红蓝队攻防演练培训

课程描述：

本课程根据贵方需求，理论与实战相结合的方式，从红队角度细致讲解了信息收集、常见漏洞检测及利用、提权，一直到权限维持和痕迹的清理。从蓝队的角度讲解了日志与流量的分析技术以及应急响应。全流程理解红蓝队攻防。

课程大纲：

一、信息收集技术

- 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

二、常见的漏洞原理及检测利用

- SQL 注入漏洞原理及检测利用
- 文件上传漏洞原理及检测利用
- 命令执行漏洞原理及检测利用
- XSS 原理及检测利用
- 文件包含漏洞原理及检测利用
- CSRF 原理及检测利用
- SSRF 原理及检测利用
- Windows 系统常见漏洞检测利用
- Linux 常见漏洞检测利用
- 数据库漏洞检测利用
- 中间件漏洞检测利用

三、权限提升

- Windows 提权技术
- Liunx 内网提权技术

四、权限维持技术

- Windows 权限维持概述及隐藏技巧；
- 关闭杀软；
- 注册表自启动；
- 计划任务；
- 服务自启动；
- 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；

五、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；

六、日志分析技术

- 日志收集技术
- 事件归一化
- 关联分析

七、网络流量分析

- 如何捕获网络流量
- Wireshark 等工具使用
- 检测活动系统并分析结果

八、应急响应概况

- 应急响应介绍
- 安全事件分类
- 应急响应启动条件
- 应急响应目标
- 应急响应预案制定

九、Windows\Linux 系统应急排查技术

- 系统排查
- 进程排查
- 服务排查
- 文件痕迹排查
- 日志分析
- 内存分析
- 流量分析
- 威胁情报