专科文凭
进攻型网络安全

tech 科学技术大学

tech 科学技术大学

专科文凭
进攻型网络安全

- 模式:**在线**
- 时长: **6个月**
- 学位: **TECH 科技大学**
- 课程表:**自由安排时间**
- 考试模式:**在线**

网页链接: www.techtitute.com/cn/information-technology/postgraduate-diploma/postgraduate-diploma-offensive-cybersecurity

目录

01

介绍

网络安全是机构保护其数字资产、维护其社会声誉和防范竞争对手间谍活动的一个重要方面。因此，越来越多的公司要求在其组织结构图中加入信息技术专家，以避免可能影响其财务能力的后果。在这种情况下，这些专家需要不断更新知识和技能，以跟上网络犯罪技术的发展。为此，TECH 开发了一个创新的专科文凭系统，在该系统中，威胁将被识别并得到缓解。值得注意的是，整个课程将采用 100% 在线教学模式，以确保学生获得更大的便利性和灵活性。

你将进一步了解 Kerberos 协议，并在网络环境中保护信息"

媒体每天都在报道黑客通过访问数据库破坏机构的案例。这些攻击造成的后果非常严重，会扰乱业务活动，使企业无法有效运作。事实上，它会直接影响经济，导致因不遵守法规和收入限制而被罚款。

从这个意义上说，TECH 已经创建了一个最先进的资格证书，用于检测最常用的入侵技术以及应对这些技术的最佳策略。在经验丰富的教学人员的指导下，教学大纲将为了解黑客的思维方式奠定重要基础。它还将提供各种解决方案，旨在为企业网络中的数字证书管理提供安全的基础设施。

同样，专业人员还将通过配置虚拟机或快照来优化虚拟环境的准备工作。此外，还将分析恶意软件，使用 API Monitor 探测调用，并使用 TCPView 观察网络请求。毕业生将在模拟环境中学习理论概念，为应对进攻型网络安全领域的现实挑战做好准备。最后，将强调该领域专家应具备的职业道德和社会责任。

为了巩固对所有这些内容的掌握，专科文凭采用了创新的 Relearning系统。TECH 率先采用这种教学模式，通过自然和循序渐进的重复，促进对复杂概念的吸收。这个课程还利用各种形式的材料，如解释性视频、互动摘要和信息图表。所有这一切都采用方便的 100% 在线模式，使每个人都能根据自己的职责和时间调整时间表。

这个**进攻型网络安全专科文凭**包含市场上最完整、最新的教育课程。主要特点是：

- 由进攻型网络安全专家介绍案例研究的发展情况
- 本书的内容图文并茂、示意性强、实用性强，为专业实践所必需的学科提供了完整而实用的信息
- 可以进行自我评估过程的实践，以推进学习
- 其特别强调创新方法
- 理论课、向专家提问、关于有争议问题的讨论区和这个反思性论文
- 可以从任何有互联网连接的固定或便携式设备上获取内容

> 在最负盛名的数字公司中发展你作为进攻型审计员的技能，迎接新的职业挑战"

你将通过 TECH 的教学工具(包括讲解视频和互动摘要)实现目标”

想成为大赏金猎人吗?有了这个程序,你就可以捕捉到互联网上的任何漏洞。

只需 6 个月,你就能掌握 Azure AD 中的身份管理。现在就报名!

这个课程的教学人员包括来自该行业的专业人士,他们将自己的工作经验融入到培训中,还有来自知名协会和著名大学的公认专家。

其多媒体内容采用最新的教育技术开发,将使专业人员能够进行情景式学习,即在模拟环境中提供身临其境的培训程序,在真实情况下进行培训。

这个课程的设计重点是基于问题的学习,藉由这种学习,专业人员必须努力解决整个学年出现的不同的专业实践情况。为此,你将获得由知名专家制作的新型交互式视频系统的帮助。

02

目标

该课程的设计提供了一种独特的教育体验，以其实用和创新的网络安全方法脱颖而出。通过这种方式，学生将学习到从漏洞分析到高级入侵技术的所有知识。在这方面，将提供评估和加强不同网络系统的最佳措施。此外，还将强调该领域专家必须承担的法律和道德责任。

根据《福布斯》报道，利用世界上最好的数字大学减少恶意软件威胁"

总体目标

- 掌握渗透测试和 Red Team模拟的高级技能，识别并利用系统和网络中的漏洞
- 培养协调进攻型网络安全专业团队的领导技能，优化 Pentesting 和Red Team项目的执行
- 培养分析和开发恶意软件的技能，了解其功能并应用防御和教育策略
- 通过编写详细的技术和执行报告，向技术和执行受众有效地介绍研究结果，磨练沟通技能
- 促进网络安全领域的道德和责任实践，在所有活动中考虑道德和法律原则
- 让学生了解网络安全领域的最新趋势和技术

> 忘掉背书！通过 Relearning 系统，你将以自然、循序渐进的方式将概念融会贯通”

具体目标

模块1.进攻性网络安全

- 让毕业生熟悉渗透测试方法，包括信息收集、漏洞分析、利用和记录等关键阶段
- 培养使用专门的 Pentesting 识别和评估系统和网络漏洞的实际技能
- 研究和了解恶意行为者使用的战术、技术和程序，从而能够识别和模拟威胁
- 在实际场景和模拟中应用理论知识，面对真实挑战，强化 pentesting技能
- 培养有效的文档编制技能，编写详细报告，反映调查结果、使用的方法和安全改进建议
- 在进攻型安全团队中开展有效协作，优化 Pentesting活动的协调和执行

模块2.对Windows网络和系统的攻击

- 掌握识别和评估 Windows 操作系统中特定漏洞的技能
- 学习攻击者用来渗透和持续攻击基于 Windows 的网络的高级策略
- 掌握减轻针对 Windows 操作系统的特定威胁的策略和工具技能
- 使毕业生熟悉适用于 Windows 系统的取证分析技术，以便于识别和应对突发事件
- 在模拟环境中应用理论知识，参与实际操作，了解并应对针对 Windows 系统的特定攻击
- 考虑到企业基础设施的复杂性，学习保护使用 Windows 操作系统的企业环境安全的具体策略
- 培养评估和改进 Windows 系统安全配置的能力，确保实施有效的措施
- 考虑到网络安全的道德原则，在对 Windows 系统实施攻击和测试时推广道德和法律实践
- 让学员了解 Windows 系统攻击的最新趋势和威胁，确保所学技能的持续相关性和有效性

模块3. 恶意软件分析与开发

- 掌握有关 恶意软件的性质、功能和行为的高级知识，了解其各种形式和目标
- 培养应用于 恶意软件的取证分析技能，从而能够识别入侵指标（IoC）和攻击模式
- 学习有效检测和预防 恶意软件的策略，包括部署高级安全解决方案
- 让学员熟悉用于教育和防御目的的 恶意软件 开发，全面了解攻击者使用的策略
- 促进恶意软件分析和开发中的道德和法律实践，确保所有活动的诚信和问责
- 在模拟环境中应用理论知识，参与实践练习，了解并应对恶意攻击
- 培养评估和选择
  反恶意软件安全工具的技能，考虑其有效性和对特定环境的适应性
- 了解如何针对恶意威胁实施有效的缓解措施，减少 恶意软件 对系统和网络的影响和传播
- 促进与安全团队的有效合作，整合战略和工作，防范 恶意软件威胁
- 让毕业生了解 恶意软件分析和开发的最新趋势和技术，确保所学技能的持续相关性和有效性

03

课程管理

TECH 致力于提供卓越的教育，拥有一支声誉卓著的教师队伍。应该指出的是，这些专家拥有广泛的专业背景，曾是致力于进攻型网络安全的知名公司的一员。因此，学术行程将包括该领域最先进的资源和技术。此外，还将提供一种全面的方法，以满足毕业生的期望，使他们能够专门从事一个能为他们提供许多机会的领域。

杰出的进攻型网络安全专业人员将为你提供支持"

管理人员

Gómez Pintado, Carlos 先生

- 网络安全和网络团队 Cipherbit 经理 (Grupo Oesía
- Wesson App 管理 顾问 兼 投资者
- 马德里理工大学软件工程与信息社会技术专业毕业
- 与教育机构合作开发网络安全高级培训周期

教师

González Parrilla, Yuba 先生

- 进攻安全线和网络小组协调员
- 项目管理研究所 预测 项目管理专家
- 智能防御专家
- eLearnSecurity 网络应用程序渗透测试 专家
- eLearnSecurity初级渗透测试员
- 毕业于马德里理工大学计算机工程专业

Gallego Sánchez, Alejandro 先生

- Oesia 集团的 Pentester
- Integración Tecnológica Empresarial, S.L. 网络安全顾问
- 视听技术员, Ingeniería Audiovisual S.A.
- 胡安-卡洛斯国王大学网络安全工程专业毕业

04

结构和内容

该课程分为 3 个模块：进攻性安全、攻击网络或 Windows 系统以及 恶意软件分析和开发。在整个课程中，将从实用角度介绍早期威胁检测。在这方面，将鼓励学生发挥创造力，通过创新的解决方案来克服挑战。此外，对漏洞进行分类，其中 CVE 是最重要的分类之一。还将探索先进的 恶意软件分析技术，以加强网络环境的安全性。

你将进入一个以重复为基础的学习系统，在整个教学大纲中采用自然和渐进式教学”

模块1. 进攻性网络安全

1.1. 定义和背景
- 1.1.1. 进攻性安全的基本概念
- 1.1.2. 当今网络安全的重要性
- 1.1.3. 进攻性安全的挑战和机遇

1.2. 网络安全基础知识
- 1.2.1. 早期挑战和不断变化的威胁
- 1.2.2. 技术里程碑及其对网络安全的影响
- 1.2.3. 现代网络安全

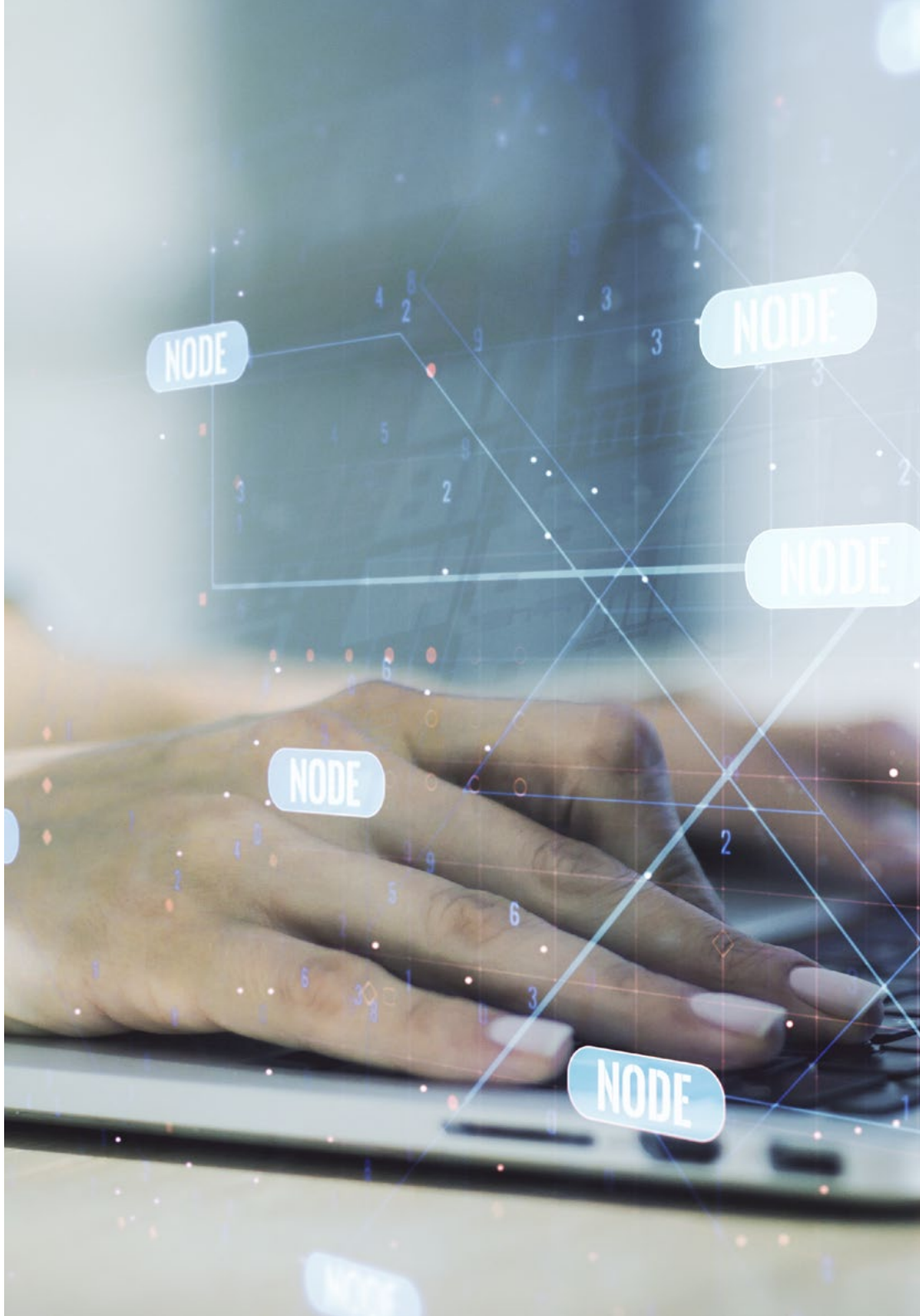
1.3. 进攻性网络安全的基础
- 1.3.1. 关键概念和术语
- 1.3.2. 跳出框框思考问题
- 1.3.3. 进攻型黑客与防御型黑客的区别

1.4. 进攻性网络安全方法
- 1.4.1. PTES（渗透测试执行标准）
- 1.4.2. OWASP（开放式网络应用程序安全项目）
- 1.4.3. 网络安全杀手链

1.5. 进攻性安全角色和责任
- 1.5.1. 主要概况
- 1.5.2. 错误赏金猎人
- 1.5.3. 研究：研究的艺术

1.6. 进攻型审计员兵工厂
- 1.6.1. 黑客操作系统
- 1.6.2. C2 简介
- 1.6.3. Metasploit：基础知识和使用
- 1.6.4. 有用资源

1.7. OSINT：开源情报
- 1.7.1. OSINT 基础知识
- 1.7.2. OSINT 技术和工具
- 1.7.3. OSINT 在进攻性网络安全中的应用



1.8. 脚本自动化简介
- 1.8.1. 脚本基础知识
- 1.8.2. 用 Bash编写脚本
- 1.8.3. 用 Python编写脚本

1.9. 漏洞分类
- 1.9.1. CVE（常见漏洞与暴露）
- 1.9.2. CWE（常见弱点枚举）
- 1.9.3. CAPEC（常见攻击模式枚举与分类）
- 1.9.4. CVSS（通用漏洞评分系统）
- 1.9.5. MITRE ATT & CK

1.10. 道德与 黑客
- 1.10.1. 黑客道德原则
- 1.10.2. 道德 黑客 与恶意黑客之间的界限
- 1.10.3. 法律影响和后果
- 1.10.4. 案例研究：网络安全中的道德状况

模块2. 对Windows网络和系统的攻击

2.1. 视窗和活动目录
- 2.1.1. Windows 的历史和演变
- 2.1.2. 活动目录基础知识
- 2.1.3. 活动目录功能和服务
- 2.1.4. 活动目录的总体结构

2.2. 活动目录环境中的联网
- 2.2.1. Windows 中的网络协议
- 2.2.2. DNS 及其在活动目录中的功能
- 2.2.3. 网络诊断工具
- 2.2.4. 活动目录网络部署

2.3. 活动目录中的身份验证和授权
- 2.3.1. 认证过程和流程
- 2.3.2. 证书类型
- 2.3.3. 凭证的存储和管理
- 2.3.4. 认证安全

2.4. 活动目录中的权限和策略
- 2.4.1. GPOs
- 2.4.2. 实施和管理 GPOs
- 2.4.3. 活动目录权限管理
- 2.4.4. 许可证中的漏洞和缓解措施

2.5. Kerberos 基础知识
- 2.5.1. 什么是 Kerberos?
- 2.5.2. 组件和操作
- 2.5.3. Kerberos 中的门票
- 2.5.4. 活动目录中的 Kerberos

2.6. 高级 Kerberos 技术
- 2.6.1. 常见的 Kerberos 攻击
- 2.6.2. 缓解和保护
- 2.6.3. Kerberos 流量监控
- 2.6.4. 高级 Kerberos 攻击

2.7. 活动目录证书服务 (ADCS)
- 2.7.1. PKI 基础知识
- 2.7.2. ADCS 作用和组件
- 2.7.3. ADCS 配置和部署
- 2.7.4. ADCS 的安全性

2.8. Active Directory 证书服务 (ADCS) 的攻击与防御
- 2.8.1. ADCS 的常见漏洞
- 2.8.2. 攻击和利用技术
- 2.8.3. 防御和缓解措施
- 2.8.4. ADCS 监控和审计

2.9. 活动目录审计
- 2.9.1. 活动目录中审计的重要性
- 2.9.2. 审计工具
- 2.9.3. 检测异常和可疑行为
- 2.9.4. 事件响应和恢复

2.10. Azure AD
- 2.10.1. Azure AD 基础知识
- 2.10.2. 与本地活动目录同步
- 2.10.3. Azure AD 中的身份管理
- 2.10.4. 与应用程序和服务集成

模块3. 恶意软件分析与开发

3.1. 恶意软件分析和开发
- 3.1.1. 恶意软件的历史和演变
- 3.1.2. 恶意软件的分类和类型
- 3.1.3. malware分析
- 3.1.4. 恶意软件开发

3.2. 准备环境
- 3.2.1. 虚拟机配置和 快照
- 3.2.2. 恶意软件分析工具
- 3.2.3. 恶意软件开发工具

3.3. 视窗基础知识
- 3.3.1. PE 文件格式(便携式可执行文件)
- 3.3.2. 进程和 线程
- 3.3.3. 文件系统和注册表
- 3.3.4. Windows Defender

3.4. 基本 恶意软件 技术
- 3.4.1. shellcode生成
- 3.4.2. 在磁盘上执行 shellcode
- 3.4.3. 磁盘与内存
- 3.4.4. 内存中 shellcode 的执行

3.5. 中级恶意软件技术
- 3.5.1. Windows 上的持久性
- 3.5.2. 主页文件夹
- 3.5.3. 注册密钥
- 3.5.4. 屏幕保护程序

3.6. 先进的 恶意软件 技术
- 3.6.1. 外壳代码 加密(XOR)
- 3.6.2. 外壳代码 加密(RSA)
- 3.6.3. 字符串混淆
- 3.6.4. 工艺注入

3.7. 静态 恶意软件分析
- 3.7.1. 使用 DIE(轻松检测)分析 封隔器
- 3.7.2. 使用 PE-Bear 分析切片
- 3.7.3. 使用 Ghidra 进行反编译

3.8. 动态 恶意软件分析
- 3.8.1. 使用流程黑客观察行为
- 3.8.2. 使用 API Monitor 分析调用
- 3.8.3. 使用 Regshot 分析注册表更改
- 3.8.4. 使用 TCPView 观察网络请求

3.9. .NET中的分析
- 3.9.1. .NET简介
- 3.9.2. 使用 dnSpy 进行反编译
- 3.9.3. 使用 dnSpy 调试
- 3.10. 分析真实 恶意软件

3.10.1. 准备环境
- 3.10.2. 恶意软件静态分析
- 3.10.3. 动态 恶意软件分析
- 3.10.4. 制定 YARA 规则

> 没有预设时间表或评估日程表。技术培训就是这样！

05

方法

这个培训计划提供了一种不同的学习方式。我们的方法是通过循环的学习模式发展起来的: **Re-learning**。

这个教学系统被世界上一些最著名的医学院所采用，并被**新英格兰医学杂志**等权威出版物认为是最有效的教学系统之一。

发现 Re-learning，这个系统放弃了传统的线性学习，带你体验循环教学系统：这种学习方式已经证明了其巨大的有效性，尤其是在需要记忆的科目中”

案例研究,了解所有内容的背景

我们的方案提供了一种革命性的技能和知识发展方法。我们的目标是在一个不断变化,竞争激烈和高要求的环境中加强能力建设。

> 和TECH,你可以体验到一种正在动摇世界各地传统大学基础的学习方式”

你将进入一个以重复为基础的学习系统,在整个教学大纲中采用自然和渐进式教学。

学生将通过合作活动和真实案例，学习如何解决真实商业环境中的复杂情况。

一种创新并不同的学习方法

该技术课程是一个密集的教学计划，从零开始，提出了该领域在国内和国际上最苛刻的挑战和决定。由于这种方法，个人和职业成长得到了促进，向成功迈出了决定性的一步。案例法是构成这一内容的技术基础，确保遵循当前经济，社会和职业现实。

> 我们的课程使你准备好在不确定的环境中面对新的挑战，并取得事业上的成功”

在世界顶级计算机科学学校存在的时间里，案例法一直是最广泛使用的学习系统。1912年开发的案例法是为了让法律学生不仅在理论内容的基础上学习法律，案例法向他们展示真实的复杂情况，让他们就如何解决这些问题作出明智的决定和价值判断。1924年，它被确立为哈佛大学的一种标准教学方法。

在特定情况下，专业人士应该怎么做？这就是我们在案例法中面对的问题，这是一种以行动为导向的学习方法。在整个课程中，学生将面对多个真实的案例。他们必须整合所有的知识，研究，论证和捍卫他们的想法和决定。

Re-learning 方法

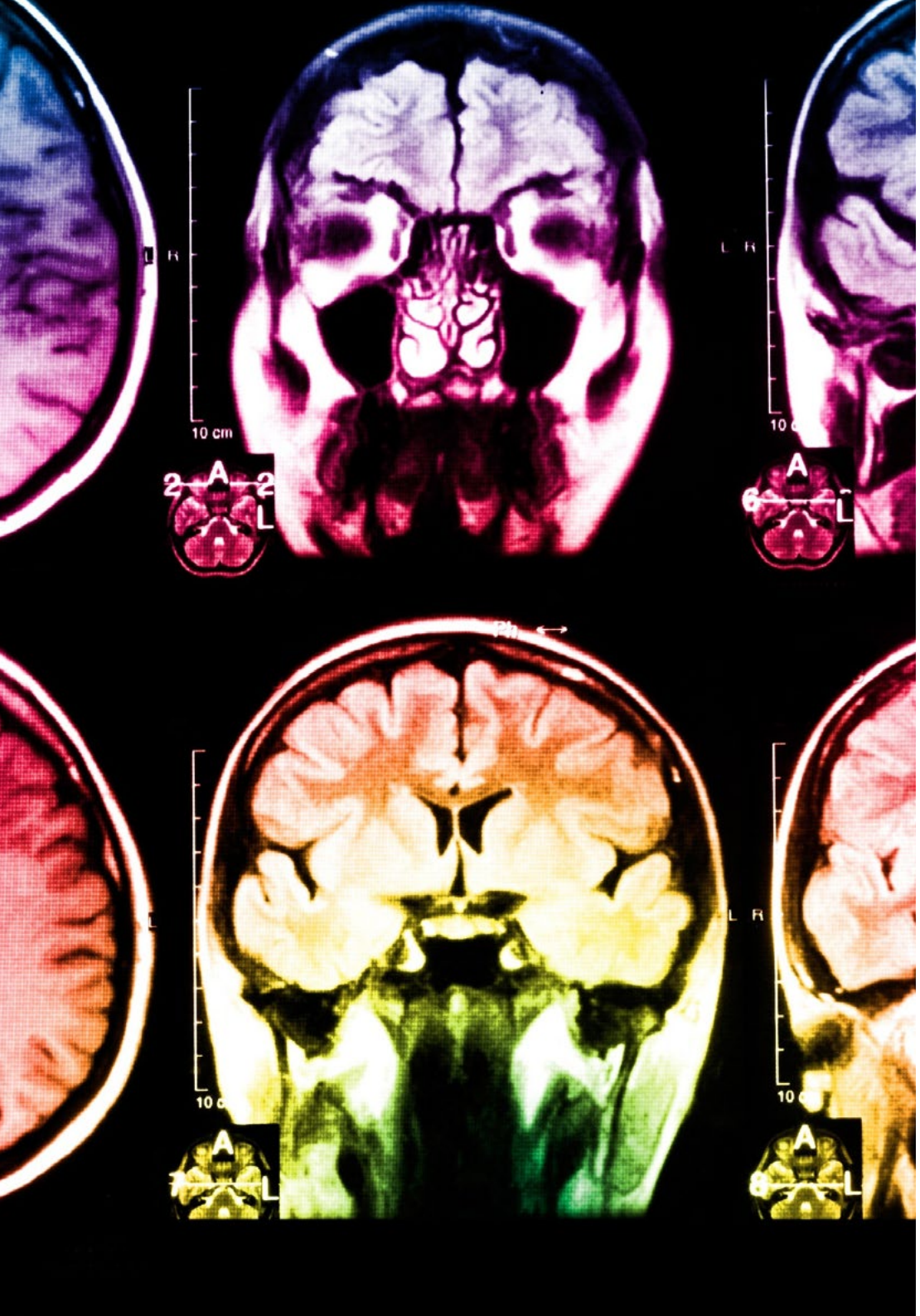
TECH有效地将案例研究方法与基于循环的100%在线学习系统相结合，在每节课中结合了个不同的教学元素。

我们用最好的100%在线教学方法加强案例研究：Re-learning。

> 在2019年，我们取得了世界上所有西班牙语在线大学中最好的学习成绩。

在TECH，你将用一种旨在培训未来管理人员的尖端方法进行学习。这种处于世界教育学前沿的方法被称为 Re-learning。

我校是唯一获准使用这一成功方法的西班牙语大学。2019年，我们成功地提高了学生的整体满意度（教学质量,材料质量,课程结构,目标……），与西班牙语最佳在线大学的指标相匹配。



在我们的方案中，学习不是一个线性的过程，而是以螺旋式的方式发生（学习，解除学习，忘记和重新学习）。因此，我们将这些元素中的每一个都结合起来。这种方法已经培养了超过65万名大学毕业生，在生物化学，遗传学，外科，国际法，管理技能，体育科学，哲学，法律，工程，新闻，历史，金融市场和工具等不同领域取得了前所未有的成功。所有这些都是在一个高要求的环境中进行的，大学学生的社会经济状况很好，平均年龄为43.5岁。

> Re-learning 将使你的学习事半功倍，表现更出色，使你更多地参与到训练中，培养批判精神，捍卫论点和对比意见：直接等同于成功。

从神经科学领域的最新科学证据来看，我们不仅知道如何组织信息，想法，图像y记忆，而且知道我们学到东西的地方和背景，这是我们记住它并将其储存在海马体的根本原因，并能将其保留在长期记忆中。

通过这种方式，在所谓的神经认知背景依赖的电子学习中，我们课程的不同元素与学员发展其专业实践的背景相联系。

该方案提供了最好的教育材料，为专业人士做了充分准备：

学习材料

所有的教学内容都是由教授该课程的专家专门为该课程创作的，因此，教学的发展是具体的。

然后，这些内容被应用于视听格式，创造了TECH在线工作方法。所有这些，都是用最新的技术，提供最高质量的材料，供学生使用。

大师课程

有科学证据表明第三方专家观察的有用性。

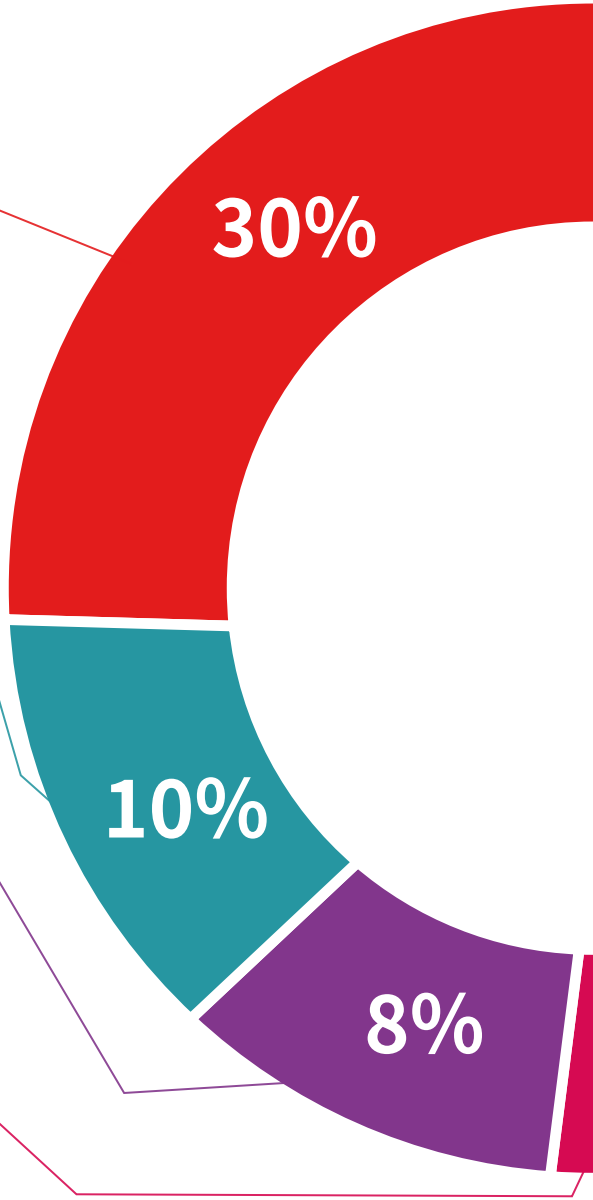
向专家学习可以加强知识和记忆，并为未来的困难决策建立信心。

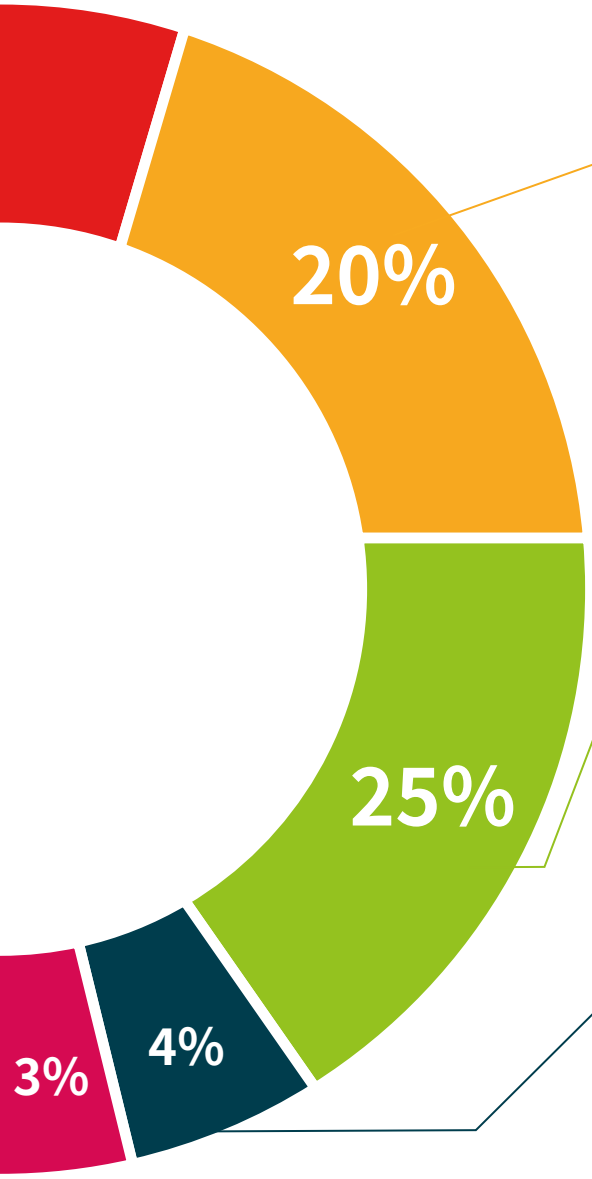
技能和能力的实践

你将开展活动以发展每个学科领域的具体能力和技能。在我们所处的全球化框架内，我们提供实践和氛围帮你取得成为专家所需的技能和能力。

延伸阅读

最近的文章，共识文件和国际准则等。在TECH的虚拟图书馆里，学生可以获得他们完成培训所需的一切。





案例研究

他们将完成专门为这个学位选择的最佳案例研究。由国际上最好的专家介绍,分析和辅导案例。

互动式总结

TECH团队以有吸引力和动态的方式将内容呈现在多媒体丸中,其中包括音频,视频,图像,图表和概念图,以强化知识。

这个用于展示多媒体内容的独特教育系统被微软授予“欧洲成功案例”称号。

测试和循环测试

在整个课程中,通过评估和自我评估活动和练习,定期评估和重新评估学习者的知识:通过这种方式,学习者可以看到他/她是如何实现其目标的。

06

学位

进攻型网络安全专科文凭除了保证最严格和最新的培训外，还可以获得由TECH科技大学颁发的专科文凭学位证书。

顺利完成这个课程并获得大学学位，无需旅行或通过繁琐的程序”

这个**进攻型网络安全专科文凭**包含了市场上最完整和最新的课程。

评估通过后，学生将通过邮寄收到**TECH科技大学**颁发的相应的**专科文凭**学位。

TECH科技大学颁发的证书将表达在专科文凭获得的资格，并将满足工作交流，竞争性考试和专业职业评估委员会的普遍要求。

学位：**进攻型网络安全专科文凭**

模式：**在线**

时长：**6个月**


tech 科学技术大学

授予

文凭

_____先生/女士，身份证号码_____

顺利通过并获得认证的课程是

专科文凭

进攻型网络安全

这是一个由本大学授予的学位，相当于450个小时，
开始日期是 dd/mm/aaaa,结束日期是dd/mm/aaaa。

截至2018年6月28日，TECH是一所被公共教育部认可的私立高等教育机构。

2020年六月17日

Tere Guevara Navarro女士
校长

Unique TECH Code: AFWORD23S techtitute.com/certificates

*海牙加注。如果学生要求为他们的纸质资格证书提供海牙加注，TECH EDUCATION将采取必要的措施来获得，但需要额外的费用。

tech 科学技术大学

专科文凭
进攻型网络安全

- 模式:**在线**
- 时长: **6个月**
- 学位: **TECH 科技大学**
- 课程表:**自由安排时间**
- 考试模式:**在线**

专科文凭
进攻型网络安全

tech 科学技术大学