专科文凭
网络安全红队

tech 科学技术大学

tech 科学技术大学

专科文凭
网络安全红队

- 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-red-team-cybersecurity

目录

01

介绍

网络安全已成为数字时代的一个基本支柱，而系统之间日益紧密的相互联系则加剧了网络攻击的威胁。对这一领域高技能专业人员的需求比以往任何时候都更加明显，特别是考虑到网络犯罪和复杂攻击呈指数级增长。在此背景下，本计划作为一项战略对策提出，旨在使专业人员掌握应对网络威胁的必要技能。在整个课程中，学生将沉浸在先进的威胁模拟中。该课程的教学方法是 100% 在线教学，具有灵活性和可访问性，提供各种多媒体内容，并采用 Relearning方法。

你将为提高网络安全和防止重大数字犯罪的发生做出贡献。不要错过这次机会，现在就报名吧！"

在复杂的网络安全形势下，拥有一名该领域的专家对于寻求加强防御不断变化的威胁的组织来说是绝对必要的。这种积极主动的方法是持续改进安全态势的基础，凸显了对专业知识的迫切需求。

Red Team 的专业培训为专业人员提供了积极预测、识别和减少系统和网络漏洞的能力。在本大学专家课程中，学生将学习渗透测试和模拟技能，解决漏洞的识别和利用问题。在这方面，它不仅能培养高级技术技能，还能促进与安全团队的有效合作，整合应对 恶意软件威胁的策略。

此外，毕业生还将牢固掌握适用于解决网络事件的数字取证调查（DFIR）基本原则。此外，这种全面的课程设置方法将确保专业人员掌握网络安全领域的尖端技能。

这一学术途径不仅以其内容，而且以其先进的方法而与众不同。该课程将完全通过网络提供给学生，使他们能够在不影响工作的情况下灵活地推进自己的职业发展。

此外，" Relearning的应用包括重复关键概念，用于巩固知识和促进有效学习。这种可访问性和强有力的教学方法相结合，使该大学专家不仅成为一种先进的教育选择，也成为那些寻求在网络安全领域取得卓越成就的人的重要推动力。

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

- 网络安全专家 "红队 "介绍的案例研究的发展情况
- 这个课程的图形化、示意图和突出的实用性内容提供了关于那些对专业实践至关重要的学科的最新和实用信息
- 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
- 可从任何连接互联网的固定或便携设备上访问内容

> 通过 TECH 独家大学课程的学习，你将在前景广阔的行业中脱颖而出"

根据 Trustpilot 平台 (4.9/5)，你将在这所全球学生评分最高的大学里深入研究详细的法证报告"

你将掌握评估和选择反恶意软件安全工具的技能。

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。

这个课程的教学人员包括来自这个行业的专业人士，他们将自己的工作经验带到了这一培训中，还有来自领先公司和著名大学的公认专家。

它的多媒体内容是用最新的教育技术开发的，将允许专业人员进行情景式学习，即一个模拟的环境，提供一个身临其境的培训，为真实情况进行培训。

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

网络 安全红队专科文凭的主要目标是培训学生发展模拟高级威胁的技能。在整个课程中，毕业生将沉浸在复制恶意行为者使用的战术、技术和程序（TTP）中。在这种情况下，专业化的方法不仅能加强专业人员的技术技能，还能使他们面对这一领域的现实挑战。此外，Relearning 方法的使用将促进学习，使关键概念的学习事半功倍。

你将找出公司网络基础设施的弱点和漏洞。通过 TECH 实现你的目标！”

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

> 通过 TECH 的教学工具（包括讲解视频和互动摘要），你将实现自己的目标”

具体目标

模块1.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

模块2.取证和数字取证基础

- 扎实了解数字取证调查（DFIR）的基本原则及其在解决网络事件中的应用
- 培养安全和取证数字证据的技能，确保保管链得到保护
- 学习如何对文件系统进行取证分析
- 使学生熟悉日志和日志分析的高级技术，从而能够重建数字环境中的事件
- 学习如何在破案过程中应用数字取证调查方法，从识别到记录调查结果
- 使学生熟悉数字证据分析和 Pentesting环境中法医技术的应用
- 培养编写详细、清晰的法医报告的技能，以易于理解的方式介绍调查结果和结论
- 促进与事件响应 (IR) 团队的有效合作，优化威胁调查和缓解方面的协调
- 促进数字取证方面的道德和法律实践，确保遵守网络安全法规和行为标准

模块3.高级红队练习

- 开发高级威胁模拟技能，复制有吸引力的恶意行为者使用的战术、技术和程序（TTPs）
- 通过逼真的 Red Team演习，学习识别基础设施中的薄弱环节和漏洞，加强安全态势
- 让毕业生熟悉先进的安全规避技术，以便评估基础设施抵御理想攻击的能力
- 培养 Red Team成员之间的有效协调和协作技能，优化战术和战略的执行，全面评估组织的安全状况
- 了解如何模拟当前的威胁情景，如 勒索软件 攻击或高级网络钓鱼活动，以评估组织的响应能力
- 让学员熟悉演习后的分析技巧，评估 Red Team 的表现，总结经验教训，不断改进
- 培养评估组织对模拟攻击的应变能力的技能，确定政策和程序中需要改进的地方
- 学习如何制作详细报告，记录高级 Red Team 演习的发现、使用的方法和提出的建议
- 在 Red Team演习中推广道德和法律实践，确保遵守网络安全法规和道德标准

03

课程管理

TECH 为该大学课程组建了一支杰出的师资队伍，由该领域最优秀的专家组成。从这个意义上讲，每位教师都拥有在网络安全领域领先企业工作的广泛和公认的专业背景。这些专业人士都是经过精心挑选的，他们拥有丰富的经验和专业知识，不仅能确保课程的学术质量，还能提供实用和最新的视角，从他们在红队环境中的实际经验中汲取宝贵的见解，丰富学员的培训内容。

> 了解顶级网络安全专家提供的最新 Shellcode (XQR) 加密技术。与 TECH 一起开启你的职业生涯!”

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**

04

结构和内容

本课程将为学生提供应用于 恶意软件的法证分析的专门课程，强调开发识别入侵指标（IoC）和攻击模式的关键技能。在整个课程中，毕业生将学习先进的方法，掌握应对复杂网络威胁所需的工具和知识。此外，这项结构严谨的计划将确保在 " Red Team领域开展全面培训，使专业人员做好准备，分析和应对恶意行为者使用的复杂策略。

你将加深对高级后剥削技术的了解，并将自己定位为一名出色的红队队员"

模块1.恶意软件分析与开发

1.1. 恶意软件分析和开发
- 1.1.1. 恶意软件的历史和演变
- 1.1.2. 恶意软件的分类和类型
- 1.1.3. malware分析
- 1.1.4. 恶意软件开发

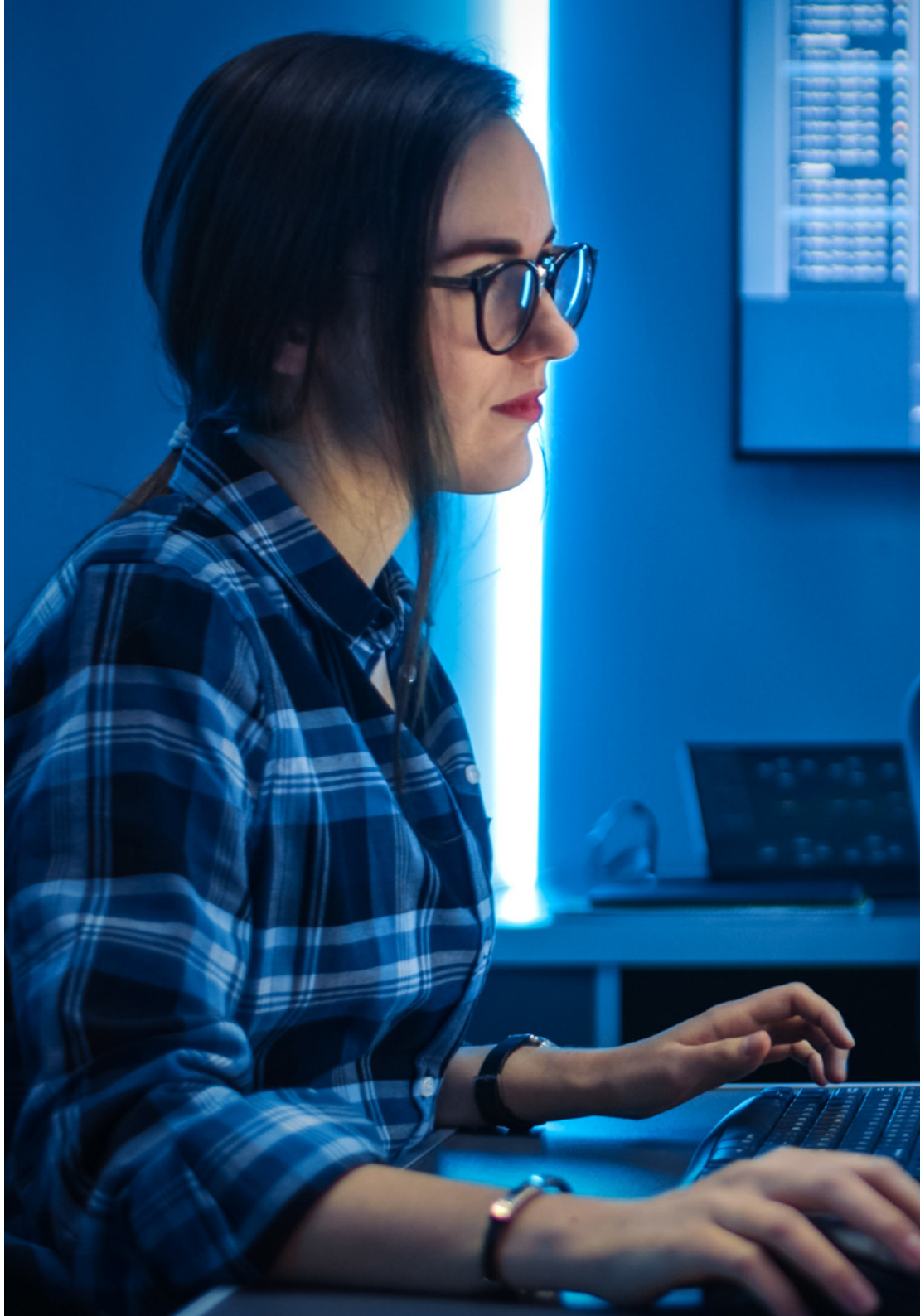
1.2. 准备环境
- 1.2.1. 虚拟机配置和 快照
- 1.2.2. 恶意软件分析工具
- 1.2.3. 恶意软件开发工具

1.3. 视窗基础知识
- 1.3.1. PE 文件格式(便携式可执行文件)
- 1.3.2. 进程和 线程
- 1.3.3. 文件系统和注册表
- 1.3.4. Windows Defender

1.4. 基本 恶意软件 技术
- 1.4.1. shellcode生成
- 1.4.2. 在磁盘上执行 shellcode
- 1.4.3. 磁盘与内存
- 1.4.4. 内存中 shellcode 的执行

1.5. 中级恶意软件技术
- 1.5.1. Windows 上的持久性
- 1.5.2. 主页文件夹
- 1.5.3. 注册密钥
- 1.5.4. 屏幕保护程序

1.6. 先进的 恶意软件 技术
- 1.6.1. 外壳代码 加密(XOR)
- 1.6.2. 外壳代码 加密(RSA)
- 1.6.3. 字符串混淆
- 1.6.4. 工艺注入



1.7. 静态 恶意软件分析
- 1.7.1. 使用 DIE (轻松检测) 分析 封隔器
- 1.7.2. 使用 PE-Bear 分析切片
- 1.7.3. 使用 Ghidra 进行反编译

1.8. 动态 恶意软件分析
- 1.8.1. 使用流程黑客观察行为
- 1.8.2. 使用 API Monitor 分析调用
- 1.8.3. 使用 Regshot 分析注册表更改
- 1.8.4. 使用 TCPView 观察网络请求

1.9. .NET中的分析
- 1.9.1. .NET简介
- 1.9.2. 使用 dnSpy 进行反编译
- 1.9.3. 使用 dnSpy 调试

1.10. 分析真实 恶意软件
- 1.10.1. 准备环境
- 1.10.2. 恶意软件静态分析
- 1.10.3. 动态 恶意软件分析
- 1.10.4. 制定 YARA 规则

模块2.取证和数字取证基础

2.1. 数字取证
- 2.1.1. 计算机取证的历史和演变
- 2.1.2. 计算机取证在网络安全中的重要性
- 2.1.3. 计算机取证的历史和演变

2.2. 计算机取证基础
- 2.2.1. 监管链及其实施
- 2.2.2. 数字证据的类型
- 2.2.3. 证据获取过程

2.3. 文件系统和数据结构
- 2.3.1. 主要文件系统
- 2.3.2. 数据隐藏方法
- 2.3.3. 分析文件元数据和属性

2.4. 操作系统分析
- 2.4.1. Windows 系统的取证分析
- 2.4.2. Linux 系统的取证分析
- 2.4.3. 对 macOS 系统进行取证分析

2.5. 数据恢复和磁盘分析
- 2.5.1. 从受损介质中恢复数据
- 2.5.2. 磁盘分析工具
- 2.5.3. 文件分配表的解释

2.6. 网络和流量分析
- 2.6.1. 网络数据包捕获和分析
- 2.6.2. 分析 防火墙日志
- 2.6.3. 网络入侵检测

2.7. 恶意软件 和恶意代码分析
- 2.7.1. 恶意软件 的分类及其特点
- 2.7.2. 静态和动态 恶意软件分析
- 2.7.3. 反汇编和调试技术

2.8. 记录和事件分析
- 2.8.1. 系统和应用中的寄存器类型
- 2.8.2. 相关事件的解释
- 2.8.3. 记录分析工具

2.9.应对安全事件
- 2.9.1. 事件响应流程
- 2.9.2. 制定事件响应计划
- 2.9.3. 与安全团队协调

2.10.出示证据和法律
- 2.10.1. 法律领域的数字证据规则
- 2.10.2. 编写法医报告
- 2.10.3. 作为专家证人出庭

模块3.高级 Red Team 演习

3.1. 高级识别技术
- 3.1.1. 高级子域枚举
- 3.1.2. 高级谷歌多金
- 3.1.3. 社交媒体与收割机

3.2. 高级 网络钓鱼 活动
- 3.2.1. 什么是 反向代理网络钓鱼
- 3.2.2. 使用 Evilginx绕过 2FA
- 3.2.3. 泄露数据

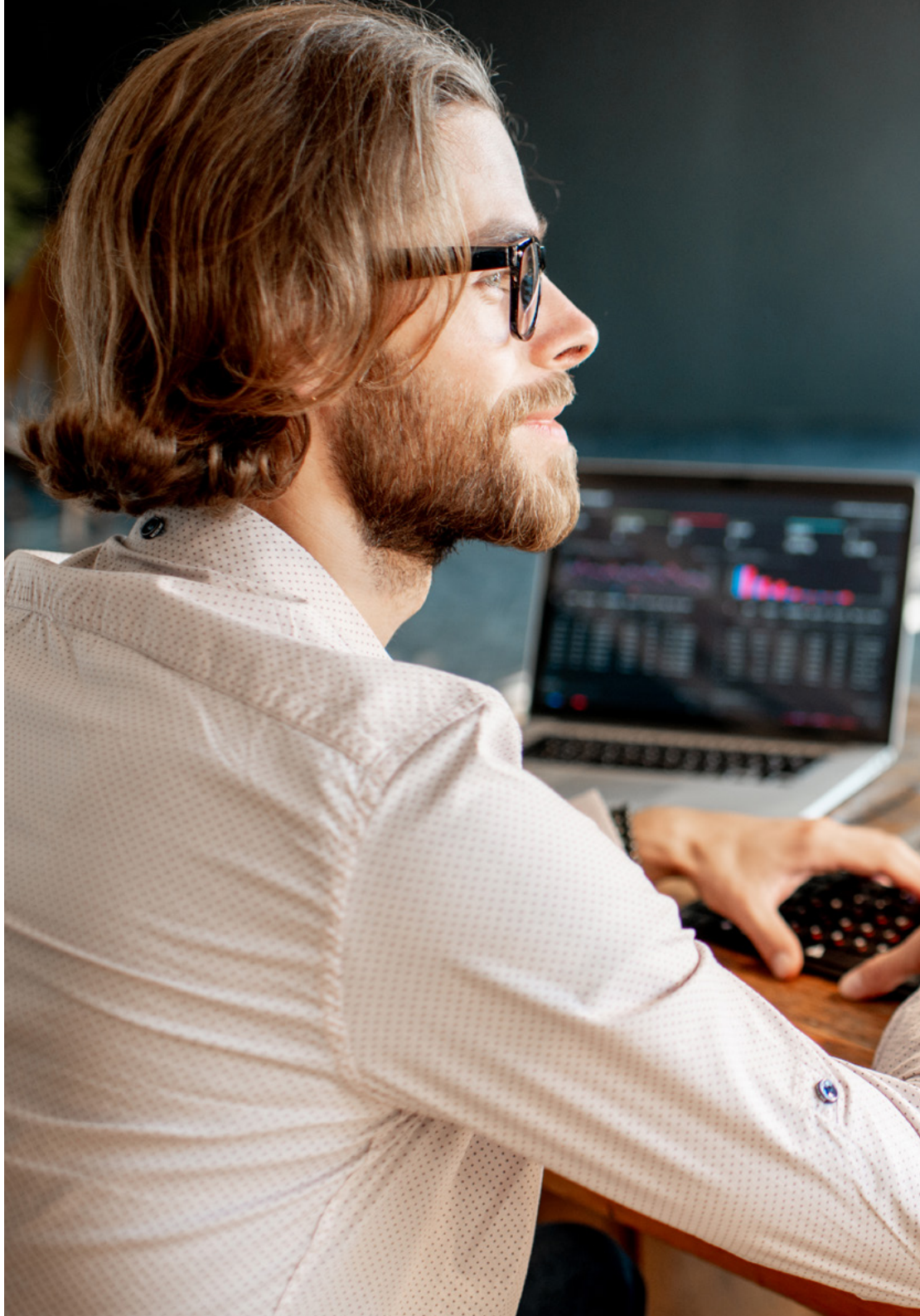
3.3. 高级持久性技术
- 3.3.1. 金色门票
- 3.3.2. 银票
- 3.3.3. DCShadow技术

3.4. 高级避险技巧
- 3.4.1. AMSI旁路
- 3.4.2. 修改现有工具
- 3.4.3. Powershell混淆

3.5. 高级横向移动技术
- 3.5.1. Pass-the-Ticket (PtT)
- 3.5.2. 哈希传球 (钥匙传递)
- 3.5.3. NTLM 中继

3.6. 先进的开采后技术
- 3.6.1. LSASS转储
- 3.6.2. 萨姆转储
- 3.6.3. DCSync攻击

3.7. 高级 旋转技术
- 3.7.1. 什么是 枢轴转动
- 3.7.2. 使用 SSH 进行隧道连接
- 3.7.3. 用凿子旋转



3.8. 物理入侵
- 3.8.1. 监视和侦察
- 3.8.2. 尾随和捎带
- 3.8.3. 开锁

3.9. Wi-Fi 攻击
- 3.9.1. WPA/WPA2 PSK 攻击
- 3.9.2. AP 流氓攻击
- 3.9.3. 对 WPA2 企业的攻击

3.10. RFID攻击
- 3.10.1. RFID 读卡器
- 3.10.2. RFID 卡处理
- 3.10.3. 制作克隆卡

> 千万不要错过通过这一创新计划提升你的职业生涯的机会。成为网络安全专家!"

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

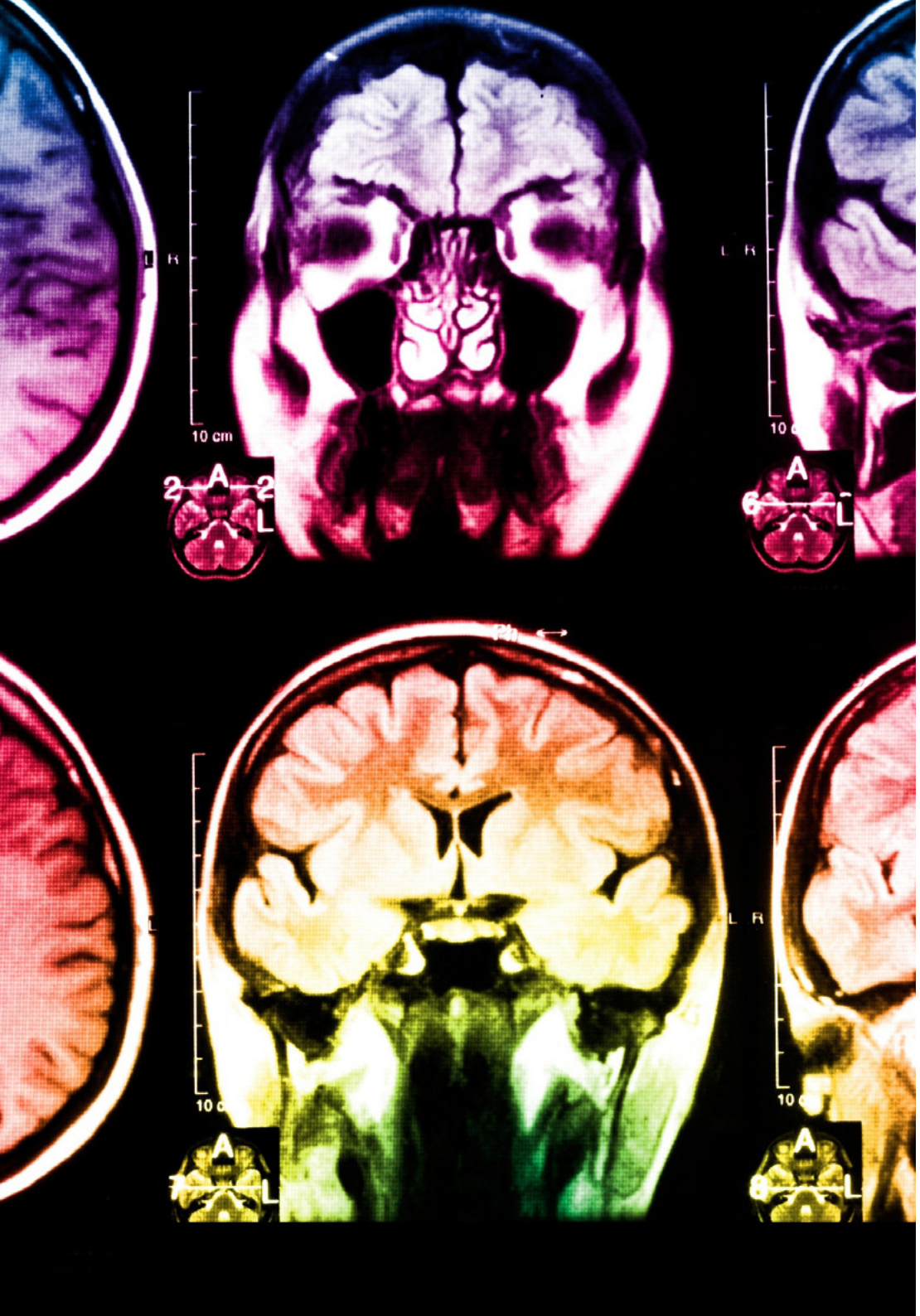
TECH有效地将案例研究方法与基于循环的100%在线学习系统相结合，在每节课中结合了个不同的教学元素。

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。

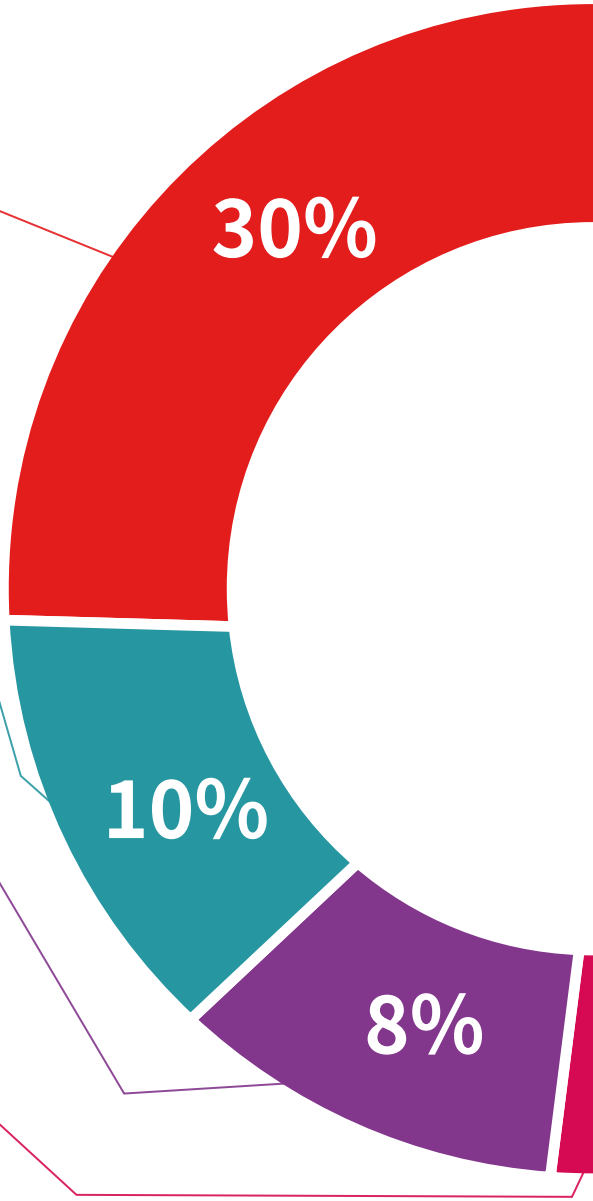
向专家学习可以加强知识和记忆，并为未来的困难决策建立信心。

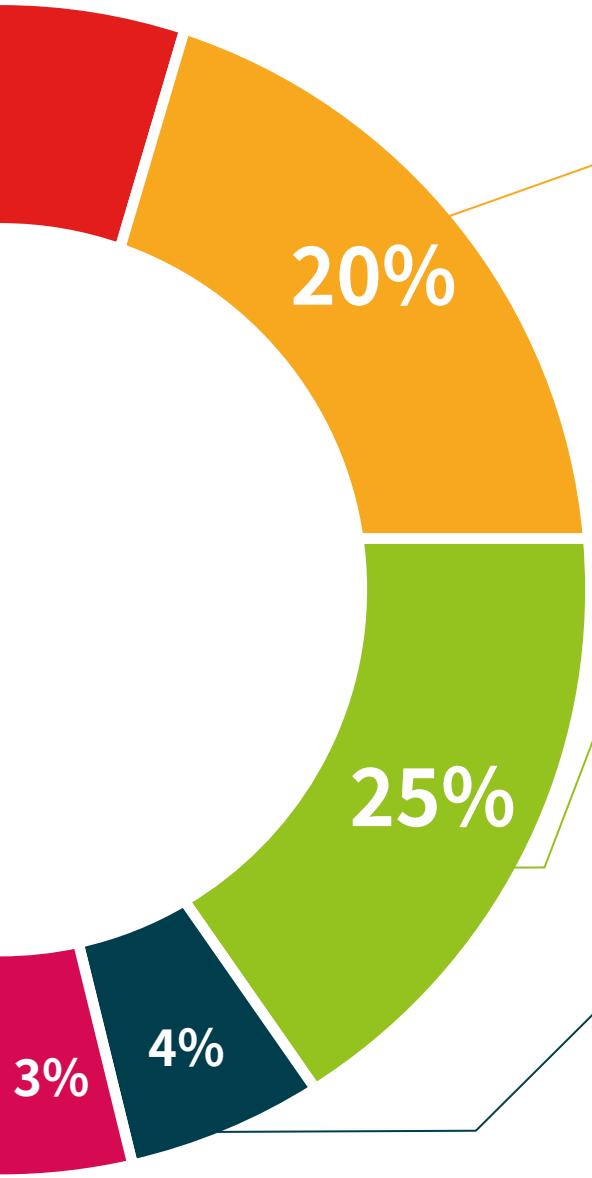
技能和能力的实践

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

网络安全红队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”

网络安全红队**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：**网络安全红队专科文凭**

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

网络安全红队

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
网络安全红队

- 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
网络安全红队

tech 科学技术大学