网络渗透测试及攻防实战

一、课程描述：

本课程主要讲述了常见的基于 Web 的漏洞渗透以及代码审计防御办法，比如 SQL 注入、XSS 跨站脚本注入、目录遍历漏洞、代码与命令执行漏洞、文件上传下载漏洞、未授权和越权访问漏洞、逻辑漏洞及弱口令等，最后讲述如何使用 WebShell 打开后门及应急办法。

二、课程大纲：

第 1 讲、技术基础
- Web 应用程序安全与风险
- HTTP 请求与响应
- HTTP 方法、消息头讲解
- 不安全的 Http 方法漏洞实战测试
- Cookie、响应状态码、身份验证讲解
- Http 编码方案
- 渗透测试环境搭建

第 2 讲、安全渗透测试工具使用
- 黑客攻击流程
- 信息收集与扫描技术
- Kali 平台使用
- 网络安全审计工具：Nmap
- Burp 基本应用
- SQLMAP

第 3 讲、跨站脚本 XSS 渗透测试
- XSS 讲解
- XSS 演示

第 4 讲、SQL 注入漏洞原理及检测利用
- SQL 注入利用思路
- MYSQL 注入的利用

第 5 讲、目录遍历漏洞原理及检测利用
- 目录遍历漏洞
- 目录遍历实战

第 6 讲、代码/命令执行漏洞原理及检测利用
- 代码/命令执行漏洞原理
- 代码/命令执行漏洞挖掘
- 代码/命令执行漏洞防护

第 7 讲、文件上传漏洞原理及检测利用
- 文件上传漏洞原理
- 文件上传漏洞实战与防护

第 8 讲、逻辑漏洞原理及检测利用
- 逻辑漏洞原理
- 逻辑漏洞实操

第 9 讲、弱口令漏洞原理及检测利用

- 弱口令介绍
- 弱口令实践

第 10 讲、权限提升

- Windows 提权技术
- Liunx 内网提权技术

第 11 讲、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；

第 12 讲、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