红队攻防实战训练

一、课程描述：

本课程采用靶场实战环境，按照真实红队攻击流程，从前期信息收集、编写免杀文件开始，直到突破边界、权限提升，内网横向渗透、权限维持、痕迹清理，全方位详细讲解最新的攻防技术及技巧。

二、课程大纲：

注：可根据实际情况，进行调整。

日期	时间	知识点
第 1 天	**上午**	**信息收集总体概念** **被动信息收集** 信息收集的总体概念以及在整个红队流程中的位置； 被动信息收集的基本结构和基本逻辑； 被动信息收集的常见手段（网络空间搜索、被动信息收集工具、传统搜索）； 被动信息收集后的信息处理； 被动信息收集工具的底层原理以及如何编写；
	下午	**主动信息收集** 信息收集完成之后的信息综合处理 主动信息收集的基本结构和基本逻辑； 主动信息收集的常见手段（仅限扫描的 nmap 和扫描带有 poc 的 goby）； 主动信息收集后的信息处理； 主动信息收集工具的底层原理以及如何编写； 如何将主动信息收集和被动信息收集的信息综合处理； 收集到的信息如何衔接到下一步的红队流程中；
第 2 天	**上午**	**社会工程学** 社会工程学的含义以及实际应用； 社会工程学的知识体系；

		社会工程学的学习方法；
	下午	**社会工程学中的交互** 社会工程学中的常见钓鱼方式以及应用； 社会工程学中如何根据收集到的信息利用目标的社会属性弱点进行交互； 社会工程学中的信任获得和信任利用方式；
第 3 天	上午	**实战中的快速审计** 寻找源码中的多种途径； 快速查找源码中可利用的脆弱点； 使用工具发现脆弱点；
	下午	**POC 的编写** POC 编写应具备的哪些条件； Idea 工具的安装； 本地 IO 进行内容读写； 网络请求进行发包模拟； POC 实战；
第 4 天	上午	**红队之反溯源** 工作机器；攻击资源； 匿名攻击； 识别反制； 反溯源案例；
	下午	**Windows 内网提权** Potato 家族提权；补丁提权；系统配置错误提权； 第三方服务提权；组策略提权；Bypassuac； 数据库提权；令牌窃取；密码收集提权；
第 5 天	上午	**Liunx 内网提权** 系统内核提权；第三方服务提权； 数据库提权；密码收集提权； 键盘记录提权；Suid 提权； Sudo 提权；反弹 shell 提权；
	下午	**内网穿透** 内网穿透概述及正向代理和反向代理； 花生壳内网穿透；Frp 内网穿透； Ngrok 内网穿透；reGeorg+Proxifier； 向日葵代理及 teamviewer； 最小化渗透概述；云函数；域前置；

第 6 天	上午	**外网打点技巧和 Kerberos 认证原理** 入口权限获取；java 中间件 Nday； php 集成环境；开源程序 Nday； 边界网络设备利用；基础服务 getshell； kerberos 认证；kerberos 认证流程；
	下午	**域内信息收集及域信任** 域内信息收集概述； 域内用户组收集；域信任关系收集； 用户目录收集；预控日志收集； Arp 信息收集；Tcpdump；Sshkey 收集； 铭感配置读取；网络拓扑架构分析判断；
第 7 天	上午	**域渗透工具实操实战** Setspn；Nslookup；AdFind； Psloggendon；360safebrowserdecrypt； SchtaskBackDoorWebshell；regeditBypassUAC；
	下午	**票据伪造、域委派攻击、域控攻击** PTH 认证过程解析；票据伪造攻击原理； Mimikatz 实现票据伪造攻击； 域委派原理；域委派攻击方法； zerologin；nopac
第 8 天	上午	**域林渗透** 域林渗透概述和父域子域及域信任关系分析；大型域渗透思路； 预控定位；Pth 喷射；域信任攻击； 组策略漏洞；Web 及系统漏洞；逃逸漏洞；
	下午	**Windows 权限维持** Windows 权限维持概述及隐藏技巧；关闭杀软； 注册表自启动；组策略脚本； 计划任务；服务自启动； 内存码；进程劫持；隐蔽隧道；
第 9 天	上午	**Liunx 权限维持** Liunx 权限维持概述及隐藏技巧； 添加用户；SUIDshell； SSH 公私钥；软连接； crontab 计划任务；Strace 后门；Openssh 后门； 隐蔽隧道；关杀软；
	下午	**痕迹清理**

		Windows 操作系统的痕迹清理； Windows 痕迹清理的基本思路和思考逻辑； Windows 清理登录痕迹、操作痕迹及时间痕迹； Linux 操作系统的痕迹清理； Linux 痕迹清理的基本思路和思考逻辑； Linux 清理登录痕迹、操作痕迹及时间痕迹；
第 10 天	上午	**Meterpreter 木马分析** 反编译 meterprter 源码； 分析 meterpreter 源码； 源码级别免杀深入浅出；
	下午	**免杀代码基础** 编程语言基础； windowsapi 基础； socket 编程基础； shellcode 加载器基础；
第 11 天	上午	**shellcode 基础** 现代远控的基本结构； shellcode 生成方式与可以使用的类型； shellcode 源码内容；
	下午	**代码上的免杀** 杀毒软件基本原理； 杀毒软件基础复现； 针对杀毒软件特点免杀； 护网过程中如何手动和自动识别恶意代码；
第 12 天	上午	**人工层面的免杀** 通信的加密； 通信内容的伪造； ip 地址的保护； 护网过程中如何识别通信特征与内容； 反调试；
	下午	**实际红队案例分享、红队攻击思路** 红队模拟面试； 实际红队案例分享； 红队攻击思路； **红队护网准备工具及蓝队分析反制方法及思路** 红队准备工具； 邮件溯源工作； 水坑反制案例