من خلال الأنشطة التعاونية والحالات الحقيقية، حل المواقف المعقدة في بيئات الأعمال الحقيقية.

منهجية إعادة التعلم *(Relearning)*

تجمع جامعة TECH بين منهج دراسة الحالة ونظام التعلم عن بعد، 100٪ عبر الانترنت والقائم على التكرار، حيث تجمع بين عناصر مختلفة في كل درس.

نحن نعزز منهج دراسة الحالة بأفضل منهجية تدريس 100٪ عبر الانترنت في الوقت الحالي وهي: منهجية إعادة التعلم والمعروفة بـ *Relearning*.

في عام 2019، حصلنا على أفضل نتائج تعليمية متفوقين بذلك على جميع الجامعات الافتراضية الناطقة باللغة الإسبانية في العالم.

في TECH ستتعلم بمنهجية رائدة مصممة لتدريب مدراء المستقبل. وهذا المنهج، في طليعة التعليم العالمي، يسمى *Relearning* أو إعادة التعلم.

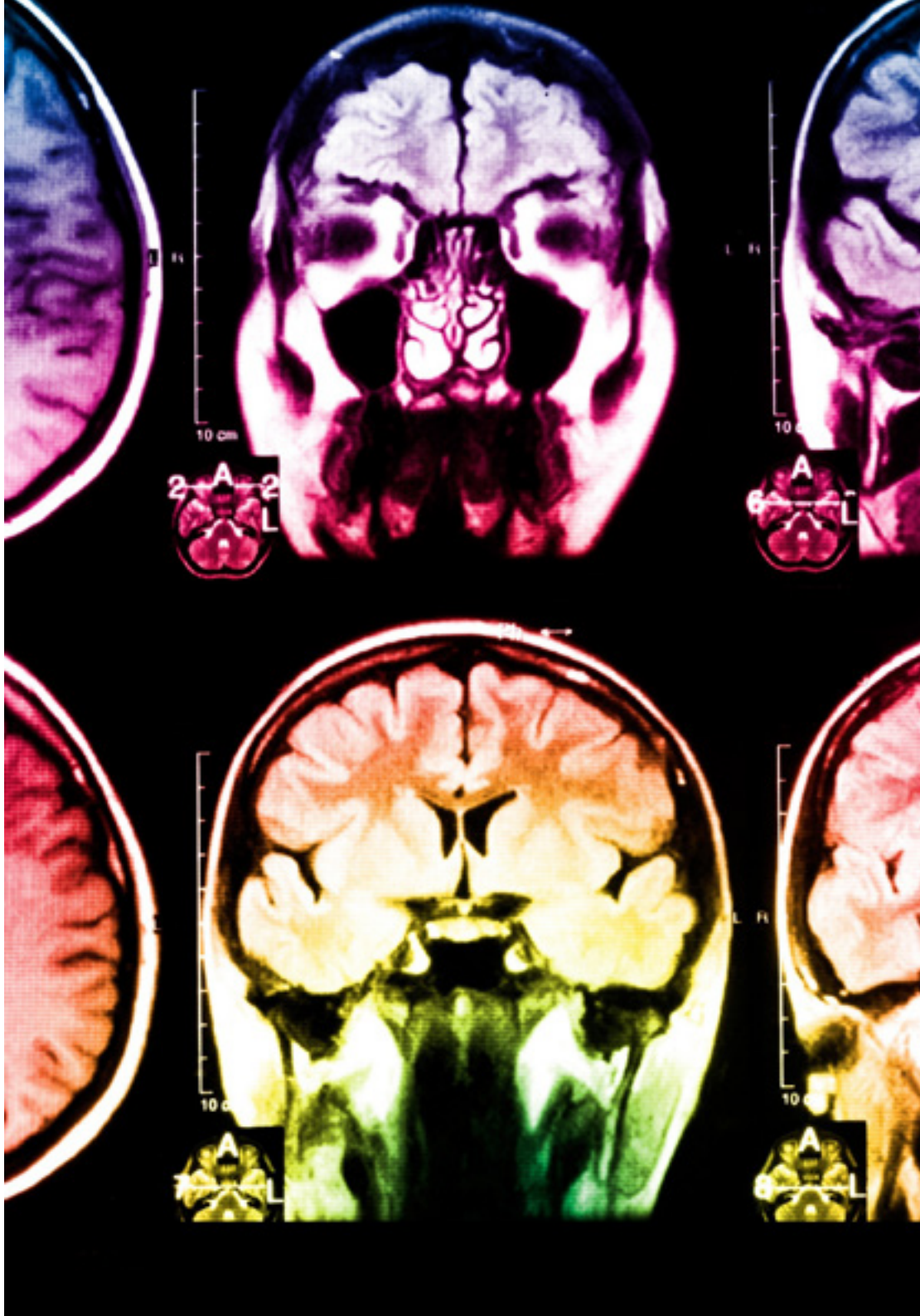
جامعتنا هي الجامعة الوحيدة الناطقة باللغة الإسبانية المصرح لها لاستخدام هذا المنهج الناجح. في عام 2019، تمكنا من تحسين مستويات الرضا العام لطلابنا من حيث (جودة التدريس، جودة المواد، هيكل الدورة، الأهداف..) فيما يتعلق بمؤشرات أفضل جامعة عبر الإنترنت باللغة الإسبانية.

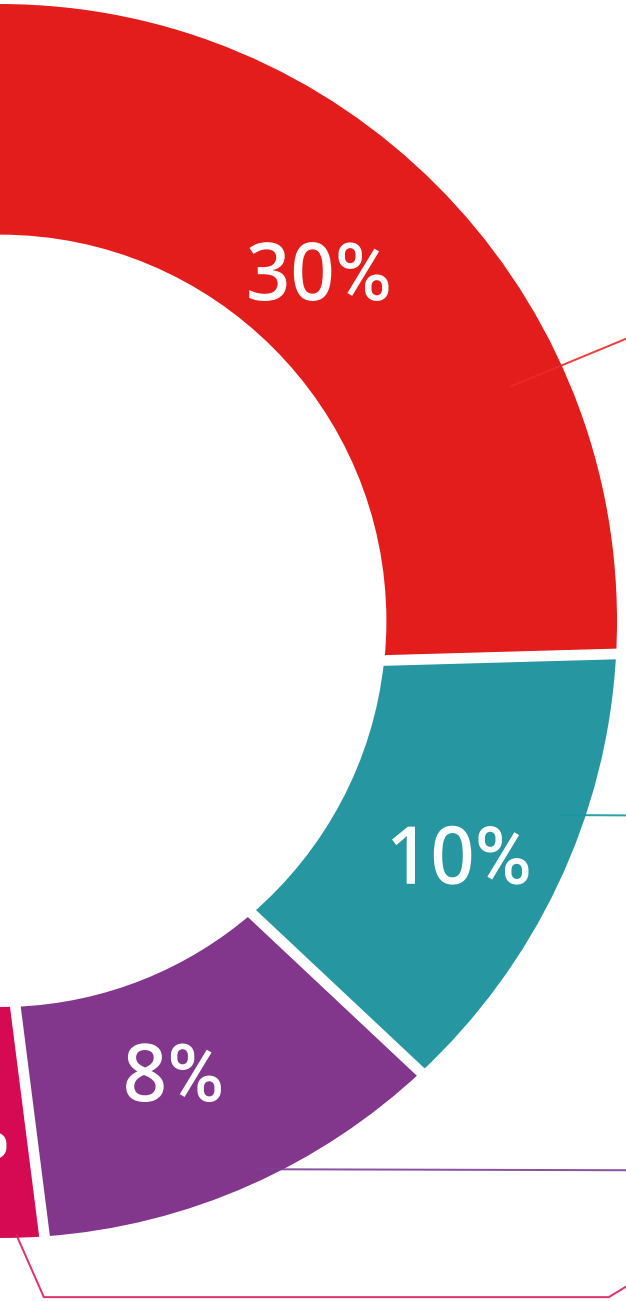
في برنامجنا، التعلم ليس عملية خطية، ولكنه يحدث في شكل لولبي (نتعلّم ثم نطرح ماتعلمناه جانبًا فننساه ثم نعيد تعلمه). لذلك، نقوم بدمج كل عنصر من هذه العناصر بشكل مركزي. باستخدام هذه المنهجية، تم تدريب أكثر من 650000 خريج جامعي بنجاح غير مسبوق في مجالات متنوعة مثل الكيمياء الحيوية، وعلم الوراثة، والجراحة، والقانون الدولي، والمهارات الإدارية، وعلوم الرياضة، والفلسفة، والقانون، والهندسة، والصحافة، والتاريخ، والأسواق والأدوات المالية. كل ذلك في بيئة شديدة المتطلبات، مع طلاب جامعيين يتمتعون بمظهر اجتماعي واقتصادي مرتفع ومتوسط عمر يبلغ 43.5 عاماً.

ستتيح لك منهجية إعادة التعلم والمعروفة بـ *Relearning*، التعلم بجهد أقل ومزيد من الأداء، وإشراكك بشكل أكبر في تدريبك، وتنمية الروح النقدية لديك، وكذلك قدرتك على الدفاع عن الحجج والآراء المتباينة: إنها معادلة واضحة للنجاح.

استنادًا إلى أحدث الأدلة العلمية في مجال علم الأعصاب، لا نعرف فقط كيفية تنظيم المعلومات والأفكار والصور والذكريات، ولكننا نعلم أيضًا أن المكان والسياق الذي تعلمنا فيه شيئًا هو ضروريًا لكي نكون قادرين على تذكرها وتخزينها في الحُصين بالمخ، لكي نحتفظ بها في ذاكرتنا طويلة المدى.

بهذه الطريقة، وفيما يسمى التعلم الإلكتروني المعتمد على السياق العصبي، ترتبط العناصر المختلفة لبرنامجنا بالسياق الذي يطور فيه المشارك ممارسته المهنية.





يقدم هذا البرنامج أفضل المواد التعليمية المُعَدَّة بعناية للمهنيين:

المواد الدراسية

يتم إنشاء جميع محتويات التدريس من قبل المتخصصين الذين سيقومون بتدريس البرنامج الجامعي، وتحديداً من أجله، بحيث يكون التطوير التعليمي محددًا وملموسًا حقًا.

ثم يتم تطبيق هذه المحتويات على التنسيق السمعي البصري الذي سيخلق منهج جامعة TECH في العمل عبر الإنترنت. كل هذا بأحدث التقنيات التي تقدم أجزاء عالية الجودة في كل مادة من المواد التي يتم توفيرها للطالب.

المحاضرات الرئيسية

هناك أدلة علمية على فائدة المراقبة بواسطة الخبراء كطرف ثالث في عملية التعلم.

إن مفهوم ما يسمى *Learning from an Expert* أو التعلم من خبير يقوي المعرفة والذاكرة، ويولد الثقة في القرارات الصعبة في المستقبل.

التدريب العملي على المهارات والكفاءات

سيقومون بتنفيذ أنشطة لتطوير مهارات وقدرات محددة في كل مجال مواضيعي. التدريب العملي والديناميكيات لاكتساب وتطوير المهارات والقدرات التي يحتاجها المتخصص لنموه في إطار العولمة التي نعيشها.

قراءات تكميلية

المقالات الحديثة، ووثائق اعتمدت بتوافق الآراء، والأدلة الدولية. من بين آخرين. في مكتبة جامعة TECH الافتراضية، سيتمكن الطالب من الوصول إلى كل ما يحتاجه لإكمال تدريبه.

دراسات الحالة (Case studies)

سيقومون بإكمال مجموعة مختارة من أفضل دراسات الحالة المختارة خصيصًا لهذا المؤهل. حالات معروضة ومحللة ومدروسة من قبل أفضل المتخصصين على الساحة الدولية.

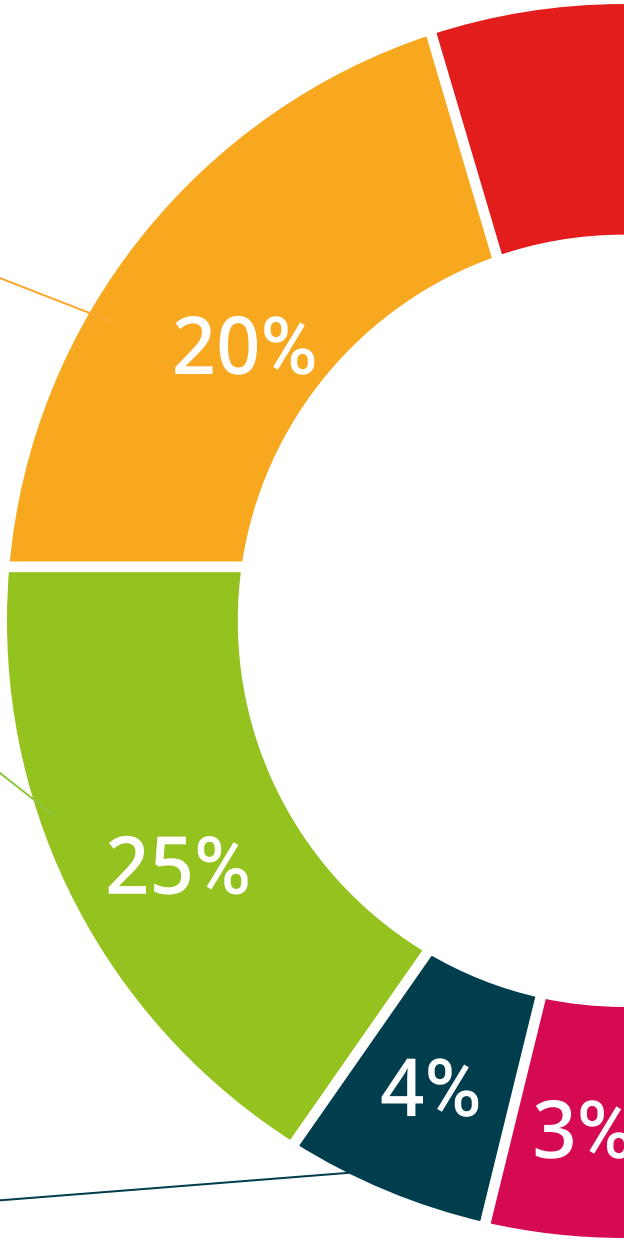
ملخصات تفاعلية

يقدم فريق جامعة TECH المحتويات بطريقة جذابة وديناميكية في أقراص الوسائط المتعددة التي تشمل الملفات الصوتية والفيديوهات والصور والرسوم البيانية والخرائط المفاهيمية من أجل تعزيز المعرفة.

اعترفت شركة مايكروسوف بهذا النظام التعليمي الفريد لتقديم محتوى الوسائط المتعددة على أنه "قصة نجاح أوروبية"

الاختبار وإعادة الاختبار

يتم بشكل دوري تقييم وإعادة تقييم معرفة الطالب في جميع مراحل البرنامج، من خلال الأنشطة والتدريبات التقييمية وذاتية التقييم: حتى يتمكن من التحقق من كيفية تحقيق أهدافه.



06

المؤهل العلمي

تضمن شهادة الخبرة الجامعية في قرصنة الويب المتقدمة التدريب الأكثر دقة وحداثة بالإضافة إلى الحصول على مؤهل شهادة الخبرة الجامعية الصادر عن TECH الجامعة التكنولوجية.

اجتاز هذا البرنامج بنجاح واحصل على شهادتك الجامعية
دون الحاجة إلى السفر أو القيام بأية إجراءات مرهقة"

تحتوي **شهادة الخبرة الجامعية في قرصنة الويب المتقدمة** على البرنامج الأكثر اكتمالا وحداثة في السوق.

بعد اجتياز التقييم، سيحصل الطالب عن طريق البريد العادي* مصحوب بعلم وصول مؤهل **شهادة الخبرة الجامعية** الصادرعن **TECH الجامعة التكنولوجية**.

إن المؤهل الصادرعن **TECH الجامعة التكنولوجية** سوف يشير إلى التقدير الذي تم الحصول عليه في برنامج المحاضرة الجامعية وسوف يفي بالمتطلبات التي عادة ما تُطلب من قبل مكاتب التوظيف ومسابقات التعيين ولجان التقييم الوظيفي والمهني.

المؤهل العلمي: **شهادة الخبرة الجامعية في قرصنة الويب المتقدمة**

اطريقة: **عبر الإنترنت**

مدة: **6 أشهر**


tech الجامعة التكنولوجية

شهادة تخرج

هذه الشهادة ممنوحة إلى

لـ

المواطن/المواطنة ..... مع وثيقة تحقيق شخصية رقم .....

لاجتيازه/لاجتيازها بنجاح والحصول على برنامج

شهادة الخبرة الجامعية

في

قرصنة الويب المتقدمة

وهي شهادة خاصة من هذه الجامعة موافقة لـ 450
ساعة، مع تاريخ بدء يوم/شهر/ سنة وتاريخ انتهاء يوم/شهر/سنة

تيك مؤسسة خاصة للتعليم العالي معتمدة من وزارة التعليم العام منذ 28 يونيو 2018

في تاريخ 17 يونيو 2020

الكود الفريد الخاص بجامعة TECH: AFWOR23S techtitute.com/certificates

*تصديق لاهاي أبوستيل. في حالة قيام الطالب بالتقدم للحصول على درجته العلمية الورقية وبتصديق لاهاي أبوستيل، ستتخذ مؤسسة TECH EDUCATION الإجراءات المناسبة لكي يحصل عليها وذلك بتكلفة إضافية.

الجامعة التيكنولوجية

شهادة الخبرة الجامعية
قرصنة الويب المتقدمة

- طريقة التدريس: **أونلاين**
- مدة الدراسة: **6 اشهر**
- المؤهل الجامعي من: **TECH الجامعة التكنولوجية**
- مواعيد الدراسة: **وفقًا لوتيرتك الخاصّة**
- الامتحانات: **أونلاين**

شهادة الخبرة الجامعية
قرصنة الويب المتقدمة

tech الجامعة التيكنولوجية