CSD 方向《灰帽大师》课程大纲

从广义来讲，所谓黑客包括一切专门研究、发现计算机和网络漏洞的信息安全领域从业人员及业余爱好者，但根据其动机和行为方式的不同，通常将世界范围内的黑客分为如下几类：

- 白帽黑客

  专门研究计算机、网络的防御技术。他们通常受雇于各大公司，对其产品进行模拟黑客攻击，以检验该产品的安全性和可靠性。他们是维护世界计算机、网络安全运行的主要力量。

- 黑帽黑客

  专门研究病毒、木马以及各种计算机系统和网络的漏洞，以个人意志为出发点，对其进行攻击，以获得个人成就感的满足。黑帽黑客虽然具有一定的破坏性，但其危害十分有限，这与能力无关，更多源自其文化、道德和信仰的约束。

- 灰帽黑客

  精通各种计算机、网络的技术性防御原理，且有能力突破这些防御，虽然一般情况下他们并不会真的这样做。尽管灰帽黑客的技术实力往往远超白帽或黑帽黑客，但他们通常既不受雇于任何机构或企业，亦无任何恶意，他们仅将黑客行为作为一种爱好或义务，以此警示世人哪些系统和网络存在漏洞及安全隐患。

- 红帽黑客

  严格来说，红帽黑客仍然属于白帽或灰帽范畴，但又与他们有一些显著的差别。红帽黑客以正义、道德、进步、强大为宗旨，以热爱祖国、坚持正义、开拓进取为精神支柱，这与计算机世界一向秉持网络无国界的信仰迥然不同。因此不能将红帽黑客简单地划归白帽或灰帽中的任何一类。红帽黑客通常会利用自己掌握的技术去维护本国网络的安全，对一切外来进攻予以坚决回击。当一个国家的网络或计算机系统遭受境外势力攻击时，第一时间做出激烈回应的，往往

就是这些红帽黑客们。

- 骇客

  本质上讲，骇客是黑客的一种，但他们的行为已经超出了正常黑客行为的界限。他们怀着各种不可告人目的——畸形的心理诉求、贪婪的物质欲望、不着边际的个人膨胀——对目标系统或网络进行毫无节制的非理性的攻击和破坏。这些人毫无道德底线，为了满足私欲无恶不作。虽然同属黑客范畴，但他们的所作所为已经对计算机和网络安全甚至国家安全构成了严重的威胁。他们的每一次攻击都会造成大范围系统性的恶劣影响，使个人、机构甚至国家蒙受巨大的经济损失，理应成为各国信息安全执法部门重点打击的对象。

本课程的目标是培养更多技术精湛并致力于抵御恶意黑客攻击的信息安全专家。本方向结合自身的专业学科特点，拟开设为期 12 天的《灰帽大师》课程，具体包括：

- 道德与法律
- 编程技能
- 静态分析
- IDA Pro
- 模糊测试
- shellcode
- Linux shellcode
- 欺骗攻击
- 攻击 Cisco 路由器
- 基本 Linux 漏洞攻击
- 高级 Linux 漏洞攻击
- Windows 漏洞攻击
- 内存保护攻击
- 访问控制攻击
- Web 应用攻击
- 堆溢出攻击
- 释放后重用攻击

- 高级客户端攻击
- 补丁比较漏洞攻击
- Android 恶意软件
- 勒索软件
- 64 位恶意软件
- 下一代逆向工程

等，共计 23 个专题。内容涵盖了作为灰帽黑客必须掌握的主要工具和常用技术，同时辅以大量攻防实验巩固所学知识。以下是本课程教学大纲：

道德与法律 (0.25 天)	敌方策略	理解敌方策略的意义
	正义黑客	渗透测试
		恶意黑客
	网络立法	法网恢恢
		工具之争
	漏洞披露	从不同角度看问题
		个中缘由
		CERT/CC
		OIS
		争议
		没有免费的 BUG
		赏金计划
编程技能 (1.75 天)	C 语言	基本结构
		程序范例
		编译链接
	内存知识	随机访问存储器
		字节序
		内存分段
		内存中的程序
		缓冲区
		内存中的字符串
		指针
		综合示例
	Intel 处理器	Intel 处理器
	汇编语言	机器指令、汇编语言与 C 语言
		AT&T 与 MASM
		寻址模式
		汇编结构
		汇编过程
	GDB 调试	GDB 命令

		GDB 反汇编
	Python 语言	安装 Python
		Hello World
		对象
		字符串
		数字
		列表
		字典
		文件
		套接字
静态分析 (0.25 天)	道德的逆向工程	道德的逆向工程
	为什么需要逆向工程	为什么需要逆向工程
	源代码分析	源代码分析工具
		源代码分析工具的实用性
		手工源代码分析
		自动化源代码分析
	二进制分析	手工二进制分析
		自动化二进制分析
IDA Pro (0.25 天)	静态分析的难点	剥离的二进制文件
		静态链接程序和 FLAIR
		数据结构分析
		怪异的 C++代码
	扩展 IDA Pro	编写 Python 脚本
		执行 Python 脚本
模糊测试 (1 天)	什么是模糊测试	什么是模糊测试
	选择目标	输入类型
		易于自动化
		复杂性
	模糊器	变异模糊器
		生成模糊器
	测试案例	寻找测试模板
		从互联网档案馆获取样本
		利用代码覆盖率选取最优模板集
		为模糊测试选取最优样本
	测试框架	Peach 模糊测试策略
		速度的重要性
		崩溃分析
		Peach 变异模糊测试
		其它变异模糊器
	生成模糊器	生成模糊器
shellcode (1 天)	用户空间 shellcode	系统调用
		基本 shellcode
		端口绑定 shellcode

		反向连接 shellcode
		查找套接字 shellcode
		命令执行代码
		文件传输代码
		多级 shellcode
		系统调用代理 shellcode
		进程注入 shellcode
	shellcode 其它因素	shellcode 编码
		shellcode 自毁
		shellcode 反汇编
	内核空间 shellcode	内核空间 shellcode
Linux shellcode (1 天)	基本 shellcode	系统调用
		使用 C 语言的系统调用
		使用汇编语言的系统调用
		exit 系统调用
		setreuid 系统调用
		execve 系统调用
	端口绑定 shellcode	C 语言端口绑定
		汇编语言端口绑定
		测试 shellcode
	反向连接 shellcode	C 语言反向连接
		汇编语言反向连接
	shellcode 编码	简单的异或编码
		编码后 shellcode 的结构
		JMP/CALL XOR 示例
		FNSTENV XOR 示例
		代码整合
	自动生成 shellcode	利用 Metasploit 生成 shellcode
		利用 Metasploit 编码 shellcode
欺骗攻击 (0.5 天)	什么是欺骗	什么是欺骗
	ARP 欺骗	利用 Ettercap 进行 ARP 欺骗
		查看网络流量
		修改网络流量
	DNS 欺骗	利用 Ettercap 进行 DNS 欺骗
		执行攻击
	NetBIOS 和 LLMNR 欺骗	利用 Responder 攻击 NetBIOS 和 LLMNR
		破解 NTLMv1 和 NTLMv2 哈希
攻击 Cisco 路由器 (0.5 天)	攻击团体字符串和密码	利用 Ncrack 猜测凭据
		利用 onesixtyone 猜测团体字符串
	SNMP 和 TFTP	利用 Metasploit 下载配置文件
		利用 SNMP 和 TFTP 修改配置
	攻击 Cisco 密码	攻击 Type-7 密码
		利用 Cain 攻击 Type-7 密码

		利用 Metasploit 攻击 Type-7 密码
		攻击 Type-5 密码
		利用 John the Ripper 攻击 Type-5 密码
	中转流量	建立 GRE 隧道
		在 GRE 隧道上中转流量
	漏洞攻击和保持访问	漏洞攻击
		保持访问
基本 Linux 漏洞攻击 (0.5 天)	栈操作	栈操作
	缓冲区溢出	C 语言缓冲区溢出
		缓冲区溢出的后果
	本地缓冲区溢出攻击	漏洞攻击的组件
		在命令行上攻击
		利用通用漏洞攻击代码攻击
		针对小缓冲区的漏洞攻击
	漏洞攻击的开发过程	构建定制漏洞攻击
		确定偏移
		确定攻击向量
		生成 shellcode
		验证攻击效果
高级 Linux 漏洞攻击 (0.5 天)	格式化字符串攻击	问题描述
		读取任意内存
		写入任意内存
		改变程序执行
	内存保护机制	编译器的改进
		绕过堆栈保护
		内核补丁与脚本
		“Return to libc”攻击
		利用“Return to libc”漏洞保持权限
		方案比较
Windows 漏洞攻击 (0.5 天)	在 Windows 上编译调试	在 Windows 上编译程序
		利用 Immunity Debugger 调试程序
		程序崩溃
	Windows 漏洞攻击程序	漏洞攻击程序开发过程回顾
		攻击 ProSSHD 服务器
	结构化异常处理	结构化异常处理
内存保护攻击 (0.5 天)	Windows 内存保护	栈缓冲区溢出检测
		SafeSEH
		SEHOP
		堆保护
		DEP
		ASLR
		EMET

	绕过 Windows 内存保护	绕过栈缓冲区溢出检测
		绕过 SafeSEH
		绕过 SEHOP
		绕过 DEP
		绕过 ASLR
		绕过 EMET
访问控制攻击 (0.5 天)	为什么要攻击访问控制	多数人不理解访问控制
		访问控制漏洞易于攻击
		访问控制漏洞数量巨大
	Windows 访问控制机制	安全标识符
		访问令牌
		安全描述符
		访问检查
	访问控制分析工具	转出访问令牌
		转储安全描述符
	特殊访问和禁止访问	特殊安全标识符
		特殊访问权限
		禁止访问
	提权漏洞	提权漏洞
	攻击不同对象	攻击服务
		攻击注册表
		攻击目录
		攻击文件
	枚举其它对象	枚举共享内存
		枚举命名管道
		枚举进程
		枚举其它命名内核对象
Web 应用攻击 (0.5 天)	Web 十大漏洞	Web 十大漏洞
	MD5 哈希注入	MD5 哈希注入
	多字节编码注入	多字节编码漏洞
		多字节编码攻击
	跨站脚本攻击	跨站脚本攻击
	Unicode 规范化形式攻击	利用 Unicode 规范化
		Unicode 规范化简介
		Unicode 规范化形式
		搭建测试环境
		利用 x5s 插件测试跨站脚本
		手动发起攻击
		添加自己的测试用例
堆溢出攻击 (0.5 天)	设置环境	配置 WinDbg
		将浏览器绑缚到 WinDbg 上
	堆喷射	堆喷射
	利用 HTML5 实现堆喷射	利用 HTML5 实现堆喷射

	利用 DOM 元素属性实现堆喷射	利用 DOM 元素属性实现堆喷射
	HeapLib2 技术	通过耗尽缓存块强制分配新块
		利用 HeapLib2 技术实现堆喷射
	基于字节数组的 Flash 堆喷射	基于字节数组的 Flash 堆喷射
	基于整数向量的 Flash 堆喷射	基于整数向量的 Flash 堆喷射
	低碎片堆	低碎片堆
释放后重用攻击 (0.25 天)	什么是释放后重用	什么是释放后重用
	分析释放后重用漏洞	分析释放后重用漏洞
	利用释放后重用漏洞	利用释放后重用漏洞
高级客户端攻击 (0.5 天)	BeEF 基础	设置 BeEF
		BeEF 控制台
	钩子浏览器	基本跨站脚本钩子
		利用网站欺骗钩子浏览器
		利用 shank 自动注入钩子
	利用 BeEF 获取指纹	利用 BeEF 获取浏览器指纹
		利用 BeEF 获取用户指纹
		利用 BeEF 获取计算机指纹
	攻击浏览器	利用 BeEF 和 Java 攻击浏览器
		利用 BeEF 和 Metasploit 攻击浏览器
	自动化攻击	自动化攻击
补丁比较漏洞攻击 (0.25 天)	二进制比较	应用程序比较
		补丁比较
	二进制比较工具	BinDiff
		turbodiff
		比较文件
	补丁管理	微软周二补丁
		获取微软补丁
		检查补丁
		利用 turbodiff 比较 MS14-006
		内核调试
		内核调试 MS14-006
Android 恶意软件 (0.25 天)	Android 平台	Android 应用程序包
		应用程序清单
		分析 DEX
		Java 反编译
		DEX 反编译
		DEX 反汇编
		在模拟器中运行 APK
	恶意软件分析	恶意软件分析入门
		利用 Droidbox 进行黑盒 APK 监控
勒索软件 (0.25 天)	勒索软件的历史	勒索软件的历史
	赎金支付选项	赎金支付选项
	Ransomlock	动态分析

		静态分析
	CryptoLocker	CryptoLocker
64 位恶意软件 (0.25 天)	AMD64 架构	AMD64 架构
	C&C 服务器	C&C 服务器
下一代逆向工程 (0.25 天)	著名的 IDA 插件	IDAscope
		IDAtoolbag
		协作
	基于 TrapX 的蜜罐与沙箱	免费的动态分析工具
		商业的动态分析工具

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》
- 《正义之战》