《众元》安全攻防大师v9.1			
能力目标	课程目标	学习周期 (1163课时)	学习内容
渗透测试	网络安全基础	6	了解安全术语、熟悉渗透测试流程
	法律法规	3	了解网络安全法、数据安全法、关基保护条例
	数通网络技术	80	熟悉网络基础、地址规划、协议基础、协议安全威胁、网络设备调试、路由协议、TCP/IP
	编程语言基础	30	熟悉html标记、php函数、sql语句、python使用等
	Linux系统	30	熟悉基本命令、vim的操作、文件的操作等
	数据库基础	18	熟悉数据库语法、操作数据库、数据表、DBMS
	web漏洞原理	120	熟悉文件上传、xss、文件解析、框架漏洞、命令执行、代码执行、csrf、ssrf、xxe、反序列化、中间件漏洞、解析漏洞、数据库漏洞、越权漏洞、信息泄露等OWASP Top漏洞
	web漏洞发现与利用	30	熟悉漏洞工具AWVS等使用、webshell的利用、蚁剑等
	代码审计	30	熟悉php代码、js代码、Java代码审计，审计工具
	权限提升	30	熟悉Windows、Linux的提权方法等
阶段考核	笔试+top企业渗透测试岗位面试要求		
CTF竞赛	web方向	60	熟悉WEB十大安全漏洞（OWASP Top 10）等解题方法和wp
	二进制pwn	120	熟悉汇编、C、栈溢出、格式化字符、栈溢出漏洞等解题方法和wp
	逆向reverse	30	熟悉静态分析、动态分析，了解几种加密方式、熟悉安卓脱壳等解题方法和wp
	密码学crypto	30	了解古典密码和熟悉使用解密工具和解密算法等解题方法和wp
	杂项misc	30	熟悉流量分析、压缩包、图片隐写、音频隐写等解题方法和wp
SRC赏金 漏洞挖掘	src概念	3	了解src意义和排名机制
	src平台	6	注册CNVD、补天、漏洞盒子、教育漏洞报告平台，挖洞
	src信息收集	12	熟悉使用资产测绘引擎、企业信息查询、域名信息查询
	挖掘技巧	12	了解绕过方式、某迅万能下载等
	1/nday利用	12	了解漏洞文库收集，关注并使用最新漏洞
	内网渗透基础	12	了解工作组、域、域环境、安全域的划分、资源、跳板等
	穿透与转发	12	熟悉frp内网穿透、portwd端口转发、venom-代理转发、多级穿透、DNS隧道

渗透测试进阶	内网信息收集	12	熟悉端口扫描、口令爆破、主机信息收集、数据库信息收集、数据分析
	通道构建	12	判断目标以哪种协议出网、反向代理、正向代理、使用socks代理
	权限提升	12	熟练Windows提权、Linux提权、本地提权、web提权、数据库提权等
	横向渗透	12	熟练在 windows 中进行横向移动、利用数据库进行横向移动、使用 cs 进行横向移动的常用命令
	权限维持	6	熟练windows 中的权限维持、linux 的权限维持、数据库中的权限维持
	痕迹清理	6	熟练防止恢复删除的文件、windows 的痕迹清理、linux 的痕迹清理等方法和工具
	域渗透	18	熟练域基础、域信息收集、域权限利用、域横向攻击
	小程序app渗透	30	熟练微信小程序、 手机 app、程序流量分析
	API渗透	18	熟练API 扫描、API 利用
	Java安全	12	熟悉Java 基础、Spring Boot 框架、 Redis MongoDB 数据库等java架构安全威胁
护网蓝队(防守方)	蜜罐技术	6	熟悉蜜罐的分类及搭建部署，微步在线、低、中、高蜜罐等
	流量分析	18	熟悉使用Wireshark、Wireshark的功能过滤
	攻击研判	18	熟悉设备监控：IPS 告警、WAF 告警、流量分析告警终端防护告警； 事件上报：保留证据、事件报告、上报处置； 后期处置：协助处理、情报联动、攻击溯源
	溯源	18	熟悉攻击源捕获，溯源反制手段，获取攻击者信息
	取证	12	熟悉webshell数据表、日志分析
护网红队(攻击方)	资产收集	12	熟悉工具的使用、端口服务、子域名、C段旁站等报告模板整理
	外网打点	12	熟练使用工具发现脆弱点、使用工具检测漏洞并利用
	蜜罐识别	6	熟悉蜜罐分类、如何识别蜜罐、常见蜜罐、交互蜜罐等
	社工钓鱼	18	熟悉社交账号、免杀马、bypass沙箱、信息收集C2搭建、邮件网关等
	内网渗透	18	熟练内网渗透基础、穿透与转发、内网信息收集通道构建、权限提升、横向渗透、权限维持痕迹清理、域渗透等
	免杀对抗	12	熟悉免杀shellcode制作，免杀软件测试
阶段考核	笔试+护网行动红/蓝队面试要求		
	等级保护标准	6	熟悉等级保护介绍、等级保护的一般流程 等级保护 2.0 安全设备

安全合规保护	内网安全部署	30	熟悉AAA 服务器技术及设备安全管理、LAN 接入基本安全、身份认证技术、网络准入控制 NAC、桌面云安全、EDR 终端检测响应技术
	公网边界防火墙部署	30	熟悉防火墙的工作层次、下一代防火墙概述 下一代防火墙组网方案、终端安全检测和防御技术、服务器安全检测和防御技术、防火墙技术--产品选型
	公网边界上网行为管理部署	18	熟悉上网行为安全概述、上网行为组网方案、 用户认证技术、应用控制技术、内容审计技术
	数据中心 WAF部署	18	熟悉web 应用防火墙概述、web 应用防火墙基本原理、web 应用防火墙部署模式
	总部与分支VPN互联	30	熟悉VPN 基础、IPSEC 的安全基础前篇、IPSEC 的安全基础后篇、IKE 工作过程、IPSEC 配置应用案例分析、SSL 移动接入方案、移动资源发布
安全(服务)运营	安全运维	6	熟悉持续监控、事件管理和响应、漏洞管理、 配置管理、日志管理、策略管理
	研判告警	6	熟悉设备监控、事件上报、后期处理
	应急响应	6	、文件痕迹排查、日志分析、内存分析、流量分析
	威胁情报	6	熟悉威胁情报的基本特征、用途、数据采集 分析方法、服务平台等
	联动处置	3	熟悉处理流程和标准
阶段考核	笔试+安全工程师及安全运营工程师岗位面试要求		
呈现表达能力	PPT制作	6	熟练使用工具制作PPT
	台风界面训练	18	《我的家乡》演讲、《就业企业介绍》演讲
	演讲技能及应变	30	《技术讲解》演讲、《产品选型》演讲、 《方案设计》演讲
面试就业能力	就业课程	18	网络安全行业介绍、网络安全企业介绍 如何做好《自我介绍》、如何写好《个人简历》
	就业能力考核和辅导	30	就业能力考核、模拟面试及辅导、面试跟踪与辅导
就业考核	简历制作通过、人事面试通过		