蚁景网安渗透测试（红队方向）课程体系			
课程分类	课程大纲	内容概述	级别
渗透测试介绍	网络安全、渗透测试概念	渗透相关概念、基本流程、网安重大事件、安全意识介绍	初级
	渗透测试法律法规	网络安全法、反间谍法、渗透测试规范、授权渗透	初级
	渗透测试就业前景、岗位及发展	网安相关岗位、hw、src、众测、就业需求、行业前景	初级
操作系统基础	基础环境安装	windows系统配置、python环境、java环境	初级
	VM虚拟机	Vmware软件安装与激活、VM虚拟网络编辑与配置	初级
	Kali Linux 基础	Kali Linux简介、Linux目录结构、文件属性、VIM编辑器、目录管理、网络配置、用户配置	初级
	Kali Linux 进阶	Linux服务管理、防火墙、APT使用、Git使用、SSH使用、Kali工具	初级
	内网靶场搭建	多层内网环境搭建、多层内网配置	中级
	云服务器	VPS介绍	初级
		云服务器对比与选购、VPS连接与使用	初级
	docker	docker简介、docker安装与配置	初级
		docker搭建漏洞靶场、docker-compose搭建漏洞靶场	中级
计算机网络	计算机网络基础	网络协议分层	初级
		IP地址、DNS、ARP、DHCP、NAT、ICMP	初级
	计算机网络安全应用	burpsuite安装、浏览器代理配置、证书配置	初级
		burpsuite-proxy模块使用	初级
		http协议、http报文分析、http请求方法、https与http	初级
信息收集	域名信息收集	信息收集分类	初级
		域名介绍、域名收集、子域名收集	初级
	IP信息收集	IP收集、C段	初级
		端口收集、常见端口及安全隐患介绍	初级
	网站信息收集	操作系统收集、网站服务、容器收集、数据库识别、CMS识别	初级
		敏感文件、目录、常见WAF识别	初级
web安全	基础环境搭建	wamp搭建靶场	初级
		lamp搭建靶场	初级
		docker、docker-compose搭建靶场	中级
	SQL注入	Mysql基础	初级
		SQL注入原理、危害、判断与分类	初级
		SQL注入显错注入、盲注、报错注入	初级
		SQLmap使用实例及参数详解	初级
	文件上传	文件上传漏洞原理、危害、检测方式常见	初级
		webshell简介、原理	初级
		webshell管理工具，菜刀、蚁剑、冰蝎、哥斯拉	初级
		文件上传绕过方式、绕过js、绕过文件后缀检测、mime类型、绕过文件内容检测	中级
		文件上传防御	中级
		常见解析漏洞	中级
	命令执行	命令执行漏洞原理	初级
		php代码执行、命令执行函数	初级
		命令执行漏洞实例，反弹shell	中级
	web扫描器	xray基础使用、爬虫扫描、被动扫描	初级
		awvs联动xray、burpsuite联动xray、rad联动xray、xray脚本编写	高级
		goby使用、nuclei使用	中级
常见漏洞	弱口令	弱口令分类与字典	初级
		网站弱口令爆破	初级
		常见服务弱口令爆破	初级
	未授权访问	未授权访问概述	中级
		redis未授权访问、redis利用写webshell、写ssh公钥、写计划任务、主从复制	高级
		hadoop未授权访问	高级
	weblogic	weblogic简介	中级
		weblogic环境搭建	中级
		weblogic历史漏洞发现与利用	中级
	jboss	jboss简介	初级
		jboss环境搭建	中级
		jboss历史漏洞发现与利用	中级
	struts2	struts2简介	初级
		struts2环境搭建	初级
		struts2历史漏洞发现与利用	中级
	thinkphp	thinkphp简介	初级
		thinkphp命令执行漏洞利用	中级
	fastjson	fastjson简介、json认识	中级
		fastjson反序列化利用	中级
		JNDI注入+RMI LDAP	高级
	shiro	shiro组件简介	中级
		shiro550、shiro721漏洞原因、特征判断与漏洞利用	中级
	log4j2	log4j2简介	初级
		log4j2漏洞环境搭建、利用与修复	中级
	metasploit	metasploit安装、配置	初级
		metasploit模块使用	初级
		msfvenom生成后门	初级
		meterpreter后渗透命令详解	中级
	viper	viper安装与配置	中级
		viper基本使用 、viper运行模块	中级

渗透测试框架	cobaltstrike	cobaltstrike简介、基本使用	初级
		监听器详解、beacon分类及工作原理、beacon使用	中级
	进阶-流量隐藏	msf与cs流量分析	中级
		隧道转发代理隐藏流量	高级
		域名+CDN上线隐藏IP	高级
		转发重定向	高级
		CS配置文件隐藏流量	高级
	进阶-拓展应用	cobaltstrike扩展脚本	中级
		CS上线linux主机	中级
		CS联动MSF、MSF联动CS	高级
	powershell渗透框架	powershell简介	初级
		powershell脚本执行策略	中级
		powershell加载器	中级
		powershell工具框架-powersploit、nishang	中级
内网渗透	内网信息收集	内网渗透简介	初级
		windows工作组环境简介	初级
		windows域环境简介	中级
		机器位置判断、机器角色判断、连通性判断	初级
		域环境搭建、域内主机及用户管理	中级
	密码凭证获取	Hash简介	中级
		LM-HASH、NTLM-HASH	中级
		windows本地认证、windows网络认证、windows域认证kerberos协议	高级
		系统用户凭证获取与破解	高级
		其他常见应用服务密码获取与解密	高级
		域环境密码凭证获取与解密	高级
	内网代理	socks代理简介	中级
		socks代理多级内网渗透环境实战	中级
		HTTP代理	中级
		DNS隧道、ICMP隧道	高级
	提权	windows、linux操作系统提权	初级
		metasploit提权、cobaltstrike提权	中级
		域提权	中级
		mysql提权、mssql提权	中级
	横行移动	内网横向移动	中级
		IPC、Schtasks、WMIC、WinRM	中级
		psexec、wmiexec	中级
		pth哈希传递	高级
		域横向移动	高级
	权限维持	windows、linux操作系统权限维持	中级
		域权限维持	高级
		ptt	高级
	痕迹清除	windows、linux日志、历史记录清除	初级
免杀	免杀基础篇	免杀概念	初级
		免杀测试环境	中级
		常见杀毒软件检测技术	中级
		shellcode简介	高级
		shellcode加载器	高级
		常见免杀方式、免杀工具	高级
	免杀进阶篇	shellcode混淆免杀	高级
		shellcode分离免杀	高级
		C++加载shellcode	高级
		python加载shellcode	高级
课程总结	渗透测试总结	渗透测试基本流程	初级
		渗透测试进阶发展	初级
		渗透测试综合实战靶场讲解	高级
综合实战靶场	多级内网、域环境实战渗透靶场		
就业指导	简历指导		
	简历制作		
	岗位内推		

蚁景网安渗透测试（红队方向）附赠课程			
课程分类	课程大纲	内容概述	级别
Linux操作系统	Linux系统简介	Linux操作系统历史及分类	初级
		Linux操作系统镜像下载	初级
	VM虚拟机	Vmware虚拟机安装	初级
		Vmware安装Centos7	初级
	Linux基础命令	命令行关机、重启	初级
		目录结构、用户、权限管理、网络配置	初级
	VIM编辑器	Vim编辑、保存、常见用法	初级
	Linux服务及软件	远程连接虚拟机、压缩包、Linux安装软件、Linux靶场环境搭建	初级
	Linux docker	docker安装、docker基础使用	初级
PHP编程	PHP基础	PHP介绍、PHP安装环境配置	初级
		基本语法、常量和变量、表达式运算符控制语句	初级
		PHP函数	初级
	PHP面向对象	面向对象基础、类和对象	中级
	PHP与Mysql数据库	mysql基础	初级
		php连接mysql数据库	初级
	PHP安全隐患	php中的xss	初级
		php文件包含问题	初级
		php文件上传	初级
网站开发	开发环境安装	phpstorm安装和运行	初级
		phpstorm配置php和nodejs	初级
	前端语言基础	HTML常用标签	初级
		CSS样式表	初级
		table标签和form表单	初级
	JavaScript	JavaScript简介	初级
		JavaScript三种用法	初级
		JavaScript数据、对象、json	初级
		JavaScript DOM	初级
	网站开发实践	实践1-POST请求	初级
		实践2-Ajax请求	初级
		实践3-输出数据到页面	初级
		实践4-增加按钮、实现后退	初级
		实践5-文件上传	初级

蚁景网安渗透测试（红队方向）学习服务	
学习服务	1v1学习计划制定
	班主任全程督学
	讲师在线答疑
	项目实战
	各阶段考核测评
	结业考核
	就业指导
	简历优化
	就业帮内推服务
	原创现金激励制度