商学院校级硕士
渗透测试和红队

tech 科学技术大学

tech 科学技术大学

商学院校级硕士
渗透测试和红队

- 模式:**在线**
- 时长: **12个月**
- 学位: **TECH 科技大学**
- 课程表:**自由安排时间**
- 考试模式:**在线**
- 目标对象: **大学毕业生、文凭和学位持有者，曾在社会和法律科学、行政管理和工商管理领域获得过任何学位**

网页链接: **www.techtitute.com/cn/school-of-business/professional-master-degree/master-pentesting-red-team**

目录

01

欢迎

如今，网络攻击已变得相当突出和强大，令公众和企业本身感到担忧。因此，公司受到了这些威胁的巨大影响，不得不为客户的数据库和敏感信息提供最大限度的保护。因此，该行业一直在寻找高素质的网络安全专家，这也是 TECH 围绕恶意行为者使用的战术、技术和程序设计这一学术课程并提供技术资源和其他发展的原因。所有这一切，都是通过 Relearning 方法和一个非常完整的 100% 在线平台实现的，该平台提供了灵活方便的时间表。

渗透测试和红队商学院校级硕士
TECH 科技大学

感谢通过这一 100% 在线课程，你将专门学习如何在对 Windows 系统实施攻击和测试时促进道德和法律实践"

02

为什么在TECH学习?

TECH是世界上最大的100%在线商业学校。它是一所精英商学院，具有最大的学术需求模式。一个国际高绩效和管理技能强化培训的中心。

TECH是一所站在技术前沿的大学，它将所有资源交给学生支配，以帮助他们取得商业成功"

TECH科技大学

创新

该大学提供一种在线学习模式，将最新的教育科技与最大的教学严谨性相结合。一种具有最高国际认可度的独特方法，将为学生提供在不断变化的世界中发展的钥匙，在这个世界上，创新必须是所有企业家的基本承诺。

“由于在节目中加入了创新的互动式多视频系统，被评为 "微软欧洲成功案例"。

最高要求

TECH的录取标准不是经济方面的。在这所大学学习没有必要进行大量投资。然而，为了从TECH毕业，学生的智力和能力的极限将受到考验。该机构的学术标准非常高。

95% | TECH学院的学生成功完成学业

联网

来自世界各地的专业人员参加TECH，因此，学生将能够建立一个庞大的联系网络，对他们的未来很有帮助。

+100,000
每年培训的管理人员

+200
不同国籍的人

赋权

学生将与最好的公司和具有巨大声望和影响力的专业人士携手成长。TECH已经与7大洲的主要经济参与者建立了战略联盟和宝贵的联系网络。

+500 | 与最佳公司的合作协议

人才

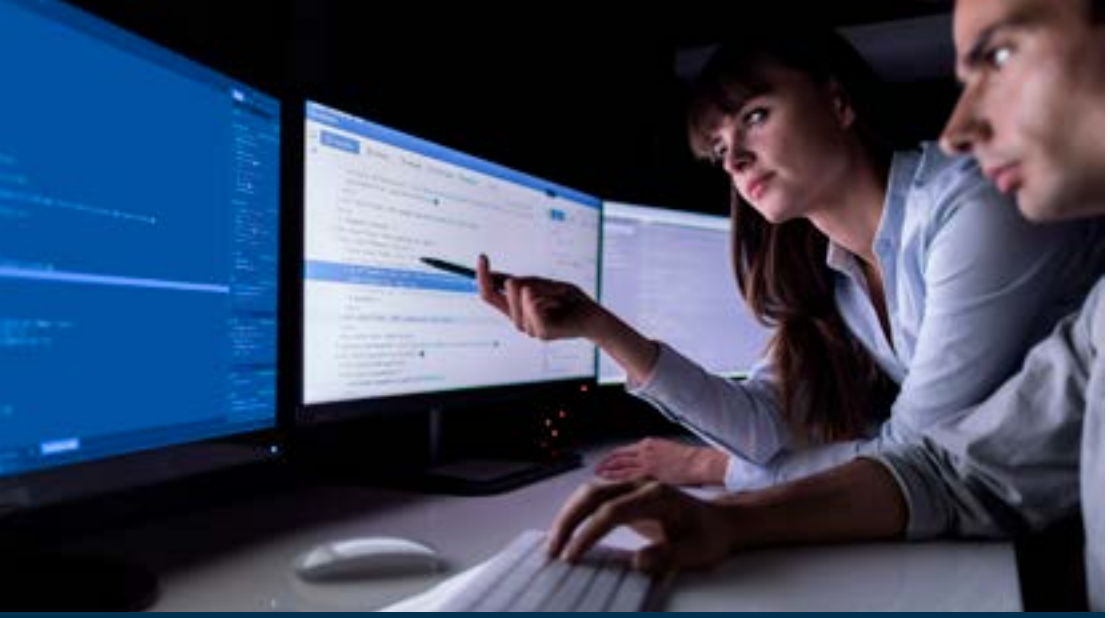
该计划是一个独特的建议，旨在发挥学生在商业领域的才能。这是一个机会，你可以利用它来表达你的关切和商业愿景。

TECH帮助学生在这个课程结束后向世界展示他们的才华。

多文化背景

通过在TECH学习，学生将享受到独特的体验。你将在一个多文化背景下学习。在一个具有全球视野的项目中，由于该项目，你将能够了解世界不同地区的工作方式，收集最适合你的商业理念的创新信息。

TECH的学生来自200多个国家。



向最好的人学习

TECH教学团队在课堂上解释了导致他们在其公司取得成功的原因，在一个真实、活泼和动态的环境中工作。全力以赴提供优质专业的教师，使学生在事业上有所发展，在商业世界中脱颖而出。

来自20个不同国籍的教师。

> 在TECH，你将有机会接触到学术界最严格和最新的案例研究"

TECH追求卓越，为此，有一系列的特点，使其成为一所独特的大学:

分析报告

TECH探索学生批判性的一面，他们质疑事物的能力，他们解决问题的能力和他们的人际交往能力。

优秀的学术成果

TECH为学生提供最好的在线学习方法。大学将 再学习 方法（国际公认的研究生学习方法）与哈佛大学商学院的案例研究相结合。传统和前卫在一个艰难的平衡中，在最苛刻的学术行程中。

规模经济

TECH是世界上最大的网上大学。它拥有超过10,000个大学研究生课程的组合。而在新经济中，**数量+技术=颠覆性价格**.这确保了学习费用不像在其他大学那样昂贵。

03

为什么选择我们的课程?

完成科技课程意味着在高级商业管理领域取得职业成功的可能性倍增。

这是一个需要努力和奉献的挑战，但它为我们打开了通往美好未来的大门。学生将从最好的教学团队和最灵活、最创新的教育方法中学习。

我们拥有最著名的教师队伍和市场上最完整的教学大纲，这使我们能够为您提供最高学术水平的培训"

该方案将提供众多的就业和个人利益,包括以下内容。

01

对学生的职业生涯给予明确的推动

通过在TECH学习,学生将能够掌握自己的未来,并充分开发自己的潜力。完成该课程后,你将获得必要的技能,在短期内对你的职业生涯作出积极的改变。

本专业70%的学员在不到2年的时间内实现了职业的积极转变。

02

制定公司的战略和全球愿景

TECH提供了一般管理的深刻视野,以了解每个决定如何影响公司的不同职能领域。

我们对公司的全球视野将提高你的战略眼光。

03

巩固高级商业管理的学生

在TECH学习,为学生打开了一扇通往非常重要的专业全景的大门,使他们能够将自己定位为高级管理人员,对国际环境有一个广阔的视野。

你将在100多个高层管理的真实案例中工作。

04

承担新的责任

在该课程中,将介绍最新的趋势、进展和战略,以便学生能够在不断变化的环境中开展专业工作。

45%的受训人员在内部得到晋升。

05

进入一个强大的联系网络

TECH将其学生联系起来，以最大限度地增加机会。有同样关注和渴望成长的学生。你将能够分享合作伙伴、客户或供应商。

你会发现一个对你的职业发展至关重要的联系网络。

06

以严格的方式开发公司项目

学生将获得深刻的战略眼光，这将有助于他们在考虑到公司不同领域的情况下开发自己的项目。

我们20%的学生发展自己的商业理念。

07

提高 软技能 和管理技能

TECH帮助学生应用和发展他们所获得的知识，并提高他们的人际交往能力，使他们成为有所作为的领导者。

提高你的沟通和领导能力，为你的职业注入活力。

08

成为一个独特社区的一部分

学生将成为由精英经理人、大公司、著名机构和来自世界上最著名大学的合格教授组成的社区的一部分：TECH科技大学社区。

我们给你机会与国际知名的教授团队一起进行专业学习。

04

目标

该大学学位将为学生提供有关 Pentesting领域网络安全项目的法规和合规性的创新性更新，为他们的职业生涯带来更多价值。从这个意义上说，TECH 将在整个计划的制定过程中提供教学资源，提高与发现异常和可疑行为有关的技能。因此，在这个课程结束时，毕业生将掌握更多有关 渗透测试和红队的知识。所有这一切，都需要 12 个月的在线培训。

获得这个商学院校级硕士后，你将掌握数字取证调查 (DFIR) 在解决网络犯罪方面的最新应用"

TECH 会把学生的目标作为自己的，并与学生一同致力达成

这个**渗透测试和红队商学院校级硕士**将培训学生：

01 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

02 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

03 了解如何在网络安全团队中有效分配资源，同时考虑到个人技能并最大限度地提高项目生产率

04 提高技术环境下的沟通技能，促进团队成员之间的理解和协调

05 学习项目监测和控制技术，发现偏差并采取必要的纠正措施

06 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

07 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

08 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

09 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

10 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

11 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

12 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

13 学习如何制作详细报告，记录高级 " 红队 "演习的发现、使用的方法和提出的建议

14 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

15 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

05

能力

该学术提案将为毕业生提供当前的 Pentesting视野。这将使你有机会提高自己的技能，担任管理职务，应对具有挑战性和不断变化的情况，甚至与 IT 行业的其他公司紧密有效地合作。这样，专业人员就可以利用信息图表和视频等多种工具，从更实用的角度来看待这一研究领域。

增强你有效检测和预防恶意软件的技能，解决 IT 领域最具挑战性的问题"

01 掌握 指导 团队成员专业发展的技能，促进成长和进步

02 培养网络安全情况下的战略决策技能，考虑对组织安全的短期和长期影响

03 掌握识别、评估和降低网络安全项目特定风险的能力

04 开发实施主动防御措施的技能，在以下基础上加强系统和网络的安全

05 学习网络流量分析技术，以识别模式和异常行为，便于发现潜在威胁

06 掌握应用于网络环境的取证分析技能，有效识别和应对网络事件

07 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

08 培养在法证调查期间识别入侵指标（IoC）的技能，促进事件检测和响应

09 掌握 红队演习的战略规划技能，考虑目标、范围、资源和现实场景

10 掌握识别和优先处理漏洞的技能，突出那些构成最大安全风险的漏洞

06

结构和内容

五项测试和红队课程主要侧重于让毕业生获得与网络安全中的计算机取证相关的能力。因此，这个学位以理论与实践相结合的结构为导向，并辅以高度专业化的专家团队的丰富经验和广泛背景。

没有预定的时间表或连续的评估:TECH 保证你以最快的速度、最灵活的方式获取其学术内容"

教学大纲

这个大学学位包括 1,500 个小时的持续学习，通过最高标准的教学，毕业生将在 IT 和商业领域获得最佳职位。这样，学习者就能克服工作环境带来的各种障碍。该资格认证将提供多种技能，以解决高级 Kerberos 技术、缓解和保护问题。

另一方面，教学团队制定了包含 10 个模块的专属教学大纲，目的是让学生获得与评估应用程序接口和网络服务安全性相关的基本能力，找出可能的漏洞点。

他还将深入探讨旨在减少漏洞和改善安全态势的实用可行建议。从这个意义上说，他们将成为测量方法和预防冲突领域的重要专家。

在这一学术课程中，企业家们将得到独特的 Relearning方法的支持，通过这种方法，他们将能够以无缝的方式研究复杂的概念并吸收其日常应用。同时，该学位将通过创新的 100% 在线学习平台进行教学，不受固定时间表或连续评估时间表的限制。

这个商学院校级硕士为期12个月，分为10个内容模块:

模块 1	进攻性安全
模块 2	网络安全团队管理
模块 3	安全项目管理
模块 4	对 Windows 系统和网络的攻击
模块 5	高级网络黑客
模块 6	网络架构与安全
模块 7	恶意软件分析与开发
模块 8	法证基础知识和 DFIR
模块 9	高级红队演习
模块 10	技术和执行报告

何时,何地,如何授课?

TECH 提供完全在线攻读 渗透测试和红队商学院校级硕士的可能性。在培训持续的12个月中,学生将能够访问这个课程的所有内容,这将使你能够自我管理你的学习时间。

这将是一个独特而关键的教育旅程,将成为你专业发展的决定性一步,助你实现明显的飞跃。

模块 1. 进攻性安全

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. 网络安全团队管理

2.1. 团队管理
2.1.1. 谁是谁
2.1.2. 主任
2.1.3. 结论

2.2. 角色和责任
2.2.1. 角色识别
2.2.2. 有效授权
2.2.3. 期望管理

2.3. 团队建设与发展
2.3.1. 团队建设的阶段
2.3.2. 团体动态
2.3.3. 评估和反馈

2.4. 人才管理
2.4.1. 人才识别
2.4.2. 能力建设
2.4.3. 留住人才

2.5. 团队领导和激励
2.5.1. 领导风格
2.5.2. 动机的理论
2.5.3. 表彰成就

2.6. 沟通和协调
2.6.1. 通讯工具
2.6.2. 沟通障碍
2.6.3. 协调战略

2.7. 战略性员工发展规划
2.7.1. 确定培训需求
2.7.2. 个人发展计划
2.7.3. 跟踪和评估

2.8. 解决冲突
2.8.1. 冲突的识别
2.8.2. 测量方法
2.8.3. 预防冲突

2.9. 质量管理和持续改进
2.9.1. 质量原则
2.9.2. 持续改进的技术
2.9.3. 反馈 和反馈

2.10. 工具和技术
2.10.1. 协作平台
2.10.2. 项目管理
2.10.3. 结论

模块 3. 安全项目管理

3.1. 安全项目管理
3.1.1. 网络安全项目管理的定义和目的
3.1.2. 主要挑战
3.1.3. 考虑因素

3.2. 安全项目的生命周期
3.2.1. 初始阶段和确定目标
3.2.2. 实施和执行
3.2.3. 评估和审查

3.3. 资源规划和估算
3.3.1. 经济管理的基本概念
3.3.2. 确定人力和技术资源
3.3.3. 预算编制和相关费用

3.4. 项目实施和监测
3.4.1. 监测和跟进
3.4.2. 项目的调整和变化
3.4.3. 中期评估和审查

3.5. 项目交流和报告
3.5.1. 有效的沟通策略
3.5.2. 编写报告和演示文稿
3.5.3. 与客户和管理层沟通

3.6. 工具和技术
3.6.1. 规划和组织工具
3.6.2. 协作与交流工具
3.6.3. 文件和存储工具

3.7. 文件和协议
3.7.1. 构建和创建文档
3.7.2. 行动协议
3.7.3. 指导

3.8. 网络安全项目中的法规和合规性
3.8.1. 国际法律法规
3.8.2. 执法
3.8.3. 审计

3.9. 安全项目的风险管理
3.9.1. 风险识别和分析
3.9.2. 缓解战略
3.9.3. 风险监测和审查

3.10. 项目结束
3.10.1. 审查和评估
3.10.2. 最终文件
3.10.3. 反馈信息

模块 4. 对 Windows 系统和网络的攻击

4.1. 视窗和活动目录
4.1.1. Windows 的历史和演变
4.1.2. 活动目录基础知识
4.1.3. 活动目录功能和服务
4.1.4. 活动目录的总体结构

4.2. 活动目录环境中的联网
4.2.1. Windows 中的网络协议
4.2.2. DNS 及其在活动目录中的功能
4.2.3. 网络诊断工具
4.2.4. 活动目录网络部署

4.3. 活动目录中的身份验证和授权
4.3.1. 认证过程和流程
4.3.2. 证书类型
4.3.3. 凭证的存储和管理
4.3.4. 认证安全

4.4. 活动目录中的权限和策略
4.4.1. GPOs
4.4.2. 实施和管理 GPOs
4.4.3. 活动目录权限管理
4.4.4. 许可证中的漏洞和缓解措施

4.5. Kerberos 基础知识
4.5.1. 什么是 Kerberos?
4.5.2. 组件和操作
4.5.3. Kerberos 中的门票
4.5.4. 活动目录中的 Kerberos

4.6. 高级 Kerberos 技术
4.6.1. 常见的 Kerberos 攻击
4.6.2. 缓解和保护
4.6.3. Kerberos 流量监控
4.6.4. 高级 Kerberos 攻击

4.7. 活动目录证书服务 (ADCS)
4.7.1. PKI 基础知识
4.7.2. ADCS 作用和组件
4.7.3. ADCS 配置和部署
4.7.4. ADCS 的安全性

4.8. Active Directory 证书服务 (ADCS) 的攻击与防御
4.8.1. ADCS 的常见漏洞
4.8.2. 攻击和利用技术
4.8.3. 防御和缓解措施
4.8.4. ADCS 监控和审计

4.9. 活动目录审计
4.9.1. 活动目录中审计的重要性
4.9.2. 审计工具
4.9.3. 检测异常和可疑行为
4.9.4. 事件响应和恢复

4.10. Azure AD
4.10.1. Azure AD 基础知识
4.10.2. 与本地活动目录同步
4.10.3. Azure AD 中的身份管理
4.10.4. 与应用程序和服务集成

模块 5. 高级网络黑客

5.1. 网站如何运行
5.1.1. URL 及其组成部分
5.1.2. HTTP方法
5.1.3. 页眉
5.1.4. 如何使用 Burp Suite 查看网络请求

5.2. 会议
5.2.1. 曲奇
5.2.2. JWT标记
5.2.3. 会话劫持攻击
5.2.4. JWT攻击

5.3. 跨站脚本 (XSS)
5.3.1. 什么是 XSS
5.3.2. XSS类型
5.3.3. 利用 XSS
5.3.4. XSLeaks简介

5.4. 数据库注入
5.4.1. 什么是 SQL 注入
5.4.2. 利用 SQLi 窃取信息
5.4.3. SQLi 盲法、时间法和误差法
5.4.4. NoSQLi 注入

5.5. 路径遍历和本地文件包含
5.5.1. 它们是什么及其区别
5.5.2. 常见的过滤器和如何绕过它们
5.5.3. 日志中毒
5.5.4. PHP 中的 LFI

5.6. 验证失败
5.6.1. 用户枚举
5.6.2. 密码
5.6.3. 2FA 旁路
5.6.4. 带有敏感和可修改信息的Cookie

5.7. 远程命令执行
5.7.1. 指令注入
5.7.2. 盲命令注入
5.7.3. 不安全的 PHP反序列化
5.7.4. 不安全的反序列化 Java

5.8. 文件上传
5.8.1. 通过 webhell获取核证的排减量
5.8.2. 文件上传中的 XSS
5.8.3. XML 外部实体 (XXE) 喷射
5.8.4. 文件上传中的路径遍历

5.9. 损坏的接入控制
5.9.1. 不受限制地接触面板
5.9.2. 不安全的直接对象引用（IDOR）
5.9.3. 过滤器旁路
5.9.4. 授权方法不足

5.10. DOM 漏洞和更高级的攻击
5.10.1. 拒绝 Regex 服务
5.10.2. DOM 克隆
5.10.3. 原型污染
5.10.4. HTTP 请求走私

模块 6. 网络架构与安全

6.1. 计算机网络
6.1.1. 基本概念：局域网、广域网、CP、CC 协议
6.1.2. OSI 模型和 TCP/IP
6.1.3. 切换：基这个概念
6.1.4. 路由：基这个概念

6.2. 开关
6.2.1. VLAN 简介
6.2.2. STP
6.2.3. 以太通道
6.2.4. 对第 2 层的攻击

6.3. VLAN
6.3.1. VLAN 的重要性
6.3.2. VLAN 的漏洞
6.3.3. 针对 VLAN 的常见攻击
6.3.4. 缓解措施

6.4. 路由
6.4.1. IP 地址 - IPv4 和 IPv6
6.4.2. 路由：关键概念
6.4.3. 静态路由
6.4.4. 动态路由简介

6.5. IGP 协议
6.5.1. RIP
6.5.2. OSPF
6.5.3. RIP 与 OSPF
6.5.4. 拓扑需求分析

6.6. 周边保护
6.6.1. DMZ
6.6.2. 防火墙
6.6.3. 通用架构
6.6.4. 零信任网络访问

6.7. IDS 和 IPS
6.7.1. 特点
6.7.2. 执行
6.7.3. SIEM 和 SIEM 云
6.7.4. 基于 蜜罐的检测

6.8. TLS 和 VPN
6.8.1. SSL/TLS
6.8.2. TLS：常见攻击
6.8.3. 使用 TLS 的 VPN
6.8.4. 使用 IPSEC 的 VPN

6.9. 无线网络安全
6.9.1. 无线网络简介
6.9.2. 协议
6.9.3. 关键要素
6.9.4. 常见攻击

6.10. 商业网络及如何与之打交道
6.10.1. 逻辑分段
6.10.2. 物理分割
6.10.3. 访问控制
6.10.4. 需要考虑的其他措施

模块 7. 恶意软件分析与开发

7.1. 恶意软件分析和开发
7.1.1. 恶意软件的历史和演变
7.1.2. 恶意软件的分类和类型
7.1.3. malware分析
7.1.4. 恶意软件开发

7.2. 准备环境
7.2.1. 虚拟机配置和 快照
7.2.2. 恶意软件分析工具
7.2.3. 恶意软件开发工具

7.3. 视窗基础知识
7.3.1. PE 文件格式(便携式可执行文件)
7.3.2. 进程和 线程
7.3.3. 文件系统和注册表
7.3.4. Windows Defender

7.4. 基本恶意软件 技术
7.4.1. shellcode生成
7.4.2. 在磁盘上执行 shellcode
7.4.3. 磁盘与内存
7.4.4. 内存中 shellcode 的执行

7.5. 中级恶意软件技术
7.5.1. Windows 上的持久性
7.5.2. 主页文件夹
7.5.3. 注册密钥
7.5.4. 屏幕保护程序

7.6. 先进的恶意软件 技术
7.6.1. 外壳代码 加密(XOR)
7.6.2. 外壳代码 加密(RSA)
7.6.3. 字符串混淆
7.6.4. 工艺注入

7.7. 静态 恶意软件分析
7.7.1. 使用 DIE(轻松检测)分析 封隔器
7.7.2. 使用 PE-Bear 分析切片
7.7.3. 使用 Ghidra 进行反编译

7.8. 动态恶意软件分析
7.8.1. 使用流程黑客观察行为
7.8.2. 使用 API Monitor 分析调用
7.8.3. 使用 Regshot 分析注册表更改
7.8.4. 使用 TCPView 观察网络请求

7.9. .NET中的分析
7.9.1. NET简介
7.9.2. 使用 dnSpy 进行反编译
7.9.3. 使用 dnSpy 调试

7.10. 分析真实恶意软件
7.10.1. 准备环境
7.10.2. 恶意软件静态分析
7.10.3. 动态 恶意软件分析
7.10.4. 制定 YARA 规则

模块 8. 法证基础知识和 DFIR

8.1. 数字取证
8.1.1. 计算机取证的历史和演变
8.1.2. 计算机取证在网络安全中的重要性
8.1.3. 计算机取证的历史和演变

8.2. 计算机取证基础
8.2.1. 监管链及其实施
8.2.2. 数字证据的类型
8.2.3. 证据获取过程

8.3. 文件系统和数据结构
8.3.1. 主要文件系统
8.3.2. 数据隐藏方法
8.3.3. 分析文件元数据和属性

8.4. 操作系统分析
8.4.1. Windows 系统的取证分析
8.4.2. Linux 系统的取证分析
8.4.3. 对 macOS 系统进行取证分析

8.5. 数据恢复和磁盘分析
8.5.1. 从受损介质中恢复数据
8.5.2. 磁盘分析工具
8.5.3. 文件分配表的解释

8.6. 网络和流量分析
8.6.1. 网络数据包捕获和分析
8.6.2. 分析 防火墙日志
8.6.3. 网络入侵检测

8.7. 恶意软件和恶意代码分析
8.7.1. 恶意软件 的分类及其特点
8.7.2. 静态和动态 恶意软件分析
8.7.3. 反汇编和调试技术

8.8. 记录和事件分析
8.8.1. 系统和应用中的寄存器类型
8.8.2. 相关事件的解释
8.8.3. 记录分析工具

8.9. 应对安全事件
8.9.1. 事件响应流程
8.9.2. 制定事件响应计划
8.9.3. 与安全团队协调

8.10. 出示证据和法律
8.10.1. 法律领域的数字证据规则
8.10.2. 编写法医报告
8.10.3. 作为专家证人出庭

模块 9. 高级红队演习

9.1. 高级识别技术
9.1.1. 高级子域枚举
9.1.2. 高级谷歌多金
9.1.3. 社交媒体与收割机

9.2. 高级 网络钓鱼活动
9.2.1. 什么是 反向代理网络钓鱼
9.2.2. 使用 Evilginx绕过 2FA
9.2.3. 泄露数据

9.3. 高级持久性技术
9.3.1. 金色门票
9.3.2. 银票
9.3.3. DCShadow技术

9.4. 高级避险技巧
9.4.1. AMSI旁路
9.4.2. 修改现有工具
9.4.3. Powershell混淆

9.5. 高级横向移动技术
9.5.1. 通行证 (PtT)
9.5.2. 哈希 传球(钥匙传递)
9.5.3. NTLM 中继

9.6. 先进的开采后技术
9.6.1. LSASS转储
9.6.2. 萨姆转储
9.6.3. DCSync攻击

9.7. 高级 旋转技术
9.7.1. 什么是 枢轴转动
9.7.2. 使用 SSH 进行隧道连接
9.7.3. 用凿子旋转

9.8. 物理入侵
9.8.1. 监视和侦察
9.8.2. 尾随和捎带
9.8.3. 开锁

9.9. Wi-Fi攻击
9.9.1. WPA/WPA2 PSK 攻击
9.9.2. AP 流氓攻击
9.9.3. 对 WPA2企业的攻击

9.10. RFID攻击
9.10.1. RFID 读卡器
9.10.2. RFID 卡处理
9.10.3. 制作克隆卡

模块 10. 技术和执行报告

10.1. 报告程序
10.1.1. 报告的结构
10.1.2. 报告程序
10.1.3. 关键概念
10.1.4. 行政人员与技术人员

10.2. 指导
10.2.1. 简介
10.2.2. 导游类型
10.2.3. 国家指南
10.2.4. 使用案例

10.3. 方法
10.3.1. 评估
10.3.2. 五重测试
10.3.3. 审查通用方法
10.3.4. 国家方法介绍

10.4. 报告阶段的技术方法
10.4.1. 了解 pentester的限制
10.4.2. 语言使用和提示
10.4.3. 信息介绍
10.4.4. 常见错误

10.5. 报告阶段的执行方法
10.5.1. 根据背景调整报告
10.5.2. 语言使用和提示
10.5.3. 标准化
10.5.4. 常见错误

10.6. OSSTMM
10.6.1. 了解方法
10.6.2. 认知
10.6.3. 文件
10.6.4. 阐述报告的内容

10.7. LINCE
10.7.1. 了解方法
10.7.2. 认知
10.7.3. 文件
10.7.4. 阐述报告的内容

10.8. 报告漏洞
10.8.1. 关键概念
10.8.2. 量化范围
10.8.3. 脆弱性和证据
10.8.4. 常见错误

10.9. 将报告重点放在客户身上
10.9.1. 工作证据的重要性
10.9.2. 解决方案和缓解措施
10.9.3. 敏感数据和相关数据
10.9.4. 实例和案例

10.10. 报告 重考情况
10.10.1. 关键概念
10.10.2. 了解遗留信息
10.10.3. 错误检查
10.10.4. 添加信息

07

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”

TECH商学院使用案例研究来确定所有内容的背景

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”

该课程使你准备好在不确定的环境中面对商业挑战，使你的企业获得成功。

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。

一种创新并不同的学习方法

该技术课程是一个密集的培训课程，从头开始创建，为国内和国际最高水平的管理人员提供挑战和商业决策。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基础的技术，确保遵循最新的经济，社会和商业现实。

> 你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”

在世界顶级商学院存在的时间里，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临的问题，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

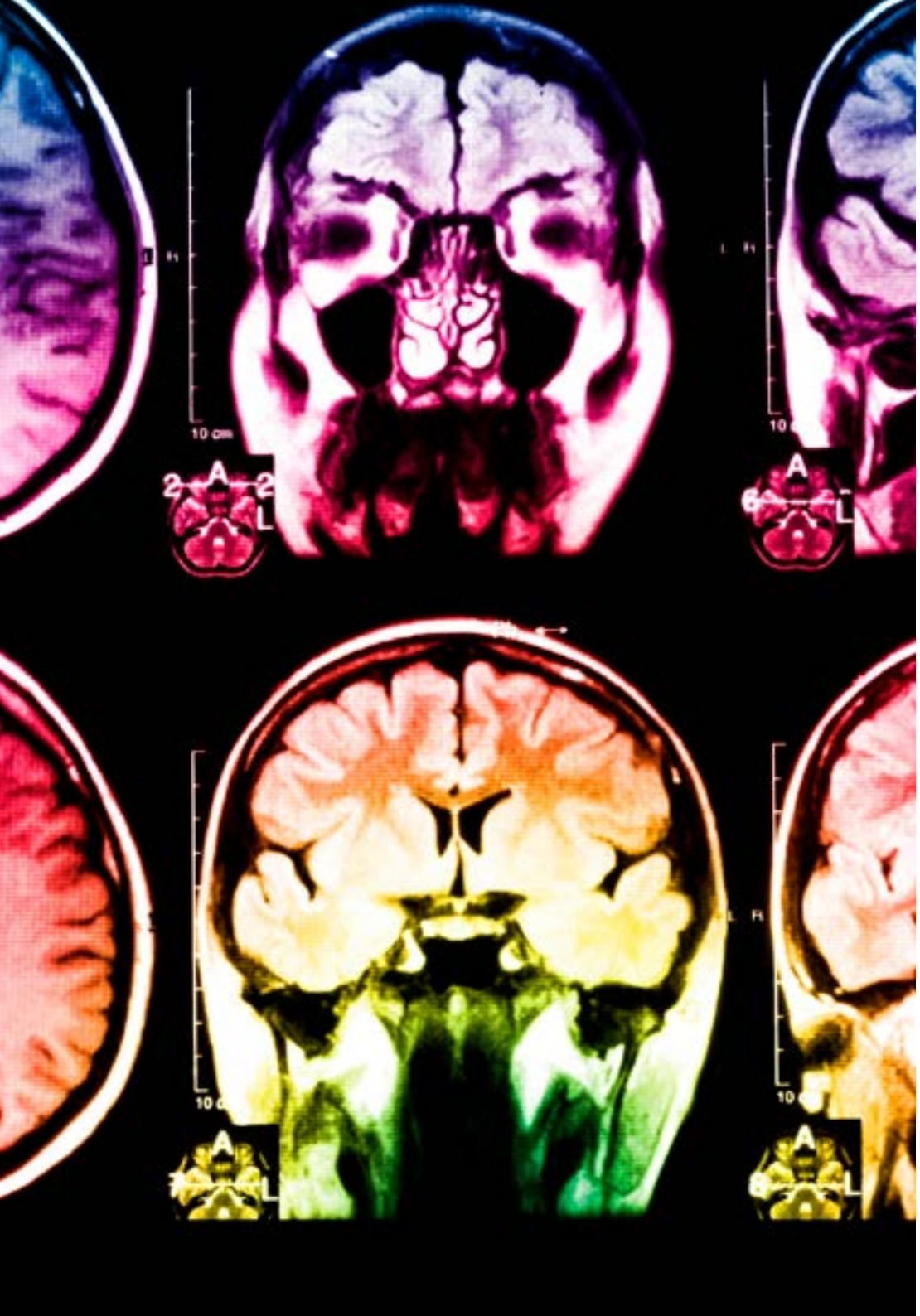
TECH有效地将案例研究方法与基于循环的100%在线学习系统相结合，在每节课中结合了个不同的教学元素。

我们用最好的100%在线教学方法加强案例研究: Re-learning。

> 我们的在线系统将允许你组织你的时间和学习节奏，使其适应你的时间表。你将能够从任何有互联网连接的固定或移动设备上获取容。

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。

我们的商学院是唯一获准采用这种成功方法的西班牙语学校。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。

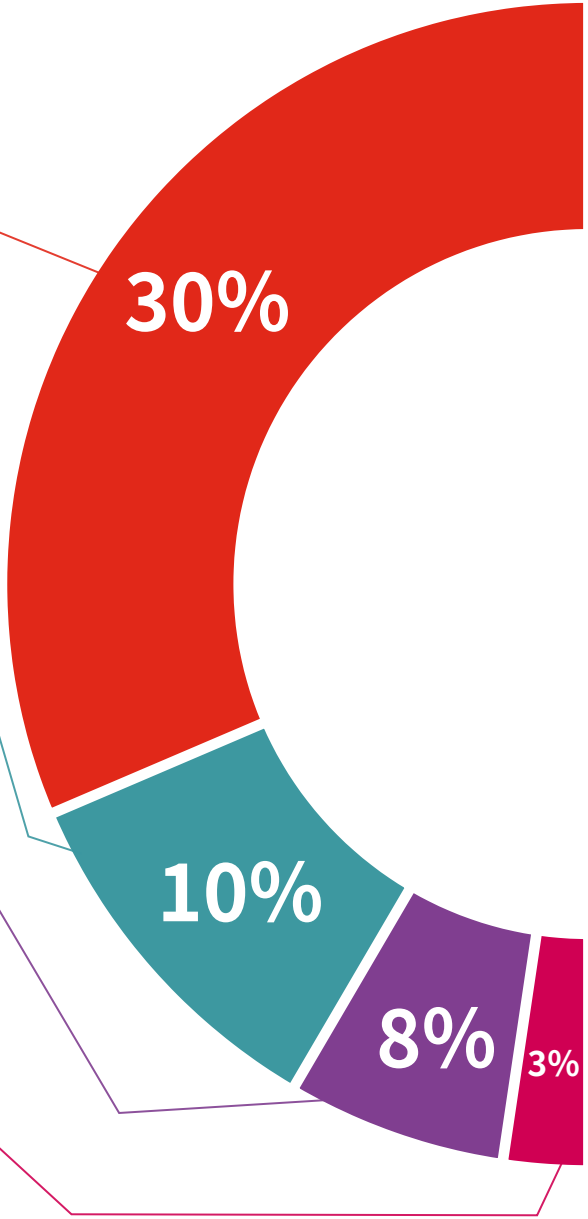
向专家学习可以加强知识和记忆，并为未来的困难决策建立信心。

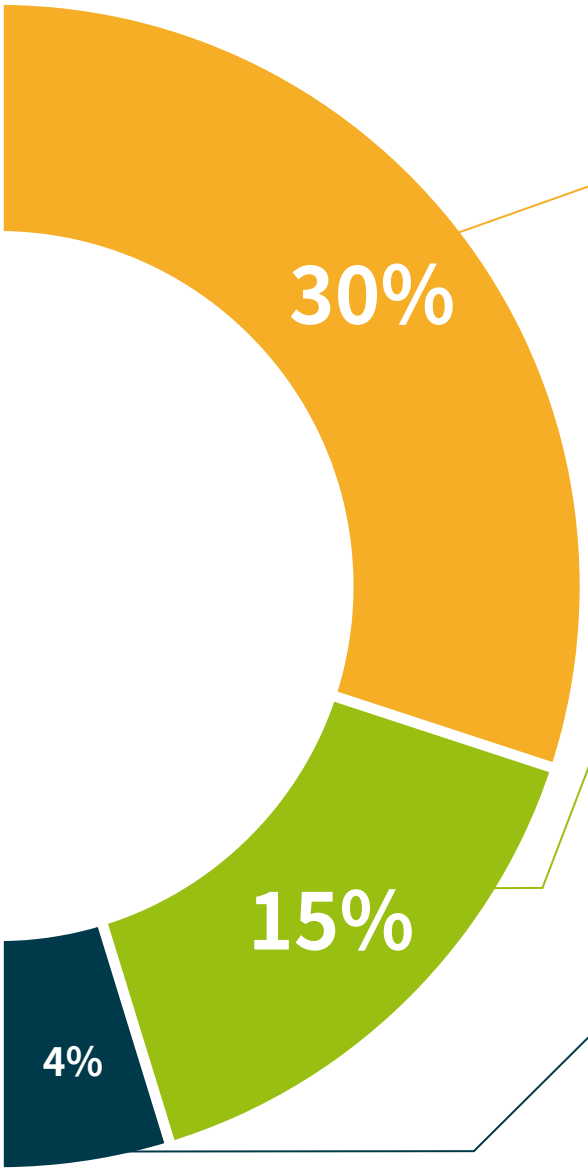
管理技能实习

他们将在每个学科领域开展具体的管理能力发展活动。获得和培训高级管理人员在我们所处的全球化框架内所需的技能和能力的做法和新情况。

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。由国际上最好的高级管理专家介绍，分析和辅导的案例。

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。

08

我们学生的特质

该课程面向大学毕业生和曾在社会和法律科学、行政管理和经济学领域获得以下学位的毕业生。

不同学术背景和来自多个国籍的参与者的多样性构成了这个项目的跨学科取向。

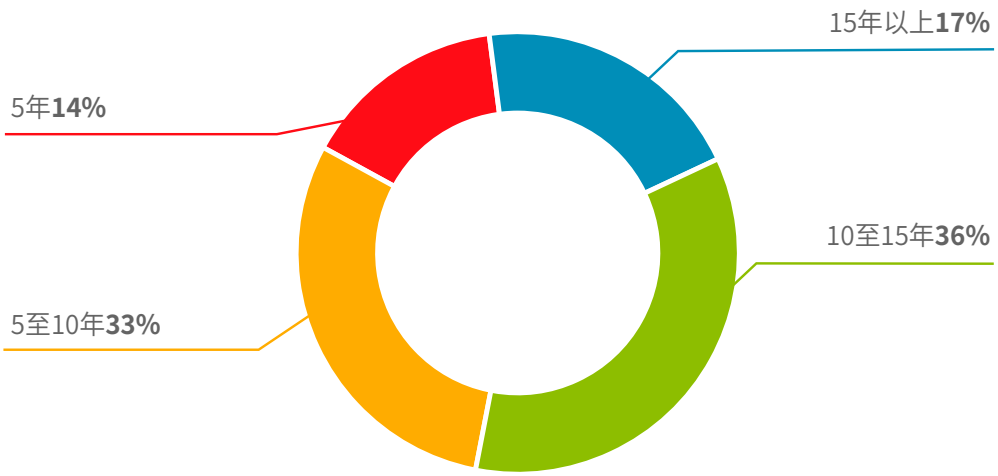
这个课程也面向拥有任何专业的大学学位和两年信息技术领域工作经验的专业人士。

如果你有 渗透测试和红队 方面的经验，并且希望在继续工作的同时，在职业生涯中获得有趣的提升，那么这项计划就是你的理想选择”

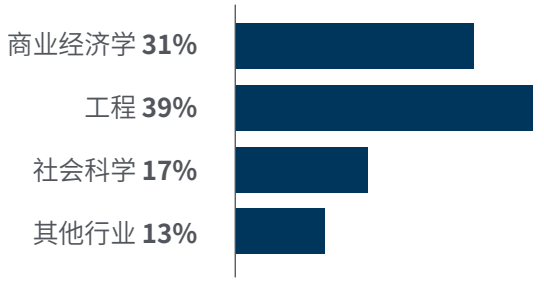
平均年龄

35岁至 **45**岁之间

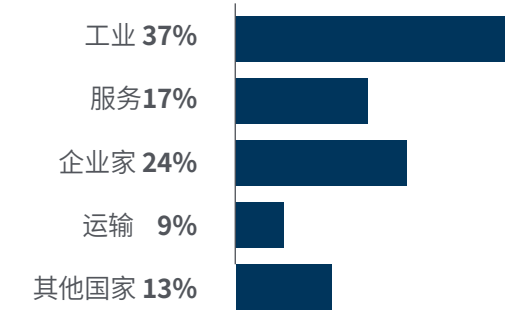
经验年限



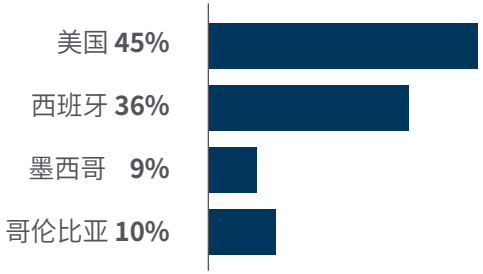
培训



学术概况



地域分布



Salomón Galvis

信息安全分析员

"从这个学位中，我强调自己能够加深对定期评估的重要性以及衡量网络安全的必要性的理解。得益于教学团队在课程开发中采用的关键工具，这项巨大的投资将在未来得到体现"

09

课程管理

这个商学院校级硕士课程拥有一支国际知名的教学团队，他们在信息社会的软件和技术以及商业技术整合中的网络安全方面拥有丰富的专业知识。因此，精英教育体现在充满活力和创新的课程设置方法上，实施网络安全方面的最新趋势。通过这种方式，模拟案例与真实情况分析相结合，为学生提供一流的实践经验，使他们能够在工作场所应对不同的专业挑战。

渗透测试和红队方面的顶尖专家将实施这项创新而严格的课程"

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

González Sanz, Marcos 先生

- 网络安全顾问-网络团队 Cipherbit in Grupo Oesía
- 马德里理工大学软件工程师
- 网络安全专家 辅导员 和核心 倾销员

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

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

Mora Navas, Sergio 先生

- Oesía 集团网络安全顾问
- 胡安-卡洛斯国王大学网络安全工程师
- 布尔戈斯大学计算机工程师

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

> 一次独特、关键且决定性的培训经验，对推动你的职业发展至关重要"

10

对你事业的影响

设计该大学课程的目的是让毕业生掌握相关知识，以应对网络安全领域的任何情况。因此，TECH 将特别注重最高质量的教学，追求每个学位的效率。这样，专业人员就能保证接受五项 测试 和 Red Team方面的专门培训。

红队和网络安全的其他 IT 方面可以通过这个强化学位融入到 Pentesting 中"

你准备好迈出这一步了吗？卓越的职业提升在等着你

TECH 的检测和网络团队硕士学位是一项强化课程，旨在帮助你做好准备，迎接 IT 领域的挑战和商业决策。主要目的是有利于你的个人和职业成长。帮助你获得成功。

如果你想提高自己，在专业水平上实现积极的变化，并与最好的人交流，这里就是你的地方。

TECH 是《福布斯》杂志评选出的世界顶级在线大学，你可以利用这一严格而全面的机会扩展自己的 Pentesting 技能。

在这个为期 12 个月的综合课程结束后，你将掌握的一些技能还包括先进的枢轴技术。

改变的时候到

改变的类型

工资提高

完成这个课程后，我们学生的工资会增长超过**25.55%**

11

对你公司的好处

这个课程通过对高级领导人进行辅导，帮助提升组织人才的能力，充分发挥其潜力。

此外，参加大学选修课也是一个独特的机会，可以利用这个强大的人际关系网络寻找未来的专业合作伙伴、客户或供应商。

在数字时代，管理者必须整合新的流程和战略，从而带来重大变革和组织发展。只有通过大学的培训和更新才能做到这一点"

培养和留住公司的人才是最好的长期投资。

01

人才和智力资本的增长知识资本

该专业人员将为公司带来新的概念、战略和观点，可以为组织带来相关的变化。

02

留住高潜力的管理人员，避免人才流失

这个计划加强了公司和经理人之间的联系，并为公司内部的职业发展开辟了新的途径。

03

培养变革的推动者

你将能够在不确定和危机的时候做出决定，帮助组织克服障碍。

04

增加国际扩张的可能性

由于这一计划，该公司将与世界经济的主要市场接触。

05

开发自己的项目

可以在一个真实的项目上工作，或在其公司的研发或业务发展领域开发新。

06

提高竞争力

该课程将使学生具备接受新挑战的技能，从而促进组织的发展。

12

学位

渗透测试和红队商学院校级硕士除了保证最严格和最新的培训外，还可以获得由TECH科技大学颁发的商学院校级硕士学位证书。

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**渗透测试和红队商学院校级硕士**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**商学院校级硕士**学位。

学位由**TECH科技大学**颁发，证明在商学院校级硕士学位中所获得的资质，并满足工作交流，竞争性考试和职业评估委员会的要求。

学位：**渗透测试和红队商学院校级硕士**

模式: **在线**

时长: **12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

商学院校级硕士

渗透测试和红队

这是一个由本大学授予的学位，相当于1,500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


渗透测试和红队商学院校级硕士

教学大纲概况

科目类型	小时
必修(OB)	1,500
选修 (OP)	0
外部实习 (PR)	0
硕士论文 (TFM)	0
总计1,500	

学期	学科	小时	性质
1°	进攻性安全	150	必修
1°	网络安全团队管理	150	必修
1°	安全项目管理	150	必修
1°	对 Windows 系统和网络的攻击	150	必修
1°	高级网络黑客	150	必修
1°	网络架构与安全	150	必修
1°	恶意软件分析与开发	150	必修
1°	法证基础知识和 DFIR	150	必修
1°	高级 红队演习	150	必修
1°	技术和执行报告	150	必修

Tere Guevara Navarro女士
校长

tech 科学技术大学

*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

商学院校级硕士
渗透测试和红队

- 模式:**在线**
- 时长: **12个月**
- 学位: **TECH 科技大学**
- 课程表:**自由安排时间**
- 考试模式:**在线**

商学院校级硕士
渗透测试和红队

tech 科学技术大学