CSD 方向《正义之战》课程大纲

在这样一个全球电子互联、计算机病毒和电子黑客充斥、电子窃听和电子欺诈肆虐的时代，“安全不是问题”早已成为历史。计算机系统及网络互联的爆炸性增长，极大地加强了机构和个人对利用这些系统存储和交换信息的依赖程度。人们越来越清醒地认识到保护数据和资源免遭泄露，保障数据和信息的真实性，以及保护基于网络的系统免受攻击等问题的必要性和紧迫性。另一方面，密码学在信息安全领域的广泛应用，基于各种信息技术的安全产品相继问世，为有效解决上述问题提供了可能。

“知己知彼百战不殆”。历史事实一再证明，对敌人了解得越多，包括他们的策略、技能、工具和动机，就越有利于制定出能够克敌制胜的战略战术，面对来犯之敌，施以精准打击，事半而功倍。今天，已经有越来越多的机构和组织出于信息安全的考虑，雇佣大批所谓“正义黑客”，即渗透测试人员，利用他们所掌握的攻击技术，尽可能模仿真正的黑客，在不造成任何实质性损失的前提下，模拟发动从系统到网络的全面进攻，以切实验证和不断完善自身的安全体系和安全策略，当真正的黑客发起攻击时，方能保护自己免受伤害。

一个网络管理员、软件工程师或者安全专家，只有真正了解黑客的攻击方法，才能模仿他们的活动，进行有效的渗透测试。这是测试系统和环境安全级别的唯一途径。当真正的攻击发生时，才能有的放矢地采取应对之策，保障系统和环境的安全。一旦踏上正义黑客之路，理解正义黑客和网络犯罪的异同就显得至关重要。正义黑客通过对恶意行为的模拟，以通过现实基准来帮助客户对系统和环境的安全性进行客观而精准的评估。这是一场正义与邪恶的较量，正义的勇士必须洞悉敌人的诡计，方能御敌于千里之外。

鉴于以上原因，本方向结合自身的专业学科特点，拟开设为期 12 天的《正义之战》课程，具体包括：

- 基础技术
- 注入技术
- 启动技术
- 自启技术

- 提权技术
- 隐藏技术
- 压缩技术
- 加密技术
- 传输技术
- 驱动技术
- 文件技术
- 注册表技术
- 钩子技术
- 监控技术
- 反监控技术
- 攻击技术

等，共计 16 个专题。内容涵盖了当前黑客攻击的各种技术手段。本课程旨在帮助信息安全领域从业人员真正理解所谓黑客攻击是怎么做到的，如何模拟这样的攻击以测试和评估其服务对象的安全状况，并据此制定出有针对性的策略和方法。以下是本课程教学大纲：

基础技术 (0.5 天)	单一实例	接口函数
		实现原理
		编写代码
		测试验证
	延迟加载	实现原理
	资源释放	添加资源
		接口函数
		实现原理
		编写代码
		测试验证
注入技术 (1 天)	全局钩子	接口函数
		编码实现
		测试验证
	远程线程	接口函数
		实现原理
		编写代码
		测试验证
	突破隔离	实现原理

		编写代码
		测试验证
	异步过程	接口函数
		实现原理
		编写代码
		测试验证
启动技术 (0.5 天)	创建进程	接口函数
		编码实现
		测试验证
	突破隔离	接口函数
		实现原理
		编写代码
		测试验证
	内存加载	实现原理
		编写代码
		测试验证
自启技术 (0.5 天)	注册表项	接口函数
		实现原理
		编写代码
		测试验证
	启动目录	接口函数
		实现原理
		编写代码
		测试验证
	计划任务	编码实现
		测试验证
	系统服务	接口函数
		编码实现
		测试验证
提权技术 (0.5 天)	进程令牌	接口函数
		实现原理
		编写代码
	绕过 UAC	借助白名单绕过 UAC
		借助 COM 组件绕过 UAC
隐藏技术 (1 天)	进程伪装	接口函数
		实现原理
		编写代码
		测试验证
	傀儡进程	接口函数
		实现原理
		编写代码
		测试验证
	进程隐藏	接口函数

		编码实现
		测试验证
	动态库劫持	编码实现
		测试验证
压缩技术 (0.5 天)	压缩函数	接口函数
		编码实现
		测试验证
	ZLIB 库	编译链接
		编码实现
		测试验证
加密技术 (0.5 天)	加密函数	HASH 摘要
		AES 加解密
		RSA 加解密
	Crypto++库	编译链接
		导入设置
		HASH 摘要
		AES 加解密
		RSA 加解密
传输技术 (1 天)	Socket 通信	TCP 通信
		UDP 通信
	FTP 通信	FTP 上传
		FTP 下载
	HTTP 通信	HTTP 上传
		HTTP 下载
	HTTPS 通信	HTTPS 上传
		HTTPS 下载
		测试验证
驱动技术 (0.5 天)	环境安装	安装驱动开发工具
	环境搭建	搭建驱动开发环境
		搭建驱动测试环境
		双机调试驱动程序
	无码调试	调试无源码驱动程序
		无源码驱动入口断点
	驱动开发	32/64 位驱动程序开发
文件技术 (0.5 天)	内核函数	创建文件或目录
		删除文件或空目录
		获取文件大小
		读写文件内容
		重命名文件
		遍历目录
	IRP 消息	接口函数
		创建或打开文件
		获取文件信息

		设置文件信息
		读写文件内容
		遍历目录
		测试验证
	NTFS 解析	文件系统
		文件定位
注册表技术 (0.5 天)	内核函数	创建注册表键
		删除注册表键
		修改注册表键
		查询注册表键
	HIVE 文件	HIVE 文件结构
		HIVE 文件解析
钩子技术 (0.5 天)	系统服务描述表钩子	系统服务描述表函数索引
		系统服务描述表及其函数地址
		系统服务描述表钩子
	过滤驱动	编码实现
		测试验证
监控技术 (1 天)	进程创建监控	接口函数
		破解内核函数强制完整性签名限制
		编码实现
		测试验证
	模块加载监控	接口函数
		编码实现
		测试验证
	注册表监控	接口函数
		编码实现
		测试验证
	对象监控	接口函数
		编码实现
		测试验证
	Minifilter 文件监控	接口函数
		编码实现
		测试验证
	WFP 网络监控	编码实现
		测试验证
反监控技术 (1 天)	反进程创建监控	编码实现
		测试验证
	反线程创建监控	编码实现
		测试验证
	反模块加载监控	编码实现
		测试验证
	反注册表监控	编码实现
		测试验证

	反对象监控	编码实现
		测试验证
	反 Minifilter 文件监控	接口函数
		编码实现
		测试验证
攻击技术 (2 天)	进程遍历	接口函数
		实现原理
		编写代码
		测试验证
	文件遍历	接口函数
		实现原理
		编写代码
		测试验证
	桌面截屏	接口函数
		实现原理
		测试验证
	按键记录	接口函数
		编码实现
		测试验证
	远程命令	接口函数
		实现原理
		编写代码
		测试验证
	U 盘监控	接口函数
		实现原理
		编写代码
		测试验证
	文件监控	接口函数
		实现原理
		编写代码
		测试验证
	自我删除	接口函数
		编码实现
	驱动隐藏	编码实现
		测试验证
	进程隐藏	实现原理
		编写代码
		测试验证
	通信隐藏	编码实现
		测试验证
	强行终止	实现原理
		编写代码
		测试验证

	文件保护	编码实现
		测试验证
	文件强删	编码实现
		测试验证

本课程共 12 天，要求学员完成如下先修课程：

- 《C/C++程序设计语言》
- 《UNIX/Linux 系统高级编程》
- 《Windows 系统高级编程》
- 《网络安全》
- 《黑客攻防》