专科文凭
高级Web黑客攻击

tech 科学技术大学

tech 科学技术大学

专科文凭
高级Web黑客攻击

- 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-advanced-web-hacking

目录

01

介绍

随着机构的数字化扩张，它们越来越多地使用技术来存储敏感数据。因此，高级 黑客攻击 对机构构成了严重威胁。如果 黑客 访问了你的网站，后果将不堪设想，包括身份盗窃、金融欺诈和勒索。因此，企业必须拥有先进安全措施方面的专家，以实施 防火墙等措施。为此，TECH 正在推出一项创新计划，帮助学生掌握最有效的网络安全技术。此外，它采用 100% 在线模式，保证了方便性和时间灵活性。

有了这位 专科文凭，你将把任何公司都改造成一个安全的环境，免受网络威胁”

信息技术专家是当今组织的宝贵无形资产。其中一个主要原因是，定期审计有助于提前发现和解决潜在的漏洞。这样，他们就能预测 黑客可能犯下的罪行，同时将虚拟环境变成安全区。

这样，用户就能保证安全、自由地在其网络上冲浪，并购买其商品和服务。然而，鉴于这些做法的增多，计算机科学家面临的挑战是不断更新知识，采用最具革命性的技术来处理这些问题。

在此背景下，TECH 开发了学术市场上最完整的高级Web黑客攻击专科文凭课程。通过该课程的学习，毕业生将站在网络安全的最前沿，掌握保护受限信息的各种策略。此外，还将深入探讨利用复杂漏洞的策略。

从业人员还将重点实施有效的安全措施，如入侵检测系统。此外，还将强调 交换 功能，以便在同一网络上实现组织结构图中各部门设备的互联。它还将提供撰写技术报告和执行报告的关键。在这方面，报告将深入探讨如何暴露敏感数据，重点关注客户。最后，还将探讨衡量实际运行安全的各种方法。

为了巩固对所学内容的掌握，培训采用了创新的 Relearning系统，通过自然和渐进的重复，促进对复杂概念的吸收。同样，该计划还辅以各种形式的材料，如信息图表或解释性视频。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调整时间表。

这个**高级Web黑客攻击专科文凭**包含市场上最完整和最新的课程。主要特点是：

- 由高级网络黑客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

> 你将破解存储在电脑中的密码，并预测黑客攻击"

“你将探索 OSI 模型，了解网络系统中的通信过程。而且只要 6 个月！”

你将深入了解 DOM 漏洞，并采用最有效的策略防止高级攻击。

忘掉背书！通过 Relearning 方法，你将以自然、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

本课程将深入探讨针对网络服务的高级黑客技术，使专业人员能够在黑客攻击发生之前实施最有效的策略。为此，将对网络设计的基本原则进行分析，并找出共同的弱点。这样，毕业生就能提供最具创新性的解决方案，在飞速发展的数字行业中脱颖而出。

你想确保网络和网络传输数据的安全吗？根据《福布斯》报道，世界上最好的数字大学在转换过程中占据主导地位"

总体目标

- 总体目标 掌握渗透测试和红队模拟的高级技能，解决系统和网络漏洞的识别和利用问题
- 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

> 你将采用最有效的安全措施，并避免出现诸如 验证失败 等漏洞。现在报名吧！"

具体目标

模块1.高级Web黑客攻击

- 掌握识别和评估网络应用程序漏洞的技能，包括 SQL 注入、跨站脚本 (XSS) 和其他常见攻击载体
- 了解如何对现代网络应用程序进行安全测试
- 掌握高级网络黑客技术，探索规避安全措施和利用复杂漏洞的策略
- 让毕业生熟悉如何评估应用程序接口和网络服务的安全性，找出可能存在的漏洞，加强编程接口的安全性
- 掌握在网络应用程序中实施有效缓解措施的技能，减少遭受攻击的风险并加强安全性
- 参与实际模拟，评估复杂网络环境中的安全性，将知识应用于实际情况
- 培养制定有效防御策略的能力，保护网络应用程序免受网络威胁
- 学习如何根据相关安全法规和标准调整高级网络黑客实践，确保遵守法律和道德框架
- 促进开发团队和安全团队之间的有效合作

模块2.网络架构与安全

- 掌握网络架构的高级知识，包括拓扑结构、协议和关键组件
- 培养识别和评估网络基础设施中特定漏洞的技能，考虑潜在威胁
- 学习如何实施有效的网络安全措施，包括 防火墙、入侵检测系统 (IDS) 和网络分段
- 让学生熟悉软件定义网络（SDN）等新兴网络技术，并了解其对安全的影响
- 培养确保网络通信安全的技能，包括防范 嗅探 和中间人攻击等威胁
- 了解如何评估和改进企业网络环境中的安全配置，确保提供充分的保护
- 培养针对企业网络威胁（从内部攻击到外部威胁）实施有效缓解措施的技能
- 促进与安全团队的有效合作，整合保护网络基础设施的战略和工作
- 在实施网络安全措施时推广道德和法律实践，确保在所有活动中遵守道德原则

模块3.技术和执行报告

- 培养编写详细技术报告的技能，清楚全面地介绍研究结果、使用的方法和建议
- 学会与技术受众有效沟通，使用准确、恰当的语言传递复杂的技术信息
- 培养制定可行和实用建议的技能，以减少漏洞并改善安全状况
- 学习评估已识别漏洞的潜在影响，同时考虑技术、操作和战略方面的问题
- 让学员熟悉执行报告的最佳做法，为非技术受众调整技术信息
- 发展能力，使调查结果和建议与组织的战略和运营目标保持一致
- 学习如何使用数据可视化工具，以图形表示报告中包含的信息，从而加深理解
- 促进在报告中纳入有关遵守法规和标准的相关信息，确保遵守法律要求
- 促进技术团队和执行团队之间的有效合作，确保报告中提出的改进行动得到理解和支持

03

课程管理

为了提供卓越的教育，TECH 组建了一支具有广泛网络安全专业背景的教学团队。这些专家拥有超过 13 年的经验，将提供最全面的方法和最新的工具来开发安全的虚拟环境。通过这种方式，学生将获得在提供多种机会的数字领域进行专业学习所需的保障。

在最优秀教师的支持下，你将深入探索 Pentester 的极限。你的活动将 100% 合法！”

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

Siles Rubia, Marcelino 先生

- 网络安全工程师
- 胡安-卡洛斯国王大学网络安全工程专业
- 知识:竞技编程、网络黑客、活动目录 和 恶意软件开发
- AdaByron 竞赛优胜者

Redondo Castro, Pablo 先生

- Oesia 集团的 Pentester
- 马德里胡安卡洛斯国王大学网络安全工程师
- 作为 网络安全评估员 Traineev的丰富经验
- 他积累了教学经验，举办了与夺旗比赛相关的培训

04

结构和内容

该课程包括 3 个综合模块：高级网络黑客；网络结构与安全；以及技术和执行报告。在资深教师的支持下，将介绍通过实施 防火墙确保企业网络安全的先进策略。入侵检测，包括 HHTP 请求走私，也将得到进一步发展。将讨论在同一虚拟环境中使用 VLAN 分离数据流量的重要性，并探讨报告流程，以便提供准确、详细的报告。

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.高级Web黑客攻击

1.1. 网站如何运行
- 1.1.1. URL 及其组成部分
- 1.1.2. HTTP方法
- 1.1.3. 页眉
- 1.1.4. 如何使用 Burp Suite 查看网络请求

1.2. 会议
- 1.2.1. 曲奇
- 1.2.2. JWT标记
- 1.2.3. 会话劫持攻击
- 1.2.4. JWT攻击

1.3. 跨站脚本 (XSS)
- 1.3.1. 什么是 XSS
- 1.3.2. XSS类型
- 1.3.3. 利用 XSS
- 1.3.4. XSLeaks简介

1.4. 数据库注入
- 1.4.1. 什么是 SQL 注入
- 1.4.2. 利用 SQLi窃取信息
- 1.4.3. SQLi 盲法、时间法和误差法
- 1.4.4. NoSQLi 注入

1.5. 路径遍历和本地文件包含
- 1.5.1. 它们是什么及其区别
- 1.5.2. 常见的过滤器和如何绕过它们
- 1.5.3. 日志中毒
- 1.5.4. PHP 中的 LFI

1.6. 验证失败
- 1.6.1. 用户枚举
- 1.6.2. 密码
- 1.6.3. 2FA 旁路
- 1.6.4. 带有敏感和可修改信息的Cookie

1.7. 远程命令执行
- 1.7.1. 指令注入
- 1.7.2. 盲命令注入
- 1.7.3. 不安全的 PHP反序列化
- 1.7.4. 不安全的反序列化 Java

1.8. 文件上传
- 1.8.1. 通过 webhell获取核证的排减量
- 1.8.2. 文件上传中的 XSS
- 1.8.3. XML 外部实体 (XXE) 喷射
- 1.8.4. 文件上传中的路径遍历

1.9. 损坏的接入控制
- 1.9.1. 不受限制地接触面板
- 1.9.2. 不安全的直接对象引用 (IDOR)
- 1.9.3. 过滤器旁路
- 1.9.4. 授权方法不足

1.10. DOM 漏洞和更高级的攻击
- 1.10.1. 拒绝 Regex 服务
- 1.10.2. DOM 克隆
- 1.10.3. 原型污染
- 1.10.4. HTTP 请求走私

模块2.网络架构与安全

2.1. 计算机网络
- 2.1.1. 基本概念：局域网、广域网、CP、CC 协议
- 2.1.2. OSI 模型和 TCP/IP
- 2.1.3. 切换：基这个概念
- 2.1.4. 路由：基这个概念

2.2. 开关
- 2.2.1. VLAN 简介
- 2.2.2. STP
- 2.2.3. 以太通道
- 2.2.4. 对第 2 层的攻击

2.3. VLAN
- 2.3.1. VLAN 的重要性
- 2.3.2. VLAN 的漏洞
- 2.3.3. 针对 VLAN 的常见攻击
- 2.3.4. 缓解措施

2.4. 路由
- 2.4.1. IP 地址 - IPv4 和 IPv6
- 2.4.2. 路由：关键概念
- 2.4.3. 静态路由
- 2.4.4. 动态路由简介

2.5. IGP 协议
- 2.5.1. RIP
- 2.5.2. OSPF
- 2.5.3. RIP 与 OSPF
- 2.5.4. 拓扑需求分析

2.6. 周边保护
- 2.6.1. DMZ
- 2.6.2. 防火墙
- 2.6.3. 通用架构
- 2.6.4. 零信任网络访问

2.7. IDS 和 IPS
- 2.7.1. 特点
- 2.7.2. 执行
- 2.7.3. SIEM 和 SIEM 云
- 2.7.4. 基于 蜜罐的检测

2.8. TLS 和 VPN
- 2.8.1. SSL/TLS
- 2.8.2. TLS：常见攻击
- 2.8.3. 使用 TLS 的 VPN
- 2.8.4. 使用 IPSEC 的 VPN

2.9. 无线网络安全
- 2.9.1. 无线网络简介
- 2.9.2. 协议
- 2.9.3. 关键要素
- 2.9.4. 常见攻击

2.10. 商业网络及如何与之打交道
- 2.10.1. 逻辑分段
- 2.10.2. 物理分割
- 2.10.3. 访问控制
- 2.10.4. 需要考虑的其他措施

模块3.技术和执行报告

3.1. 报告程序
- 3.1.1. 报告的结构
- 3.1.2. 报告程序
- 3.1.3. 关键概念
- 3.1.4. 行政人员与技术人员

3.2. 指导
- 3.2.1. 简介
- 3.2.2. 导游类型
- 3.2.3. 国家指南
- 3.2.4. 使用案例

3.3. 方法
- 3.3.1. 评估
- 3.3.2. 五重测试
- 3.3.3. 审查通用方法
- 3.3.4. 国家方法介绍

3.4. 报告阶段的技术方法
- 3.4.1. 了解 pentester的限制
- 3.4.2. 语言使用和提示
- 3.4.3. 信息介绍
- 3.4.4. 常见错误

3.5. 报告阶段的执行方法
- 3.5.1. 根据背景调整报告
- 3.5.2. 语言使用和提示
- 3.5.3. 标准化
- 3.5.4. 常见错误

3.6. OSSTMM
- 3.6.1. 了解方法
- 3.6.2. 认知
- 3.6.3. 文件
- 3.6.4. 阐述报告的内容

3.7. LINCE
- 3.7.1. 了解方法
- 3.7.2. 认知
- 3.7.3. 文件
- 3.7.4. 阐述报告的内容

3.8. 报告漏洞
- 3.8.1. 关键概念
- 3.8.2. 量化范围
- 3.8.3. 脆弱性和证据
- 3.8.4. 常见错误

3.9. 将报告重点放在客户身上
- 3.9.1. 工作证据的重要性
- 3.9.2. 解决方案和缓解措施
- 3.9.3. 敏感数据和相关数据
- 3.9.4. 实例和案例

3.10. 报告 重考情况
- 3.10.1. 关键概念
- 3.10.2. 了解遗留信息
- 3.10.3. 错误检查
- 3.10.4. 添加信息

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

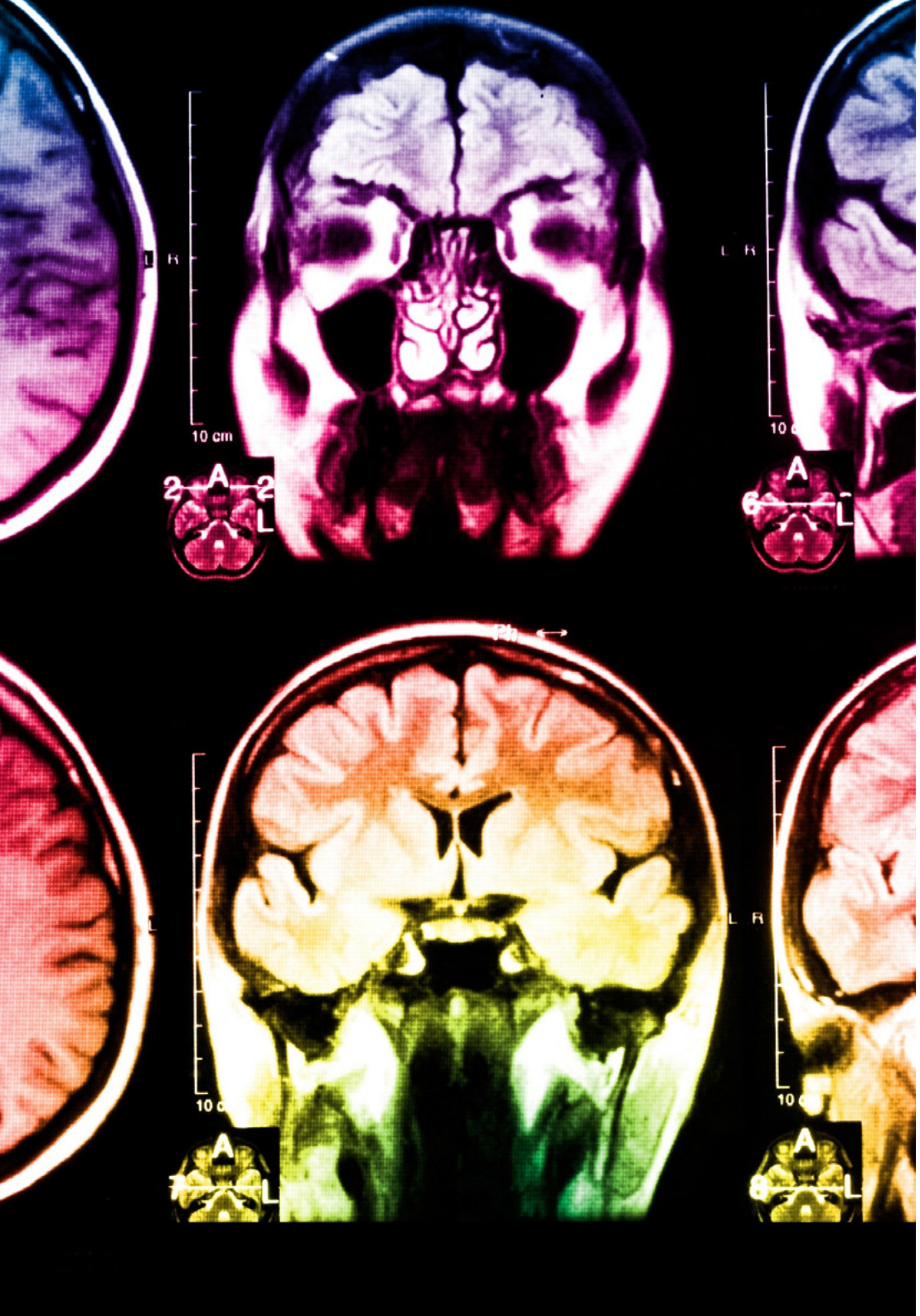
TECH有效地将案例研究方法与基于循环的100%在线学习系统相结合，在每节课中结合了个不同的教学元素。

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。

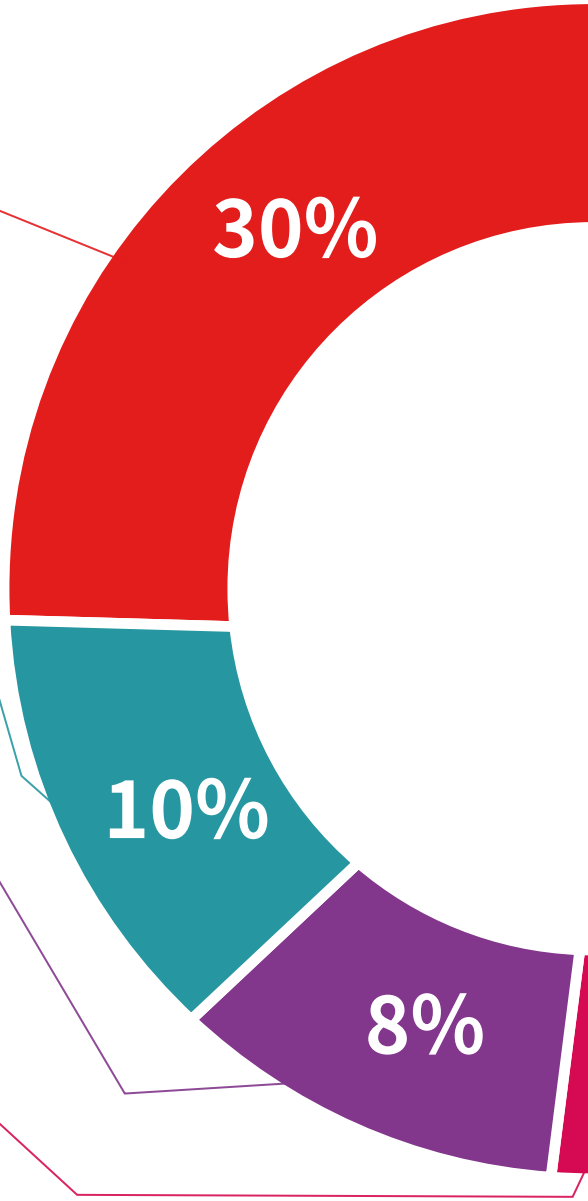
向专家学习可以加强知识和记忆，并为未来的困难决策建立信心。

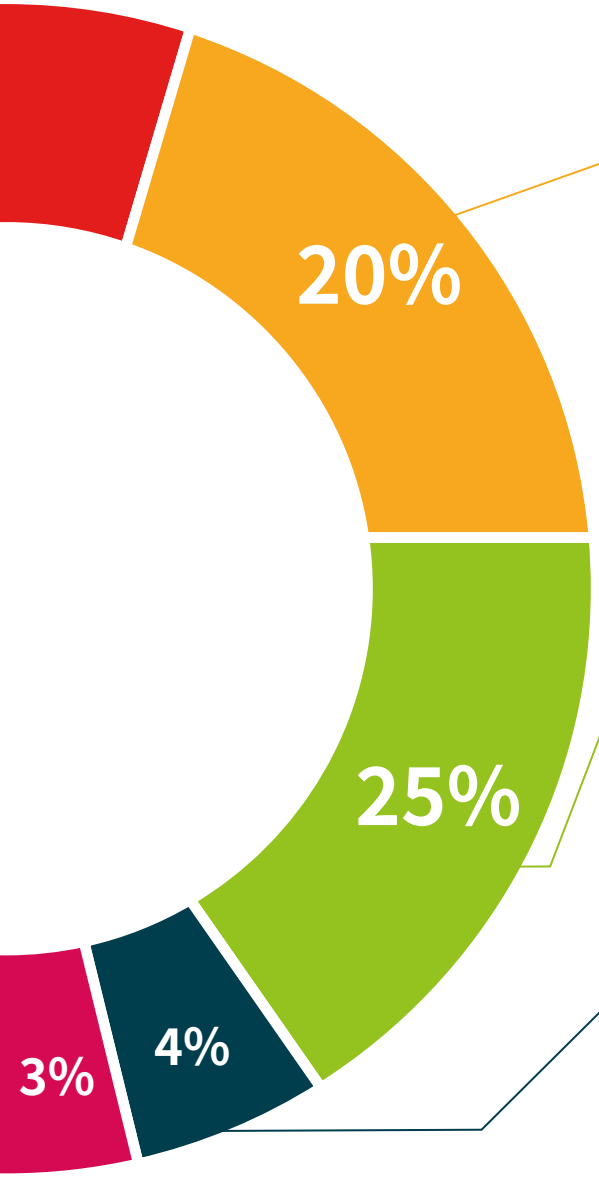
技能和能力的实践

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

高级Web黑客攻击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**高级Web黑客攻击专科文凭**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：**高级Web黑客攻击专科文凭**

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

高级Web黑客攻击

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
高级Web黑客攻击

- 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
高级Web黑客攻击

tech 科学技术大学