红队攻防实战

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	模块	知识点
第 1 天	上午	信息收集	大数据引擎 CDN 绕过 google hacking 供应链渗透 主动信息收集 被信息收集
	下午	文件的免杀	免杀中使用的编程语言及相关知识基础； 程序的基本结构； Meterpreter 源码剖析； 编写免杀框架； 免杀中使用的编程语言及相关知识基础； payload 的基本结构和编程语言的实战；
第 2 天	上午	边界突破——**外网打点**	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
	下午	边界突破——近源渗透	近源渗透

			Badusb 使用 其他近源攻击手法 无线渗透
第 3 天	上午	权限提升	**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 **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	横向渗透	**隐蔽隧道** Dns 隧道 Icmp 隧道 端口复用 https 隧道 socks 隧道 cs 魔改 **最小化渗透** 云函数 预前置 Arp 记录 Tcpdump Ssh key 敏感信息读取
第 4 天	上午	横向渗透——域渗透	域内信息收集 域控定位 Kerberos 认证 Pth 喷射 票据伪造 域信息攻击 域委派攻击

			林渗透 密码获取 组策略漏洞
	下午	权限维持——Windows	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 5 天	上午	权限维持——Liunx	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； 内存码
	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；