CSD 方向《黑客攻防》课程大纲

“黑客”一词源于英语“Hacker”的音译，是指专门研究、发现计算机和网络漏洞的计算机爱好者。因此黑客在业内带有浓厚的褒义色彩。但同样是“黑客”一词，在圈外或大众媒体上却通常被定义为，专门入侵他人计算机系统，从事破坏或窃取信息等不法行为的人。这其实是对黑客文化的一种误解，因为从严格意义上讲，后者应该被称为“骇客”，即“Cracker”。黑客与骇客所采取的技术性攻击手段也许非常相似，但它们的目的却有着天壤之别，前者是为了发现系统中潜在的缺陷，及时采取措施加以防范，而后者则纯粹是为了利用系统中的漏洞，以达到其不可告人的罪恶目的。

真正意义上的黑客显然不可能仅仅满足于使用现成的工具，他们必须具备独立编写程序，开发各种攻防利器的能力。黑客编程带有鲜明的两面性，一方面关注攻击，如：扫描器、嗅探器、后门、查壳器、动态调试器、静态分析器、补丁等，另一方面关注防范，如：杀毒软件、防火墙、主动防御系统、加壳、加密狗、电子令牌等。攻击并非黑客编程的目的，而是提高防范能力的手段。这需要学习和从业者具备良好的心态和足够高的道德水准。

放眼国内外，当前的社会背景和政策环境都对信息安全产业释放出重大利好信号。无论是党的十八大以来信息安全不断被提升到国家安全的战略高度，还是震惊全球的“棱镜门”事件，抑或是当前势不可挡的互联网大潮，无不预示着信息安全领域及其从业者，在可以预见的未来，势必彻底摆脱被边缘化的命运，进而成为整个 IT 产业主流群体中的一员，甚至是中流砥柱。这些改变将进一步加剧当前信息安全领域高端人才稀缺的矛盾，同时为信息安全领域创造出数量空前的就业岗位。

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 10 天的《黑客攻防》课程，具体包括：

- 黑客编程入门
- 黑客网络编程
- 黑客系统编程
- 黑客内核编程

- 黑客逆向分析
- 黑客代码破解
- 黑客钩子编程
- 黑客编程实战

等，共计 8 个专题。内容涵盖了当前黑客技术的主要领域和方向。为了提高学员的动手实操能力，课程中的每个专题皆伴随有若干实训案例，边学边练，既巩固了所学理论知识，同时又兼顾了一定的实用性。以下是本课程教学大纲：

黑客编程入门 (0.5 天)	Windows 消息	演示测试
		代码解释
		窗口类名
	过程驱动与事件驱动	代码的执行流程
		典型的 Windows 应用程序
	鼠标与键盘	通过发送消息模拟鼠标键盘操作
		通过调用函数模拟鼠标键盘操作
	进程间通信	通过自定义消息实现进程间通信
		通过 WM_COPYDATA 消息实现进程间通信
	开发与调试工具	Error Lookup
		Windows Error Lookup Tool
		Visual C++调试器
黑客网络编程 (1 天)	Winsock 编程基础	网络基础知识
		面向连接协议与面向无连接协议
		Winsock 常用函数
		字节序
	Winsock 编程实例	基于 TCP 的通信
		基于 UDP 的通信
		口令暴力猜解
	非阻塞模式	Winsock 工作模式
		简单远程控制
	原始套接字	ping 命令的使用
		ping 命令的构造
		ping 命令的实现
黑客系统编程 (1 天)	文件	文件操作函数
		制作 U 盘病毒
		免疫 U 盘病毒
	注册表	注册表结构
		注册表函数
		注册表启动项
	服务	查看系统服务

		管理系统服务
	进程与线程	创建进程
		终止进程
		枚举进程
		暂停与恢复进程
		多线程编程
	动态链接库	构建动态链接库
		远程线程注入
黑客内核编程 (1 天)	驱动	编写驱动
		编译驱动
		装载驱动
		装载工具
	文件	文件读写程序
		文件读写函数
	注册表	注册表读写程序
		注册表读写函数
黑客逆向分析 (1 天)	汇编语言	寄存器
		指令集
		寻址方式
	调试工具	OllyDbg 简介
		OllyDbg 实例
	反汇编工具	IDA 使用方法
	C 语言逆向基础	函数
		条件选择
		开关分支
		循环
	逆向分析实例	wcslen 函数的逆向分析
		扫雷游戏的逆向破解
黑客代码破解 (2 天)	PE 结构简介	PE 结构的总体概况
		PE 结构的组成部分
	PE 结构详解	DOS 头
		Windows 头
		文件头
		可选头
		节区头
	PE 结构地址	三种地址
		地址转换
	PE 结构编程	PE 查看器
		查壳工具
		地址转换器
		添加节区
	破解与补丁	编写 CrackMe
		破解 CrackMe

		文件补丁与内存补丁
	调试 API	三种断点
		调试 API 函数及相关结构体
	密码显示器	借助调试 API 显式正确的密码
	破解工具	KeyMake 使用方法
黑客钩子编程 (1.5 天)	钩子简介	DOS 的中断向量与 Windows 的钩子
	内联钩子	基本原理
		具体实现
		应用案例
		目标地址
		注意事项
	导入表钩子	导入表基本概念
		导入表数据结构
		手动分析导入表
		编程遍历导入表
		导入表钩子原理
		导入表钩子实例
	Windows 钩子	基本原理
		常用函数
		编程实例
黑客编程实战 (2 天)	恶意程序	恶意程序的自启动
		木马的配置生成与反弹端口
		病毒的感染
		病毒的自删除
		隐藏动态链接库
		端口复用
		远程命令
	黑客工具	端口扫描
		嗅探器
	反病毒	病毒专杀
		行为监控
		U 盘防御
		目录监控
	主引导记录	手动分析主引导记录
		主引导记录数据结构
		硬盘设备的符号链接
		编程解析主引导记录
	壳	手动加壳
		编程加壳
	进程遍历	配置驱动调试
		手动遍历进程
		编程遍历进程
	系统服务描述表钩子	系统服务描述表

		系统服务描述表钩子
		系统服务描述表内联钩子

本课程共 10 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》