

# 大学课程 高级红队演习



**tech** 科学技术大学

## 大学课程 高级红队演习

- » 模式:在线
- » 时长: 6周
- » 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.techtitude.com/cn/information-technology/postgraduate-certificate/advanced-red-team-exercises](http://www.techtitude.com/cn/information-technology/postgraduate-certificate/advanced-red-team-exercises)

# 目录

01

介绍

---

4

02

目标

---

8

03

课程管理

---

12

04

结构和内容

---

16

05

方法

---

20

06

学位

---

28

# 01 介绍

在网络威胁日益复杂的情况下，需要训练有素的专业人员来识别和消除攻击，这一点至关重要。在这方面，这个大学课程旨在满足这一需求，提供一种全面的方法，培养毕业生应对网络安全方面最复杂的挑战。通过该课程，学生可掌握高级威胁模拟的特定技能，复制恶意行为者采用的战术和程序。此外，该课程 100%在线授课，提供广泛的多媒体内容，并采用 Relearning 方法，通过重复关键概念来强化学习，确保提供全面和最新的培训。



“

你将领导防御网络威胁的工作。在短短 6 周内成为 Red Teaming 领域的佼佼者”

在当今复杂的网络安全形势下,数字威胁日益复杂,参加高级红队演习是绝对必要的。这不仅关系到应对当今的威胁,还关系到培养一种不断改进网络安全的组织文化。在高度动态的环境中,预测和适应不断变化的恶意策略的能力对于保护组织的完整性至关重要。

高级网络团队演习大学课程是对这些需求的全面回应,为专业人员提供了身临其境的机会。这个课程不仅要应对现有的威胁,还要帮助参与者做好准备,以预测和应对未来的挑战。它提供以先进实践为重点的扎实培训,旨在加强组织的安全态势。

作为课程的核心,学员将通过实际和现实的演练,掌握识别基础设施脆弱性的关键技能。红队团队的有效协调成为一个至关重要的方面,可以优化战术和战略的执行,从而全面评估组织的安全性。此外,课程还注重模拟当前的威胁场景,从勒索软件攻击到高级网络钓鱼活动,让专业人员有能力评估组织对危急情况的应对措施。

该课程以 100% 在线模式提供,不仅为在职专业人员提供了灵活性,也体现了应对网络威胁所需的灵活性。此外,还实施了 Relearning 方法,该方法以重复关键概念为基础,以固定知识并促进持续学习。这一战略组合不仅确保了培训的时效性和有效性,而且还使学员具备了在不断挑战的网络安全领域进行战略领导所需的能力。

这个**高级红队演习大学课程**包含市场上最完整和最新的课程。主要特点是:

- 在高级网络团队演习中由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

“

有了这个 100% 在线学习计划和 TECH 质量印章,你将在蓬勃发展的行业中脱颖而出”

“

你将深入了解先进网络组队工具的使用,从而有效执行威胁模拟”

选择TECH吧!你将掌握先进的数字取证技术,以调查网络事件。

在这所被福布斯评为全球最佳数字大学里,你将掌握当今威胁模拟的最新技术。

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

高级网络团队演习课程的主要目标是让毕业生掌握高级威胁模拟技能。这个课程的重点是复制有吸引力的恶意行为者使用的战术、技术和程序 (TTP)，深入了解网络攻击中使用的策略。通过实际演练和现实场景，学生将掌握识别漏洞、评估安全态势和加强基础设施抵御新兴网络威胁的关键技能。





“

升级你的 DCSync 攻击技术, 成为人人都在寻找的红队成员。报名参加, 实现目标”

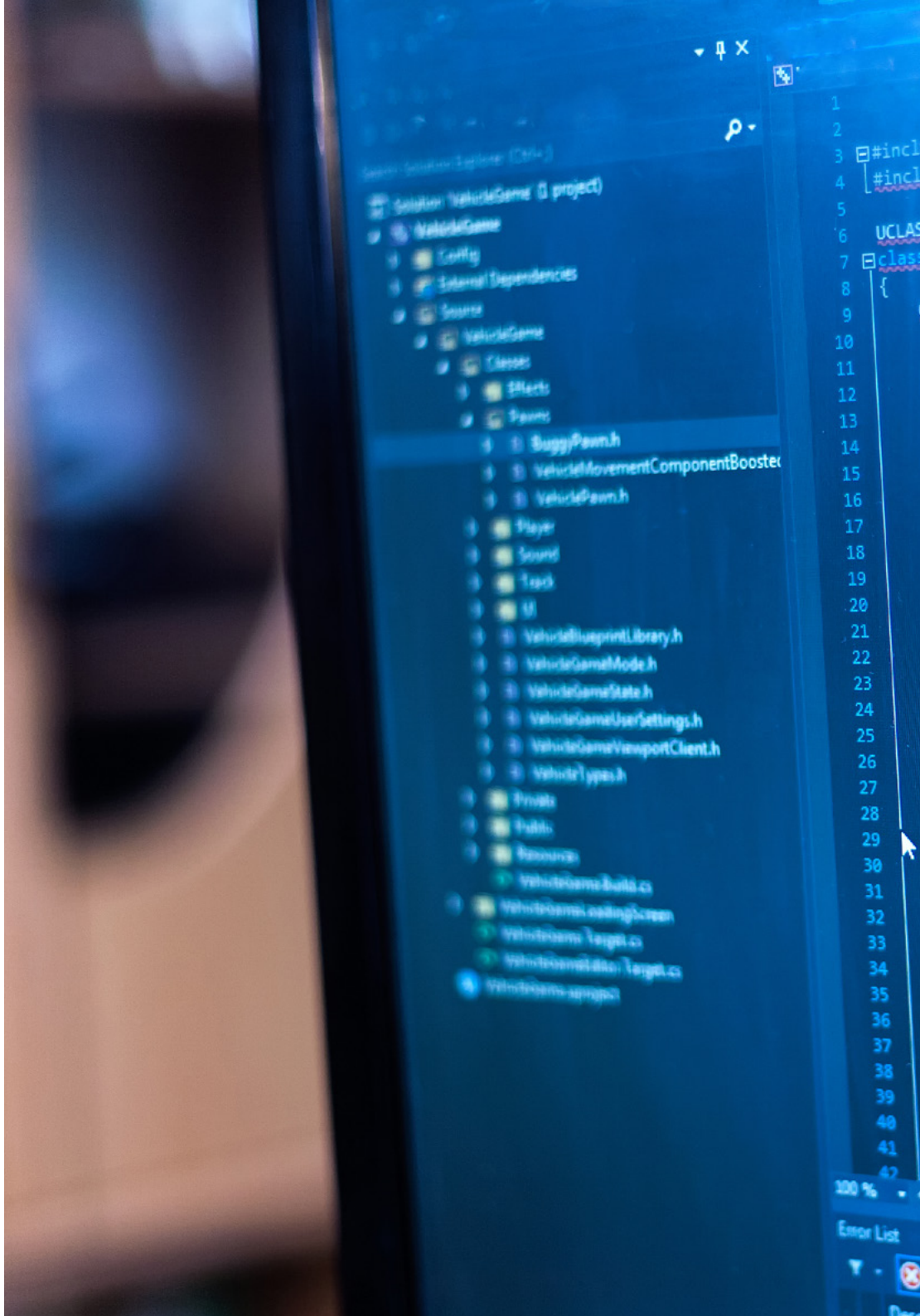


## 总体目标

- 掌握渗透测试和红队模拟的高级技能, 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



你将学习如何识别和利用系统和网络中的复杂漏洞。通过 TECH 实现你的目标!”





## 具体目标

- 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
- 培养红队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,评估红队的表现,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 "红队" 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

```
Output
...
#include "VehicleTypes.h"
#include "BuggyPawn.generated.h"

UCLASS()
ABuggyPawn : public AActor
{
    GENERATED_UCLASS_BODY()

    // Begin Actor overrides
    virtual void PostInitialSetup() override;
    virtual void Tick(float DeltaSeconds) override;
    virtual void ReceiveHit(class UPrimitiveComponent* Component, FVector ImpactLocation) override;
    virtual void FellOutOfLevel(const class UDamageType* DamageType, const class AActor* Instigator) override;
    // End Actor overrides

    // Begin Pawn overrides
    virtual void SetupPlayerInputComponent(class UInputComponent* InputComponent) override;
    virtual float TakeDamage(float Damage, struct FDamageEvent const& DamageEvent, class AActor* Instigator, class AController* Controller) override;
    virtual void TurnOff() override;
    // End Pawn overrides

    /** Identifies if pawn is in its dying state */
    UPROPERTY(VisibleAnywhere, BlueprintReadWrite, Category = "Health", meta = (AllowPrivateAccess = true))
    uint32 bIsDying:1;

    /** replicating death on client */
    UFUNCTION()
    void OnRep_Dying();

    /** Returns True if the pawn can die in the current state */
    virtual bool CanDie() const;

    /** Kills pawn. [Server/authority only] */
    virtual void Die();

    /** Event on death [Server/Client] */
    virtual void OnDeath();

    /** notify about touching new checkpoint */
    void OnTrackPointReached(class AVehicleTrackPoint* TrackPoint);
}

87 Errors 0 Warnings 0 Messages
```

# 03 课程管理

TECH 为这一学术途径组建了一支精英教师队伍。在这方面，每位讲师都是经过精挑细选的，他们在网络安全领域的领先企业中拥有广泛和公认的专业背景。此外，这些专家还带来了丰富的实践经验和专业知识，确保课程毕业生能从红队领域的最新趋势和最佳实践中受益。这支世界一流的师资队伍采用直接、基于现实的方法，推动有效学习，培养专业人员应对网络安全领域的现实挑战。



“

你将从该领域最优秀的专家那里了解到更多关于高级网络团队工具的信息。与 TECH 一起开启你的职业生涯!”

## 管理人员



### Gómez Pintado, Carlos 先生

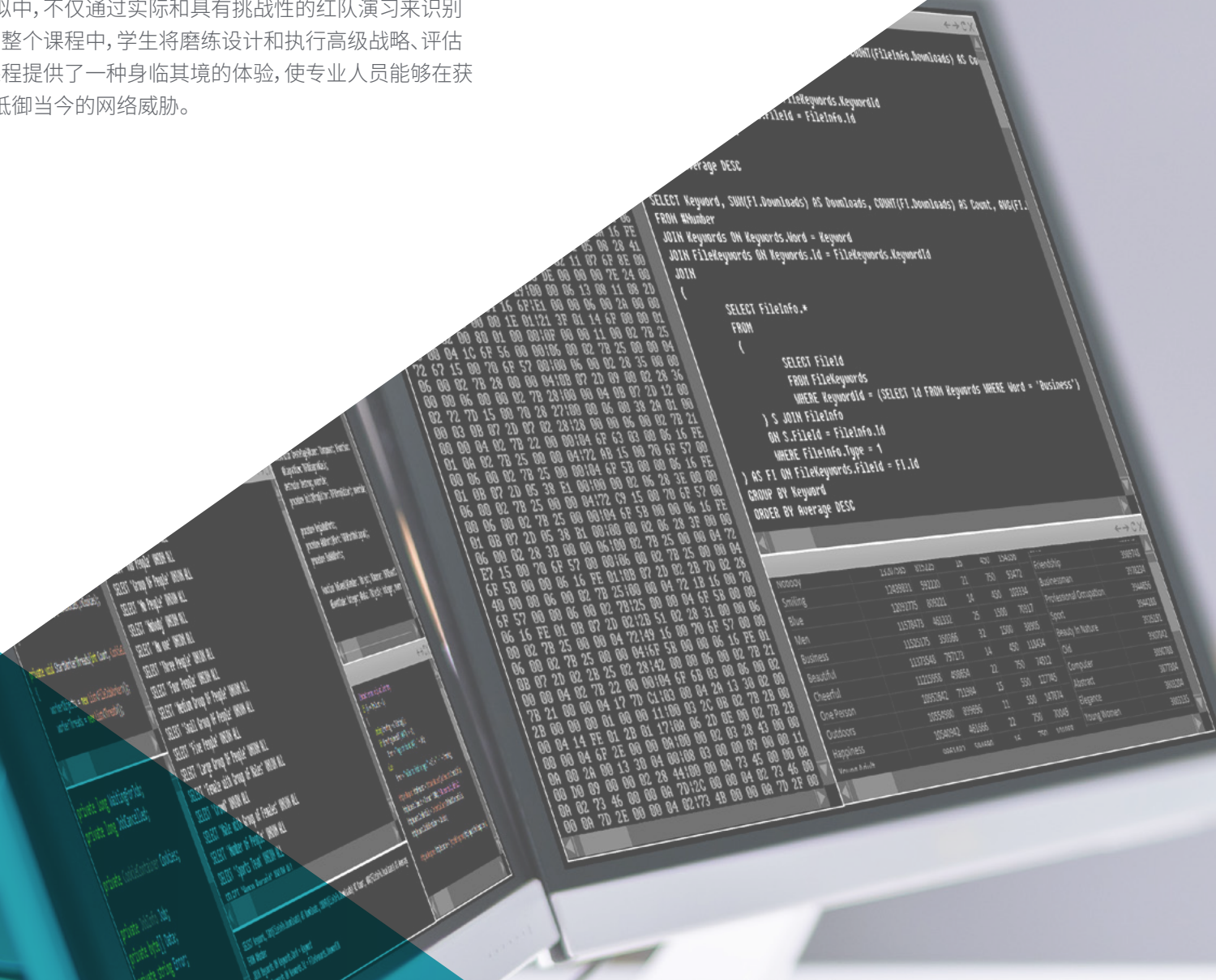
- 网络安全和网络团队 CIPHERbit 经理 (Grupo Oesía)
- Wesson App 管理 顾问兼投资者
- 马德里理工大学软件工程与信息社会技术专业毕业
- 与教育机构合作开发网络安全 高级培训周期



# 04

## 结构和内容

这个课程让毕业生沉浸在逼真的模拟中，不仅通过实际和具有挑战性的红队演习来识别基础设施中的薄弱环节和脆弱性。在整个课程中，学生将磨练设计和执行高级战略、评估和改进组织安全态势的技能。这个课程提供了一种身临其境的体验，使专业人员能够在获得扎实知识的同时，加强网络防御，抵御当今的网络威胁。



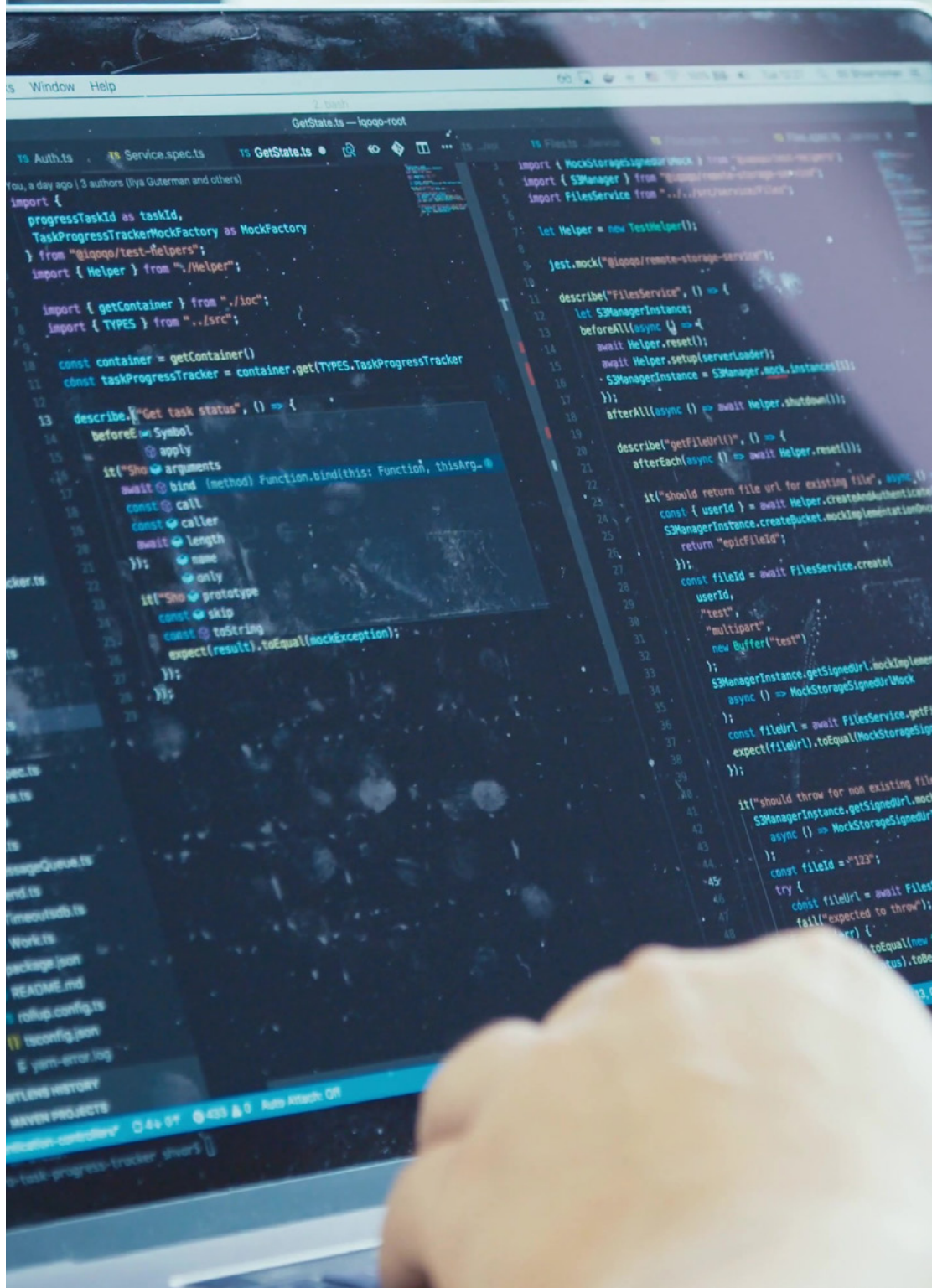


“

通过 150 小时的最佳数字教学，  
你将设计出有效的网络钓鱼活动”

## 模块 1. 高级红队演习

- 1.1. 高级侦察技术
  - 1.1.1. 高级子域枚举
  - 1.1.2. 高级谷歌多金
  - 1.1.3. 社交媒体与收割机
- 1.2. 高级网络钓鱼活动
  - 1.2.1. 什么是反向代理网络钓鱼
  - 1.2.2. 使用 evilginx 旁路 2FA
  - 1.2.3. 泄露数据
- 1.3. 高级持久性技术
  - 1.3.1. 金色门票
  - 1.3.2. 银票
  - 1.3.3. DCSshadow 技术
- 1.4. 高级避险技巧
  - 1.4.1. AMSI 旁路
  - 1.4.2. 修改现有工具
  - 1.4.3. Powershell 混淆
- 1.5. 高级横向移动技术
  - 1.5.1. 通行证 (PtT)
  - 1.5.2. 哈希传球 (钥匙传递)
  - 1.5.3. NTLM 中继
- 1.6. 先进的开采后技术
  - 1.6.1. LSASS 转储
  - 1.6.2. 萨姆转储
  - 1.6.3. DCSync 攻击



- 1.7. 高级旋转技术
  - 1.7.1. 什么是枢轴转动
  - 1.7.2. 使用 SSH 进行隧道连接
  - 1.7.3. 用凿子旋转
- 1.8. 物理入侵
  - 1.8.1. 监视和侦察
  - 1.8.2. 尾随和捎带
  - 1.8.3. 开锁
- 1.9. Wi-Fi 攻击
  - 1.9.1. WPA/WPA2 PSK 攻击
  - 1.9.2. AP 流氓攻击
  - 1.9.3. 对 WPA2 企业的攻击
- 1.10. RFID攻击
  - 1.10.1. RFID 读卡器
  - 1.10.2. RFID 卡处理
  - 1.10.3. 制作克隆卡



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

# 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。



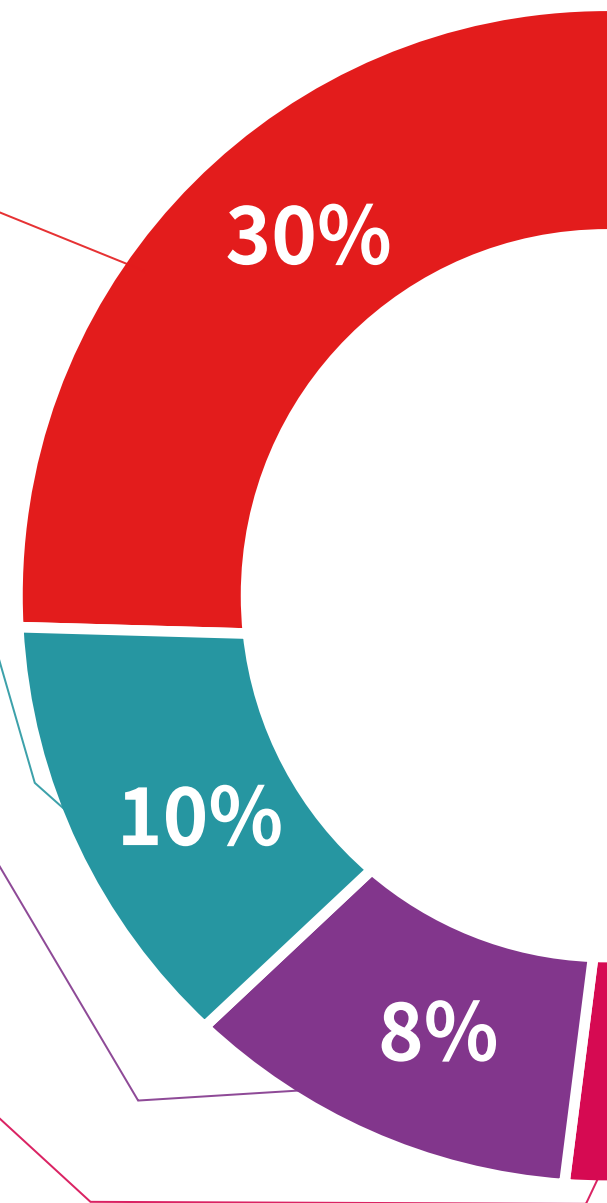
### 技能和能力的实践

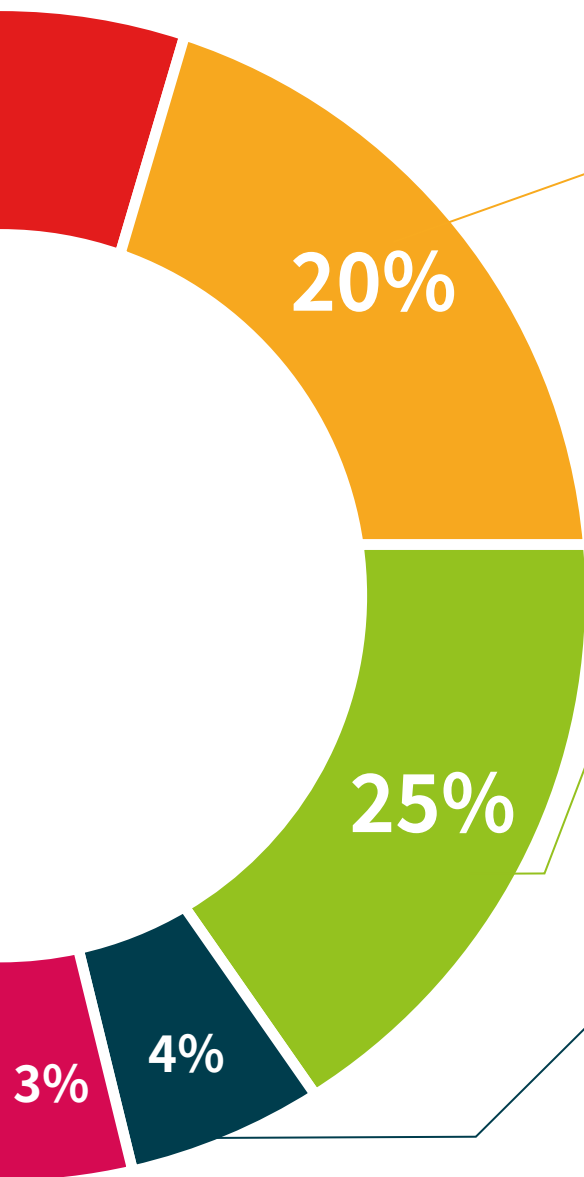
你将开展活动以发展每个学科领域的具体能力和技能。在我们所处的全球化框架内,我们提供实践和氛围帮你取得成为专家所需的技能和能力。



### 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

高级红队演习大学课程除了保证最严格和最新的培训外,还可以获得由TECH科技大学颁发的大学课程学位证书。





“

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”

这个高级红队演习大学课程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大学课程学位。

TECH科技大学颁发的证书将表达在大学课程获得的资格, 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: 高级红队演习大学课程

模式: 在线

时长: 6周



健康 信心 未来 人 导师  
教育 信息 教学  
保证 资格认证 学习  
机构 社区 科技 承诺  
个性化的关注 现在 创新  
知识 网页 质量  
网上教室 发展 语言 机构

**tech** 科学技术大学

大学课程  
高级红队演习

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

# 大学课程 高级红队演习

