**网络安全红蓝对抗实战演练**

**培训班**

|  |  |  |
| --- | --- | --- |
| **培训地点** | **北京** | **北京** |
| **培训时间** | **5月**  **27-31** | **11月**  **待定** |
| **培训方式** | **面授+直播** | |
| **增值服务** | **1.参加线下面授课程，可享受视频回放免费学一年；**  **2.参加在线直播课程，可享受视频回放免费学一年；**  **3.提前缴费即可开通录播视频超前学习。** | |
| **备注** | **本课程全国常年开班，如部分地区课程已结束，请致电：方老师13910781835 （微信同号）QQ：1808273142 咨询最新培训课程!**  **也可通过录播视频在线学习！此课程也提供企业内训，欢迎咨询！** | |

1. **培训背景**

近年来，国家对信息安全问题逐渐重视起来，今年“两会”上，信息安全问题也成为重点。未来，无论是个人、企业还是机构，对信息安全必定会更加重视。随着全球进入数字化时代，关键信息基础设施安全保障不仅是国家信息安全保障工作重要的一环，网络战也从传统作战的辅助手段变成首选，成为数字时代下最具可能性的战争形式之一。当下网络安全态势之严峻，迫切需要国家、行业及各单位在网络安全领域具备打硬仗的能力。网络安全行业的特殊性决定了网络安全人才除了需要有扎实的理论基础，更需要有高超的实战能力，才能应对纷繁复杂的网络环境及层出不穷的攻击手段，网络安全虽是幕后工作，不见刀光剑影，却同样危机四伏，红蓝对抗演习实为培养实战型人才的绝佳手段，也是快速检验网络安全人才技能的途径。网络信息安全的时代到来，只有掌握攻防技能的人才，才有登上舞台的资格。通过学习 将所学运用到自身业务中，提升业务水平，成为安全时代大舞台上的佼佼者！

1. **培训简介**

网络安全形式严峻，国内外接二连三发生的网络安全事件表明，越复杂的网络与信息技术漏洞与安全隐患越多，黑客的手段千变万化，威胁的未知远远大于已知，再严密的网络防线也难免百密一疏，固有的网络安全理念与防御措施不断受到挑战。2017年5月12日起席卷全球150多个国家30余万计算机的“WannaCry”勒索软件攻击，事件发生和蔓延的速度、后果的严重程度均创纪录。事件再次敲响警种，网络攻击“没有最坏，只有更坏”，也再度表明信息社会技术发展远超前于政府监管。

2017年6月1日，《网络安全法》正式生效，标志我国维护网络与信息安全的工作进入一个全新阶段。作为首部统领国家网络安全工作的综合性法律，以维护国家网络空间主权、安全和发展利益为根本，以筑牢网络安全防线为目标，为网络强国建设大业保驾护航。《网络安全法》展现了国家维护网络空间安全的决心与信心。

网络安全已成为国家继海陆空天四大疆域之外的第五疆域，网络安全也体现国家主权，保障网络安全就是保障国家主权。习主席强调：“没有网络安全就没有国家安全。”网络安全的竞争归根到底是安全人才的竞争。目前国内网安人才缺口数百万，实战型人才更稀缺，无法满足企业、行业的需求。因此，培养网络安全实战型人才迫在眉睫。

传统网络安全人才成长，以“白帽子”自身对网络安全知识的浓厚兴趣为驱动，以自发迎难而上、擅于多角度切入、创造性解决问题的“极客精神”为引导。因网络安全领域的高门槛，传统方式学习成长曲线陡峭，真正成长起来的实战型人才极为少数。以清华大学、美国乔治亚大学, 多年从事网络安全教育行业的深厚积累，形成一套系统完善、可成长度高的培训知识体系。“未知攻、焉知防”，知识体系以“攻防技术”为核心，着眼攻防实战，紧跟前沿领域，打破网络安全知识学习壁垒，面向高校和各行业领域，提供一套快速、有效的网络安全人才培养解决方案。

1. **培训特色**

1.理论与实践相结合、案例分析与行业应用穿插进行；

2.专家精彩内容解析、学员专题讨论、分组研究；

3.通过全面知识理解、专题技能和实践结合的授课方式。

1. **日程安排**

|  |  |
| --- | --- |
| **时间安排** | **培训内容** |
| **第一天上午** | 1、HTTP基础  2、数据包的结构与分析  3、web应用安全总结  - 关于漏洞挖掘的技巧分享  - 红队黑客攻击渗透测试的常规流程以及前期打点  4、信息收集  - 网站基本信息收集  - 爆破子域名、目录、旁站、端口  - 谷歌hack语法  - 社会工程学  - 其他高级技巧讲解  6、蓝队应急响应与溯源反制  - 告警日志分析高级技巧讲解  - 告警日志分析案例以及溯源解析  - Linux 应急响应流程及实战演练  - Windows 应急响应流程及实战演练 |
| **第一天下午** | 1、web安全应用中的黑客工具  - 数据包分析工具burp wireshark等等  - Metasploit、cobalt strike多人协同作战平台  2、哥斯拉、冰蝎shell连接工具流量免杀特征介绍  3、木马介绍以及木马免杀实操  4、如何制作木马获取操作系统权限  实验：如何开启傀儡机摄像头  谨防钓鱼：如何目标中马上线Ccobalt strike |
| **第二天上午** | 1、逻辑漏洞  - 短信验证码的绕过 实现任意账号登录  - 支付漏洞（实现0元进行购物、0积分换取）  - cookie仿冒  - 其他逻辑漏洞  2、越权访问  - 越权访问的定义  - 未授权访问页面  SQL注入漏洞讲解  1、Sql注入漏洞  - sql注入在代码中的漏洞成因  - 利用sql注入进行注入数据窃取实战  2、SQL注入深入剖析  - sql注入原理深入剖析  - 手工注入+sql注入靶场练习（基础题）  - sqlmap的使用方法  - sql报错、sql盲注、宽字节注入、二次注入、cookie注入等  - sql注入bypass绕waf技巧  - sql注入自动化脚本编写 |
| **第二天下午** | 1、文件包含+文件上传漏洞  1）深度剖析文件包含与文件上传漏洞成因  2）文件包含常见伪协议利用  3）文件包含包含日志getshell  4）实战绕过服务端Disable\_function限制  5）宝塔waf文件上传绕过三种姿势介绍 |
| **第三天上午** | 1、XXE  - XXE相关代码讲解  - 从代码层面分析XXE漏洞成因  - 实战中XXE实现内网探测  - XXE漏洞的修复  2、redis非关系型数据库与基础介绍  实战redis未授权攻击手法三种  1：利用redis未授权漏洞写webshell  2：利用redis未授权漏洞写ssh公钥  3：利用redis未授权漏洞写定时任务反弹shell  详解ssrf漏洞  1：剖析ssrf漏洞成因  2：ssrf配合伪协议进行攻击  3：ssrf攻击内网与内网信息收集、探测存活主机  4：gopher协议的构造与配合ssrf漏洞打exp |
| **第三天下午** | 框架/模板漏洞以及常见CVE漏洞介绍  1：shiro、ThinkPhp、Struts2 RCE方法介绍  2：phpmyadmin Tomcat 经典漏洞介绍  3：Laravel Debug mode RCE（CVE-2021-3129）漏洞利用  4：docker逃逸常见利用场景与逃逸方式介绍  渗透测试中的后渗透模块  - 内网渗透的信息收集  - 内网中的ssh代理、socket代理、反弹shell、socks隧道 |
| **第四天上午** | 1：权限提升  介绍windows提权与linux提权  实战  windows下提权神器：烂土豆  Linux提权实战dirtycow、suid提权 |
| **第四天下午** | 1：不同环境下的渗透思路  工作组环境的渗透姿势  域环境下的渗透姿势  2：杀软对抗-免杀  免杀制作思路  分离式免杀  C#免杀以及免杀脚本分享  bypass and user  3、Ccobalt strike流量加密 |
| **第五天**  **实战演练一** | 1：Linux主机渗透  涉及知识点：  1、信息收集（nmap+dirb)  2、web漏洞-文件包含  3、ssh配置文件的熟悉  4、msfvenom生成木马  5、metasploit反弹shell  6、meterpreter模块的运用  7、linux提权基本思路  8、SUID提权  9、linux命令的熟练掌握 |
| **实战演练二** | 2：三层内网靶场渗透  st漏洞利用  phpmyadmin getshell  tomcat 漏洞利用  docker逃逸  ms14-068  ssh密钥利用  流量转发  windows内网渗透 |

1. **授课专家**

**赵老师** 中国信息安全测评中心特聘安全研究员，工信部网络安全技能大赛专家，擅长课程：网络攻防、渗透测试、漏洞挖掘、应用安全、逆向分析、木马病毒、主机数据库安全测试加固、安全编程，项目经历有贵阳大据及网络安全攻防演练，全国网络安全攻防大赛个人第三名/团队第一，湖北移动2020CTF集训-逆向（4天）、某部队2020-CTF集训-PWN+逆向(5天)/攻防渗透+web（5天）、广西电网2020CTF集训提高班（15天）、广西国税2020竞赛集训-逆向、网络空间安全精英集训营201908（讲师代表/技术评委）、中国电建网络安全集训等。

**徐老师** 十年信息安全工作经验，热爱研究网络安全技术。主攻Web、渗透测试、安全研究、漏洞挖掘、代码审计擅长 web 方向，热爱 ctf 和 awd。在 web 方向的 php 代码审计尤为擅长，曾参与审计某司自研项目并审计到高危漏洞。有丰富的政府，内网 外网项目渗透经验。多次在 ctf 比赛中获取名次，并担任出题者和裁判。曾任职国内某top10安全公司，奇安信及多个公司的特聘安全培训讲师。

1. **培训费用**

线下面授培训费8800元/人（含培训费、场地费、资料费、学习期间午餐以及录播视频回放一年）食宿可统一安排，费用自理。

网络直播培训费：7800元/人（含培训费、平台费、资料费及直播视频回放一年）。

本课程由中国信息化培训中心颁发《网络安全红蓝对抗实战演练技术工程师》证书，证书查询网址：www.zpedu.com; 证书可作为专业技术人员职业能力考核的证明，以及专业技术人员岗位聘用、任职、定级和晋升职务的重要依据。

1. **报名回执《网络安全红蓝对抗实战演练》**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 单位名称  （开发票名称） |  | | | | | |
| 快递地址 |  | | | | 邮编 |  |
| 联 系 人 |  | | 职 位 |  | 电话 |  |
| Email |  | | 传 真 |  | | |
| 学员姓名 | 身份证号  （做证书使用） | 邮箱 | 联系电话 | | 培训地点  （培训方式 ） | 是否  住宿 |
|  |  |  |  | |  |  |
|  |  |  |  | |  |  |
|  |  |  |  | |  |  |
|  |  |  |  | |  |  |
|  |  |  |  | |  |  |
| 汇 款  方 式 | 户 名：北京中培伟业管理咨询有限公司  开户行：北京农村商业银行卢沟桥支行营业部  帐号：0203 0101 0300 0033 172 | | | | | 备注： |
| 发票信息： | 单位名称：  统一社会信用代码：  开户银行：  账号：  地址：  电话： | | | | | |

1. **联系方式**

联系人：方老师

手 机（微信）：13910781835

QQ：1808273142

邮 箱：1808273142@qq.com

二〇二二年一月一日