校级硕士
Pentesting 和 Red Team

tech 科学技术大学

tech 科学技术大学

校级硕士
Pentesting 和 Red Team

- 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**

网页链接: www.techtitute.com/cn/information-technology/professional-master-degree/master-pentesting-red-team

目录

01

介绍

网络攻击的数量和复杂程度已达到令人震惊的地步。随着从 勒索软件 攻击到高级入侵等威胁的指数级增长，对训练有素的网络安全专业人员的需求至关重要。正是在这一背景下，本计划应运而生，它不仅将提供全面的先进安全技术，而且还将应对不断发展的数字环境的现实。通过这种方式，学生将加深对攻击和防御技术的了解，面对最复杂的安全挑战。在加强网络防御需求的推动下，该课程的特点是采用 100% 在线教学方法，并有效利用 Relearning 方法来优化学习效果。

你将在 TECH 的保证下，通过这一开创性计划设计出坚不可摧的安全协议"

与时俱进对于保持抵御当前和新出现威胁的有效性至关重要。在这方面，技术和网络战术的快速发展使得不断更新势在必行。威胁的激增凸显了拥有训练有素的专业人员的紧迫性。

在这种情况下，该大学课程是一项必要的应对措施，因为它不仅能让学生深入了解网络安全领域最先进的技术，还能确保专业人员站在最新趋势和技术的最前沿。

在Pentesting 和 Red Team校级硕士课程的教学大纲中，毕业生将全面了解网络安全领域的需求。它将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。为此，专家们将采用数字取证调查方法来解决案件，从识别到记录调查结果。

此外，他们还将发展高级威胁模拟技能，复制恶意行为者最常用的战术、技术和程序。此外，TECH 的创新方法将确保学生获得在网络安全工作环境中适用且有价值的技能。

学术路径的方法加强了其创新性，因为它将提供 100% 的在线教育环境。这个课程将针对希望提升职业生涯的繁忙专业人士的需求量身定制。此外，它还将采用Relearning方法，通过重复关键概念来固定知识和促进学习。这样，灵活性和强有力的教学方法相结合，不仅可以使其易于使用，而且还能非常有效地培养计算机科学家应对网络安全的动态挑战。

这个**Pentesting 和 Red Team校级硕士**包含市场上最完整和最新的课程。主要特点是：

- 由 Pentesting 和 Red Team 专家介绍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
- 可以进行自我评价过程的实践练习，以提高学习效果
- 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

> 只需 12 个月，你就能为自己的职业生涯带来所需的动力。现在报名，体验立竿见影的进步！"

你想体验职业生涯质量的飞跃吗？在 TECH，你将接受有效实施网络安全项目战略方面的培训"

通过这所《福布斯》杂志评出的全球最佳数字大学，你将学到更多有关识别和评估网络应用程序漏洞的知识。

你将掌握 pentesting 环境中的取证技术。将自己定位为每家公司都在寻找的网络安全专家！

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

这个课程的主要目的是对毕业生进行渗透测试和 Red Team模拟方面的培训。在整个课程中，计算机科学家将沉浸在实用和专业的方法中，培养识别和利用系统和网络漏洞的技能。此外，本课程还旨在让学生深入了解网络安全战术和策略，为应对现实世界的挑战和领导网络安全措施的有效实施做好准备。

你将加深对恶意软件分析和开发的了解，将自己定位为领先的专业人士。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.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.网络安全团队管理

- 培养网络安全团队特有的领导技能，包括激励、鼓舞和协调各方努力实现共同目标的能力
- 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
- 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
- 学习识别和处理网络安全团队内部冲突的策略，促进合作和高效的工作环境
- 了解如何建立衡量标准和评估系统来衡量网络安全团队的绩效，并根据需要做出调整
- 促进将道德实践纳入网络安全团队的管理，确保以合乎道德和法律的方式开展所有活动
- 培养准备和有效管理网络安全事件的能力，确保对威胁做出快速有效的反应

模块3.安全渗透测试项目管理

- 培养规划网络安全项目的技能，确定目标、范围、资源和实施时间表
- 学习有效执行安全项目的策略，确保成功实施计划措施
- 培养在安全项目中有效管理预算和资源分配的技能，最大限度地提高效率和降低成本
- 加强与 stakeholders的有效沟通，以清晰易懂的方式介绍报告和最新情况
- 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
- 让学生熟悉敏捷 Pentesting方法
- 培养详细记录和报告的技能，清楚地说明项目进展情况和取得的成果
- 促进安全项目中不同团队和学科之间的有效合作，确保采用整体协调的方法
- 学习评估和衡量已实施措施有效性的策略，确保持续改进组织的安全态势

模块4.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5.高级网络黑客

- 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6.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7.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8.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9.高级Red Team演习

- 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

模块10.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

能力

通过该课程的学习，毕业生将掌握实施积极防御措施的专业技能，并根据网络安全最佳实践加强系统和网络的安全。此外，学生还将掌握渗透测试和 Red Team模拟的高级技能，擅长主动识别和缓解漏洞。从这个意义上说，专业人员将掌握应对现实世界威胁所需的技术技能，为在动态网络环境中领导有效的安全评估和强化战略做好准备。此外，100% 在线的学习方式使学习更加灵活。

通过 1,500 小时的最佳多媒体内容，成为网络安全专家，并获得 TECH 质量印章"

总体能力

- 掌握规划、执行和管理网络安全项目的能力，确保取得有效成果和实现目标
- 掌握网络架构及其安全方面的高级知识，评估漏洞并实施加强基础设施的战略
- 培养数字取证和事件响应方面的能力，从证据收集到威胁缓解和业务恢复
- 在规划和执行 Red Team演习时应用先进战术，模拟现实世界的情景，评估基础设施的恢复能力，发现薄弱环节，提高应对网络威胁的能力

> 了解识别、评估和降低网络安全项目特定风险的最新流程。选择 TECH！”

具体能力

- 掌握指导团队成员专业发展的技能，促进成长和进步
- 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
- 掌握识别、评估和降低网络安全项目特定风险的能力
- 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
- 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
- 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
- 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
- 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
- 掌握 Red Team演习的战略规划技能，考虑目标、范围、资源和现实场景
- 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

04

课程管理

TECH 汇集了最优秀的专家，他们在该领域的领先企业中拥有广泛和公认的专业背景，为 Pentesting 和 Red Team校级硕士课程的教学团队的建立提供了支持。在这方面，每位教师都将贡献自己的实践经验和专业知识，确保学生从高素质专业人员的教学中受益。此外，对这些专家的精心挑选不仅能确保学术质量，还能确保内容在动态网络安全环境中的相关性和直接适用性。

网络安全行业的巨头们将通过这个独一无二的 TECH 大学课程，在短短 12 个月内助你走向成功”

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

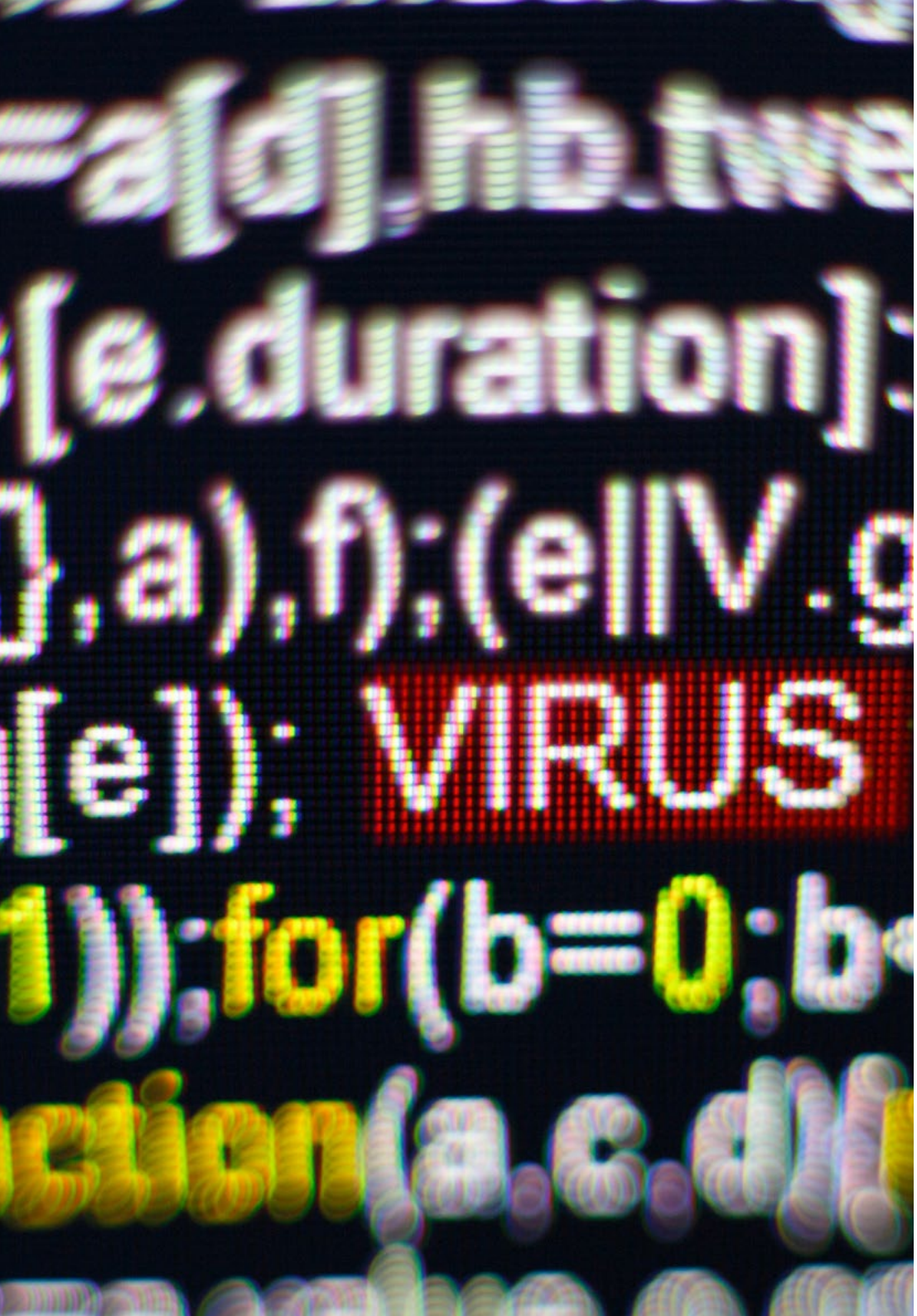
教师

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



Gallego Sánchez, Alejandro 先生
- 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

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

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学工程师

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

05

结构和内容

这个大学课程提供了渗透测试和 Red Team模拟等关键学科的完整课程。在整个课程中，毕业生将掌握高级技能，利用现代技术和工具识别并利用系统和网络中的漏洞。这个专业注重实践，将使网络安全专业人员能够应对现实世界的挑战。因此，在行业专家的指导下，学生将从理论与实践的独特结合中受益，从而加强对网络环境中安全评估策略的理解和有效实施。

你将深入了解网络安全团队的
不同角色和职责。现在报名吧！"

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. 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.安全渗透测试项目管理

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网络和系统的攻击

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. 取证和数字取证基础

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 Red Team 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. Pass-the-Ticket (PtT)
- 9.5.2. Overpass-the-Hash (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. Tailgating 和Piggybacking
- 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

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

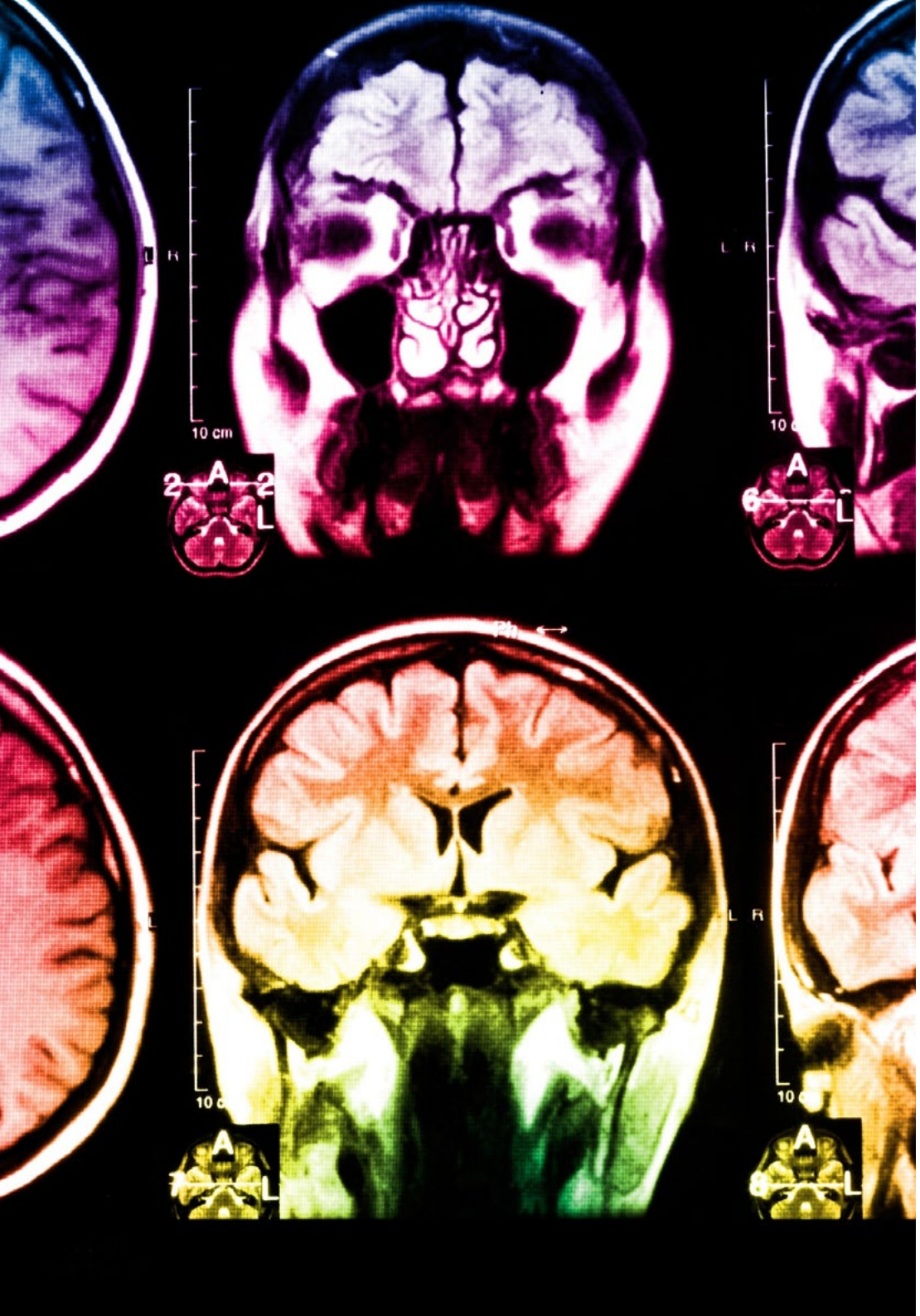
TECH有效地将案例研究方法与基于循环的100%在线学习系统相结合，在每节课中结合了个不同的教学元素。

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。

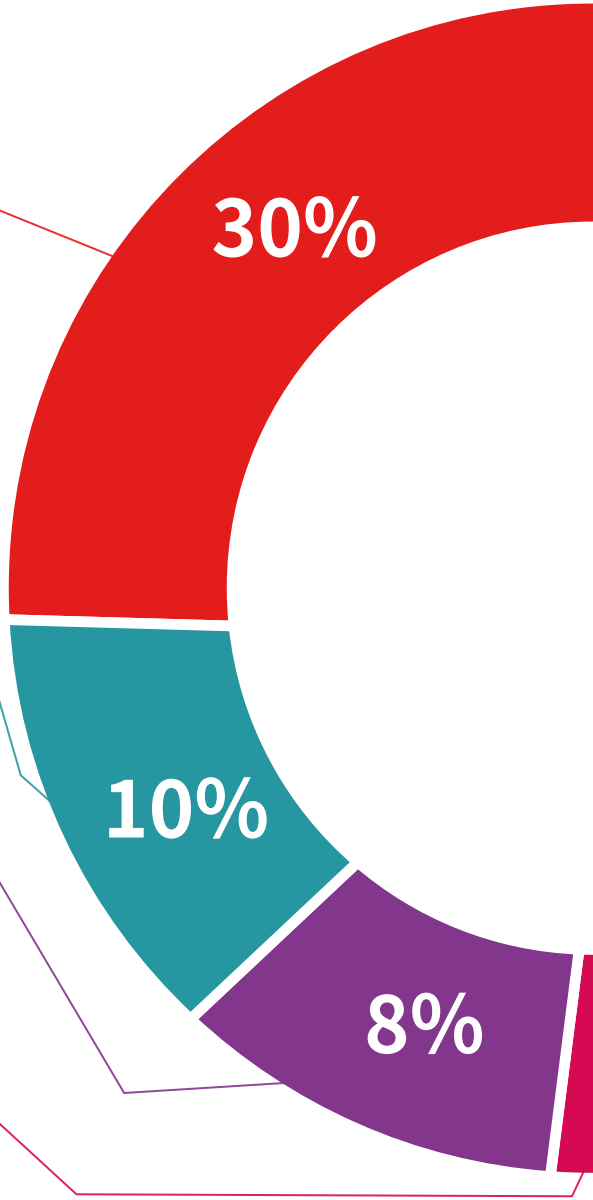
向专家学习可以加强知识和记忆，并为未来的困难决策建立信心。

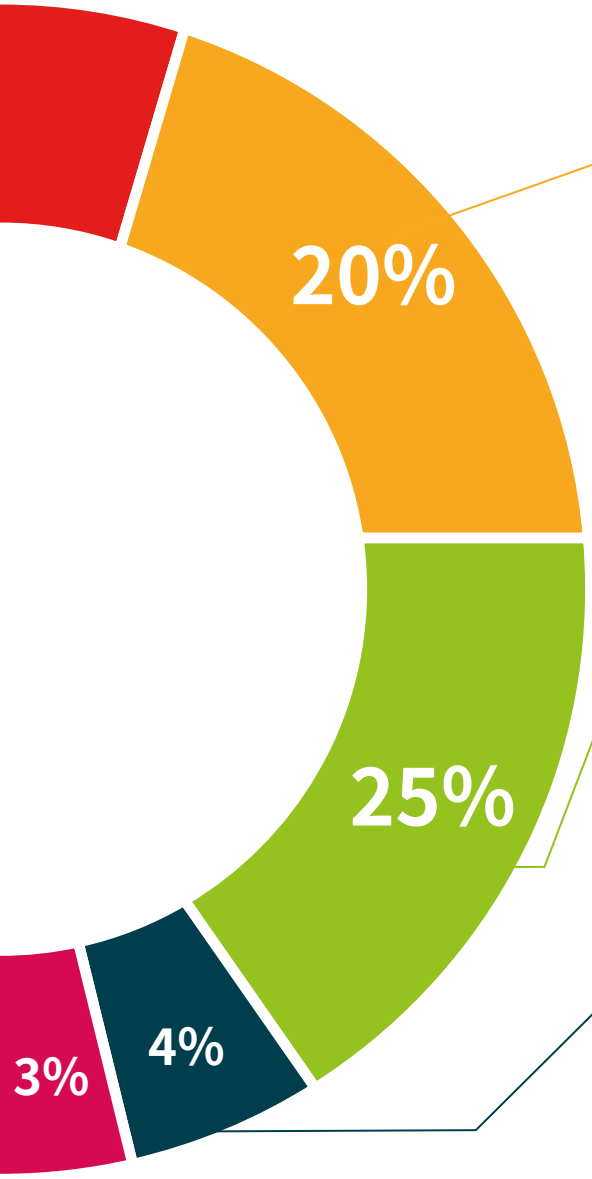
技能和能力的实践

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。

07

学位

Pentesting 和 Red Team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**Pentesting 和 Red Team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**校级硕士**学位。

学位由**TECH科技大学**颁发，证明在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：**Pentesting 和 Red Team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

校级硕士

Pentesting 和 Red Team

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


Pentesting 和 Red Team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°	进攻性网络安全	150	必修
1°	网络安全团队管理	150	必修
1°	安全渗透测试项目管理	150	必修
1°	对Windows网络和系统的攻击	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°	取证和数字取证基础	150	必修
1°	高级 Red Team 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

校级硕士
Pentesting 和 Red Team

- 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**

校级硕士
Pentesting 和 Red Team

tech 科学技术大学